KTO KARATAY ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
TEZLİ YÜKSEK LİSANS PROGRAMI

HACKER'LARIN FİDYE ZARARLI YAZILIMLARI KULLANARAK İŞLEYEBİLECEĞİ SUÇLAR

Cansu ADAM

Yüksek Lisans

KONYA
Nisan 2022

HACKER'LARIN FİDYE ZARARLI YAZILIMLARI KULLANARAK İŞLEYEBİLECEĞİ SUÇLAR

Cansu ADAM

KTO Karatay Üniversitesi
Lisansüstü Eğitim Enstitüsü
Kamu Hukuku Anabilim Dalı
Tezli Yüksek Lisans Programı

Yüksek Lisans

Tez Danışmanı: Dr. Öğr. Üyesi Mehmet Savaş ÖZDAĞ

Konya
Nisan 2022

BİLDİRİM

Enstitü tarafından onaylanan Yüksek Lisans/Doktora tezimin tamamını veya herhangi bir kısmını basılı veya dijital biçimde arşivleme ve aşağıda belirtilen koşullar dahilinde erişime açma iznini KTO Karatay Üniversitesine verdiğimi bildiririm. Bu izinle, Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak ve gelecekteki çalışmalar (makale, kitap, lisans, patent vb.) için tezimin tamamının veya bir bölümünün kullanım hakları yalnızca bana ait olacaktır.

Tezimin bütünüyle kendi çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Telif hakkı bulunan ve sahiplerinden yazılı izinle kullanılması zorunlu olan kaynakları, yazılı izin alarak kullandığımı ve istenildiğinde izinlerin suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayımlanan "Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge" kapsamında, tezim, aşağıda belirtilen koşullar haricince, YÖK Ulusal Tez Merkezi ve KTO Karatay Üniversitesi Açık Erişim Sisteminde erişime açılır.

☐ Enstitü / Fakülte Yönetim Kurulu kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren 2 yıl ertelenmiştir.[1]

☐ Enstitü / Fakülte Yönetim Kurulunun gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren …ay ertelenmiştir.[2]

☐ Tezimle ilgili gizlilik kararı verilmiştir.[3][4]

20 Nisan 2022

_____

Cansu ADAM

[1] MADDE 6(1) Lisansüstü tezle ilgili patent başvurusu yapılması veya patent alma sürecinin devam etmesi durumunda, tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulu iki yıl süre ile tezin erişime açılmasının ertelenmesine karar verebilir.

[2] MADDE 6(2) Yeni teknik, materyal ve metotların kullanıldığı, henüz makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış ve internetten paylaşılması durumunda 3. şahıslara veya kurumlara haksız kazanç imkanı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulunun gerekçeli kararı ile altı ayı aşmamak üzere tezin erişime açılması engellenebilir.

[3] MADDE 7(1) Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı, tezin yapıldığı kurum tarafından verilir. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise, ilgili kurum ve kuruluşun önerisi ile enstitü veya fakültenin uygun görüşü üzerine üniversite yönetim kurulu tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.

[4] MADDE 7(2) Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir.

ETİK BEYAN

KTO Karatay Üniversitesi Lisansüstü Eğitim Enstitüsü Tez Hazırlama ve Yazım Kurallarına uygun olarak Dr. Öğr. Üyesi Mehmet Savaş ÖZDAĞ danışmanlığında tarafımdan üretilen bu tez çalışmasında; sunduğum tüm veri, enformasyon, bilgi ve belgeleri bilimsel etik kuralları çerçevesinde elde ettiğimi, tüm değerlendirme, analiz, bulgu ve sonuçları bilimsel usullere uygun olarak sunduğumu, tez/proje çalışmasında yararlandığım kaynakların tümüne bilimsel normlara uygun biçimde atıfta bulunarak kaynak gösterdiğimi, tezimin/projemin kaynak gösterilen durumlar dışında özgün olduğunu bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

20 Nisan 2022

_____

Cansu ADAM

TEŞEKKÜR

Tez çalışmasının yürütülmesi sırasında değerli bilgi ve deneyimleriyle bana yol gösteren destek ve emeklerini esirgemeyen tez danışmanım sayın Dr. Öğr. Üyesi Mehmet Savaş ÖZDAĞ'a, lisans ve yüksek lisans eğitimim boyunca bilgileriyle ışık tutan ve manevi desteğini esirgemeyen sayın Dr. Öğr. Üyesi Hakkı Mert DOĞU'ya, beni hukuk fakültesine gönderebilmek için tüm fedakârlıklarda bulunan haklarını asla ödeyemeyeceğim kıymetli babam ve annem Murat & Zeynep AĞBABA'ya, yoğun çalışmalarım sırasında bana sabır gösteren ve bana güç veren hayatımın her anında yanımda olan sevgili eşim Mustafa ADAM'a ve bu süreçte çalışmama izin veren motivasyon kaynağım canım kızıma sonsuz teşekkürlerimi sunarım.

Nisan, 2020 Cansu ADAM

ÖZET

Cansu ADAM

Hacker'ların Fidye Zararlı Yazılımları Kullanarak İşleyebileceği Suçlar

Yüksek Lisans

Konya, 2022

Son yıllarda internet ve teknolojide yaşanılan gelişmeler hayatımızda büyük bir yer edinmeye başlamış ve bu durum birçok sorunu da beraberinde getirmiştir. Bu gelişmeler neticesinde "hacker'lar" sanal dünyanın tehditleri olarak hayatımıza girmiş ve 2017 yılında hacker'lar bütün dünyayı sarsan fidye yazılımı saldırısıyla Siber Dünya'da yerini almaya başlamıştır. Fidye zararlı yazılımı, başta Amerika Birleşik Devletleri olmak üzere birçok devlet, banka ve hastaneleri etkileyerek büyük bir kaosa neden olmuş, 2021 yılı itibariyle fidye yazılımları geleceğin en büyük siber tehdidi olarak görülmeye başlanmıştır. Fidye yazılımları niteliği itibariyle bir zararlı yazılım türü olup etki ve kapsamı Türk Ceza Hukuku'nda birçok suçun işlenmesine olanak sağlamaktadır.

Çalışma üç bölümden oluşmakta olup birinci bölümde hacker'lığın tanımı, çeşitleri tarihçesi ile fidye yazılımı kavramı ve gelişimi incelenmiş; ikinci bölümde, Türk Ceza Kanun'unda düzenlenen"Şantaj", "Kişisel Verilerin Kaydedilmesi", "Kişisel Verilerin Hukuka Aykırı Olarak Verilmesi Veya Ele Geçirilmesi", "Bilişim Sistemine Girme", "Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme" ve "Yasak Cihaz Ve Program" ,"Yağma" suçları fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılara konu olabilecek suçlar açısından incelenmiş; üçüncü bölümde ise Dünya'da gerçekleştirilen fidye yazılımı saldırılarına yer verilerek Amerika Birleşik Devletlerinde fidye yazılımı saldırısına karşı alınan önlemler ve bu kapsamda Türk Ceza Hukukunda yapılması öngörülen değişiklikler incelenmiştir.

Anahtar Kelimeler

Hacker'lık, Fidye Yazılımları, Bilişim Sistemleri, Ceza Hukuku.

ABSTRACT

Cansu ADAM

Crimes That Hacker’s Can Commit Using Ransomware

Master’s / Ph. D. Thesis

Konya, 2022

Inrecerts years, the developments in the Internet and technology have started to take abig place in our live sand this has brought many problems with this situation. As a result of these developments“hacking” has entered our lives as threats to the virtual world, and in 2017, hackers began to take their place in the Cyber World with a ransomware has caused a great deal of chaos by affecting many states, banks and hospitals, especially in the United States, and as of 2021, ransomware has come to be seen as the biggest cyber threat of the future. Ransomware is a type of malware by its nature, and its impact and scope allow many crimes to be committed in Turkısh Criminal Law.

The study is divited in three parts and the first part offt he hacker definition, types, history development of the conceptand discusses the ransomware; in these condsection, in the Turkısh Penal Codefor “Blackmail”, “Personal Data Recording”, Hacking İnto The Computer System, System Blocking, Destruction, Or Modify Data” and “The Forbidden And The Program Device”, “Plunder”crime sexamined by including the ransomware attacaks; in the third section, the precautions taken aganist ransomware attacaks in the United States and thea mendments envisaged to be made in the Turkısh Crimınal Law in this context are examined by including the ransomware attacaks carried out in the world.

Keywords

Hacking, Ransomware, İnformation Systems, Criminal Law.

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

KISALTMALAR DİZİNİ

Kısaltma	Açıklama
ABD	Amerika Birleşik Devletleri
AES	Advanced Encryption Standart (Gelişmiş Şifreleme Standartı)
AİHM	Avrupa İnsan Hakları Mahkemesi
bkz	Bakınız
C.	Cilt
DDoS	Distributed Denial Of Service (Dağıtık Hizmet Engelleme)
E.T	Erişim Tarihi
ETCK	Eski Türk Ceza Kanunu
Et al.	Ve diğerleri
IP	Internet Protocol Address (İnternet Protokolü)
m.	Madde
MIT	Massachusetts Institute Techonology (Massachusetts Teknoloji Ensititüsü
NSA	National Security Agency (Ulusal Güvenlik Dairesi)
RDP	Remote Desktop Connection (Uzak Masaüstü Bağlantısı)
s.	Sayfa
S.	Sayı
TCK	Türk Ceza Kanunu
TDK	Türk Dil Kurumu
TBBD	Türkiye Barolar Birliği Dergisi
V.	Volume

1. GİRİŞ

Türkiye diğer ülkelere nazaran internete ve teknolojiye geç kavuşması nedeniyle bilişim suçlarına ilişkin durum ve kavramlara oldukça yenidir. Yapılan araştırmalar Türkiye'deki hacker'ların daha çok mili duygularla hareket eden kişiler olduğunu ve birçoğunun sistemlere veya kişilere zarar verme amacı taşımadığını göstermiştir. Ancak şuana kadar Türkiye'ye yapılan siber saldırılarında dinamik IP adresleri kullanmak suretiyle global saldırıların yapılması ve fidye zararlı yazılımı saldırılarının Dünya'nın gündeminde olması Türkiye için hâlâ bir tehdit niteliği taşımaktadır.

Hacker'lık kavramının geçmişi eskiye dayanmaktadır. Bilgisayar korsanı anlamına gelen hacker'lık aslında geniş bir kavramdır. Zarar verme amacıyla hareket eden başlarda phreakar olarak adlandırılan bu kişilere zamanla hacker denmiş ve günümüzde siber uzman adı altında beyaz şapkalı hacker'ların varlığı onları da bu kavram altına almıştır. Hacker'lık, siyah şapkalı hacker'lar, beyaz şapkalı hacker'lar ve gri şapkalı hacker'lar olarak sınıflara ayrılsa da hacker dendiği zaman akla ilk olarak kötü niyetli siyah şapkalı hacker'lar gelmekte ve bu anlamda kullanılmaya devam edilmektedir.

Fidye yazılımları esas itibariyle zararlı yazılım türlerinden biridir. İngilizce ransomware kelimesinden fidye yazılımı olarak Türkçeye çevrilen ve tarihçesi oldukça eskiye dayanan fidye zararlı yazılımı kendisini tüm Dünya'ya 2017 yılında gerçekleşen WannaCry saldırısı ile tekrar hatırlatmıştır. Küresel çapta zarar veren fidye yazılımı saldırılarında hacker'ların dinamik IP adres kullanmaları, ödeme yöntemi olarak sanal para kullanmaları ve gün geçtikçe çeşitlerinin artması gibi nedenlerinden ötürü fidye zararlı yazılımları günümüzün en büyük siber tehdidi haline gelmiştir. Nitekim her geçen gün farklı tür ve isimde bilişim sistemi üzerindeki verileri veya dosyaları şifrelemek üzere programlanan fidye yazılımlarının ortaya çıktığı gözlenmiştir.

Türkiye teknolojik gelişmelere bağlı olarak interneti diğer ülkelere nazaran geç ulaşmış, bu bağlamda bilişim suçlarının sayısında zamanla ciddi artış olmuş ve bu durum Türkiye içinde büyük sorun ve tehdit oluşturmaya başlamıştır. Ülkemizde de 2016 yılında 5237 sayılı Türk Ceza Kanunu'na eklenen madde ile "Yasak Cihaz Ve Programlar" suç haline getirilerek zararlı yazılım ve programların kullanılması engellenmek istenmiştir.

Çalışmamızın birinci bölümünde hacker'lığın ve fidye zararlı yazılımın tanımına ve tarihsel gelişimine ilişkin bilgi verilmiş, ikinci bölümde 5237 sayılı TCK'da yer alan Şantaj, Kişisel Verileri Kaydetme, Kişisel Verilerin Hukuka Aykırı Olarak Verilmesi Veya Ele Geçirilmesi, Bilişim Sistemine Girme, Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme ve Yasak Cihaz veya Programlar, Yağma suçları incelenmiş, üçüncü bölümde ise fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırıların Dünya'da ve mukayeseli hukuktaki durumu incelenerek Türkiye'de yapılması önerilen değişiklikler açıklanmıştır.

2. HACKER KAVRAMI, TARİHSEL GELİŞİMİ VE FİDYE YAZILIMLARI

2.1. Hacker Kavramı

2.1.1. Tanımı

İngilizce bir terim olan hacker kavramı Türk Dil Kurumu internet sözlüğünde; "bilgisayar ve haberleşme teknolojileri konusundaki bilgisini gizli verilere ulaşmak, ağlar üzerinde yasal olmayan zarar verici işler yapmak için kullanan kimse" anlamına gelen "bilgisayar korsanı" şeklinde tanımlanmıştır.[5] Hacker kavramı, Türk Dil Kurumu Yayınlarının Bilgisayar Terimleri Karşılıkları Kılavuzunda; "çökertici, korsan"[6] anlamında, Türk Standartlar Enstitüsü (TSE) tarafından yayımlanan Bilişim terimleri sözlüğünde ise " teknik olarak bilgisayar uzmanı, korunma altındaki kaynakları yetkisiz şekilde erişerek elde etmeyi tasarlayan teknik olarak bilgili bir bilgisayar uzmanı" olarak tanımlanmıştır[7]. Bilgisayar dünyasında ise hacker; bir amaç doğrultusunda sistem açıklıklarından faydalanarak sistemi ele geçiren, çeşitli yazılımlar ile onu çalışmaz hale getiren, kıran, programlaştıran kişi demektir.[8] Öğretide ise hacker'lık kelimesini suç ile bağdaştırıp bu kapsamda ilişkilendiren bir görüş olduğu gibi bu görüşün tam aksine hacker'lığı etik hacker'lık vurgusu dâhilinde ele alan ve bu anlamda kullanan aksi bir yaklaşımda mevcuttur[9].

Dünyaca ünlü hacker topluluğu Anonymous hacker kelimesinin " hem hevesli yazılımcı hem de siber suçlu" anlamına geldiğinden belirsizlik taşıdığını bu nedenle Anonymous'daki hacker'lara"hacktivist" şeklinde hitap edildiğini belirtmişlerdir[10]. Hacktivist, hack ve hacking kelimelerinden oluşmaktadır. Hack; sözlük anlamı olarak " sızmak, kırmak, darbe yapmak…" anlamına gelmektedir. Hacking; kişinin kullanmakta olduğu bilgisayar veya telefonundaki ağ, yazılım veya güvenlik zafiyetinden

---

[5] Türk Dil Kurumu Resmi İnternet sayfası, https://sozluk.gov.tr/, E.T 10.11.2019.

[6] AKALIN, Şükrü Haluk, CEBECİ, Zeynel, BADA, Erdoğan, MITIŞ, Bülent, ACAR, Levent, TAN, Ali, Bilgisayar Terimleri Karşılıklar Kılavuzu, Türk Dil Kurumu Yayınları, 3. Baskı, Ankara 2013, s. 112.

[7] ARİFOĞLU, Ali, DEMİRER, Mehmet, Şengül, Gökhan, Öz, Osman, Bilişim Terimleri Sözlüğü, Türk Standartları Enstitüsü Yayınları, 1.Baskı, Ankara 2006, s. 95.

[8] BÜYÜKGÖZE, Selma, EL, Çağrı, Kendi Siteni Kendin Koru, Kodlab Yayınevi, 1. Baskı, İstanbul 2018, s. 3.

[9] ÇOBAN, Serhat, "*Hackerlık Kavramı, Modeller ve Medyada Hackerlığın Sunumu*", Bilişim Teknolojileri Online Dergisi, C. 11, S.40, 2020, https://dergipark.org.tr/en/download/article-file/1096412, E.T 28.01.2022.

[10] OLSON, Parmy, Biz Anonsymous'uz, Çeviren; AĞIRNASLI, Suphi Nejat, Paloma Yayınevi, 1. Baskı, İstanbul 2014, s. 16.

yararlanarak saldırılması amaçlanan sisteme veya kişiye ait bilgi ve verilere ulaşmak izinsiz şekilde sisteme girilmesine verilen isimdir.[11]. Hacking saldırısını yapan kişiye hacker, sosyal veya ideolojik bir mesaj vermek için hacking olayını gerçekleştiren hackerlara ise Hacktivist denir[12].

2.1.2. Çeşitleri

Günümüzde hacker terimi hem faydalı eylemler yapan yetenekli bilişim uzmanlar için hem de siber saldırıları gerçekleştiren kişiler için kullanılsa da aslında birçok hacker türü vardır[13]. Hacker'lar genel olarak amaçlarına göre çeşitli gruplara ayrılırlar. Bunlar; siyah şapkalı hacker'lar, beyaz şapkalı hacker'lar, gri şapkalı hacker'lar, hacktivistler, phreaker'lar, cracker'lar, lamer'ler ve scriptkiddie'lardır.

2.1.2.1. Beyaz Şapkalı Hacker'lar

Beyaz şapkalı hacker'lar, siyah şapkalı hacker'ların saldırılarını gerçekleştirirken kullandıkları yazılım ve yöntemleri bilen, onlarla aynı bilgi ve yeteneğe sahip olan ancak amaçları doğrultusunda siyah şapkalı hacker'lardan ayrılan bilişim (güvenlik) uzmanlarıdır[14].Beyaz şapkalı hacker'lar, yasal şekilde yetkili oldukları sistemler üzerinde güvenlik zafiyetlerini tespit edebilmek için sızma testini (Penetration) gerçekleştirirler[15]. Sızma testi sırasında saldırgan gibi davranarak sistemi test ederler ve buldukları açıkları raporlarlar[16]. Böylelikle ortaya çıkabilecek saldırı risklerini en aza indirgerler. Beyaz şapkalı hacker'lar, siyah şapkalı hacker'larla aynı bilgi ve yeteneğe sahip olmakla birlikte onlardan gelecek muhtemel saldırıları engelleyen kişilerdir[17].

BÜLBÜL'e göre beyaz şapkalı hacker'ların tanımlaması yanlıştır. Zira hacker'ların saldırgan kişiler olduğunu, güvenlik sağlamanın hacker'lığa ters bir durum olduğunu,

---

[11] "Hacking Nedir?", http://siberguvenlikhaberleri.blogspot.com/2014/05/hacking-nedir.html, E.T. 10.11.2019.
[12] OLSON, s. 382.
[13]SANDILAÇ, Nurullah, "Siber Dünyada Hacker Kültürü, HacktivizmVe Bilişim Suçları", Yayımlanmamış Yüksek Lisans Tezi, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sakarya 2021, s.82.
[14] "Beyaz Şapkalı Hacker Nedir?", https://sibertehdit.com/beyaz-sapkali-hacker-nedir/, E.T. 11.11.2019.
[15]ALP, s. 49.
[16] ALTUNTAŞ, Abdülaziz, KalıLınux, Kodlab Yayınevi, 11. Baskı, İstanbul 2019, s. 9.
[17]ÖZÇOBAN, Cuma, 21. Yüzyılda Ulusal Güvenliğin Sağlanmasında Siber İstihbaratın Rolü, Yayımlanmamış Yüksek Lisans Tezi, Milli Savunma Üniversitesi Harp Akademileri Stratejik Araştırmalar Enstitüsü, İstanbul 2014, s. 55.

bu nedenle beyaz şapkalı hacker denmesinin doğru olmayacağını belirtmiştir[18]. Buna karşın Türkiye'nin ilk bilgisayar korsanı olan Tamer ŞAHİN'in "Hackerın Aklı" isimli kitabında beyaz şapkalıların hacker kavramı ile özdeşleşmediğine ilişkin eleştirilere yanıt olarak: *" Son zamanlarda çokça kullanılarak yıpratılan " Beyaz Şapkalılar" terimi bazı kişiler tarafından hacker camiasında gerçek hacker'ların adının istismar edilmesi olarak yorumlansa da belirli kriterler dahilinde gerçekleştirildiği zaman gerçek bir hacker'ın elde ettiği yetenekleri doğru şekilde kullanabilmesine olanak tanır. 10 yıldan uzun süredir bir nevi "Beyaz Şapkalı" olarak yaşamını sürdüren biri olarak söyleyebilirim ki; terimi duyan kimileri önce biraz şaşırsalar da hack etmenin etik bir tarafı, en önemlisi hacker'lığın bir felsefesi olduğunu ve bunun bir iş haline getirilerek kişinin fayda yaratabileceğini gördüklerinde hacker kavramı onlar için bambaşka bir anlama bürünüyor"*[19]cevabını vermiştir. Gerçekten de beyaz şapkalı bazı hacker'ların güvenlik güçleri tarafından yakalanmış eski hacker'lar olduğu nazara alındığında bu düşünceye katılmak mümkün olacaktır. Örneğin; efsanevi hacker olan John Drapper[20], dünya tarihinin en ünlü bilgisayar korsanı olarak kabul edilen Kevin Mitnick[21], bir dönem siyah şapkalı hackerlik yapan Santhosh Tuppad[22], ilk siber casusluk programını gerçekleştiren ünlü Hacker Kevin Lee Poulsen[23], Türkiye'nin ilk bilgisayar korsanı olan ve yargılanan Tamer ŞAHİN[24] gibi isimler artık kendi kurdukları şirketlerde veya resmi kurumlarda tecrübe ve yeteneklerini siber güvenliği sağlamak için kullanmaktadırlar. Bunun yanı sıra bilişim uzmanı ya da siber güvenlik uzmanı adı altında önemli beyaz şapkalı hacker'lar da vardır. Örneğin; Türkiye Savunma Sanayi Müsteşarlığında siber güvenlik uzmanı olarak görev alan beyaz şapkalı hacker Kürşat Oğuzhan Akıncı[25], ADEO Bilişim Danışmanlık Hizmetleri AŞ'nin kurucusu olan adli bilişim uzmanı Halil Öztürkci[26], ABD Savunma Bakanlığı İleri Araştırma Projeleri

[18] BÜLBÜL, BİNGÖL, s. 14.
[19] ŞAHİN, Tamer, Hacker'ın Aklı, Doğan Yayıncılık, 3. Baskı, İstanbul 2012, s. 17.
[20]ERGİN, Toprak, Elif, KÜPELİ, B. Gökay, Siber Kırılma, Altıkırkbeş Yayınları, 1. Baskı, İstanbul 2018, s. 29.
[21] ELBAHADIR, Hamza, Hacking İnterface: Bilişimin Yer altı Dünyası, Kodlab Yayıncılık, 12. Baskı, İstanbul 2016, s. 18.
[22] Sonsöz Gazetesi, "Hacker Gibi Düşünerek Saldırılardan Korunun", https://sonsoz.com.tr/, E.T. 11.11.2019
[23] SPIN Media LLC, C. 9, S. 10, 1994, s. 63
[24] ŞAHİN, s. 12.
[25] "ABD Savunma Bakanlığından Türk Hacker'eTeşekkür", http://www.haber7.com/, E.T. 11.11.2019
[26]Halil Öztürkci hakkında bkz.,http://halilozturkci.com/hakkimda/

Ajansında görevli PeiterZatko[27], dünyaca ünlü hacker Kevin Mitnick'i yakalanmasını sağlayan ve FBI ile birlikte çalışan Tsutomu Shimomura[28], birden fazla uçak sistemini hackleyen ve uçak hacker'ı olarak adlandırılan siber güvenlik uzmanı Chris Roberts[29]gibi ünlü beyaz şapkalı hacker'lar da vardır.

Ülkemizde son zamanlarda siber güvenliğin önemi arttıkça beyaz şapkalı hacker eğitimleri verilmeye başlanmıştır. 2016 yılında Türkiye'de 20 bin siber güvenlik elamanına ihtiyaç duyulmuştur[30] ve Bilgi Teknolojileri Kurumu tarafından 2017 yılında çok sayıda beyaz şapkalı hacker alımı yapılmıştır. Yine 2018 yılında İstanbul'da düzenlenen Hack Istanbul Capture The Flag ile en yetenekli hackerlar tespit edilerek ödüllendirilmiştir[31].

2.1.2.2. Siyah Şapkalı Hacker'lar

Siyah Şapkalı (Black Hat) hacker kavramı, sistemlere veya kişilere zarar vermek için hack eylemini gerçekleştiren kişiler için kullanılır[32]. Teknik bilgi ve birikimleri beyaz şapkalılar aynı olup amaçları bakımından ayrılırlar[33]. Amaçları eğlenmek ve para kazanmaktır[34]. Terör örgütü gibi illegal örgütlere para karşılığı hizmet vermek onlar için sorun değildir[35]. Bilinen en tehlikeli hacker'lardır ve saldırdıkları sistemi çökerterek gizli belgeleri ele geçirirler[36]. Yasa dışı gruplar olduğundan yakalanmamak için kriptolu ağlara bağlanarak veya Darknet adı verilen derin ağları kullanarak iletişime geçerler[37]. Siyah şapkalı hacker'lar, amaçlarına ulaşabilmek için teknik yetenekleriyle sınırlı kalmayıp sosyal yeteneklerini de kullanırlar[38]. İkna kabiliyetinin ön plana çıktığı sosyal

---

[27] ELBAHADIR, s. 24.
[28] ERGİN, KÜPELİ, s. 21.
[29] Türkiye Gazetesi, "Canı Sıkıldı NASA'yı Hackledi", https://www.turkiyegazetesi.com.tr/, E.T. 15.12.2019.
[30] "Beyaz Şapkalı Hacker'ler", (2016, 14 Şubat), https://www.bizimsakarya.com.tr/haberler/beyaz-sapkali-hackerler-h23855.html, E.T. 18.11.2019.
[31]"132 Ülkeden Binlerce Hacker HackİstanbuI 2018 Yarışmasında Bir Araya Gelecek", E.T 18.11.2019. https://www.sondakika.com/haber/haber-132-ulkeden-binlerce-hacker-hackistanbul-2018-11153525/
[32] ELBAHADIR, s. 8.
[33] "Siyah Şapkalı Hacker Kimdir?", http://www.dijitalteknoloji.net/internet/siyah-sapkali-hacker-kimdir.html, E.T 18.11.2019.
[34] ÖZKAN, İbrahim, Siber Saldırıların Ekonomik Boyutu, Yayımlanmamış Yüksek Lisans Tezi, Bilecik ŞehyEdabali Üniversitesi Sosyal Bilimler Enstitüsü, Bilecik 2019, s. 5.
[35] ÖZKAN, s. 5.
[36] BÜYÜKGÖZE, EL, s. 3.
[37] ÖZKAN, s. 5.
[38] ALP, Özgür, Akıllı Şehirlerde Siber Güvenlik, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2018, s. 48.

mühendislik, yazılım hatalarından kaynaklanan açık exploitler, şifre kırma, sahte e posta yanıltmaları, zararlı yazılımlar, iki ağ arasındaki güvenlik zafiyetlerini kullanıldığı Man in the Middle (MiTM) gibi saldırılar hacker'ların kullandığı en sık yöntemlerdendir[39].

Siyah şapkalı hacker'lar, saldırdıkları sistemler üzerinden birçok veri ve bilgiyi çalarak dünyada büyük kaoslara neden olmuşlardır. Yahoo, 2013 yılında hackerlar tarafından 1 milyar kişinin hesap bilgilerinin çalındığını duyurarak, dünya tarihindeki en büyük veri hırsızlığı olarak kayıtlara geçmiştir[40]. 21 Ekim 2016 tarihinde Türkiye'de dahil birçok ülkede, Twitter, Spotify, Pinterest gibi siteler hacker'lar tarafından çökertilerek bir süre bu sitelere erişim sağlanamamıştır[41]. 12 Mayıs 2017 tarihinde ise hacker'lar tarafından yayılan "Wannacry" isimli fidye yazılımı ile yaklaşık 150 ülke 200.000'den fazla bilgisayara vurgun yapılmıştır[42]. FBI'ın en çok arananlar listesinde olan ve yaklaşık 1 milyon bilgisayara zarar veren siyah şapkalı hacker Evgenıy Mıkhaılovıch Bogachev[43], Google, Yandex gibi ağları hackleyen Adrian Lamo[44], 2 yıl gibi kısa bir sürede 170 milyon kredi kartını hackleyen Albert Gonzoles[45] gibi isimler bilinen siyah şapkalı hackerlardır. Yetenek ve bilgilerini suç işlemek için kullanan; motivasyonlarını bu doğrultuda kullanan ve suç işleme potansiyeline sahip olan siyah şapkalı hacker'lar tezimizin ana başlığını oluşturacak olup fidye zararlı yazılım saldırıları bu çerçevede anlatılacaktadır.

2.1.2.3. Gri Şapkalı Hacker'lar

Gri Şapkalı hacker kavramı, siyah ve beyaz şapkalı hacker'ların ortasında olan ve genellikle girdikleri sisteme zarar vermeyen kişiler için kullanılır[46]. Gri şapkalı hacker'lar, siyah şapkalı hacker'lar gibi yasa dışı yöntemler kullanarak sistemlere sızarlar ve güvenlik zafiyeti buldukları takdirde bu durumu raporlarlar ya da

[39] ALP, s. 48.
[40] STM Mühendislik Teknoloji Danışmanlık, 2016 Ekim- Aralık Dönemi Siber Tehdit Durum Raporu, 2016, s. 8, E.T. 12.01.2020.
[41] BAŞARAN, Alper, Siber Kıyamet, Arıon Yayınevi, 1. Baskı, İstanbul 2017, s. 78.
[42] BAŞARAN, s. 14-15.
[43] "FBI Tarafından Aranan 10 Hacker", https://www.webtekno.com/sektorel/fbi-tarafindan-aranan-10-hacker-h12346.html, E.T. 18.11.2019.
[44] "AdrianLamoCv", https://www.tarihiolaylar.com/biyografiler/adrian-lamo-cv-239, E.T. 18.11.2019.
[45] ERGİN, KÜPELİ, s. 27.
[46] ŞAHİN, s. 17.

karşılaştıkları duruma göre ne yapacaklarına karar verirler[47]. Beyaz şapkalı hacker'lar gibi sızma işlemini yazılı izinle yapmazlar[48]. Gri şapkalı hacker'lar, siyah ve beyaz şapkalı hacker'ların özelliklerini taşımakla birlikte kişisel çıkar gütmediklerinden hacker'lığı hobi olarak görmektedirler.

2.1.2.4. Hacktivist

Siyasi ya da ideolojik mesajlarını yaymak için belirli siteleri hackleyenkişilere hacktivist denir[49]. "DDOS saldırıları", web sitesini çökertme, gizli verilerin çalınması gibi saldırılar hacktivistler tarafından en çok kullanılan saldırı yöntemlerindendir[50]. Hacktivistler içinde milli duygularla hareket edenler olduğu gibi toplumsal duyarlılığı ön planda tutan kişiler de vardır[51]. Farklı isimlerde birçok gruplar vardır. Örneğin en iyi bilinen hacktivist grup "Anonymous"dur. "Orduyuz, Unutmayız, Affetmeyiz, Bizi Bekleyin " şeklindeki sloganlarını hackledikleri web sitelerine, bloglara yerleştirerek tüm dünyaya isimlerini duyurmuşlardır[52]. 2015 yılında Anonymous tarafından yaklaşık 10 gün süren bir saldırı neticesinde Türkiye'de 50.000 bilgisayar hacklenmiştir[53]. Yine "LulzSec" isimli hacktivist grup FBI gibi devlet kuruluşlarına saldırmak için Anonymous'dan ayrılan ve 2011 yılında kurulan bir gruptur[54]. Türkiye de ise "Ayyıldız Team", Türk Hack Team" isimlerinde hacktivist gruplar vardır[55].

2.1.2.5. Phreaker

Telefon sistemlerini çok iyi bilen ve ücretsiz telefon görüşmesi yapabilmek adına telefon sistemlerini hackleyen kişilere phreaker denir[56].En ünlü phreaker tarihte ilk kez

---

[47] BÜLBÜL, BİNGÖL, s. 15; ÖZKAN, s. 15; KARA, Mahruze, Siber Saldırılar – Siber Savaşlar Ve Etkileri, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2013, s. 14.
[48] ALP, s. 49.
[49] BÜYÜKGÖZE, EL, s. 3.
[50] OLSON, s. 382.
[51] ÖZKAN, s. 8.
[52] OLSON, s. 16.
[53] ARSLAN, Rengin "Türkiye'ye Siber Saldırının 10 Günü: Ne Oldu?", https://www.bbc.com/turkce/haberler/2015/12/151224_siber_saldiri_arslan, E.T. 25.12.2019.
[54] OLSON, s. 383.
[55] ÖZKAN, s. 8.
[56] EMRE KAYA, Ayşe Elif, "*Enformasyon Toplumunun Suçluları: Hacker'lar*", Marmara İletişim Dergisi, C. 0, S. 16, 2010, s. 52, https://dergipark.org.tr/tr/download/article-file/233521, E.T. 25.12.2019.; BÜYÜKGÖZE, EL, s. 3.

telefon sistemlerini hackleyen John Draper'dir[57]. John Draper diğer adıyla Kaptan Crunch telefon hatlarını hackleyen ilk kişi olarak kayıtlara geçmiştir[58]. Artık teknolojinin ilerlemesiyle birlikte klasik phreaker kavramı bilişim dünyasından silinmek üzeredir[59].Günümüzde modern phreakar olarak adlandırılan kişiler telesekreter ve modem gibi cihazları hacklemektedirler[60].

2.1.2.6. Cracker

Ücretli yazılım programlarını kırarak, kopyalarını ücretsiz şekilde dağıtan kişilere cracker denir[61]. Kullandıkları yöntemlerle hacker'lardan ayrılırlar[62]. Genellikle hedef sisteme arka kapı yerleştirerek güvenlik açıklarını bulup sistemi kırarlar[63]. Siyah şapkalı hacker'lar olup beyaz veya gri şapkalı hacker kategorisinde olamazlar[64]. Tamamen kötüniyetli olan cracker'ların amaçları sistem ve programlara yetkisiz erişim sağlamaktır.

Bilinen en ünlü cracker, Unix işletim sistemini inceleyip Linux'i bulan Linux Torvalds'dır[65]. Günümüzde çok sayıda ücretsiz şekilde yayımlanan "warez siteleri" adında korsan yazılım ve programlar vardır[66].

2.1.2.7. Lamer

Hacker olmak için yeteri kadar teknik bilgisi olmayan, hazır kodları kopyalayan kişilere lamer denir[67]. Aslında bir nevi hacker heveslisi kişilerdir. Hacker grupları birbirlerine hakaret ederken "Lamer" veya"ScriptKiddie" ifadelerini kullanırlar[68].

---

[57] BÜLBÜL, BİNGÖL, s. 17; ERGİN, KÜPELİ, s. 28-29.
[58] BÜLBÜL, BİNGÖL, s. 17
[59] ELBAHADIR, s. 9.
[60] "Phreakar Nedir?", https://phreaker.nedir.org/, E.T. 11.11.2021.
[61] BÜLBÜL, BİNGÖL, s. 17
[62] BIÇAKCI, Salih, "*NATO'nun Gelişen Tehdit Algısı: 21 Yüzyılda Siber Güvenlik*", Uluslararası İlişkiler Dergisi, C. 10, S. 40, 2014, s. 115, https://dergipark.org.tr/tr/download/article-file/540269, E.T. 11.11.2021.
[63] JELEN, Sara, "Hacker Vs Cracker: Main DifferencesExplained", https://securitytrails.com/blog/hacker-vs-cracker, E.T. 11.11.2021.
[64] JELEN, Sara, https://securitytrails.com/blog/hacker-vs-cracker, E.T. 11.11.2021.
[65] ÖZKAN, s. 9.
[66] ÖZKAN, s. 9.
[67] BÜYÜKGÖZE, EL, s. 4.
[68] ÖZKAN, s. 9.

2.1.2.8. ScriptKiddie

Programla bilgisi olmayan, hacker lığa ilgi duyan genellikle çocuk yaştaki kişilerdir[69]. "Çömez hacker'lar" olarak da adlandırılır[70]. Lamer'lara göre daha bilgi sahibidirler. Genellikle kişilerin e posta hesaplarını veya şifrelerini çalarlar[71]. Script Kiddie'lar, başkalarının hesaplarını hackleyerek arkadaş ortamında ün kazanmaya çalışırlar[72]. Script Kiddie'lar zaman zaman tehlikeli olabilmektedirler. Örneğin, Amazon, Yahoo gibi web sitesine DDoS saldırısını gerçekleştiren 17 yaşındaki Mafiaboy takma isimli kişi saldırıdan hemen sonra sanal sohbet ortamı olan IRC'de saldırısını anlatarak hava atmak istemişse de sisteme verdiği zararlardan dolayı tutuklanmıştır [73].

2.2. Tarihsel Gelişimi

2.2.1. Hacker'lığın Dünyadaki Tarihsel Gelişimi

2.2.1.1. Amerika Birleşik Devletleri

Bilgisayar fikrinin mucidi olan Charles Babbage, 1837 yılında bu fikri ortaya atarken bilgisayarların asırlar sonrasının siber kıyameti olacağını belki de hiç düşünmemiştir[74].Hack kavramı ilk kez 1960'lı yıllarda ABD'deki "Massachusetts Institute Techonology (MIT)" isimli enstitü öğrencileri tarafından kullanılmıştır[75]. MIT öğrencileri devasa boyuttaki bilgisayarların daha hızlı çalışması için program geliştirmeye başlamışlar ve geliştirdikleri bu programa hack (kırmak) ismini vermişlerdir[76]. 1960'lı yıllarında hacker'lar, kırıcı (phreaker) ismi ile Amerika'da

[69] ELBAHADIR, s. 9.
[70] OLSON, s. 381.
[71] ELBAHADIR, s. 9.
[72] OLSON, s. 381.
[73] "ScriptKiddie Nedir", http://www.dijitalteknoloji.net/internet/script-kiddie-nedir.html, E.T. 07.12.2021.
[74] YILMAZ, Seda, Siber Güvenliğin Sağlanmasında Yazılım Kalite Süreçlerinin Önemi, Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara 2015, s. 3,
[75] YANAR, Yasin, Ceza Hukuku Ve Bağlamında Hukuku Bağlamında TCK Md. 245/A Yasak Cihaz Veya Programlar Suçu, Yayımlanmamış Yüksek Lisans Tezi, İstanbul 2019, s. 34; ÇAKIR, Hüseyin, Nursel, YALÇIN, KILIÇ, Mehmet Serkan, "*İnternet Sitelerine Yapılan Siber Saldırılar: 2015 yılı Türk Kamu Siteleri İncelemesi*", Güvenlik Stratejileri Dergisi, C. 13, S. 25, 2017, s. 158, https://dergipark.org.tr/tr/download/article-file/298060, E.T. 18.11.2019.
[76] ERGİN, KÜPELİ, s. 15.

bulunan bir şirketin bilgisayar sistemlerini karıştırarak ilk faaliyetlerine başlamışlardır[77]. İleriki zamanlarda ise kendilerini hacker olarak tanımlamışlardır[78].

1969 yılında Ken Thampson ve Dennıs Ritche adında iki bilgisayar bilimcisi dönemin en büyük hacking olayını gerçekleştirmişlerdir[79]. Ken Thampson, Dennıs Ritche birlikte C programlama dilini yazarak UNIX işletim sistemini yaratmışlardır[80].1970'li yıllarının başında ise ücretsiz telefon görüşme yapabilmek adına uluslararası telefon şebekelerine sızmaya çalışan hacker'lar ortaya çıkmaya başlamıştır[81]. Dünyanın en yetenekli hacker'larından olan John Draper, Crunch adlı mısır gevreğinin içinden çıkan düdük sesinin telefon şebekeleri tarafından 2600 Hertz'lik ses olarak algılandığını fark ederek düdük sesini kullanmış ve tarihin ilk ücretsiz telefon görüşmesini yapan kişi olmuştur[82]. 1988 yılında kaleme alınan "Stalking The Wily Hacker" başlıklı makalede ilk kez bilgisayar korsanı terimi suç kavramı ile birlikte kullanılmıştır[83]. Aynı yıllarda Cornell Üniversitesinde öğrenci olan Robert Tapan Morris isimli kişi, ARPANET[84] sistemine yaydığı virüs ile altı bine yakın bilgisayarı kullanamaz hale getirerek hacker kavramının geniş kitleler tarafından öğrenilmesini sağlamıştır[85].

2.2.1.2. Almanya

ABD' de hacker kültürünün yaygınlaşmasıyla birlikte çeşitli hacker grupları ortaya çıkmaya başlamıştır. Bunlardan biri de Batı Almanya'da kurulan"Chaos Computer Club" isimli hacker grubudur[86]. Bu hacker grubu "Bildschirm-text"isimli Alman Telekomünikasyon şirketinin bilgisayar sistemine sızarak 130.000 mark" zarara uğratmıştır[87].1989 yılında ABD'ye ait bilgisayarlara girerek sistem kodlarını "KGB" (Komitet Gosudarstvennoy Bezopasnosti) isimli Sovvetler Birliği'nin istihbarat

[77] YANAR, s. 34.
[78] YANAR, s. 34.
[79] BAHADIR, s. 12.
[80] BAHADIR, s. 12.
[81] "Hacker'ların Tarihi", http://arsiv.ntv.com.tr/news/119212.asp, E.T. 18.11.2019.
[82] ERGİN, KÜPELİ, s. 28-29.
[83] ERİŞ, Ufuk, Türkiye'de Kırıcı (Hacker) Kültürü, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, Eskişehir 2009, s. 64.
[84] Ayrıntı için bkz. YANAR, s. 22-23; ERGİN, KÜPELİ, s. 16.
[85] ERGİN, KÜPELİ, s. 18; ERİŞ, s. 64.
[86] Charlıe Gere, Dijital Kültür, Çeviren; AYDOĞDU, Akın, İstanbul 2019, s. 202.
[87] GÜNGÖR, Murat, "Ulusal Bilgi Güvenliği: Strateji Ve Kurumsal Yapılanma", Uzmanlık Tezi, T.C Kalkınma Bakanlığı-Bilgi Dairesi Toplumu Başkanlığı, Ankara 2015, s. 40, dipnot:45

servisine satmışlardır[88] . Bu olay açığa çıkan ilk casusluk vakıası olarak tarihe geçmiştir[89].

2.2.1.3. İsveç

Sızdırılan milyonlarca gizli belgelerle bütün dünyayı alt üst eden ve Ortoğu'da "Arap Bahar'ının başlamasına neden olan "Wikileaks"[90] isimli web site eski hacker Julian Assange tarafından 2006 yılında İsveç'te kurulmuştur[91]. "Şimdiye değin kamuya açıklanan en yüksek miktardaki gizli belge yığını" olarak tarihe geçen 1966 yılları ile 2010 yılları arasını kapsayan 250.000'e yakın belge Wikileaks tarafından yayınlanmıştır[92]. Sızdırılan bu belgelerin hacker'lar tarafından hackelenerek sistemlere sızıldığını iddia edenler olduğu gibi CIA çalışanları tarafından Wikileaks'e ulaştırıldıkları söylenmektedir[93].

2.2.1.4. Rusya

1982 yılında soğuk savaş zamanında ilk siber saldırı örneği olarak gösterilen Sibirya doğalgaz patlaması olayında Rus'lar doğalgaz boru hattında kullanılmak için oluşturulan yazılımı çalmışlar ve ABD tarafından içerisine zararlı yazılım yüklenerek borunun akışını bozmasına neden olan doğalgaz borusunu patlatıldığı olayın faili olarak yer almışlardır[94].

Dünya'nın en etkili siber saldırılarını gerçekleştiren REvil Hacker Grubu'nun Rusya merkezli olduğu bilinmektedir. Yine Dünya'da kaosa neden olan birçok siber saldırının arkasında da Rus hacker gruplarının olduğu tahmin edilmektedir. Nitekim 1988 yılında ABD'nin NASA gibi önemli kurumlarından bilgi ve belgelerin çalındığı tarihin en önemli siber casusluk olayı olarak kayıtlara geçen "Ay Işığı Labirenti" olayının

[88] ERİŞ, s. 69.
[89] ERGİN, KÜPELİ, s. 19
[90] ÖZCAN, Fethi Feyyaz, Yeni Medya Ve Dijital Aktivizm, Yayımlanmamış Yüksek Lisans Tezi, Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2012, s. 31.
[91] ADAKLI, Gülsen, "*Hakim Güçlere Ve Hakim Gazeteciliğe Meydan Okuyan Bir Girişim:Wikileaks*", Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi, C. 66, S. 1, 2011, s. 189, https://dergipark.org.tr/tr/download/article-file/35885, E.T. 18.11.2019.
[92] ÇALIŞKAN, Behlül, Ağ Toplumunda Bilgi Sızıntılarının Gazeteciliğe Etkisi: Redhack Örneği, Yayımlanmamış Doktora Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2016, s. 1.
[93] "Wikileaks ABD'ye ait Şimdiye Kadarki En Büyük Casusluk Dosyalarını Yayınladı", https://siyasihaber4.org/e/wikileaks, E.T. 15.12.2019.
[94] KARA, s. 40.

saldırganları olarak Rus hacker'lar gösterilmiştir[95]. Yine Nitekim LinkedLn, Dropbox ve Formspring'i hackleyen Yevgeny Nikulin, Kelihos botnetini işleterek on binlerce bilgisayarlara fidye yazılım saldırısı gerçekleştiren Pyotr Levashou'da rus asıllı hacker'lardır.

2.2.2. Hacker'lığın Türkiye'deki Tarihsel Gelişimi

Türkiye'nin teknolojik gelişmelere bağlı olarak interneti diğer ülkelere nazaran geç kullanmaya başlamasından ötürü bilişim alanında sansasyonel olaylara ileriki zamanlarda şahitlik etmiştir. Aynı zamanda Türkiye'de hacker kavramı yetenekli ve zeki bilgisayar uzmanı anlamına karşılık gelecek şekilde pek anılmamıştır[96]. Bu nedenledir ki Türkiye'de birçok haber sitesine konu olan olaylarda kullanılan hacker teriminden aslında siber suçlu olan siyah şapkalı hacker'lar ifade edilmektedir.

2000-2001 yıllarında Türkiye'nin en eski bankası olan Osmanlı Bankasının milyonlarca dolar zarara girip varlığını sona ermesine neden olan bir olay yaşanmıştır. Tamer Şahin isimli hacker, Osmanlı Bankasının güvenlik açığını tespit ederek bu durumu mail ile bankaya bildirmiş; ancak banka güvenlik açıklarının olmadığını bildirerek durumu ciddiye almamışlardır. Bunun üzerine Tamer Şahin; *"Hello T.Ş was were"* mesajı ile Osmanlı bankasının sistemini hackleyerek Türkiye'nin ilk siyah şapkalı hacker'ı olarak literatüre geçmiş ve bu isimde yargılanan ilk kişi olmuştur[97]. Türkiye'nin ilk hacker'i olan ve bunu Türkiye'ye duyuran Tamer Şahin aynı zamanda, 1999 yılında Superonline ve 2002 yılında Microsoft bilgisayar sistemini hackleyerek Bill Gates'e ait gizli yazışmaları internette yayımlamıştır[98]. Doçent Dr. Ufuk Eriş "Türkiye'de Kırıcı (Hacker) Kültürü üzerine yazmış olduğu doktora tezinde Türkiye'deki hacker'lık üzerine anket yapmış ve bu ankette; "14-21 yaşları arasında çoğunluğunun erkeklerden oluştuğunu, hacker'lığı"zevk almak veya bir amaca hizmet etmek için" yaptıklarını ve büyük çoğunluğunun site kırma eylemini" gerçekleştirdiğini tespit etmiştir[99]. Yine aynı ankette, "Hacker'lık suç mudur?" sorusuna katılımcıların

[95] KARA, s. 69.
[96] SANDILAÇ, s. 102.
[97] Osmanlı bankasına yapılan hack saldırısı hakkında detaylı bilgi için bkz. ŞAHİN, s. 71-80.
[98] Tamer Şahin Geçmiş bkz.,https://tamersahin.com/tr/#/medya, E.T. 06.01.2019.
[99] Anket hakkında detaylı bilgi için bkz., ERİŞ, s. 140-165.

çoğunluğu "suçtur" diye yanıtlarken[100], "Türk hacker'lar ile yabancı hacker'lar arasındaki fark nedir? " sorusuna ise, Türk kırıcıların daha zeki ve meraklı olduklarını aynı zamanda milli ve dini duygularla hareket ettiklerini belirtmişlerdir[101]. Türkiye, teknolojiye geç ulaşması nedeniyle Türkiye'deki hacker (kırıcı) kültürü batıdaki hacker kültüründen farklı şekilde ortaya çıkmıştır[102]. Türkiye'de hacker'lık, "bir ülkü bağlamında milliyetçi değerler temelinde protesto aracı olarak" görülmektedir[103].

2.3. Fidye Zararlı Yazılımları

2.3.1. Tanımı ve Gelişimi

Zararlı yazılım türlerinden olan fidye yazılımı, İngilizce bir terim olan "ransomware" kelimesinden çevrilmiştir. Türkçe "fidye yazılımı"[104] (virüs) anlamına gelmektedir. "*Bilgisayar sistemlerine veya dosyalara erişimi kısıtlayan ve veri sahibine geri yüklenen erişim karşılığında fidye ödemekle yükümlü kılan zararlı yazılımlara*"[105] fidye yazılımı denir. Fidye yazılımında saldırgan, hedef sistemdeki bilgi veya verileri şifreleyip erişilmez hale getirdikten sonra verileri vermek veya şifreyi çözmek için kurbanlardan fidye istemektedir. Bazen ise saldırgan verileri şifrelemek yerine sistemi tamamen kilitleyerek kurbanın sisteme girmesini engeller[106].Fidye zararlı yazılımları saldırılarında genellikle phishing (oltalama) saldırı yöntemi kullanılmaktadır[107]. Sosyal mühendisliğin de kullanıldığı phishing saldırılarında saldırganlar kişisel bilgileri elde etmek amacıyla sahte e-posta veya web adresler kullanarak hedef bilgisayarı kullanamaz hale getiriler[108]. Fidye yazılımları diğer zararlı yazılımlardan farklı olarak sisteme bulaştıktan sonra yazılımcısının yardımı olmadan kurbanın sisteme erişmesi

---

100 ERİŞ, s.174.
101 ERİŞ, 182.
102 ERİŞ, s.183
103 ERİŞ, 183.
104 Türkçe karşılığı için bkz.,https://tureng.com/tr/turkce-ingilizce/ransomware, E.T. 08.01.2020.
105 ÇELİK, Soner, ÇELİKTAŞ, Barış, "*Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar",* CyberpolitikJournal, C. 3, S. 5, 2018, s. 108, https://dergipark.org.tr/en/download/article-file/536201, E.T. 08.01.2020.
106 AİDAN, J.S, VERMA, H.K, AWASTHİ, L.K, "*ComprehensiveSurvey On PetyaRansomware Attack",* 2017 İnternational Conference On NextGeneration Computing AndİnformatıonSystems, Jammu 2017, s.122, doi:10.1109/ICNGCIS.2017.30.
107 ÇUBUKÇU, Fatih, Bilgi Güvenliği Yönetim Sistemi, Pusula 20 Teknoloji Ve Yayıncılık, 1. Baskı, İstanbul 2018, s. 10.
108 TAHİR, Asaf, Sanal Gerçeklik, Payidar Yayınevi, 1. Baskı, İstanbul 2021, s. 28.

veya dosyalarının şifresini çözmesi oldukça zordur[109]. Fidye yazılımlarında çok güçlü şifreleme algoritmalar kullanılması ve yine kripto paralarla finanse edilmesi gibi nedenler siyah şapkalı hacker'lar tarafından en çok tercih edilen saldırı çeşidi olmasına neden olmuştur[110].

Tarihin bilinen İlk fidye zararlı yazılımını 1989 yılında Joseph Popp adında bir biyolog araştırmacı yazmıştır[111]. Josepp Popp, fidye yazılımının adının verilmesine sebep olan PC Cyborg adında bir şirket kurmuş[112] ve bu hayali şirket "PC Cyborg Corporation" tarafından zararlı yazılım dağıtılmıştır[113]

Joseph Popp, AIDS hastalığına yakalanma riskini tespit eden uygulamanın olduğu 20.000 disketi doksan ülkedeki araştırmacılara göndererek içindeki zararlı yazılımın devreye girmesiyle birlikte kullanıcılardan "lisans" bedeli adında 189 ila 378 dolar" arasında fidye talep eden zararlı yazılım geliştirmiştir[114]. Harvard Üniversitesi'nde biyolog olan Joseph Popp, binlerce kişinin zarar görmesine sebep olmuş ve İngiltere'ye şantaj yaptığı gerekçesiyle tutuklanmıştır[115]. Ancak yetkililer Joseph Popp'un akli dengesinin yerinde olmadığına karar vererek ABD'ye iade etmişlerdir[116]. İlk fidye yazılımları ancak belirli türdeki ", jpg, .pdf, .zip, ve .doc" gibi dosyaları şifreyebilir iken artık bu tür sınırlamalar olmaksızın her türlü dosyalar şifrelenebilmektedir[117]. Fidye zararlı yazılımlarının hacker'lar(saldırganlar)için büyük oranda gelir kaynağı olması bu zararlı yazılımın çeşitlenerek artmasına neden olmuştur[118]. 2013 yılından itibaren hacker'lar fidye ödemeyi reddeden kurbanlarının verilerini silmeye başlayarak saldırılarını daha da etkili hale getirmeyi başlamışlardır[119]. Sentinel One şirketi tarafından yapılan bir araştırmaya göre fidye yazılımından kurtulmak için fidye ödeyen

---

109 ALSHAİKH, Hesham, RAMADAN, Nagy, Ahmet H., HEFNY, "*Ransomware Prevention and Mitigation Techniques*", İnternationa Journal Of Computer Applacations, V. 77, N. 40, 2020, s. 31, https://www.researchgate.net/publication/339326833_Ransomware_Prevention_and_Mitigation_Techniques, E.T 05.02.2022.

110 ALSHAİKH, e.t al., 2020, s. 31.

111 BAŞARAN, Alperen, Zararlı Yazılımlar, Arıon Yayınevi, 1. Baskı, İstanbul 2019, s. 101.

112 GRİMES, A. Roger, Ransomware Protection Playbook, Wiley Publisher, 1st.Edition 2021, s. xxvii.

113 SARAN, A.Nurdan, "Fidye Yazılımlar", Siber Güvenlik ve Savunma Kitap Serisi 3, SAĞIROĞLU, Şeref,(Ed), Grafiker Yayınları, 1. Baskı, Ankara 2019, s. 232.

114 BAŞARAN, 2019, s 101.

115 KILIÇ, Çiğdem, Dünden Bugüne Fidye Yazılımların (Ransomware) Gelişimi Ve Geleceği, Yayımlanmamış Yüksek Lisans Tezi, Bilgi Üniversitesi Lisansüstü Programlar Enstitüsü, İstanbul 2019, s. 8.

116 TheAtlantic.com, Kaveh Waddel, 10.5.2016'dan aktaran; KILIÇ, s. 8.

117 BAŞARAN, 2019, s. 101

118 ÇELİK, ÇELİKTAŞ,2018, s. 107.

119 BAŞARAN, 2019, s. 102.

kuruluşlardan tekrar fidye istenilenlerin oranı %58 iken; fidyeyi ödemelerine rağmen verileri yine de silinenlerin oranı%42 olarak tespit edilmiştir[120]. 2017 yılında Barkly şirketinin yayınladığı istatistiklere göre, şirketlerin 40 saniyede 1 fidye yazılımı saldırısına uğradığını ve her 10 zararlı yazılımdan 6 tanesinin zararlı fidye yazılımı olarak tespit edildiği belirtilmiştir[121]. Dünyanın en güvenli yazılım firması Webroot'da araştırmacı olan Tyler Moffit, fidye yazılımları hakkında; *" Siber suçluların para kazanmak için en çok tercih ettikleri yöntem bilgisayarlara fidye yazılımı bulaştırarak dosyaları şifrelemek ve karşılığında para istemek*" ifadelerini kullanmıştır[122]. Saldırganlar deşifre olmamak için ödeme aracı olarak bitcoini tercih etmektedirler. Bitcoin, "herhangi bir merkezi banka tarafından basılmayan, aksine bilgisayarlar tarafından üretilen ve sadece internet ortamında geçerli olan" sanal para birimidir[123]. İnternet ağı bulunan her noktadan bitcoin transfer işlemi yapılabilmektedir[124]. Bitcoin "dünyanın en gizli para transfer sistemi" olup kullanıcıların isim ve kimlik bilgileri yer almamaktadır[125]. Bu yönüyle fidye ödeme aracı olarak saldırganlar tarafından tercih edilen para transfer biçimi olmuştur.

2.3.2. Türleri

Fidye zararlı yazılımları temelde 2 kategoriye ayrılmaktadır. Bunlar Locker (kilitleyici fidye yazılımları) ve Crypto (şifreleyici) fidye yazılımlarıdır.

2.3.2.1. Kilitleyici (Locker) Fidye Yazılımları

2011 ve 2012 yıllarında daha çok kullanılmış olan kilitleyici fidye yazılımı türünde[126]mağdurun bilgisayar sistemine erişimi kısıtlanmaktadır[127].Mağdurun

---

120 BAŞARAN, 2019, s. 102
121 ÇELİK, ÇELİKTAŞ, 2018, s. 107.
122 BAŞARAN, 2019, s. 102
123 BÜYÜKGÖZE, EL, s. 13; NEBİL, Füsun Sarp, Bitcoin Ve Kripto Paralar, Pusula Yayıncılık, 1. Baskı, İstanbul, 2018, s. 21.
124 "Yeni Başlayanlar İçin 12 Maddelik Kripto Para Başlangıç Rehberi", https://coin-turk.com/yeni-baslayanlar-icin-13-maddelik-bitcoin-rehberi, E.T. 03.01.2020.
125 KONUKSEVEN, Saadettin, ÖZEN, Tuna, 50 Yıllık Hayal Bitcoin, MediaCat Yayıncılık, 1. Baskı, İstanbul 2018, s. 60.
126 YILDIZ, Eyyüp, BARAN, Ahmet, ASLAY, Fulya, "Ransomware Tehdidinin Evrimi, Bilişim Sistemlerinin Korunması Ve Zarar Hafifletme Stratejileri", Mühendislik Alanında Araştırma Ve Değerlendirmeler, HASDEMİR, Zehra, TURHAN, Mahmut, (Ed.), Gece Kitaplığı, C.1, 1.Basım, Ankara 2021, s. 66

bilgisayara erişimini engellediği için "ComputerLocker" olarak da adlandırılmaktadır[128]. Bu tür fidye yazılımlarında crypto fidye yazılımlarından farklı olarak saldırganlar hedef bilgisayardaki tüm dosyalar şifrelemeyip sistemin kendisi kilitleyerek erişemez hale getirmektedir[129].Locker fidye yazılım türünde saldırganlar mağdurun yalnızca fidye ödemesini sağlayacak şekilde erişimlere izin vermektedirler ve bu nedenle genellikle fidye olarak sanal parayı tercih etmemektedirler[130]. Yine bu yazılım türünde bilgisayar sisteminin kullanılması kısıtlandığından çoğunlukla var olan dosya veya verilere zarar verilmemektedir[131].

Hacker'lar Crypto fidye yazılımlarının çeşitli varyasyonları geliştirmekle beraber saldırılarında daha güçlü fidye yazılım türü olan crypto fidye yazılımlarını tercih etmektedirler[132]. 2016 yılında ortaya çıkan Reveton fidye yazılımı locker fidye yazılım türüdür[133]. 2019 yılında saldırganların sistemin şifrelerini değiştirip cihazları kapatarak erişilmez hale getirdiği İsveçli Alüminyum şirketi Hydro'ya gerçekleştirilen "LockerGoga" isimli fidye yazılım saldırısı da kilitleyici bir fidye yazılım türü olarak karşımıza çıkmıştır.

2.3.2.2. Şifreleyici (Crypto) Fidye Yazılımları

Çok güçlü algoritmaya sahip olan crypto fidye yazılımı hacker'lar tarafından en fazla kullanılan fidye yazılım türüdür[134]. Saldırgan, bulaştığı sistemdeki hedef veri dosyalarını şifreleyerek mağdurun tekrardan dosyalarına erişmesi için karşılığında fidye

---

[127] KUMAR, R., QUANG,N.H, KUMAR SOLANKI, V., CORDANA, M., KUMAR PATTNAİK (Ed.), Research In İntelligent And Computing İn Engineering: Select Proceedings Of Rıce 2020, Springer Puplisher, 1.st.ed., 2021,s. 381.

[128] BHATTACHARYYA, S., HASSANİEN, A.E, GUPTA, D., KHANNA, A., PAN, I., (Ed.), İnternationalConference OnİnnovativeComputing and Communations, Proceedings of ICICC 2018, Volume 2, Springer Puplisher, 2018, s. 27.

[129] KARA, İlker, "*İnterpol Fidye Yazılım Saldırısı Ve Analiz*i", İleri Teknoloji Bilimleri Dergisi, C.8, S. 2, 2019, s. 118, https://dergipark.org.tr/tr/download/article-file/918843, E.T. 03.01.2020.

[130] YILDIZ/BARAN/ASLAY, 2021, s. 66.

[131] YILDIZ/BARAN/ASLAY, 2021, s. 66.

[132] SCOTT, James, SPANIEL, "Drew, The Icıt Ransomware Rapor", Insututefor Crıtıcıal InfrastructureTechnology, 2016, s. 10.,https://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report2.pdf,E.T 08.02.2022.

[133] BHATTACHARYYA, e.t al., 2018, s. 27.

[134] YILDIZ/BARAN/ASLAY, 2021, s. 67.

istemektedir[135].Bu türdeki yazılım dosya veya sistemdeki verileri şifrelemek için programlanmıştır[136].Crypto fidye yazılımında mağdur şifrelenen dosyalara erişmek dışında bilgisayarını kullanabilmektedir[137]. Fidyenin genelde Bitcoin gibi kripto paralar ile ödenmesi istenmektedir[138]. İlk kez 2013 yılında Cryptolocker ismiyle ortaya çıkan şifreleyici fidye yazılımları, 2014 yılında Crypto Defense, CryptoWall, 2015 yılında mobil ransomware LockerPin, 2016 yılında Petya, Crypt XXX gibi birçok crypto fidye yazılımları kendini göstermiştir[139]. Şimdiye kadar ise gerçekleştirilen en büyük siber saldırı olarak kabul edilen WannaCry fidye yazılım saldırısı da şifreleyici fidye yazılım türüdür[140].

2.3.3.Dünya'da Büyük Etki Yaratan Fidye Zararlı Yazılımları

Fidye yazılımlarının özellikle son yıllarda artmasıyla birlikte dünya gündemine bomba gibi düşen çeşitli türlerde fidye yazılım saldırıları olmuştur. Bunlardan; "WannaCry, Petya, TeslaCrpyt, CryptoLocker, Samsam, Ryuk," en önemlileridir.

2.3.3.1. WannaCry

Hacker'ın sızdığı bilgisayar veya sistemlerdeki verilere erişmek yoluyla kullanıcının verilerine erişimini kısıtlayarak fidye talep eden fidye yazılımına"WannaCry" denir. "Shadow Brokers" isimli bir grup NSA (National Security Agency) tarafından kullanılan yazılımı çalıp geliştirerek WannaCry saldırısını gerçekleştirmişlerdir[141]. Başta WannaCry olmak üzere çeşitli fidye yazılımları bitcoin'in yaygınlaşmasıyla birlikte artmıştır[142]. İlk kez 12 Mayıs 2017 tarihinde ortaya çıkan WannaCry isimli fidye yazılımı 150 den fazla ülkedeki büyük ve önemli kuruluşlara verdiği zararla dünya çapındaki en büyük siber saldırı olarak tarihe geçmiştir[143]. 13 Mayıs 2017 tarihinde Krebson Security tarafından paylaşılan bilgiye göre saldırganlar, kurbanlarını 26 bin

---

135 KARA, s. 118.
136 ÇELİK, s. 110.
137 SCOTT, SPANIEL, 2016, s. 10.
138 ÇELİK, s. 110.
139 YILDIZ/BARAN/ASLAY, 2021, s. 63-64.
140 KILIÇ, s. 15
141 BAŞARAN, 2019, s. 103.
142 BÜYÜKGÖZE, EL, s. 14
143 SELİMOĞLU, Seval, ALTUNEL, Mehtap, "*Siber Güvenlik Risklerinden Korunmada Köprü Ve Katalizör Olarak İç Denetim",* Denetişim Dergisi, C. 0, S 19, 2019, s. 7, https://dergipark.org.tr/tr/download/article-file/750860, E.T. 03.01.2020.; BAŞARAN, 2019, s. 102.

dolar zarara uğratmıştır[144]. WannaCry saldırısı 2017 yılının"*siber risklerin örgütsel farkındalığında başlangıç noktası*" olmuştur[145].

2.3.3.2. Petya

WannaCry saldırısından kısa bir süre sonra 27 Haziran 2017 tarihinde Ukrayna'da başlayan ve hızla dünyaya yayılan Petya isimli fidye yazılım saldırısı meydana gelmiştir[146]. Petya fidye yazılımı aslında 2016 yılında ortaya çıkmasına rağmen yeni versiyonuyla ilk saldırısını 2017 yılında gerçekleştirmiştir[147]. WannaCry saldırısını gerçekleştiren hacker'lar 24 saatte 30.000 dolar ele geçirmişken Petya saldırısında hacker'ların 10.000 dolar haksız kazanç sağlamaları bu saldırıdaki asıl amaçlarının sistemlere veya önemli kuruluşlara ağır hasar vermek olduğu ileri sürülmektedir[148]. Petya, WannaCry 'a benzemekle beraber yöntem olarak daha güçlü ve ağır bir saldırıdır[149].Petya saldırısında farklı olarak tek tek dosyaları şifrelemek yerine bütün dosyaların depolandığı "MBR (Master Boot Record)" sistemi şifrelenerek daha güçlü bir saldırı gerçekleştirilmiştir[150].

2.3.3.3. TeslaCrpyt

İlk kez 20 Şubat 2015 tarihinde ortaya çıkmıştır[151]". "TeslaCrpyt "fidye yazılım saldırısında oyun dosyaları ve kullanıcılar hedef alınmıştır[152]. Teslacrpyt'da hackerlar (saldırganlar) kullanıcının dosyalarını şifreledikten sonra çözmek için 500 dolar miktarında bitcoin ile fidye talep etmektedir[153]. Teslacrpyt saldırısına genellikle küçük

---

144 BÜYÜKGÖZE, EL, s. 14

145 ÇOTAK, Alper, Sigortacılık Sektöründe Siber Güvenliği, Dünyada Ve Türkiye'deki Gelişmelerin İncelenmesi, Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Bankacılık Ve Sigortacılık Enstitüsü, İstanbul 2019, s. 84.

146 STM Mühendislik Teknoloji Danışmanlık, 2017 Nisan-Haziran Dönemi Siber Tehdit Durum Raporu, 2017, s. 9, https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-nisan-haziran-2017, E.T. 12.01.2020.

147 AİDAN, VERMA, AWASTHİ, s.124, doi:10.1109/ICNGCIS.2017.30.

148 Habertürk, "*Ece Üner'le 1 Gün*", 2017, (04:03 - 04:16), https://www.youtube.com/watch?v=WjcsHbA, E.T. 12.01.2020.

149 Habertürk, (01:11 - 01:23).

150 KILIÇ, s. 13.

151 "Vvv Uzantılı Virüs Nasıl Temizlenir?", https://uzmanim.net/soru/vvv-uzantili-virus-nasil-temizlenir/63219, E.T 15.01.2020.

152 KILIÇ, s. 12.

153 "TeslaCrpyt Nedir Ve Nasıl Kaldırılır?", https://blog.360totalsecurity.com/tr/, E.T. 15.01.2020.

şirket ve kurumlar maruz kalmaktadır[154].Son zamanlarda Türkiye'deki sanal oyun oynayan kitle sayısı da dikkate alındığında TeslaCrpyt fidye yazılımına karşı dikkatli olmakta fayda olacaktır.

2.3.3.4. CryptoLocker

2013 yılının Eylül ayında ortaya çıkan Crypto Locker, Gameover Zeus Botnet üzerinden Windows işletim sistemlerine bulaşarak bilgisayar verilerini RSA-2048 şifreleme algoritması ile şifrelemiştir[155]. Crypto Locker'ın bulaştığı sistemlerin büyük bir çoğunluğunun yer aldığı ABD ve Büyük Britanya'da ki mağdurlara 72 saat içinde 300$ ödemeleri gerektiği aksi halde bilgisayar sistemlerindeki tüm veri ve dosyaları silerek erişimsiz hale getirecekleri tehdidinde bulunmuşlardır[156]. 2014 yılında ise Zeus Botnet'in ele geçirilmesiyle CryptoLocker fidye yazılımı saldırısı durdurulmuş ancak milyonlarca zarara sebep olmuştur[157]

2.3.3.5. CryptoWall

2014 yılında ortaya çıkan ve Windows işletim sistemine bulaşan CryptoWall fidye yazılımının ilk varyantlarında RSA-şifreleme algoritması kullanılmışken daha sonra AES 256algoritması ile şifrelenmiştir[158]. CryptoWall fidye yazılımında ABD, Hollanda Büyük Britanya ve Almanya en fazla etkilenen ülkelerden olmuştur[159]

2.3.3.6. Ryuk

Hedef odaklı olarak en fazla miktarda fidye alabileceği büyük ölçekli şirketlere saldıran Ryuk fidye yazılımı 2018 yılında ortaya çıkmıştır [160]. WIZARD SPIDER Rus hacker grubuna ait olduğu düşünülen Ryuk fidye yazılımı 2019 yılında 12,5 milyon dolar fidye

[154] KARA, İlker *"TeslaCrypt Fidye Yazılım Virüsünün Tespiti, Teknik Analiz Ve Çözümü*", Uluslararası Yönetim Bilişim Sistemleri Ve Bilgisayar Bilimleri Dergisi, C. 2, S. 2, 2018, s. 92, https://dergipark.org.tr/tr/download/article-file/610483, E.T. 15.01.2020.
[155]SCOTT, SPANIEL, 2016, s. 13.
[156]SCOTT, SPANIEL, 2016, s. 14.
[157]SCOTT, SPANIEL, 2016, s. 14.
[158] ÇELİK, ÇELİKTAŞ, 2018, s. 116.
[159]SCOTT, SPANIEL, 2016, s. 14.
[160] YILDIZ/BARAN/ASLAY, 2021, s. 72.

talep etmişken 2020 yılında bu rakam 150 milyon dolara kadar çıkmıştır[161]. Ryuk fidye yazılımı en tehlikeli fidye yazılımlardan biri olmakla beraber pandeminin etkisiyle birlikte birçok sağlık kuruluşu hedef almış ve milyonlarca dolar fidye toplamıştır[162]

2.3.4. En Sık Rastlanan Bulaşma Yöntemleri

Fidye yazılımlarında saldırganlar çeşitli sızma yöntemleri ile hedef bilgisayara bulaşmaktadırlar. Nitekim TeslaCrypt fidye yazılımında saldırganlar oyun vb. sitelerdeki ücretsiz indirilen dosyalar üzerinden[163], Cryptolocker fidye yazılımında e posta uzantısından[164], WannaCry ve Petya fidye yazılımlarında ise sunucu ileti bloğu olan SMB (Server Message Block) güvenlik açığı üzerinden sızmışlardır[165].

Fidye yazılımlarının en sık sistemlere bulaşma yöntemlerini şu şekilde sıralayabiliriz;

- Sosyal Mühendislik: İnsan faktörünün etkili olduğu bu yöntemde kullanıcının dalgınlığından veya dikkatsizliğinden faydalanılmaktadır. Genellikle oltalama (phishing) saldırısı ile şeklinde karşımıza çıkmakla birlikte siyah şapkalı hacker'lar tarafından sıklıkla kullanılan bir yöntemdir.Saldırgan kurbana spam e-posta veya kimlik avı e-postaları göndererek linkin tıklanmasını sağlar ve fidye yazılımı sistemi ele geçirmiş olur[166]
- Malvertisement: Kötü amaçlı reklam anlamına gelen bu yöntemde internetteki reklamlar aracılığıyla sisteme zararlı yazılım bulaştırılmaktadır. Hatta öyle ki kullanıcı yasal bir sitedeyken reklamı tıklamasa dahi haberi olmaksızın sistemine fidye yazılımı bulaştırılır ve saldırgan kullanıcının konumu, ziyaret ettiği siteler, saatleri gibi bilgileri tespit ederek sistem açıklıklarından faydalanarak saldırıyı gerçekleştirir[167].
- Güvenlik Zafiyeti: Büyük çaptaki fidye yazılım saldırılarının birçoğu sistemlerin güvenlik açıklıklarından faydalanılarak gerçekleşmiştir. Şirket ve kuruluşlar için

[161] Ryuk Fidye Yazılımı Nedir?,TrendMicro, https://www.trendmicro.com/tr_/what-is/ransomware/ryuk-ransomware.html,E.T 02.03.2022.
[162] Ryuk Fidye Yazılımı Nedir?,TrendMicro.
[163] KARA, s. 88.
[164] ERİŞ, KAYA, s. 113.
[165] ÖZÇAKMAK, Burak, "Fidye Yazılım Analizleri Ve Korunma Yöntemleri", Gazi Üniversitesi Fen Bilimleri Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Ankara 2018, s. 71.
[166] SCOTT, SPANIEL, 2016, s. 17.
[167] SCOTT, SPANIEL, 2016, s. 17.

büyük tehlike arz etmektedir. Hatta günümüzde çoğu şirket etik hacker'lar ile çalışarak sistemlerindeki zafiyetleri tespit etmek adına sızma testleri yapmaktadırlar.

Ayrıca önemle belirtmek gerekir ki saldırganlar bulaşma yöntemlerini günden güne geliştirmektedirler. Örneğin Self Propagation[168]denilen kendi kendine yayılma yöntemiyle fidye yazılımı bulaştığı bilgisayarı şifreledikten sonra ağdan ağa yayılarak diğer sistemlere de erişimsiz hale getirir. Locker fidye yazılımlarından ziyade Crypto fidye yazılım türlerinde görülmektedir[169]. Örneğin şifreleme hızı diğer fidye yazılımlardan oldukça yüksek olan ve kendi kendine hızla yayılan Lockbit fidye yazılımı[170], 2021 yılında yeni bir sürümü ortaya çıkan ve kendi kendine yayılma özelliğine sahip varyantı geliştirilen Ryuk fidye yazılımları[171]örnek olarak gösterilebilir. Yine aynı şekilde WannaCry fidye yazılımı da büyük bir hızla milyonlarca sisteme yayılarak küresel ölçekte siber felakete neden olmuştu.

2.3.5. Haksız Kazanç Fidye

Fidye yazılımları, karşılığında haksız bir kazanç sağlamak üzere programlanmış zararlı yazılımlardır. Nitekim saldırganlar deşifre olmamak için sanal para birimlerini ödeme yöntemleri olarak kullanmaktadırlar. Bütün dünyayı etkisi altına alan WannaCry ve Petya fidye yazılımı saldırısında 300- 600 dolar arasında bitcoin talep edilmiş, Vault Crpyt saldırısında şifrelenen dosya sayısı kadar bitcoin talep edilmiş ve TeslaCrypt fidye yazılımında 500 dolar değerinde bitcoin talep edilerek geçen her 60 saat için fidye miktarı iki katına çıkarılmıştır[172].

---

168 SCOTT, SPANIEL, 2016, s. 18.
169 SCOTT, SPANIEL, 2016, s. 18.
170 LockBit2.0 Fidye Yazılımı Tarafından Kullanılan Teknikler, 2021,https://cyberartspro.com/-locbit-yazilimi-kullanilan-teknikler/, E.T. 15.02.2022.
171 SEALS, Tara, "RyukRansomware: NowWithWorming Self- Propagation", Threat Post, 2021, https://threatpost.com/ryuk-ransomware-worming-self-propagation/164412/,E.T. 15.02.2022.
172 ÖZÇAKMAK, s. 79.

2.4.Fidye Zararlı Yazılımlarının Çalışma Anatomisi

2.4.1. Yayılma (Deployment)

Fidye zararlı yazılımı saldırılarının ilk evresi olan yayılma aşamasında saldırganlar hedef sistemi tespit edip fidye yazılımını çeşitli yöntemlerle sisteme bulaştırmaları gerekmektedir[173].Hacker'lar saldırıyı gerçekleştirecekleri kurum veya kuruluşların ağ yapısına göre hareket etmektedir. Dolayısıyla büyük bir şirkete gerçekleştirecekleri saldırıda kullanacakları bulaşma yöntemleri ile bir kişi veya küçük ölçekli bir şirkete gerçekleştirecekleri bulaşma veya yayılma yöntemleri farklılık gösterebilmektedir. Ancak fidye zararlı yazılımlarının bulaştırılmasında en çok kullanılan yöntem hedef bilgisayara e-posta göndererek kurbanın linki tıklamasını sağlamaktır[174].Bu yöntemde saldırganlar kullanıcının mailine banka ekstresi, telefon faturası veya anket göndererek mağdurun dikkati çeker ve linki tıklamasını sağlar. Böylelikle fidye yazılımı sisteme yayılmış olur. Bazen de saldırganlar mağdur kullanıcının haberi olmaksızın sisteme zararlı yazılımı otomatik olarak (drivebydowland)indirilmesini sağlayarak fidye yazılımını yayarlar[175]. Petya fidye yazılımı *"CVE-2017-0199"* exploiti kullanılarak yayılmışken "PC- Cyborg" CD dağıtımı ile yayılmıştır[176].

2.4.2.Kurulum (Installatıon)

Fidye zararlı yazılımı saldırılarının kurulum aşaması saldırganın hedef sistemi ele geçirmeye başladığı yerdir[177]. Fidye yazılımı bilgisayara bulaştıktan sonra öncelikle gerçek bir sistemde olup olmadığını tespit etmeye başlayacaktır[178].Sistem hakkında bilgi toplayarak şifreleyeceği verileri belirler ve bunun için de genellikle sık kullanılan dosyalara bakarak değerli dosyaları belirler[179]. Mağdur için önemli ve değerli olan

---

[173] DEĞİRMENCİ, Olgun, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi",* Yaşar Hukuk Dergisi, C. 1, S. 2, 2019, s. 181, https://dergipark.org.tr/en/download/article-file/1335226, E.T. 15.01.2020.

[174] KILIÇ, s. 16.

[175] LİSKA, Allan, GALLO, Timothy, Ransomware Defending Againist Digital Extortion, O'Relly Publisher, ABD 2017, s. 6.

[176] ÖZÇAKMAK, Burak, "Fidye Yazılımları Analizleri Ve Korunma Yöntemleri", Gazi Üniversitesi Fen Bilimleri Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Ankara 2018, s. 72.

[177] LİSKA, GALLO, s. 9.

[178] KILIÇ, s. 16.

[179] YILDIZ/BARAN/ASLAY, 2021, s. 67

verileri tespiti saldırgan için epey önem arz etmektedir. Zira mağduru bu verilerle tehdit ederek fidye miktarını belirlerken bunu bir şantaj aracı olarak kullanır[180].

Bu aşamada saldırgan fidye yazılımının hangi sistemlere bulaştığını belirlemek için genellikle bilgisayar sistem adını MD5 özet fonksiyonunu veya Mac adresini kullanarak kendisini benzersiz hale getirir[181]. Fidye yazılımında öncelikle antivürüs programlarının kendisini tespit etmesine izin vermeden saldırganın komuta kontrol sistemi ile iletişimini kurmasını sağlayacak dropper metodolojisi ile küçük bir kod parçacığı sisteme yerleştirilir ve ardından komutlar alarak kendini bilgisayara indirir[182]. BCDEit komut dosyası kullanılarak Dropper adı verilen kötü amaçlı yazılım dosyası indirilir ve sistem kurtarma özelliklerini kapatarak Windows korumaları devre dışı bırakılır[183].

2.4.3. Komuta ve Kontrol (Command And Control)

Fidye zararlı yazılımlarında komut dosyaları kurbanın sistemine fidye yazılımını indirip yüklenmek için tasarlanmıştır ve bulaştığı kurban sistemdeki verilere ulaşmak için komuta ve kontrol sunucuyla iletişiminin sağlanması gerekmektedir[184]. Bu sunucular kullanıcı/mağdur ile iletişim sağladığı gibi saldırganlar tarafından hazırlanan fidye yazılım notunu iletmek, para akışını sağlamak gibi durumlar içinde kullanılmaktadır[185]. Fidye yazılımının bulaştığı sistemde hangi dosyaları şifreleyeceği, ne zaman şifrelemeye başlayacağı ya da ne kadar süre virüsün sistemde kalması gerektiği gibi hususlarının fidye yazılımına istek olarak gönderilmesi gerekir[186]. Bazı fidye yazılımları IP adresi, domain adı veya antivirüs programları gibi bilgileri de komuta ve kontrol sunucusuna bildirir[187]. Komuta ve kontrol aşamasının fidye yazılımı bulaştığı sistemin tespitini, güvenirliğini ve verinin değerini belirlemek gibi önemli amaçları bulunmaktadır[188].

---

[180] Bilişim Profesyonelleri, KURNAZ, Sümeyye, "*Labirent Fidye Yazılımı Nedir*?, 30 Temmuz 2021, https://bilisimprofesyonelleri.com/labirent-fidye-yazilimi-nedir/, E.T. 24.03.2022.
[181] LİSKA, GALLO, s. 9.
[182] LİSKA, GALLO, s. 8.
[183] LİSKA, GALLO, s. 9-10.
[184] "Phobos Fidye Yazılımı", https://www.enigmasoftware.com/tr/phobosfidyeyazilimi-cikarma/, E.T. 12.12.2021.
[185] KILIÇ, s. 77.
[186] KILIÇ, s. 77.
[187] LİSKA, GALLO, s. 9.
[188] DEĞİRMENCİ , "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi*, s. 182.

2.4.4. Şifreleme/ Kilitleme

Bu aşamada kullanıcının verileri şifrelenmekte veya bilişim sistemi kilitlenmektedir[189]. Sistem hakkında bilgileri ve şifreleme anahtarını saklamak için kayıt defteri anahtarları oluşturur[190]. Fidye zararlı yazılımı bulaştığı sistemde kayıt defterine girilen kod sayesinde sistemin her açılmasında kendisini çalıştırır[191]. Saldırgan mağdurun sunucusuna bağlanarak sistemin uzaktan kontrolünü ele geçirir ve dosya ve klasörlerine erişim sağlayarak şifreleme işlemini başlatır**.** Saldırganlar sistemdeki güvenlik zafiyetine göre sunucuya olan erişimi genel olarak RDP bağlantısı sağlayan araçlarla veya metaspoloit gibi benzeri araçlar ile gerçekleştirir. RDP (Remote Desktop Protocol) uzak masaüstü protokolü, Windows işletim sistemine sahip bir bilgisayara veya sunucuya uzak masaüstü bağlantısı kullanarak aynı ağa veya internet üzerinden Windows çalıştıran başka bilgisayara bağlanılmasıdır[192]. RDP bağlantısıyla saldırgan, hedef bilişim sisteminin sunucusuna, klavyesine ve monitörüne hâkim olarak tüm dosya ve klasörlere erişim sağlar ve böylelikle dosyalar üzerinde istediği işlemi yapabilir[193]. Yani kısacası RDP ile saldırganlar bilişim sistemini uzaktan kontrol ederek sistem üzerindeki tam hâkimiyeti sağlamış olur. Nitekim 2020 yılında pandemi nedeniyle uzaktan çalışma sistemine geçilmesi RDP kullanılmasını %41 oranında artmasına sebep olmuş ve bu durum hacker'ların RDP aracılığıyla fidye yazılımı saldırılarını gerçekleştirmelerine sebep olmuştur[194]. Örneğin çok tehlikeli olduğu bilinen LockBit fidye yazılım grubu genellikle RDP açığını kullanarak uzak masaüstü bağlantısı ile saldırılarını gerçekleştirmektedirler[195]. Nitekim saldırganlar sunucuya doğrudan erişim olmadığı hallerde kullanılan zafiyetler, çeşitli sosyal mühendislik yöntemleri, sistem üzerinde admin yetkisi olan bilgisayar veya kullanıcıların şifrelerini ele geçirme gibi birçok yöntem de kullanabilmektedirler**.** Şifreleme işlemi esnasında mağdur bu durumdan haberdarsız bir şekilde arka planda fidye yazılımı dosyaları şifreler ve

---

189 DEĞİRMENCİ , "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi*, s. 184.
190 ERİŞ, KAYA, "*Cryptolocker Saldırılarının İncelenmesi*", s. 117.
191 ERİŞ, KAYA, "*Cryptolocker Saldırılarının İncelenmesi*", s. 115.
192 "RDP Bağlantısı Nasıl Yapılır?",https://bidb.amasya.edu.tr/media/4594/rdp-4.pdf, E.T. 27.03.2022.
193 Eset, GORETSKY, Aryeh, "*RDP'yi İnternetten Ayırma Zamanı Geldi*", 23 Aralık 2019, https://www.eset.com/tr/blog/rdpyi-internetten-ayirmanin-zamani-geldi/, E.T. 27.03.2022.
194 BGA Security Blog, "Ransomware Saldırılarını Nasıl Tespit Edebilirsiniz", 5 Kasım 2021, https://www.bgasecurity.com/2021/11/ransomware-saldirilarini-nasil-tespit-edebilirsiniz/,E.T. 27.03.2022.
195 "*Ransomware Teknikleri Ve Analizleri*", https://www.infinitumit.com.tr/ransomware-trendleri-ve-analizler/, E.T. 27.03.2022.

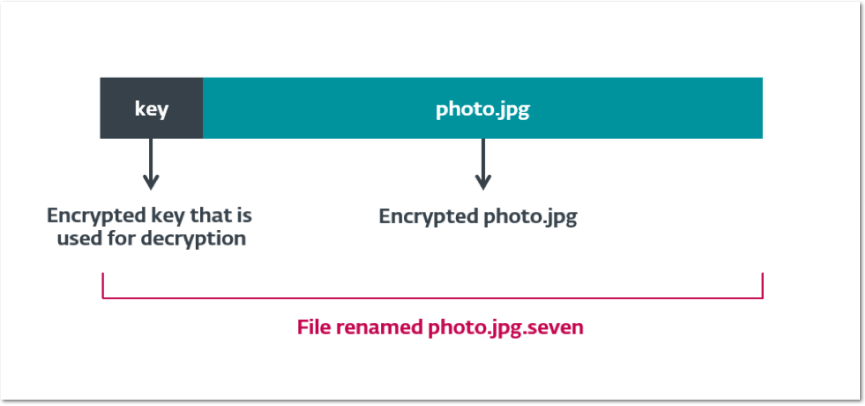
mağdur ancak dosyalar şifrelendiğinde farkına varır. Komuta kontrol aşamasında belirlenen her türlü dosya biçimleri malcode (zararlı yazılım kodu) ile şifrelenir[196]. Şifreleme fidye yazılımı saldırılarında en önemli safhalardan biridir. Zira fidye yazılımının anatomisi gereği saldırgan tarafından şifrelenen dosyaların açılmaması ve bu anahtarın sadece saldırganda olması gerekmektedir[197]. Mağdur için değerli olan veri ve dosyaları şifreleme aşaması bittikten sonra artık şifre anahtarı olmadan çözmek imkânsız hale gelir. Fidye zararlı yazılımında güçlü bir şifreleme algoritmasıyla çoğu dosyaları şifreleyen simetrik ve asimetrik şifreleme kullanılır[198].

Simetrik şifreleme algoritmasında, kurbana gönderilen mesajın şifrelenmesinde kullanılan anahtar ile çözmek için kullanılan tek bir gizli anahtar vardır[199]. Simetrik şifreleme algoritmasında ise mesajın şifrelenmesinde kullanılan anahtar ile şifre çözme için kullanılan anahtar farklıdır[200]. Simetrik şifrelemede tek bir anahtar kullanıldığından saldırganın şifreleme işlemi için ayrıca hedefteki bilişim sistemiyle bağlantıya geçmesine gerek kalmamaktadır[201]. Asimetrik şifre algoritmasında ise açık ve özel anahtar olmak üzere iki anahtar vardır ve açık anahtar sistemdeki dosyaları şifrelerken özel anahtar ise şifreli mesajı deşifre etmeye imkân sağlamaktadır[202].

Dosyaları şifreleme mekanizması olarak öncelikle genel ve özel olan farklı anahtarlar oluşturularak şifrelenir ve saldırganın sunucusuna gönderilir[203]. Dosyalar şifrelendikten sonra şifrelenen her dosya için AES anahtarı oluşturulur ve aşağıdaki görselde gösterildiği gibi dosya oluşturulur[204].

---

196 LİSKA, GALLO, s. 11.
197 KILIÇ, s. 73.
198 https://www.enigmasoftware.com/tr/phobosfidyeyazilimi-cikarma/, E.T 12.12.2021.
199 KODAZ, Halife, BOTSALI, M.Fatih, "*Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması", Selçuk Teknik Dergisi",* C. 9, S. 1, 2010, s. 13.
200 KODAZ, BOTSALI, "*Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması*, s. 14.
201 DEĞİRMENCİ, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi*, s. 183.
202 DEĞİRMENCİ, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi*, s. 183.
203 https://www.enigmasoftware.com/tr/phobosfidyeyazilimi-cikarma/, E.T 12.12.2021.
204 https://www.eset.com/tr/blog/android-fidye-yazilimi-geri-dondu/, E.T 12.12.2021.



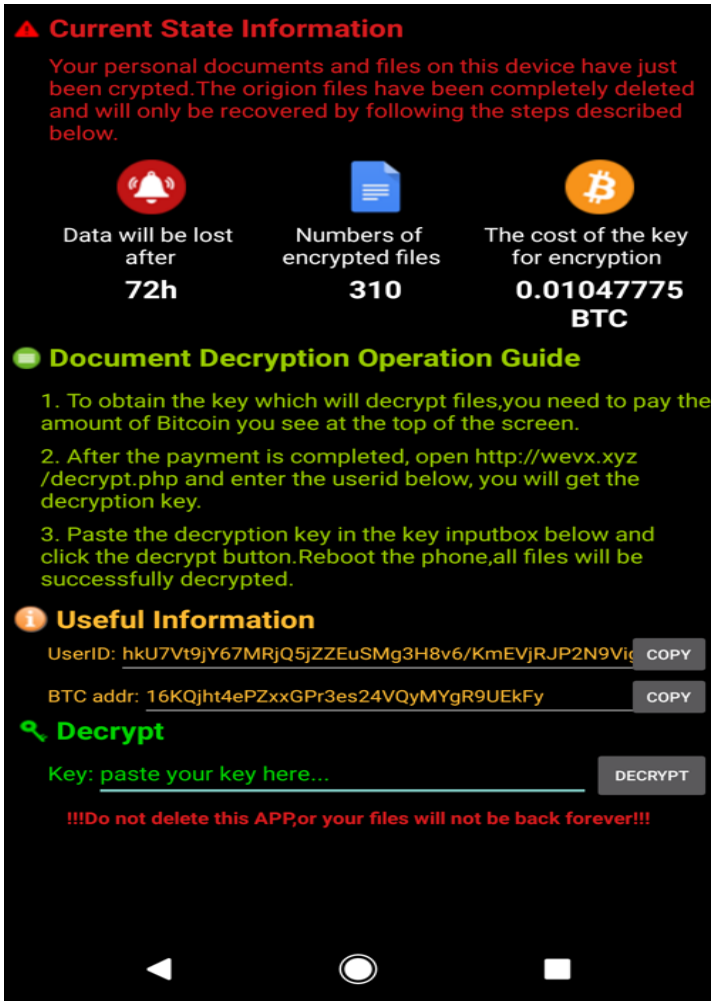
Şekil 1. Şifreli Dosya Yapısı

Simetrik şifrelemede antivirüs programı tarafından tespitini güçleştiren hedefteki kurbanın bilişim sistem kullanılır[205]. Asimetrik şifrelemede ise şifrelenen süreçler için farklı anahtarlar oluşturulur[206] . En tehlikeli fidye yazılımı ailelerinden olan Ryuk fidye yazılımında kurbanın belgeleri önce simetrik şifreleme türü olan AES -256 ile şifrelenmiş daha sonra asimetrik RSA-4096 ile şifrelenmiştir[207].

2.4.5. Fidye Ödemesi

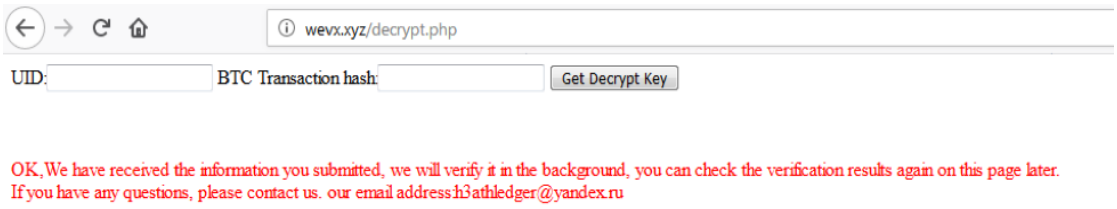
Saldırganlar fidye zararlı yazılımını bulaştırdıktan sonra fidye talebinde bulunurlar ve nasıl ödeme yapacakları konusunda mağdurları yönlendirirler. [208].

[205] DEĞİRMENCİ, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi*, s. 183.
[206] DEĞİRMENCİ, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi*, s. 183.
[207] Ryuk Fidye Yazılımı Nedir?,TrendMicro
[208] Fidye Ödemesi Ekran Görüntüsü için bkz.;https://www.eset.com/tr/blog/android-fidye-yazilimi-geri-dondu/,



Şekil 2. Fidye Notu

Fidye yazılımını çözecek kod kendi içinde bulunur ve mağdur ödemeyi yaparsa saldırganlar tarafından şifre çözme anahtarı gönderilir[209].



Şekil 3. Fidye Ödemesi İçin Doğrulama Web Adresi

[209] Bkz.;https://www.enigmasoftware.com/tr/phobosfidyeyazilimi-cikarma/, E.T 12.12.2021.

3. FİDYE ZARARLI YAZILIMI KULLANILARAK İŞLENEBİLECEK SUÇLAR

Küresel çapta en büyük fidye zararlı yazılımı saldırılarını 12 Mayıs 2017 tarihinde gerçekleştiren hacker'lar, 2020 yılında pandeminin de etkisiyle birlikte güçlerini daha da artırarak çok sayıda önemli kurum ve kuruluşlara zarar vermeye devam etmiştirler. Türkiye'nin de maruz kaldığı bu saldırının gelecekte daha ciddi zararlara neden olacağı tahmin edilmektedir. Bu sebeple böyle tehlikeli ve büyük bir saldırının meydana getireceği zararlar için önlemler alınması ihtiyacı ortaya çıkmaktadır.

İngilizce ransomware kelimesinden fidye yazılımı olarak Türkçeye çevrilen ve şantaj yazılımı olarak da adlandırılan bu saldırı yöntemi adından da anlaşılacağı üzere şantaj şeklinde programlanmıştır. Hacker'lar başlarda virüsü bulaştırdıkları sistem üzerindeki verileri erişimsiz kılmakla tehdit etmekteyken son zamanlarda bunlarla sınırlı kalmayarak Grubman Shire Meiselas & Sack hukuk bürosu[210] ve Transform Hospital Group[211]'a yapılan saldırı örneklerinde olduğu gibi kurbanlarının şeref ve saygınlığına zarar verecek nitelikteki hususları açıklamakla tehdit etmeye başlamışlardır. Bilgisayarın anavatanı olan ve ilk kez siber saldırıya maruz kalan Amerika Birleşik Devletleri'nde[212] fidye yazılım programları Bilgisayar Dolandırıcılığı Ve Kötüye Kullanımı Yasası'na göre suçtur[213]. Fidye yazılımı, ilgili yasanın 18. bölümünün 1030. maddesi ve özellikle bir kişiden para ve değerli bir şeyi almaya yönelik hacker'lığı yasaklayan alt bölüm (a)(7) ile ters düşmektedir[214]. İlgili yasa uyarınca *" Para veya para hükmünde olan herhangibir değeri elde etmek maksadıyla, bir bilgisayar sistemine zarar verme yönünde tehditler savurmak"* suç olarak kabul edilmiştir[215]. ABD' de OFAC tarafından belirlenen terörist gruplarına yapılan fidye ödemeleri federal yasanın

---

[210] "Lady Gaga'ya Siber Saldırı: 42 Milyon Dolar İstediler", https://www.gazeteduvar.com.tr/dunya/2020/ 05/18/lady-gagaya-siber-saldiri-42-milyon-dolar-istediler, E.T. 12.02.2020.

[211] TRT Haber, "İngiltere'de Hastaneye Siber Saldırı: Ünlülerin Estetik Fotoğrafı Yayılabilir", https://www.trthaber.com/haber/dunya/ingilterede-hastaneye-siber-saldiri-unlulerin-estetik-fotograflari-yayilabilir-541036.html, E.T. 12.02.2020.

[212] TURHAN, Oğuz, "Bilgisayar Ağları İle İlgili Suçlar(Siber Suçlar), Planlama Uzmanlığı Tezi, T.C Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Ankara, 2006, s. 83.

[213] STARK, John Reed, "RansomwarePayment: Legality, Logistics, andProof Of Life", NasdaqGovernanceClearinghouse, Temmuz, 2017, s. 1, https://listingcenter.nasdaq.com/assets/Ransomware White Paper 2.pdf, E.T. 12.02.2020.

[214] STARK, s.1.

[215] Damon, W.D. Wright" Cybercrimes". Venable LLP. 1 Ocak 2003. 18 Mayıs 2005, https://www.venab le.com/docs/resources/ebookcybercrimes.cfm'den aktaran; TURHAN, s. 83.

18. bölümün 2339B kapsamında maddi destek olarak kabul edilmekte olup yasaya aykırılık teşkil etmektedir[216]. Keza ABD Hazine Bakanlığı 1 Ekim 2020 tarihinde "Fidye Ödemelerini Kolaylaştırmaya Yönelik Olası Yaptırım Riskleri Hakkında Tavsiye" yayınlayarak fidye yazılım saldırısına maruz kalan ve fidye ödeyen kişi veya kurumlara yaptırım uygulanabileceğini hüküm altına almıştır[217]. 23 Ekim 2020 tarihinde OFAC "triton" isimli kötücül yazılım geliştirerek ABD'nin siber güvenliğini hedef alan Rus hükümetine bağlı bir kuruma ABD Düşmanlarına Yaptırım Yoluyla Mücadele Yasasının 244. maddesi uyarınca yaptırım kararı aldığını açıklamıştır[218]. Görüleceği üzere ABD'de artan fidye yazılımı saldırı vakalarına karşı önlemler alınmaya başlanarak birtakım yasa düzenlemelerine gidilmiştir. Zira söz konusu saldırılardaki tehlikenin boyutu artmaya devam etmektedir.

2020 yılında bütün dünyaya etkisi altına alan pandemiyle birlikte hacker'ların hedeflerinde mağdurların kişisel verileri yer almıştır. Fidye zararlı yazılımı saldırılarında ise hacker'lar çoğunlukla sağlık hizmetlerini ve hasta verilerini hedef almışlardır. Öyle ki 10 Eylül 2020 tarihinde Almanya'da bir hastaneye yapılan fidye yazılımı saldırısında hastane yetkilileri hastaya müdahale edemedikleri için yapılan fidye yazılımı saldırısı ilk defa bir kişinin ölümüne neden olmuştur[219]. FBI'ın geçtiğimiz günlerde yayınladığı bildiride ise fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılarda saldırganların çoğunlukla hedeflerinde hastane ve sağlık hizmetleri olduğu belirtilmiştir[220]. Yine Amerikan Tıbbi Tahsilât şirketinin açıkladığı istatistiklere göre hacker'lar 12 milyon hastanın verilerini çalıp bunları "dark web" te satışa çıkarmışlardır[221]. ABD' de Sağlık Ve İnsan Hizmetleri Bakanlığının kuralı gereğince hastanelerin tıbbi ve finansal verilerini çalındığı saldırıların rapor edilmesi

---

[216] STARK, s.4.

[217] DARKReading, "US Treasury's OFAC RansomwareAdvisory: NavigatingTheGrayAreas", 11/24/2020, https://www.darkreading.com/risk/us-treasurys-ofac-ransomware-advisory-navigating-the-gray-areas/a/d-id/1339394, E.T. 01.01.2021.

[218] JDSUPRA, "JonesDay Global Privacy&Cybersecurity Update", January 8, 2021, https://www.jdsupra.com/legalnews/jones-day-global-privacy-cybersecurity-3823733/, E.T. 02.05.2021.

[219] "Hastane Siber Saldırıya Uğradı: Bir Hasta Hayatını Kaybetti", 24 Eylül, 2020, https://www.yenisafak. com/teknoloji/fidye-yazilimi-ilk-defa-bir-olume-neden-oldu-3568434, E.T. 05.01.2021.

[220] "ABD Hastaneleri Sanal Fidyecilerin Saldırısı Altında", 29 Ekim, 2020, https://www.amerikaninsesi. com/a/abd-hastaneleri-sanal-fidyecilerin-saldirisi-altinda/5640544.html, E.T. 05.01.2021.

[221] "ABD'de 12 Milyon Hastanın Bilgileri 'darkweb'te Satışa Çıkarıldı", 18 Haziran, 2019, https://www.bloomberght.com/abd-de-12-milyon-hastanin-bilgileri-dark-web-te-satisa-cikarildi-2225734, E.T. 05.01.2021.

gerekmektedir[222]. Fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılarda ise çalınan verilerin bu kapsamda olup olmadığının belirlenmesi zor olacağından sağlık kuruluşlarında genellikle fidye yazılımı saldırıları bildirilmemektedir[223]. Nitekim 25 Mayıs 2018 tarihinde yürürlüğe giren Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca ise kişisel verinin ihlali halinde veri sorumlusu en geç 72 saat içerisinde yetkili denetim makamına bildirimde bulunma zorunluluğu getirilmiştir[224]. Fidye yazılım saldırılarında sağlık hizmetleri ön planda olmakla birlikte hacker'lar sadece bunlarla sınırlı kalmamaktadır. Nitekim Pakistan'ın enerji tedarik şirketine yapılan fidye yazılım saldırısında hacker'lar 7, 7 milyon değerinde bitcoin talep ederek ödenmediği takdirde şirketin hassas verilerini yayınlamakla tehdit etmişlerdir[225]. Yine 1 Haziran 2020 tarihinde California Üniversitesine gerçekleştirilen fidye yazılımı saldırısında hacker'lar üniversitenin verilerini şifreleyerek 1,14 milyon dolar talep etmişler ve üniversite verileri geri almak için söz konusu fidyeyi ödemek zorunda kalmıştır[226].

Her şeyden önce fidye zararlı yazılımı saldırısı bir bilişim sistemine girilmesi suretiyle işlenmektedir. Zira hacker hedef bilgisayara erişerek sisteme hukuka aykırı giriş yapmaktadır. Fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılar genellikle kullanıcıya gönderilen sahte e-posta bağlantısına tıklamasıyla meydana gelmektedir. Yine fidye yazılımı saldırılarında "İnternete Açık Masaüstü Protokolü" sıklıkla kullanılan yöntemlerden biridir[227]. Bunun haricinde hacker'lar çeşitli sosyal mühendislik yöntemiyle birçok sisteme hukuka aykırı olarak erişim sağlayabilmektedir. Birçok zararlı yazılım saldırılarında olduğu gibi fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılarda da bilişim sistemine girme suçu oluşacaktır. Bilişim sistemine girme suçu ise hemen hemen bütün ülkelerde cezalandırılmaktadır. Öyle ki

---

222 STARK, John Reed, Kevin M. LaCroix (By), "RansomwarePayment: Legality, Logistics, Mitigation, AndInsurance", July 12, 2017, https://www.dandodiary.com/2017/07/articles/uncategorized/guest-post-ransomware-payment-legality-logistics-mitigation-insurance/, E.T. 11.02.2021.

223 STARK, John Reed, Kevin M. LaCroix (By).

224 STARK, John Reed, Kevin M. LaCroix (By).

225 Huobi, BullTrader, "Pakista'nın En Büyük Güç Sağlayıcısı, NetWalker Tarafından Hacklendi", https://muhabbit.com/pakistanin-en-buyuk-guc-saglayicisi-netwalker-tarafindan-hacklendi/, 01.01.2021.

226 Hürriyet, "Hacker'lar, California Üniversitesi'nden 1, 1 milyon Dolar Fidye Aldı", https://www.hurriyet.com.tr/teknoloji/hackerlar-california-universitesinden-1-1-milyon-dolar-fidye-aldi-41553360, E.T. 14.02.2021.

227 "Fidye Yazılımı(Ransomware) Nasıl Bulaşır?", https://sparta.com.tr/makaleler/fidye-yazilimi-nasil-bulasir/, E.T. 14.02.2021.

Çin Halk Cumhuriyetinde hacker'lığın cezası ölümdür[228]. Nitekim 1998 yılında Çin' de gerçekleşen olayda bir bankanın bilişim sistemini kırarak giren ve kendi hesaplarına para gönderen kişilerden biri ölüm cezasına çarptırılmıştır[229].

Bilişim sistemine girilmesiyle birlikte fidye yazılımında kullanılan şifreleme yöntemi ile mağdurun sisteme girilmesi engellenmektedir. Hatta mağdur şifrelenen verilerini geri almak için talep edilen miktarı ödemezse verileri saldırganlar tarafından yok edilmektedir. Daha önce bahsedildiği üzere bazen mağdurlar talep edilen miktarı ödeseler bile verileri yok edilerek sisteme girişleri engellenmektedir.

Fidye zararlı yazılımları sistem üzerindeki verileri veya dosyaları şifrelemek üzere programlanmıştır. Söz konusu programlar çok güçlü algoritmalarla hukuka aykırı şekilde tasarlanmakta olup her geçen gün farklı tür ve isimde fidye yazılımları geliştirilmektedir. Ülkemizde de TCK'ya 2016 yılında eklenen madde ile "Yasak Cihaz Ve Programlar" suç haline getirilerek zararlı yazılım ve programların kullanılması engellenmek istenmiştir.

Siber yağma olarak da adlandırılan fidye zararlı yazılımı saldırılarında esasen mağdur gasp edilmekte ve fail bunu bir bilişim sistemi üzerinden gerçekleştirmektedir. Fidye yazılımı saldırılarında erişimsiz kılmakla tehdit edilen veriler mağdur için "malvarlığı açısından büyük bir zarar" oluşturabilmekte ve hatta saldırıya uğrayan şirketlerin saldırı nedeniyle hizmet verememekten kaynaklı zarara uğraması malvarlığı açısından büyük bir zarara neden olmaktadır. Dolayısıyla fidye zararlı yazılımlarında yağmanın varlığından bahsedilebilecektir.

Bu bölümde, şimdiye kadar yapılan açıklamalar ışığında fidye yazılım saldırıları Türk Ceza Kanunun sistematiği çerçevesinde; "Şantaj, Kişisel Verileri Kaydetme, Kişisel Verilerin Hukuka Aykırı Olarak Verilmesi Veya Ele Geçirilmesi, Bilişim Sistemine Girme, Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme ve Yasak Cihaz veya Programlar", "Yağma" suçları ile ilişkilendirilerek anlatılmaya çalışılacaktır.

---

[228] DÜLGER, Murat, "*Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı Ve Uygulaması*", Türkiye Adalet Akademisi Dergisi, C. 0, S. 31, 2017, s. 159, https://dergipark.org.tr/tr/download/article-file/981531, E.T. 14.02.2021.

[229] CongLixian, "Chinise E- Commerce (2) and Legal Environment", Chinise Intellectual Property and Technology Laws, Ed: Rohan Kariyawasam, Edward Elgar Publishing, 2011, s. 279. Walden, pn. 2.142'den aktaran; DÜLGER, *Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı Ve Uygulaması*", s. 159.

3.1. Şantaj

Son zamanlarda hacker'lar tarafından sıklıkla kullanılan fidye yazılımlar diğer zararlı yazılım türlerinden farkı olarak "şantaj" şeklinde programlanmaktadır. Şantaj yazılım[230] veya sanal şantaj olarak da adlandırılan bu saldırı yönteminde virüs, bilgisayara veya sisteme bulaştığında başta belgeler olmak üzere, resimler, filmler, veri tabanları ve birçok türdeki dosyayı şifrelemekte ve bu dosyalara mağdurun veya kurbanın erişebilmesi için para talep edilmektedir. Her geçen gün fidye yazılım saldırılarının artması ve bu saldırıyla birlikte tehdit kişi ve kurumları hedef alan tehdit şantajların uluslararası boyuta ulaşması bu saldırının ne kadar ciddi boyuta ulaştığını gözler önüne sermektedir.

5237 sayılı TCK'nın 107. maddesinde düzenlenen şantaj suçu kişilere karşı suçlar başlıklı ikinci kısmın "Hürriyete karşı suçlar" bölümünde düzenlenmiştir. Buna göre TCK 107. madde;

> *(1) "Hakkı olan veya yükümlü olduğu bir şeyi yapacağından veya yapmayacağından bahisle bir kimseyi kanuna aykırı veya yükümlü olmadığı bir şeyi yapmaya ve yapmamaya ya da haksız çıkar sağlamaya zorlayan kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır".*
>
> *(2) "Kendisine veya başkasına yarar sağlamak maksadıyla bir kişinin şeref ve saygınlığına zarar verecek nitelikteki hususların açıklanacağı veya isnat edileceği tehdidinde bulunulması halinde de birinci fıkraya göre cezaya hükmolunur."*şeklindedir.

Şantaj suçunun kanundaki düzenleme alanına bakıldığında fidye yazılımı saldırısıyla şantaj suçu bazı hallerde işlenmesi mümkün olabilecektir. Bilişim Teknolojileri ve Siber Güvenlik Derneği Yönetim Kurulu Başkanı Yavuz Sultan Selim Yüksel, son zamanlarda artan fidye yazılım saldırılarına dikkat çekerek hacker'ların "sextortion"

---

230 KILIÇ, s. 1.

yöntemini kullanarak sanal parayla fidye istediklerini ve sanal şantaj ve fidye tehdidi konusunda dikkatli olunması gerektiğini ifa etmiştir[231].

2020 yılının Aralık ayında fidye yazılımı çetesi olarak bilinen REvil hacker grubu İngiltere'deki birçok ünlü oyuncu ve sanatçılarında bulunduğu Transform Hospital Group'a fidye yazılım saldırısı gerçekleştirmiş, darknet web sayfasında "*müşterilerin samimi fotoğraflarının tamamen hoş bir manzara olmadığını* "söyleyerek basına sızdırmakla tehdit etmiş ve yüklü miktarda bitcoin talep etmişlerdir[232]. Yine 2020 yılının mayıs ayında REvil hacker grubu tarafından New York hukuk firması Grubman Shire Meiselas & Sack' e yapılan fidye yazılım saldırısında birçok ünlünün de yer aldığı 1terebayt boyutunda dosya ele geçirilerek 42 milyon dolar değerinde kripto para fidyesi talep edilmiş ancak hukuk firması ödemeyi reddedince REvil, fidye talebini 2 katına çıkararak Donald Trump'ın bütün kirli çamaşırlarını ortaya çıkararak gizli bilgilerini ifşa edeceğini, bu bilgilerin Trump'ı yok edeceğini ve bu ifşadan sonra hiç kimsenin Trump'ı görmek istemeyeceği açıklamışlardır[233]. FBI ise gerçekleştirilen bu saldırıyı terör suçu olarak kabul ettiğini bildirmiş[234] ve ABD'de terörizme finans sağlamak suç olduğundan bu olayda saldırganlara ödeme yapılmaması konusunda uyarı yapılmıştır. Keza, ABD fidye yazılımına karşı da aynı tutumu sergilemiştir. 1 Ekim 2020 tarihinde OFAC (Amerika Birleşik Devletleri Hazine Bakanlığı Yabancı Varlıkların Kontrolü Bürosu) fidye yazılım ödemelerini kolaylaştırmaya yönelik tavsiye yayınlayarak fidye yazılım taleplerini kabul eden kuruluşların Uluslararası Acil Durum Ekonomik Güçler Yasası (IEEPA) kapsamında yaptırımlara tabi olunacağı konusunda uyarıda bulunmuştur[235]. Dolayısıyla ABD'de fidye yazılım saldırısına maruz kalan kurum veya kuruluşların fidye ödemesi yapması yasaklanarak cezai yaptırıma bağlanmıştır.

---

[231] YÜKSEL, Yavuz Sultan Selim, Hürriyet, "Bilgisayar Korsanlarından "Sextortion İle Şantaj", 12 Ağustos, 2020, https://www.hurriyet.com.tr/gundem/bilgisayar-korsanlarindan-sextortion-ile-santaj-40926096, E.T E.T 15.01.2021.

[232] 1MH, "Bilgisayar Korsanları Estetik Ameliyat Fotoğraflarını Sızdırmakla Tehdit Ediyor", Aralık 24, 2020, https://www.1mh.org/bilgisayar-korsanlari-estetik-ameliyat-fotograflarini-sizdirmakla-tehdit-ediyor/, E.T. 15.01.2021.

[233] Turner Wright, Cointelegraph Türkçe, "Donald Trump'a Hacker Tuzağı- 42 Milyon Dolarlık XMR İstiyorlar", Mayıs 15, 2020, https://tr.cointelegraph.com/news/ransomware-gang-demands-42m-or-it-releases-trumps-dirty-laundry, E.T. 15.01.2021.

[234] Barış Taşkın, Be[IN]Crypto, "İşler Karışabilir: Kripto Para Fidyecileri Donald Trump'ı Tehdit Etti", Mayıs 16 2020, https://beincrypto.com.tr/isler-karisabilir-kripto-para-fidyecileri-donald-trumpi-tehdit-etti/, E.T. 15.01.2021.

[235] Edward Roche, RAC monitör, "Federal Authorities May ImposeCivilPenaltiesAgainstHospitalsPayingRansomwareDemands", October 28, 2020,

Şantaj suçunun TCK'nın hürriyete karşı işlenen suçlar bölümünde düzenlendiği hususu dikkate alındığında korunan hukuki yararın "kişinin karar verme ve hareket etme özgürlüğü[236] olduğu söylenebilir. Şantaj suçunun maddi çıkar elde edilmesi amacıyla işlenmesi halinde ise kişilerin malvarlığı değerleri korunmaktadır[237]. Fidye yazılım saldırılarında ise saldırganın mağdurdan maddi bir çıkar sağlamak için suç işlediği dikkate alındığında fidye zararlı yazılımı kullanarak işlenebilecek şantaj suçunda korunan hukuki yarar kişilerin hürriyetleri ve malvarlığı değerleri olacaktır.

Şantaj suçu ilk fıkra bakımından fail açısından özellik gösteren özgü suç niteliğindedir. Zira failin bir hak ve yükümlülüğe sahip olması gerekmektedir. Bu bakımdan fidye zararlı yazılımı kullanılarak işlenebilecek şantaj suçunun ilk fıkrası bakımından oluşması mümkün görünmemektedir. 2. fıkra ise herkes tarafından işlenebilen bir suçtur olup fail herkes olabilmektedir.[238].Zira kanun koyucu herhangi bir ayrıma gitmemiştir. Burada suçu işleyen fail hacker olarak adlandırılmaktadır. Ancak hacker olarak adlandırılması suçun niteliği bakımından bir özellik arz etmemektedir. Bu suçun mağduru herkes olabilir. Tüzel kişilerin ise şantaj suçunun mağduru olup olamayacağı noktasında doktrinde çeşitli görüşler vardır. Bir görüşe göre; saygınlık kavramının sadece gerçek kişilere özgü olmayıp tüzel kişilerinde bir saygınlığının olabileceğini dolayısıyla suçun mağdurunun tüzel kişilerin de olabileceği ileri sürülmüştür[239]. Diğer bir görüşe göre tüzel kişilerin mağdur olamayacakları ancak tüzel kişiliği temsil eden gerçek kişilerin bu suçun mağduru olabilecekleri ileri sürülmüştür[240]. Katıldığımız

---

https://www.racmonitor.com/federal-authorities-may-impose-civil-penalties-against-hospitals-paying-ransomware-demands, E.T. 15.01.2021.

[236] BAYRAKTAR ve diğerleri, s. 46; Şantaj suçunda mağdur belli bir yönde hareket etmeye zorlandığından şantaj suçu ile korunan hukuki yarar "kişinin iç hürriyeti, yani kendi yeteneklerine ve şartlarına göre irade oluşturabilme imkânıdır. (ÜZÜLMEZ, s. 142.)

[237] TANER, s. 122.

[238] ÜZÜLMEZ, s. 151; BAYRAKTAR ve diğerleri, s. 46.

[239] TANER, s. 125; "*Örneğin; bir şirkete yönelik olarak kendisine belli bir miktar para verilmediği taktirde, şirketin sahip olduğu otelin genelev olarak çalıştırıldığı yönünde internette yer alan forum sitelerinde asılsız beyanlarda bulunacağını ifade eden failin davranışı, şantaj suçuna vücut vermektedir. Burada söz konusu olan otelin ve dolayısıyla sahibi olan şirketin saygınlığıdır ve şirket suçun mağduru olarak kabul edilmelidir*".

[240] BAYRAKTAR ve diğerleri, s. 47; SOYASLAN, Doğan, Ceza Özel Hükümler, Yetkin Yayınları, 5. Bası, Ankara 2005, s. 612'den aktaran; ÜZÜLMEZ, s. 151; BİLGE, Burak, "*Şantaj Suçu*", İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi C.6, S.1, 2019, s. 139, https://dergipark.org.tr/tr/download/article-file/1102151, E.T. 15.01.2021.

görüşe göre suç tipi dikkate alınarak tüzel kişi de mağdur olabilecektir[241]. Zira fidye yazılım saldırılarındaki asıl hedefler göz önüne alındığında tüzel kişiliklerin bu suçun mağduru olması konusu önem arz etmektedir.

3.1.1. Fidye Zararlı Yazılımı Saldırılarında 107/1. Maddesine Göre Fiil

Suçun 107. maddesinin 1. fıkrası bakımından "Hakkı olan veya yükümlü olduğu bir şeyi yapacağından veya yapmayacağından bahisle bir kimseyi kanuna aykırı veya yükümlü olmadığı bir şeyi yapmaya ve yapmamaya ya da haksız çıkar sağlamaya zorlamak" şantaj suçunun ilk halini oluşturmaktadır[242]. Maddenin 1. fıkrasında var olan yasal hak ve yükümlülük kötüye kullanılmaktadır[243]. Şantaj suçu ilk fıkrada düzenlenen hali bakımından seçimlik hareketli bir suçtur[244]. Fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılarda saldırganların hukuka aykırı olarak elde ettiği bilgi veya belgeler nedeniyle hakkı veya yükümlü olduğu bir durumdan bahsedilemeyeceğinden şantaj suçunun fidye yazılımı saldırıları bakımından suç teşkil etmeyecektir[245].Örneğin; fidye zararlı yazılımı saldırısıyla mağdurun vergi kaçırdığını öğrenen veya bunu bilen saldırganlar tarafından istedikleri fidye miktarını ödemezlerse buna ilişkin evrakları maliyeye bildireceklerini söylemeleri halinde fidye yazılımlarının ilgili fıkra bakımından suç teşkil edip etmeyeceği sorusu akla gelebilir. Ancak burada dikkat edilecek bir husus vardır. Failin elde ettiği deliller hukuka aykırı olarak ele geçirilmiştir ve burada saldırganın hakkı veya yükümlü olduğu bir durumdan bahsedilememektedir. Dolayısıyla suçun 107. maddesinin 1. fıkrası açısından işlenmesi mümkün olmayacaktır.

---

[241] TANER, s. 125.

[242] DEMİRKOL, Neslihan, "Türk Ceza Hukukunda Şantaj Suçu", Yayımlanmamış Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi, Isparta 2017, s. 48; ÜZÜLMEZ, s. 143; BAYRAKTAR ve diğerleri, s. 47-48.

[243] BİLGE, s. 141.

[244] ÜZÜLMEZ, s. 144; Aksi görüş için bkz.; BAYRAKTAR ve diğerleri, s. 48'den aktaran; HAFIZOĞULLARI, Zeki, ÖZEN, Muharrem, Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar, 3. Basım, Ankara 2013, s. 48.

[245] DEĞİRMENCİ, Olgun, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi",* s. 199.

3.1.2. Fidye Zararlı Yazılımı Saldırılarında 107/2. Maddesine Göre Fiil

Suçun 107. maddesinin 2. fıkrası bakımından söz konusu fiil "Kendisine veya başkasına yarar sağlamak maksadıyla bir kişinin şeref ve saygınlığına zarar verecek nitelikteki hususların açıklanacağı veya isnat edileceği tehdidinde bulunulmasıdır"[246]. Maddede düzenlenen şeref kavramı Türk Dil Kurumunun sözlüğünde *"başkasının birine gösterdiği saygının dayandığı kişisel değer, onur*"[247], saygınlık kavramı ise *"saygıgörme, değerli, güvenilir olma*[248]" şeklinde tanımlanmıştır. Şeref gerçek kişilere ait bir kavram iken saygınlık hem gerçek kişilerin hem de tüzel kişilerin kullanabileceği bir kavramdır[249].Ancak daha önce de açıklandığı üzere doktrinde hâkim olan görüşe göre bu suçun mağduru tüzel kişiliği temsil eden gerçek kişiler olabilmektedir. Şeref ve saygınlığa zarar verecek eylem veya fiillerin gerçek olup olmaması arasında bir fark yoktur[250]. Önemli olan isnat edilen hususun kişinin şeref ve saygınlığına zarar verici nitelikte olmasıdır[251]. Fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırıların 107. maddenin 2. fıkrası bakımından da suç teşkil edip etmeyeceği öğretide tartışmalıdır. Bir görüşe göre mağdurun fidye yazılımı saldırılarında verilerine erişemediğinden dolayı şeref ve saygınlığı doğrudan veya dolaylı olarak zarar görmüş olsa bile "açıklama ve isnat" kapsamında olmadığından 107. maddenin 2. fıkrası bakımından da suç teşkil etmemektedir. Ancak biz bu görüşe katılmamaktayız. Zira daha önce de açıklandığı üzere fidye yazılımları kullanılarak gerçekleştirilen saldırılarda saldırganlar açıklayacakları bilgi, belge veya görüntülerle mağdurların itibar veya saygınlıklarına zarar vermekle tehdit etmektedirler. Dolayısıyla şantaj suçunun 107. maddesinin 2. fıkrası bakımından şantaj suçu işlenmesi mümkün olacaktır.Şantaj suçu maddenin her iki fıkrası bakımından da kasten işlenebilen suçlardandır[252]. Fidye zararlı yazılımı kullanarak işlenebilecek olan şantaj suçunda da suç taksirle işlenemeyecek olup her iki fıkrasında da düzenlenen hali içinde suçun oluşması için saldırganın özel amaçlarla hareket etmesi gerekecektir.

---

246 BİLGE, s. 141; ÜZÜLMEZ, s. 146.
247 Türk Dil Kurumu, Türk Dil Kurumu Sözlükleri, https://sozluk.gov.tr/, E. T 03.11.2020
248 Türk Dil Kurumu, Türk Dil Kurumu Sözlükleri, https://sozluk.gov.tr/, E. T 03.11.2020
249 DEMİRKOL, s. 76.
250 BAYRAKTAR ve diğerleri, s. 51.
251 BAYRAKTAR ve diğerleri, s. 51.
252 ÜZÜLMEZ, s. 152.

Şantaj suçunun her iki maddesinde düzenlenen hali sırf hareket suçu olduğundan tehdit olgusunun fail tarafından gerçekleştirilmesiyle suç oluşmaktadır[253]. Suçun teşebbüs aşamasında kalıp kalmadığını belirlemede kullanılacak kıstas ise doğrudan fiilin icrasına başlanıp başlanmadığı olacaktır[254]. Fidye zararlı yazılımı saldırısı teşebbüs hükümleri açısından düşünüldüğünde ise teşebbüse elverişli gözükmemektedir. Zira söz konusu yazılım diğer zararlı yazılımlardan farklı olarak şantaj şeklinde programlandığından ve bu yazılımın amacının mağdurlardan çıkar sağlamak olduğu hususları dikkate alındığında hareket parçalara ayrılamayacağından söz konusu suça teşebbüs mümkün olmayacaktır. İştirak açısından şantaj suçu herhangi bir özellik göstermediğinden[255]fidye zararlı yazılımı kullanarak işlenebilecek şantaj suçu bakımından da aynısı söz konusu olacaktır. Şantaj suçu herhangi bir başka suçun unsuru veya nitelikli hali olarak düzenlenmediğinden diğer suçlarla birleşmesi mümkün olmayacaktır[256]. TCK'nın zincirleme suç hükümleri kapsamında ise şantaj suçunun 107/1 ve 107/2 ye göre işlenmesi mümkün olacaktır[257]. Fail, tek bir eylemiyle hem şantaj suçuna hem de başka bir suçun oluşmasına neden olmuşsa bu durumda faile en ağır olan ceza verilecektir[258]. Fidye yazılımı mahiyeti itibariyle birden fazla suçun oluşmasına sebebiyet vereceğinden içtima hükümlerinin uygulanması mümkün olacaktır.

Şantaj suçunun her iki fıkrada düzenlenen hali için de bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası öngörülmüştür[259]. Şantaj suçunda lehine haksız yarar sağlanan tüzel kişiler hakkında TCK'nın 60. maddesinde yer alan güvenlik tedbirleri uygulanacaktır[260]. Fidye yazılımı kullanarak işlenebilecek şantaj suçu bakımından saldırganlar suçta ve cezada kanunilik ilkesi gereğince aynı ceza ile cezalandırılacaktır. Ancak kanımca fidye yazılım saldırısının yarattığı infialler ve mağduriyetler dikkate alındığında cezalandırma yolunda değişikliğe gidilmelisi gerekmektedir. Nitekim ABD'de fidye yazılım programları federal bilgisayar suçları yasasına aykırıdır. Yine fidye ödemeleri AML (Kara Para Aklama Önleme) yasalarını ihlal etmekle birlikte

253 BAYRAKTAR ve diğerleri, s. 52.
254 BİLGE, s. 150.
255 BİLGE, s. 151; BAYRAKTAR ve diğerleri, s. 56.
256 ÜZÜLMEZ, s. 157, Aksi görüş için bkz.; DEMİRKOL, s. 103.
257 BİLGE, s. 151.
258 DEMİRKOL, s. 102.
259 BAYRAKTAR ve diğerleri, s. 53; ÜZÜLMEZ, s. 159.
260 ÜZÜLMEZ, s. 160.

fidye yazılım taleplerini kabul eden kurum veya kuruluşların IEEPA (Acil Durum Ekonomik Güçler Yasası) kapsamında para cezası ile cezalandırılmaktadır[261]. ABD hükümeti fidye yazılım saldırılarını ulusal güvenliğine tehdit olarak algıladığından bu denli sert önlemler almakta ve yeni yönetmelik ve yasalar çıkarmaktadır. Dolayısıyla küresel tehdit haline gelen fidye yazılımları açısından Türk Ceza Hukuk sistemimizde de değişikliğe gidilerek sert yaptırım kararların alınması gerekmektedir. Fidye zararlı yazılımı kullanarak işlenebilecek şantaj suçu bir bilişim sistemi aracılığıyla işlendiğinden ve Hâkimler Ve Savcılar Kurulu'nun 25.11.2021 tarih ve 1229 sayılı kararı ile bilişim suçlarına bakmakla görevli ihtisas mahkemeleri kurulduğundan görevli mahkeme 15 Aralık 2021 tarihi itibariyle uzman asliye ceza bilişim mahkemeleri olacaktır[262].

3.2. Kişisel Verileri Kaydetme Suçu

Siber saldırganların ilk hedeflerinde olan kişisel verilerin son zamanlarda korunması daha güç hale gelmiştir. Fidye zararlı yazılımları başlangıçta bilişim sistemleri üzerindeki verileri şifrelemekteyken 2019 'un sonlarına doğru hacker'lar kişisel ve hassas verileri de şifreleyerek tehdit unsuru haline getirmişlerdir. 2012 yılında Linkedln'den çalınan 117 milyon kişisel veri 2016 yılında internette yayılarak büyük infiale sebep olmuştu[263].2014 yılında dünyada büyük ses getiren siber saldırı olayında ise Yahoo'nun 500 milyon kullanıcısının kişisel verileri çalındığı ortaya çıkmıştı[264].

TCK'nın 135. maddesinde yer alan kişisel verilerin kaydedilmesi suçu kişilere karşı suçlar başlıklı ikinci kısmının "özel hayata ve hayatın gizli alanına karşı suçlar" bölümünde düzenlenmiştir. TCK 135.madde;

(1) Hukuka aykırı olarak, kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir."

---

[261] https://www.jdsupra.com/legalnews/jones-day-global-privacy-cybersecurity3823733/, E.T 25.01. 2021.

[262] Hâkimler Ve Savcılar Kurulu'nun 25.11.2021 tarih ve 1229 sayılı kararı için bkzhttps://www.hsk.gov.tr/Eklentiler/30112021092825112021-1229pdf.pdf, E.T 01.12.2021.

[263] Milliyet, "2016'nın En Büyük Siber Saldırıları Nerelere Yapıldı?" 29 Aralık, 2016, https://www.milliyet.com.tr/galeri/2016-nin-en-buyuk-siber-saldirilari-nerelere-yapildi-2369865/1, E.T. 09.02.2021.

[264] NTV, "Bilgileri Çalınan Yahoo Kullanıcıları Ne Yapmalı?", 23 Eylül, 2016, https://www.ntv.com.tr/galeri/teknoloji/bilgileri-calinanyahookullanicilarineyapmali, IAVLacY7MUaokX95-v1CLg/VxQFBonBo0i5JnQCl7QZ4g, E.T. 09.02.2021.

(2) Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır." şeklindedir.

24.03.2016 kabul tarihli 6698 sayılı Kişisel Verileri Koruma Kanununda kişisel veri; "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" olarak tanımlanmıştır. 6698 sayılı KVKK, kişisel verilere ilişkin suçlar bakımdan 5237 sayılı TCK 'ya atıfta bulanarak ilgili suçlarda kanunun 135-140. madde hükümlerinin uygulanacağını hüküm altına almıştır[265]. Esasen *"kişisel verilerin korunması hakkı"* ile "*özel hayatın gizliliği*" arasında doğrudan bir bağlantı olduğu söylenebilir[266]. Nitekim AİHM'de kişisel verilerin kaydedilmesi fiilini sözleşmenin 8. maddesi kapsamında kabul etmiştir[267]. Nitekim Kişisel Verilerin Korunması Kanunun 1. Maddesinde Kanun'un amacının özel hayatın gizliliği ile birlikte temel hak ve özgürlüklerinin korumak olduğu hüküm altına alınmıştır[268].Maddenin düzenlendiği kısım da dikkate alındığında bu suçla ile korunan hukuki yararın 1982 Anayasası ile güvence altına alınan özel hayatın gizliliği olduğu kabul söylenebilir[269]. Ancak çok sayıda kişisel veri çeşitleri olduğundan buna bağlı olarak da suçla korunan hukuki değerin değişebileceği unutulmamalıdır[270]. Örneğin sağlık verisine ilişkin bir suçta korunan hukuki değer sağlık hakkı olacaktır[271]. Hassas veri olarak kabul edilen sağlık verisi ise TCK'nın 135. maddesinin ikinci fıkrasında nitelikli hal olarak düzenlendiğinden suçun sağlık verisine karşı işlenmesi halinde daha fazla cezaya hükmolunacaktır[272]. Söz konusu nitelikli hal fidye yazılımı saldırısında en fazla hedef halinde olan sağlık verisi açısından

---

[265] DOĞU, Ali Haydar, "*Kişisel Verilerin Korunmasına Genel Bir Bakış*", 34. Bilişim Kurultayı, 2017, s. 177, http://ceur-ws.org/Vol-2045/34_Bilisim_2017_paper_23.pdf, E.T. 09.02.2021.

[266] Marmara Belediyeler Birliği, Belediyelerde Veri Yönetiminde Kişisel Verilerin Korunması Kanuna Uyum Süreci Raporu, 2018, s. 9, https://marmara.gov.tr/UserFiles/Attachments/2018/06/08/7d98853e-8dea-4b52-ad86-978f7f1604fb.pdf, E.T. 09.02.2021.; KORKMAZ, Ali " *İnsan Hakları Bağlamında Özel Hayatın Gizliliği Ve Korunması*", Karamanoğlu Mehmet Bey Üniversitesi Sosyal Ve Ekonomik Araştırmalar Dergisi 16, S. 1, 2014, s. 100, https://dergipark.org.tr/tr/download/article-file/107205, E.T. 09.02.2021.

[267] KORKMAZ, s. 100.

[268] KANGAL, s. 58-59.

[269] KANGAL, Zeynel T.,Kişisel Verilerin Ceza Ve Kabahatler Hukukunda Korunması, On İki Levha Yayıncılık, 1. Baskı, İstanbul 2019, s. 57; AYDIN, Sedat Erdem Aydın, AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, On İki Levha Yayıncılık, 1. Baskı, İstanbul 2015, s. 125

[270] AYDIN, s. 126.

[271] DÜLGER, Murat Volkan, Bilişim Suçları Ve İnternet İletişim Hukuku, 4. Bası, Seçkin Yayınevi, Haziran 2014, s. 581'den aktaran; AYDIN, s. 126.

[272] DÜLGER, Murat Volkan, "*Kişisel Verilerin Korunması Kanunu Ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması*", İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi C.3, S. 2, 2016, s. 122, https://dergipark.org.tr/tr/download/article-file/1102227, E.T. 09.02.2021.

düşünüldüğünde oldukça isabetli olacaktır. Zira bir hastane fidye yazılımına maruz kaldığında büyük hasara uğramaktadır. Öncelikle hastane hizmet sağlayamadığı için büyük gelir kaybı yaşararak teknik hizmet için yaklaşık 1.950$ rakamında yüksek maliyet harcar ve tüm bunların yanında verileri ifşa olan hastalara karşı bütün sorumluluğu üstlenmek zorunda kalır[273]. Bunun yanında hastane veya hastalar büyük kayıpla da karşılaşabilir. Nitekim Almanya'da Düesseldorf Üniversitesi Kliniğine yapılan fidye yazılım saldırısı 1 hastanın hayatını kaybetmesine neden olmuştu. Dolayısıyla sağlık verisi gibi özel nitelikli hassas verilere karşı bu suçun işlenmesi halinde de failin daha fazla ceza alması fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılar açısından da isabetli olacaktır. Zira kişisel veriler mahiyetleri gereği kişilerin özel hayatlarının gizliliğini muhteva ettiği için sıkı sıkıya korunması gerekmektedir.

Kişisel verilerin kaydedilmesi suçunun faili herkes olabilir. TCK 137. Maddesinde suçun nitelikli hali olarak suçun failinin kamu görevlisi veya suçun işlenmesinde kolaylık sağlayan bir meslek veya sanatı icra etmekte olan kişi olması cezayı artıran nitelikli hal olarak düzenleme altına alınmıştır[274]. Tüzel kişiler ise TCK'nın 20. maddesi uyarınca bu suçun faili olamayacaklardır[275]. Lehine haksız yarar sağlanan kişinin tüzel kişi olması durumda TCK'nın 140.maddesi gereğince tüzel kişilere özgü güvenlik tedbiri uygulanacaktır. Fidye zararlı yazılımı kullanarak işlenebilecek kişisel verileri kaydetme suçu bakımından fail herkes olabilmektedir. Zira kanun koyucu herhangi bir ayrıma gitmemiştir. Burada suçu işleyen fail genellikle siyah şapkalı hacker olarak adlandırılmaktadır. Ancak hacker olarak adlandırılması suçun niteliği bakımından bir özellik arz etmemektedir. Kişisel verilerin kaydedilmesi suçu kanunda herhangi bir sınırlandırma yapılmamıştır. Keza TCK 135. maddesinin gerekçesinde kişisel veri tanımı yapılırken "gerçek kişi ile her türlü bilgi" denilerek suçun mağdurunun ancak gerçek kişiler olabileceği belirtilmiştir[276]. Dolayısıyla bu suçun mağduru ancak gerçek kişilerdir[277]. Bu durumda tüzel kişiler ancak suçtan zarar gören olarak kabul

[273] RAC monitor, "Federal Authorities May Impose Civil Penalties AgainstHospitals Paying Ransomware Demands".
[274] AYDIN, s. 127.
[275] SARUSTA, s. 122.
[276] GÜLTEKİN, Melek Nil, "Kişisel Verilerin Ceza Hukuku Yönünden Korunması", Yayımlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2012, s. 129.
[277] KANGAL, s. 61, AYDIN, s. 131, KOCA, ÜZÜLMEZ, s. 75.

edilecektir[278]. Ancak KOCA ve ÜZÜLMEZ'e göre tüzel kişilerin suçtan zarar gören olarak kabul edilmeleri mümkün değildir. Şayet suçun konusu ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki belgeler oluşturuyorsa bu durumda TCK'nın 239. maddesindeki suç oluşacak ve tüzel kişilere ait bu bilgi veya belgelerin açıklanması halinde tüzel kişiler suçtan zarar gören olabilecektir[279].

7 Eylül 2020 tarihinde Şili'nin tek kamu bankası olan Banko Estado'nın bankan veri ve bilgisayar sistemlerine karşı gerçekleştirilen fidye yazılım saldırısı sonucunda banka ülkedeki bütün işlemlerini durdurmak zorunda kalmıştı[280]. Yine 2020 yılında Estee Lauder'a gerçekleştirilen saldırıda milyonlarca müşterinin verileri ifşa edilmişti[281]. Söz konusu saldırılarda suçun mağdurunun veya suçtan zarar görenlerinin kim olduğu düşünüldüğünde ortaya şu sonuç çıkmaktadır: Öncelikle kişisel verileri kaydetme suçunun mağduru ancak gerçek kişiler olabileceği için söz konusu saldırılarda verileri kaydedilen gerçek kişiler suçun mağdur olabilecektir. Tüzel kişilik açısından düşünüldüğünde ise tüzel kişilerin suçtan zarar gören olarak kabul eden hakim görüşe göre Banko Estado ve Estee Lauder, kişisel verileri kaydetme suçunda suçtan zarar gören olacaktır. Fakat kişisel verileri kaydetme suçu açısından tüzel kişileri suçtan zarar gören olarak kabul etmeyen görüşe göre değerlendirildiğinde ise Banko Estado ve Estee Lauder kişisel verileri kaydetme suçundan değil, TCK 239.madde hükümlerine göre suçtan zarar gören olarak kabul edilecektir.

TCK 135 maddesindeki suçun konusu; kişisel verilerdir[282]. Kişisel Verileri Koruma Kanununda kişisel veri; "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" olarak tanımlanmıştır. Bu bağlamda bir kişinin kimlik bilgileri, telefon numarası posta adresi, mesleği, adli sicil kayıtları, sağlık bilgileri, kredi kartı bilgileri, pasaport bilgileri, dernek veya sendika üyelik bilgileri vs. kişisel verilerdir[283]. Nitekim 5271 sayılı Ceza Muhakemesi Kanun'un 75 ila 81. maddeleri uyarınca gerçekleştirilecek

---

278 KANGAL, s. 62, AYDIN, s. 131

279 KOCA, ÜZÜLMEZ, s. 75.

280 Investing.com, *"Fidye Saldırısından Sonra Ünlü Banka Tüm Şubelerini Kapattı"*, 8 Eylül, 2020, https://tr.investing.com/news/cryptocurrency-news/fidye-saldrsndan-sonra-nlu-banka-tum-ubelerini-kapatt-2006411, E.T. 12.12.2020.

281 ÖZÜNALDIM, Anıl, "*2020 Yılının En Büyük Faaliyetleri*", https://www.tamindir.com/haber/2020-en-buyuk-hackler_64127/, E.T. 02.12.2020.

282 PARLAR, Ali, ÇOBANOĞLU, Yekta, Uygulamada Özel Hayata Ve Hayatın Gizli Alanına Karşı Suçlar, Aristo Yayınevi, 1. Baskı, İstanbul 2018, s. 303; AYDIN K., ÜSTÜNDAĞ, s. 113.

283 KANGAL, s. 63.

işlemler sonucunda elde edilen bilgiler kişisel veri olarak kabul edilecektir[284]. Kişisel veriler genellikle "sır" olarak nitelendirilmektedir[285]. Ancak bir kişisel verinin mutlak surette sır niteliğinde olma zorunluluğu bulunmamaktadır[286]. Alenileştirilmiş bir bilginin kişisel veri olarak kabul edilip edilmeyeceği konusunda doktrinde çeşitli görüşler mevcut olmakla birlikte 6698 sayılı KVKK'nın "Kişisel Verilerin İşlenme Şartlarını" taşıyan 5/2-d maddesine göre ilgili kişinin alenileştirdiği kişisel verilerin işlenmesi mümkün olduğundan bu kapsamdaki kişisel veriler TCK'nın 135. maddesinin konusunu oluşturmayacaktır[287]. Ancak DÜLGER' e göre herkes tarafından bilinen ya da alenileştirilmiş bilgilerin kişisel veri kapsamında olup olmadığını her vakaya göre ayrı ayrı değerlendirmek daha doğru olacaktır[288].

Bu kapsamda fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılarda her somut olaya göre suçun konusunu değerlendirmek gerekmekle birlikte hacker'ların kaydettikleri bilgilerin saldırı gerçekleştirilen kurumlarda veri sorumlusu sıfatıyla gizli tuttukları bilgiler olduğu dikkate alındığında fidye yazılımı saldırılarında ele geçirilen bilgilerin saldırı gerçekleştirilen kurum açısından alenileştirilmiş kişisel veri olarak kabul edilebileceği düşünülse de fidye zararlı yazılımıkullanarak işlenebilecek kişisel verileri kaydetme suçunun konusu her zaman kişisel veriler olacaktır.Suçu oluşturan fiil kişisel verileri hukuka aykırı olarak kaydetmektir[289].Kaydetme fiilinden maksat söz konusu verilerin herhangi bir araç kullanmaksızın "*bir yere yazılması, saklanması, depolanması*"[290], *"tekrar kullanılmak üzere fiziki yahut elektronik ortama verinin kaydedilmesidir"*[291]. Kanunda sadece kaydetme fiilinden bahsettiğinden bu suç tek hareketlidir[292]. Suç ancak "kaydetme" ile işlenebileceğinden tek hareketli suçlardandır[293]. Suçun oluşması herhangi bir süreye bağlı değildir[294]. Nasıl kayıt

---

284 KANGAL, s. 63.
285 AYDIN, s. 130; KANGAL, s. 63.
286 DÜLGER, "*Kişisel Verilerin Korunması Kanunu Ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması*", s. 121.
287 KANGAL, s. 65.
288 DÜLGER, "*Kişisel Verilerin Korunması Kanunu Ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması*", s. 126-127.
289 AYDIN, s.131;AYDIN K., ÜSTÜNDAĞ, s. 113.
290 AYDIN, s.131.
291 AYDIN K., ÜSTÜNDAĞ, s. 113.
292 AYDIN, s.132.
293 GÜLTEKİN, s. 126.
294 DOĞU, s. 178.

edildiği önemli olmayıp, kişisel verilerin kaydedildiği anda suç oluşur[295]. Bu suçun ihmali hareketle işlenmesi mümkün olmayıp ancak icrai hareketle işlenebilmektedir[296]. Fidye zararlı yazılımlarında kaydetme fiili dijital bir ortamda gerçekleşmektedir. Zira fidye yazılımı bulaştığı sistem üzerindeki dosya ve klasörleri şifrelediği için burada suçu oluşturan fiil kişisel verilerin elektronik veri tabanına, CD'ye veya USB belleğe kaydedilmesidir.

Kişisel verileri kaydetme suçu kasten işlenebilen bir suçtur[297]. Madde fıkrasında suçun taksirle işlenebileceği düzenlenmediğinden taksirle işlenmesi mümkün değildir[298]. Dolayısıyla fidye yazılımı saldırıları kapsamında işlenen kişisel verileri kaydetme suçu da taksirle işlenemeyecektir. Ancak Türk Ceza Kanunundaki bu düzenlemenin aksi Fransız Ceza Kanununda düzenlenmiş olup bu suçun taksirle işlenebileceği hüküm altına alınmıştır. Suçun olası kastla işlenmesinin mümkün olup olmadığı konusunda farklı görüşler ileri sürülmekle birlikte kaanatimizce kanunda kişisel verinin hukuka aykırı olarak kaydedilmesi fiilinden özellikle bahsedildiği için suçun olası kastla işlenmesi mümkün görünmemektedir[299].Fidye zararlı yazılımı kullanarak işlenebilecek kişisel verileri kaydetme suçu olası kastla işlenmesi mümkün olmayacaktır. Kişisel verileri kaydetme suçu açısından kanunda özel olarak hukuka uygunluk nedeni görülmemiştir[300]. Dolayısıyla TCK'nın genel hükümlerdeki hukuka uygunluk nedenleri uygulama alanı bulacaktır[301]. Kanun hükmünün yerine getirildiği ya da ilgilinin rızasının bulunduğu hallerde kişisel verilerin kaydedilmesi fiili hukuka uygun hale getireceğinden suç oluşmayacaktır[302]. Fidye yazılım saldırısı başlı başına hukuka aykırı bir eylem olduğundan ve hukuka uygunluk nedenlerinin bulunma hali mümkün

---

295 GÜLTEKİN, s. 127.

296 AYDIN, s.134.

297 SARIUSTA, Kader, "Kişisel Verilerin Ceza Hukuku Yoluyla Korunması", Yayımlanmamış Yüksek Lisans Tezi, Gaziantep Üniversitesi Sosyal Bilimler Enstitüsü, Gaziantep 2018, s. 126; HAFIZOĞILLARI, ÖZEN, s. 21.

298 KOCA, Mahmut, ÜZÜLMEZ, İlhan, "*Kişisel Verilerin Kaydedilmesi Suçu*", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr Durmuş TEZCAN'a Armağan, C. 21, Özel S. 2019, s. 81, https://hukuk.deu.edu.tr/wp-content/uploads/2019/09/MAHMUT-KOCA-ILHAN-UZULMEZ.pdf, E.T. 02.12.2020.

299 ÖZGENÇ, İzzet, Türk Ceza Hukuku Genel Hükümler, Seçkin Yayınevi, 9. Bası, Eylül 2013, s.289, aksi görüş için bkz. KANGAL, s.71.

300 PARLAR, ÇOBANOĞLU, s. 306.

301 KANGAL, s. 73.

302 HAFIZOĞULLARI, Zeki, ÖZEN, Muharrem, "*Özel Hayata Ve Hayatın Gizli Alanına Karşı Suçlar*", Ankara Barosu Dergisi, C. 0, S.4, 2009, s. 20, https://dergipark.org.tr/tr/download/article-file/397650, E.T. 02.12.2020.

olmadığından Fidye zararlı yazılımı kullanarak işlenebilecek kişisel verileri kaydetme suçunda hukuka uygunluk nedeni bulunmamaktadır.

Kişisel verilerin kaydedilmesi suçu teşebbüs hükümleri açısından herhangi bir özellik göstermemektedir[303]. Kural olarak sırf hareket suçlarına teşebbüs mümkün değildir[304]. Ancak sırf hareket suçlarında icra hareketleri kısımlara ayrıldığında teşebbüsten söz edilebilmektedir[305]. Kişisel verilerin kaydedilmesi suçu sırf hareket suçu olduğundan icra hareketlerinin bölünebildiği hallerde bu suça teşebbüs mümkün olacaktır[306]. Fidye yazılımı bulaştığı sistem üzerindeki dosya ve klasörleri otomatik olarak şifrelediğinden ve kilit altına alarak kaydettiğinden fidye yazılımı kurban bilgisayara bulaştığı anda suç tamamlanacak olup bu anlamda fidye yazılımı saldırılarında kişisel verileri kaydetme suçuna teşebbüsten bahsedilemeyecektir.

Kişisel verilerin kaydedilmesi suçu iştirak açısından bir özellik göstermeyip iştirake ilişkin genel hükümler uygulanacaktır[307]. Kişisel verilerin kaydedilmesi iştirak açısından herhangi bir özellik göstermediğinden TCK'nın iştirake ilişkin hükümleri uygulanacak olup Fidye zararlı yazılımı kullanarak işlenebilecek kişisel verileri kaydetme suçu bakımından da aynı durum söz konusu olacaktır.

Kişisel verilerin kaydedilmesi suçu zincirleme suç olarak işlenmesi mümkündür[308]. TCK'nın 43. maddesine göre fail aynı kişiye ait kişisel verileri aynı suçu işleme icrası kapsamında farklı zamanlarda hukuka aykırı olarak kaydetmişse zincirleme suç oluşacaktır ve faile tek bir suçtan ceza verilecek olup ceza oranında artışa gidilecektir[309]. Şayet fail tek bir fiiliyle birden fazla kişinin kişisel verisini kaydettiyse faile tek bir suçtan dolayı ceza verilecek ancak ceza oranında artırım yapılacaktır[310]. Yine kişisel verilerin kaydedilmesi suçunda gerçek içtima hükümleri uygulanabilir[311]. Örneğin; kişisel verilerin kaydedilmesi ve bu bilgilerin ifşalanması halinde eylem

303 ÜZÜLMEZ, KOCA, s. 89.
304 BONCUK, İsmail, "Türk Ceza Hukukunda Teşebbüs", İstanbul Kültür Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul 2018, s. 85.
305 TOROSLU, Nevzat, Ceza Hukuku Özel Kısım, Savaş Yayınları, 1. Baskı, Ankara 2005, s. 271.
306 PARLAR, ÇOBANOĞLU, s. 306.
307 ÜZÜLMEZ, KOCA, s. 89
308 ÜZÜLMEZ, KOCA, s. 90; KANGAL, s 89; AYDIN, s. 165.
309 KANGAL, s. 89.
310 KANGAL, s. 89.
311 KANGAL, s. 86.

hakaret suçunu da oluşturuyorsa gerçek içtima hükümleri uygulanacaktır[312]. Fail kişisel veriler kaydetmesiyle birlikte bunları başkasına vermiş veya yaymış ise bu durumda TCK'nın 136. maddesi gündeme gelecek ve farklı neviden içtima hükümleri gereğince fail daha ağır ceza yaptırımı olan TCK'nın 136.maddesi uyarınca cezalandırılacaktır[313]. Kişisel verilerin kaydedilmesi suçunun genellikle bilişim sistemleri aracılığıyla işlenmesi mümkün olduğundan bu kapsamda içtima hükümleri ilişkisine değinmek gerekmektedir[314]. Doktrindeki bir görüşe göre kişisel verilerin kaydedilmesi suçu ile TCK'nın 243. maddesi arasında geçit suç ilişkisi olduğu kabul edilmektedir[315]. Geçit suç failin bir suçu işlemek için aynı hukuksal değeri koruyan daha hafif bir yaptırımı olan bir suçu işlemek zorunda kaldığı hallerde söz konusu olur[316]. Geçit suçların uygulama alanı konusunda gerek doktrinde gerekse de Yargıtay Ceza Daireleri arasında görüş birliği bulunmamakla birlikte kanımızca içtima kuralarının uygulanması daha yerinde olacaktır[317]. Keza öğretide tartışmalı diğer bir konu da kişisel verileri kaydedilmesi suçu ile TCK md. 244 arasında yaşanmaktadır. Bizimde katıldığımız görüşe göre TCK md.135 ile md. 244 arasında farklı neviden içtima hükümlerinin uygulanacağını dolayısıyla failin daha ağır bir cezayı öngören kişisel verileri kaydetme suçundan cezalandırılacağı görüşü ileri sürülmektedir[318]. Ancak diğer bir görüşe göre TCK md.135 ile md. 244 arasında özel norm- genel norm ilişkisinin olduğu, TCK'nın 244. maddesinin TCK 135.maddesine göre daha özel bir düzenleme olduğu dolayısıyla failin yalnızca TCK'nın 244. maddesine göre cezalandırılması gerektiği kabul edilmektedir[319]. Fidye yazılım saldırıları mahiyetleri itibariyle birden fazla suçun

---

312 PARLAR, ÇOBANOĞLU, s. 306.

313 SARIUSTA, s. 137; KANGAL, s. 90.

314 SARIUSTA, s. 140.

315 SARIUSTA, s. 140.

316 İÇEL, Kayıhan, "*Görünüşte Birleşme (İçtima) ilkeleri Ve Yeni Türk Ceza Kanunu*", İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, S. 14, 2008, s. 46, https://kutuphane.dogus.edu.tr/mvt/pdf.php, E.T. 12.12.2020.

317 Yargıtay Ceza Genel Kurulu geçitli suçtan bahsedebilmek için belirli şartlar aramıştır; *"Geçitli suçun söz konusu olabilmesi için; görünüşte içtima eden normlar arasında açık nitelikte asli-yardımcı norm ilişkisinin bulunmaması, ağır suç ile bu suça ulaşabilmek için aşılması zorunlu basamak durumunda bulunan hafif suçu düzenleyen normların korudukları hukuki değerlerinin aynı nitelikte ve aynı türden olmaları, ağır suçun işlenmesi için mutlaka geçit durumundaki daha hafif bir suçun işlenmesinin gerekmesi, hafif suçun faili ve mağduru ile ağır suçun faili ve mağdurunun aynı kişiler olmaları, failin tek hareketi ile ağırlaşan neticeler arasında nedensellik bağının bulunması ve failin kastının başlangıçtan itibaren ağırlaşan neticeleri gerçekleştirmeye yönelmiş olması gerekmektedir…."* (Yargıtay CGK 09.05.2017 tarihli 11-211/259 sayılı kararı).

318 KANGAL, s. 90.

319 DÜLGER, Murat, Bilişim Suçları Ve İnternet İletişim Hukuku, 4. Baskı, Seçkin Yayınevi, Ankara 2014, s. 616.

oluşmasına sebebiyet vermektedirler. Bu doğrultuda kişisel verilerin kaydedilmesi suçu ile TCK md. 136 md, md. 243 ve md. 244 'de düzenlenen suçlar gündeme gelecektir.

Takma adı Peter Severa olarak bilinen Rus asıllı Pyotr Levashou, Kelihos botnetini işleterek on binlerce bilgisayarlara fidye yazılım saldırısı gerçekleştirerek kullanıcılarım kimlik bilgilerini ele geçirmiş ve kişisel verileri çalmak ve bilgisayarlara spam ve fidye yazılımı virüsleri gönderme suçlamaları ile FBI'ın talebi üzerine 10 Nisan 2017 tarihinde İspanya'da yakalanarak ABD'ye iade edilmişti[320]. Pyotr Levashov'un ABD'de yapılan yargılamasında bilgisayara yetkisiz ve izinsiz erişim sağlama, sisteme spam ve fidye yazılımı virüsleri gönderme ve veri kimlik hırsızlığı başta olmak üzere gibi birçok suçtan suçlanmış; iddianamesinde ise Pyotr Levashov'un Federal Temel Yasanın 18. Bölümünün md. 1028A, md.1030 (a) (5) (A) (c) (4) (B) ve md.1030 (a) (4) (c) (3) (A)[321] ve ilgili devamı maddelerini ayrı ayrı ihlal ettiği gerekçesiyle hapis cezası ile cezalandırılması talep edilmiş ve tutuklanarak Connecticut'ta hapishaneye gönderilmesine karar verilmiştir. Federal Temel Yasanın 18. Bölümünün md. 1028A maddesi kimlik bilgilerinde değişiklik yapmak amacıyla bilgisayarlarda dahil olmak bunlar üzerinde değişiklik yapacak her türlü cihazın kullanılmasını, üretilmesini ve başka yerlere gönderilmesini yaptırım altına alan bir düzenlemedir.[322]. Görüleceği üzere söz konusu fidye yazılım saldırısında hacker Pyotr Levashov sadece bilgisayara yetkisiz ve izinsiz erişim sağlama suçundan değil verileri çalmak gibi birçok suçtan ayrı ayrı hüküm giymiştir. Bu bakımdan söz konusu saldırıyı Türk Ceza Hukuk sisteminde açısından düşündüğümüzde TCK md. 135, TCK md. 136, TCK md. 243 ve TCK md. 244 düzenlenen suçlar açısından içtima hükümleri gündeme gelecek ve bu çerçevede değerlendirilerek failin cezalandırılması gerekecektir.

TCK'nın 135.maddesinin ikinci fıkrasında ve TCK'nın 137.maddesinde cezanın artırılması gereken haller düzenlenmiştir. Maddenin 2. Fıkrasında belirtilen veriler hassas verilerdir[323]. Hassas veriler ise KVKK'nın 6. maddesinde; "*Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi ve diğer inançları, kılık ve kıyafeti, dernek, vakıf yada sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik*

---

320 Bilgi Güvende, "Kelihos Botnet'ini İşleten Rus Siber Korsan Suçunu Kabul Etti", 16 Eylül 2018, https://bilgiguvende.com/kelihos-botnetini-isleten-rus-siber-korsan-sucunu-kabul-etti/, E.T. 12.12.2020.

321 Pyotr Levashou'un iddianamesine ulaşmak için bkz.; United States Department of Justıce, "United States Peter Levashov", https://www.justice.gov/usao-ct/us-v-peter-levashov, E.T 02.03.2021.

322 TURHAN, s. 87, dp.198.

323 AYDIN, s.135.

tedbirleriyle ilgili biyometrik ve genetik veriler özel nitelikli kişisel veridir" şeklinde tanımlanmıştır. 6698 sayılı kanun "mutlak hakkın derecesine göre "ayrım yapmış ve "basit" kişisel verinin işlenme şartına göre hassas verileri daha sıkı koşullara bağlamıştır[324]. Özel nitelikli (hassas) veriler ise; *"başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikteki"* verilerdir[325]. Bu veriler veri sahibi dışında başkalarının eline geçtiğinde çeşitli sorunlara neden olacağından daha sıkı koruma altına alınmıştır[326]. Bu verilerin kaydedilmesi durumunda ise verilecek ceza yarı oranında artırılacaktır. Yine TCK'nın 137. maddesinde bu suçun failinin kamu görevlisi veya belli bir meslek ve sanat sahibi kişiler olması halinde nitelikli hal sayılacağından verilecek ceza yarı oranında artırılacaktır.

Fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılarda kaydedilen bilgilerin genellikle hassas veriler olduğu göz önüne alındığında failin cezasının yarı oranında artırılması gerekecektir. Yine failin TCK'nın 137. maddesinde belirtilen kamu görevlisi veya belli bir meslek ve sanat sahibi kişi olması halinde nitelikli hal sayılacağından verilecek ceza yarı oranında artırılacaktır. Bu kapsamda belli bir meslek ve sanat sahibi kişi olması ifadesinden ne anlaşılması gerektiği her olay açısından ayrı ayrı değerlendirerek nedensel bağının aranması gerekecektir[327]. Zira burada önemli husus faile bu yetkinliğinin suçu işlemeye kolaylık sağlayıp sağlamadığıdır. Fidye yazılımı saldırılarında failin etik hacker olduğu durumlarda nitelikli halin uygulanması gerekecektir.

Kişisel verileri kaydetme suçunun birinci fıkrasında düzenlenen hali için bir yıldan üç yıla kadar hapis cezası öngörülürken ikinci fıkrasında düzenlenen hali için birinci fıkra uyarınca verilecek ceza yarı oranında artırılacaktır. Kişisel verileri kaydetme suçunun her iki fıkrada düzenlenen halinin de soruşturma ve kovuşturması re'sen yapılmaktadır. Hâkimler Ve Savcılar Kurulu'nun 25.11.2021 tarih ve 1229 sayılı kararı ile bilişim

---

[324] AKINCI, Ayşe Nur, "Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti", Uzmanlık Tezi, T.C Cumhurbaşkanlığı Strateji Ve Bütçe Başkanlığı, Yayın No: 001, s. 144.

[325] Kişisel Verileri Koruma Kurumu, 100 Soruda Kişisel Verileri Korunması Kanunu, KVKK Yayınları, Ankara 2018, s. 20.

[326] ALTINDERE, Murat, Kişisel Verilerin Korunması Hukuku ve Uygulaması, Adalet Yayınevi, 1. Baskı, Ankara 2020, s. 51.

[327] KANGAL, s. 70.

suçlarına bakmakla görevli ihtisas mahkemeleri kurulduğundan 15 Aralık 2021 tarihi itibariyle uzman asliye ceza bilişim mahkemeleri görevli olacaktır.

3.3. Kişisel Verilerin Hukuka Aykırı Olarak Verilmesi Veya Ele Geçirilmesi

Fidye zararlı yazılımlarında gelinen son noktaya bakıldığında verilerimiz hedef haline gelmeye başlamıştır. Bitdefenter Antivürüs'ün 2020 Tüketici Tehdit Görünümü Raporuna göre fidye yazılım saldırıları 2020 yılında 2019 yılına kıyasla %485 oranında artmıştır[328]. 2021 yılı itibariyle hedefli fidye yazılımlarının artması, çeşitli tür ve sayıda gelişim göstermesi saldırılarının odak noktası olan verilerimiz için ciddi tehdit oluşturmaktadır.Maze Team tarafından geliştirilen ve 2019 yılında ortaya çıkan büyük ölçekli kurum ve kuruluşları hedef alan Maze fidye yazılımında hacker'lar fidye ödemeyi kabul etmeyen kurum ve kuruluşların verilerini ifşa etmek için kullandıkları web sitelerinde"Dünyayı Güvende Tutuyoruz" başlığıyla herkesin ayrıntılarıyla görebileceğisosyal medya paylaşımına açık bir link ekleyerek verileri yaymış, saldırıya uğrayanların fidyeyi ödemedikleri takdirde ise;

" - Güvenlik ihlalleri hakkında bilgi ifşa etme ve medyayı bilgilendirme

- Çalınan bilgileri karanlık web üzerinde maddi değer karşılığında satma

- Şirketin hisse senedi değerini düşürmek için korsanlık eylemi ve hassas bilgilerin kaybı hakkında ilgili borsaları bilgilendirme

*- Çalınan bilgileri müşterilere ve ortaklara saldırmak için kullanma ve onları şirketin korsanlık kurbanı olduğu konusunda bilgilendirme"*yapacakları tehdidinde bulunmuşlardır[329]. Hatta Southwire isimli ABD'nin en büyük kablo üreticisine gerçekleştirilen Maze fidye yazılımı saldırısındahacker'lar internet sitelerinde "*Southwire'in eylemleri nedeniyle, şimdi onların özel bilgilerini sizinle paylaşmaya başlayacağız. Bu sadece bilgilerin %10'u ve müzakare etmeyi kabul edene kadar her hafta verilerin diğer %10'luk kısımlarını yayınlayacağız*" diyerek verilerin 14.4 GB'ını

[328] Hürriyet, "*Fidye Yazılımı Saldırılarında Büyük Artış*", https://www.hurriyet.com.tr/teknoloji/fidye-yazilimi-saldirilarinda-buyuk-artis-41783058, E.T. 25.03.2021.

[329] Kaspersky, " *Maze Fidye Yazılımı Nedir? Tanım ve Açıklama*", https://www.kaspersky.com.tr/resource-/definitions/what-is-maze-ransomware, E.T. 23.03.2022.

yayınlamışlardır[330]. 2020 yılının Kasım ayında ise web sitelerini güncellemeyeceklerini söyleyen Maze fidye yazılım grubu Canon, Xerox ve Cognizant gibi şirketlere fidye yazılımı saldırısında bulunarak ciddi zararlara ve veri ihlallerine neden olmuşlardır[331]. Görüleceği üzere özellikle son yıllarda fidye yazılımı zararlı yazılımı kullanılarak gerçekleştiren saldırılarda mağdurun bilişim sisteminin salt şekilde kilitlenmesi veya şifrelenmesiyle yetinilmeyip verilerin elde edilmesi ve bunların yayılması saldırıların amacı haline gelmiştir. Hatta çoğufidye yazılım saldırılarında ele geçirilen verilerin hacker'lar tarafından Deep Web'te satışa çıkarılmaya başlanması gelenek haline gelmiş ve büyük veri ihlalleri yaşanmaya başlanmıştır. Mount Locker adlı fidye yazılımı İsveç güvenlik firmasına ait 18 GB hassas belgeyi ele geçirerek bir forum sitesinde yayımlamıştır[332]. Yine İsrail'de Black Shadow isimli hacker grubu İsrailli sigorta şirketi Shirtbit'e fidye yazılım saldırısı gerçekleştirerek müşterilerin verilerini çalıp bunların ekran görüntüsünü bir forumda paylaşarak şirketi 1 milyon dolar zarara uğratmıştır[333]. 2021 yılının ilk fidye yazılım saldırısı olarak kayıtlara geçen "BabukLocker" adlı fidye yazılımı ile çalınan veriler bir internet sitesinde sergilenerek mağdur olan şirketlerden yüklü miktarda fidye talebinde bulunulmuştur[334]. Kaspersky tarafından yapılan araştırma sonucuna göre Türkiye'de fidye yazılım kullanılarak gerçekleştirilen fidye yazılımı saldırılarında mağdurların %36'sı fidyeyi öderken %27'si fidyeyi ödemesine rağmen verilerini geri alamamıştır[335].Aslında Kişisel Verileri Koruma Kurumu tarafından ilan edilen veri ihlal bildirimleri durumun ne kadar ciddi olduğunu göstermektedir[336]. Her geçen gün fidye yazılımı saldırısına uğrayan kişilerin, kurum ve kuruluşların artması, hatta bu saldırılarda ne kadar veri ihlalinin yaşandığının tespitinin

---

330 HackPress, " *HackerlarSouthwire'ın Verilerini Yayınlıyor,* 11 Ocak 2020, https://hackpress.org/haber/sizintilar/hackerlar-southwirein-verilerini-yayinliyor, E.T. 23.03.2022.

331 Kaspersky, " *MazeFidye Yazılımı Nedir?".*

332 Siber Magazin, "*MountLockerRansomware, Hackerlara Çifte Gasp İmkanı Sunuyor*", 13 Aralık 2020, https://www.sibermagazin.com/mount-locker-ransomware-hackerlara-cifte-gasp-imkani-sunuyor/, E.T 25.03.2021

333 Star, "*Müşteri Verileri Sızdırıldı! İsrailli Şirketten Fidye İstiyorlar*", 3 Aralık 2020, https://www.star.com.tr/dunya/musteri-verileri-sizdirildi-israilli-sirketten-fidye-istiyorlar-haber-1592037/, E.T. 25.03.2021

334 Siber Care, "*Fidye Yazılımcılar "BabukLocker " İle 2021'e Merhaba! Dedi*!", 1 Ocak 2021, https://www.siber.care/blog/fidye-yazilimcilar-babuk-locker-ile-2021e-merhaba-dedi, E.T. 25.03.2021.

335 CyberMag, "*Fidye Yazılımı Kurbanlarının Yarısından Fazlası Fidyeyi Ödüyor, Yalnızca Dörtte Biri Tüm Verileri Geri Alabiliyor*", 7 Nisan 2021, https://www.cybermagonline.com/fidye-yazilimi-kurbanlarinin-yarisindan-fazlasi-fidyeyi-oduyor-yalnizca-dortte-biri-tum-verileri-geri-alabiliyor, 12.04.2021.

336 KVKK'nın Veri İhlal Bildirimleri için bkz; https://www.kvkk.gov.tr/veri-ihlali-bildirimi/,

bile yapılamaması konumuz olan Kişisel Verilerin Hukuka Aykırı Olarak Verilmesi Veya Ele Geçirilmesi suçu bakımından oldukça önem arz etmektedir.

TCK'nın 136. Maddesinde düzenlenen Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme suçu;

" (1)Kişisel verileri hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.

(2) Suçun konusunun, Ceza Muhakemesi Kanununun 236'ıncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat arttırılır"

şeklinde düzenlenmiştir. Bu madde ile hukuka aykırı olarak kaydedilmiş olsun veya olmasın kişisel verileri hukuka aykırı şekilde başkasına verilmesi, yayılması veya ele geçirilmesi bağımsız bir suç tipi olarak düzenleme alanı bulmuştur[337]. Ayrıca madde başlığında her ne kadar yayma fiiline yer verilmese de kişisel verileri yaymak da cezalandırılan fiiller arasında düzenlenmiştir[338].

TCK'nın 136. Maddesinde düzenlenen suç ile korunan hukuki değer kişinin özel hayatıdır[339]. Söz konusu madde ile bütün kişisel veriler korunmak istendiğinden kişisel verilerin mutlaka sır veya gizli nitelikte olma zorunluluğu yoktur[340].Fidye zararlı yazılımları kapsamında ele geçirilen bilgilerin mahiyetleri dikkate alındığında suçla korunan hukuki değer kişilerin özel hayatı olmaktadır. Bu suçun faili herkes olabilir[341]. Madde metninde "kişi" kelimesine yer verildiğinden özgü suç kapsamında değildir[342]. Dolayısıyla suç fidye yazılımı saldırısına konu olabilecek ve bu kapsamda hacker'lar suçun faili olacaklardır. Yine bu suçun faili ancak gerçek kişiler olabileceğinden tüzel kişinin faaliyeti çerçevesinde bu suçun işlenmesi halinde suçun faili eylemi bizzat gerçekleştiren kişi olacaktır[343]. TCK'nın 137. Maddesince suçun failinin kamu görevlisi veya belli bir meslek ve sanat sahibi kişiler olması durumunda suçun nitelikli halinden

---

337 YILMAZ, Sacit, Türk Ceza Hukuku Sisteminde Siber Suçlar, 1. Basım, Adalet Yayınevi, Ankara 2016, s. 267.
338 KANGAL, s. 93
339 ÖZBEK, Veli Özer, DOĞAN, Koray, BACAKSIZ, Pınar, TEPE, İlker, "Türk Ceza Hukuku Özel Hükümler", Seçkin Yayıncılık 13. Baskı, Ankara 2018, s.596; YILMAZ, s. 268; KANGAL, s. 96.
340 YILMAZ, s. 268.
341 BAYRAKTAR ve diğerleri, s. 635.
342 KANGAL, s. 98.
343 KANGAL, s. 98.

bahsedilecek ve failin cezası arttırılacaktır[344]. Bu bakımdan bilişim alanı sektörü veya bu alanda uzman kişiler, kişisel verilere ulaşmakta zorluk çekmeyeceğinden bu gibi durumların varlığı halinde suçun nitelikli halinden bahsedilecektir[345]. Fidye zararlı yazılımları mahiyetleri itibariyle oldukça karmaşık ve güçlü algoritmalara sahip olduğundan genellikle bu zararlı yazılımın geliştiricileri bu alanda uzman kişiler olmaktadır. Bazıları bu durumu iyiye kullanırken bazıları da bunu kötüye kullanarak suç işlemektedir. .Dolayısıyla fidye zararlı yazılımları kullanılarak gerçekleştirilen saldırılarda TCK'nın 136. maddesinde düzenlenen suçu işleyen kişinin bu alanda uzman olması halinde failin cezası arttırılacaktır. Bu suçun mağduru kişisel verileri hukuka aykırı şekilde başkasına verilen, yayılan ve ele geçirilen kişidir. Doktrinde bu suçun mağdurunun tüzel kişilerin olup olamayacağı tartışmalıdır. Bir görüşe göre bu suçun mağduru ancak gerçek kişiler olabilir. Zira KVKK'nın 3/1-ç ve d maddelerinde kişisel verilerin yalnızca gerçek kişilere ait olabileceği belirtildiğinden suçun mağduru yalnızca gerçek kişilerdir[346]. Bizimde katıldığımız diğer görüşe göre ise bu suçun mağduru yalnızca gerçek kişiler olmayıp tüzel kişiler de suçun mağduru olabilecektir[347]. Fidye yazılımı saldırılarında kurum veya kuruluşların verileri hedefte olduğundan mağdurun tüzel kişi olarak kabul edilmemesi halinde birtakım sorunlar ortaya çıkabilir. Zira fidye yazılımı saldırılarında üretim, perakende, devlet kurumları ve sağlık sektörlerindeki kurum ve işletmeler en çok fidye yazılım saldırısına maruz kalan sektörlerdendir. Sadece 2019 yılında ABD'de New Orleans belediyesine yapılan fidye yazılım saldırısında belediye saldırı sonunda 7 milyon dolar zarara uğramıştır[348]. Türkiye ise böyle bir duruma çok yakın bir zaman önce tanıklık etmiş ve 12 Şubat 2022 tarihinde Kişisel Verileri Korumu Kurumu tarafından yayınlanan veri ihlalleri bildiriminde; İstanbul Şişli Belediyesinin fidye yazılımı saldırısına uğradığı, dosya ve klasörlerin şifrelendiği ve bu saldırıda ihlalden etkilenen sayı kişi ve kayıt sayısının tespit edilemediği bildirilmiştir[349]. Yine 9 Şubat 2022 tarihinde Kişisel Verileri Korumu Kurumuna gönderilen veri ihlalleri bildirimine göre T.C Acıbadem Mehmet Ali

---

344 ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 597.
345 YILMAZ, s. 268.
346 BAYRAKTAR ve diğerleri, s. 635; KANAGAL, s. 99.ç
347 SOYASLAN, s. 369.
348 SC Magazine, ROBİNSON, Teri, " RansomwareAttackCost New Orleans $7 MillionAndCounting", 17 January 2020, https://zephyrnet.com/tr/ransomware-attack-cost-new-orleans-7-million-and-counting/, E.T. 25. 03. 2021.
349 İstanbul Şişli Belediye Başkanlığı İhlal Bildirimi için bkz; https://www.kvkk.gov.tr/Icerik//Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Sisli-BelediyeBaskanligi, E.T. 25. 03. 2022.

Aydınlar Üniversitesi fidye yazılımı saldırısına uğramış ve ihlal eden etkilenen kişisel veri kategorilerin tespit edilemediği ve incelemelerin devam ettiği belirtilmiştir[350]. 6698 sayılı KVKK' unun 12.maddesine göre veri sorumlusu kişisel verilerin hukuka aykırı olarak işlenmesini- erişilmesini önlemek ve muhafazasını sağlamakla yükümlüdür. Yine ilgili kanunun 18. maddesine göre kanunun 12. maddesinde öngörülen veri güvenliklerine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk Lirasından 1.000, 000 Türk lirasına kadar idari para cezası verileceği hüküm altına alınmıştır. Bu bakımdan tüzel kişiler hem olayın mağduru olabileceği gibi hem de veri sorumlusu sıfatıyla ciddi cezalarla karşılaşabilmektedirler. Nitekim 2021 yılının Mart ayında Yemek Sepetine gerçekleştirilen fidye yazılımı saldırısında 21 milyon 504 bin 83 yemek sepeti kullanıcısının kişisel verisi ihlal edilmiş ve Kişisel Verileri Korumu Kurumu Yemek Sepeti Elektronik İletişim Parakende Gıda Lojistik Anonim Şirketinin veri sorumlu sıfatıyla yükümlülükleri yerine getirmediği nedeniyle 1.900,000 Türk lirası idari para cezası verilmesine karar vermiştir[351].Böyle durumlarda veri sorumlusu sıfatına sahip tüzel kişilerin hem ihlalden etkilenen kişilere karşı hem de Kişisel Verileri Korumu Kurumuna karşı yükümlülükleri bulunduğundan tüzel kişiler Türk Ceza Kanun'unu kapsamında korunmalı ve fidye zararlı yazılımı kullanarak işlenebilecek suçlarda suçun mağdurunun tüzel kişilerin de olabileceği kabul edilmelidir.

Kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçunun konusu kişisel veridir[352]. Kişisel verinin tanımı kişisel verilerin kaydedilmesi suçunda ayrıntılı olarak açıklandığından aynı açıklamalar burada da geçerli olacaktır. Yine TCK'nın 136. maddesinde düzenlenen suç seçimlik hareketli bir suçtur[353]. Seçimlik hareketler olan başkasına verme, yayma ve ele geçirme fillerinin birinin gerçekleştirilmesiyle suç tamamlanacaktır[354].

Kişisel verileri başkasına verme, kişisel verilerin bir başkasına aktarılmasıdır[355]. Kişisel verilerin ne şekilde ve nasıl aktarılacağına ilişkin kanunda sınırlandırma

---

[350] T.C Acıbadem Mehmet Ali Aydınlar Üniversitesi İhlal Bildirimi için bkz;https://www.kvkk.gov.tr/Icerik/7184/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-T-C-Acibadem-Mehmet-Ali-Aydinlar-Universitesi, E.T. 25. 03. 2022.

[351] Sözcü, "*Yemek Sepetine Veri İhlalinden Ceza Kesildi*", 7 Şubat 2022, https://www.sozcu.com.tr/2022/ekonomi/yemek-sepetine-veri-ihlalinden-ceza-kesildi, E.T. 25. 03. 2022.

[352] ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 597.

[353] YILMAZ, s. 269.

[354] YILMAZ, s. 269; KANGAL, s. 106.

[355] ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 597.

yapılmadığından aktarma fiili her şekilde gerçekleşebilir[356]. Kişisel verilerin başkasına verilmesinde "başkası" gerçek veya tüzel kişi olabilir[357]. Kişisel verilerin hukuka aykırı veya hukuka uygun şekilde elde edilmiş olmasının herhangi bir önemi bulunmamakta olup başkasına verme eyleminin hukuka aykırı şekilde elde edilmiş olması yeterlidir[358].

Kişisel verileri yayma, esasen verme suretiyle gerçekleşmekle birlikte verme eyleminin iki kişi arasında olması nedeniyle verme fiilinden ayrılır[359].Yayma fiili bir web sitesi üzerinden gerçekleşebileceği gibi e-posta veya mesaj yolu ile de gerçekleşebilir[360].

Kişisel verilerin ele geçirilmesi, kişisel verinin bulunduğu sistemden veya ortamdan alınmasıdır[361]. Ele geçirme fiili kaydetme şeklinde mümkün olmakla beraber kişisel verilerin kaydedilmesi fili TCK 135. Maddesinde bağımsız bir suç olarak düzenlendiğinden kişisel verilerin ele geçirilmesinden kaydetme fili dışında kalan eylemlerin anlaşılması gerekmektedir[362].

Bu suçun oluşması için seçimlik hareketlerden birinin yapılmış olması yeterli olup herhangi bir zararın meydana gelmiş olması aranmadığından suç soyut tehlike suçudur[363].Yine ele geçirilmesi fiili açısından verinin bir süre saklanması şartı aranmadığından ani bir suçtur[364]. Nitekim LinkedLn, Dropbox ve Formspring'i hackleyen Rus asıllı Yevgeny Nikulin 2012 yılında gerçekleştirilen siber saldırıda 117 milyon kişinin kişisel verilerini ele geçirip sattığı gerekçesiyle Kuzey Kaliforniya Bölge mahkemesince 29 Eylül 2020 tarihinde davası sonuçlandırılarak Federal Temel Yasanın 18. Bölümünün md.1030 (a) (5); md. 1028A (1) maddelerince kötü amaçlı yazılım yükleme ve kişisel verileri satma suçları gibi çeşitli suçlardan seksen sekiz ay hapis cezasına mahkûm edilmiştir[365].

---

356 KANGAL, s. 106-107.
357 YILMAZ, s. 269.
358 YILMAZ, s. 269.
359 ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 597.
360 YILMAZ, s. 269.
361 YILMAZ, s. 269.
362 ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 598.
363 ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 598; YILMAZ, s. 270
364 ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 598.
365 Yevgeny Nikulin'un iddianamesine ulaşmak için bkz.; United StatesDepartment of Justıce, "United States Yevgeny Nikulin, https://www.justice.gov/usao-ndca/pr/russian-hacker-sentenced-over-7-years-prison-hacking-three-bay-area-tech-companies, E.T 16.03.2021.

Kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu kasten işlenebilen bir suç olup taksirle işlenmesi mümkün değildir[366]. Kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu için failin belirli bir maksatla hareket etme şartı aranmamış olup failin doğrudan kastla hareket etmesi suçun oluşumu için yeterlidir[367]. Bu bakımdan suçun olası kastla işlenmesi de mümkündür[368].Fail suçun maddi konusunda hataya düşerse örneğin başkasına verdiği, yaydığı veya ele geçirdiği verinin kişisel veri olduğunu bilmiyorsa TCK md. 30/1 gereğince kast ortadan kalkacağından fail TCK 136'dan cezalandırılmayacaktır[369]. Şayet fail mağdurun şahsında hataya düşerse düşünülen ile gerçekleştirilen fillerin konuları aynı değere sahip olduğundan fail hata hükümlerinden yararlanamayacaktır[370]. Örneğin; Almanya'da bir hastanın ölmesine sebep olan fidye yazılım saldırısında hacker'lar aslında hastaneye saldırtmak istemediklerinde amaçlarının üniversitenin hastanesinin değil üniversite olduğunu açıklamışlardı. Bu bakımdan söz konusu olayda aslında fail, mağdurun kimliğinde hataya düşmüştür. Ancak TCK hükümleri açısından failin mağdurun kimliğinde hataya düşmesi kastı ortadan kaldırmayacağından TCK md. 136'dan sorumlu tutulacaktır.

Kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçunda kanunda özellikle hukuka aykırılık ifadesine yer verildiğinden TCK'daki genel hükümlerdeki hukuka uygunluk nedenleri geçerli olmakla birlikte bu suç için hukuka uygunluk nedeni olarak kanun hükmünün yerine getirilmesi ve ilgilinin rızası düşünülebilir[371]. Ancak doktrinde bazı yazarlara göre kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu şikâyete tabi olmadığından ve dolayısıyla bu suçta kamunun menfaati ağır bastığından ilgilinin rızasının suçu hukuka uygun hale getirmeyecektir[372].

Kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu neticesi harekete bağlı bir suç olduğundan kural olarak bu suça teşebbüs elverişli değildir[373].Fidye zararlı yazılımı kullanarak işlenebilecek suçlardahacker kişisel verileri ele geçirdiği anda suç tamamlanacağından kişisel verilerin hukuka aykırı olarak

366 KANGAL, s. 120.
367 KANGAL, s. 120.
368 ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 599.
369 KANGAL, s. 122.
370 KANGAL, s. 122.
371 SOYASLAN, s. 371; YILMAZ, s. 271.
372 ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 599.
373 ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 600.

verilmesi veya ele geçirilmesi suçuna teşebbüsten bahsedilemeyecektir. Bu suç iştirak açısından bir özellik göstermeyip iştirake ilişkin genel hükümler uygulanacaktır[374]. Kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu iştirak açısından herhangi bir özellik göstermediğinden TCK'nın iştirake ilişkin hükümleri uygulanacak olup fidye yazılımı saldırısında işlenen kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu bakımından da aynı durum söz konusu olacaktır. Bu suçun zincirleme suç olarak işlenmesi mümkündür[375]. Kişisel veriler fail tarafından hukuka aykırı olarak kaydedilip başkasına verilip yayılabilir. Bu durumda fikri içtima hükümlerinin mi yoksa gerçek içtima hükümlerinin mi uygulanacağı doktrinde tartışmalıdır. Bazı yazarlara göre böyle bir durumda fikri içtima hükümleri uygulanmalı ve faile en ağır ceza olan TCK md. 136'dan ceza verilmelidir[376]. Bazı yazarlara göre ise böyle bir durumda iki ayrı suçun varlığı kabul edilerek buna göre ayrı ayrı suçlardan cezalandırılma yoluna gidilmelidir[377]. Yine kişisel veriler genellikle bir bilişim sisteminde tutulduğundan TCK md. 243 ile TCK md. 136'da düzenlenen suçlar aynı anda gerçekleşebilir. Böyle bir durumda faile tek bir cezadan mı yoksa ayrı ayrı suçlardan mı ceza verileceği doktrinde tartışmalıdır. Bazı yazarlara göre böyle bir durumda bilişim sistemine hukuka aykırı olarak girme veya kalma suçu kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu açısından geçit suçu oluşturduğundan faile yalnızca ikinci suç olan TCK md. 136'dan ceza verilecektir[378]. Bazı yazarlara göre ise böyle bir durumda gerçek içtima hükümleri söz konusu olacak ve fail iki suçtan ayrı ayrı cezalandırılacaktır[379].

Ayrıca önemle belirtmek gerekir ki DEĞİRMENCİ'ye göre fidye yazılım virüsü herhangi bir veriyi ele geçirip veya ifşa etmediğinden dolayı TCK md.135 ve md. 136'daki suçları oluşturmamaktadır[380]. Ancak bu görüşe katılmak mümkün görünmemektedir. Zira ilgili suç bölümünde anlatıldığı üzere fidye yazılım saldırılarında başta kişisel veriler olmak üzere verilerimiz hacker'ların hedefi halindedir. Doğrudan hedef sistemdeki verileri şifreleyen ve hatta ne kadar ciddi olduklarını

374 ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 600; YILMAZ, s. 272.
375 ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 600.
376 ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 600; SOYASLAN, s. 371.
377 YILMAZ, s. 273.
378 SOYASLAN, s. 371.
379 YILMAZ, s. 273.
380 DEĞİRMENCİ, Olgun, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi",* s. 185.

göstermek için verileri web sayfalarında yayınlayan Maze fidye yazılım çetesi birçok kurumun itibar kaybına veri ihlaline neden olmuştu. Rus merkezli hacker'lar tarafından yönetilen Conti Fidye yazılım grubu "CONTİ NEWS" isimli web sitelerinde ele geçirdikleri verileri yayınlamakladırlar. Hatta web sitelerinde anlaşmayı reddeden şirketlerin verilerinin sitede bulamamış olmalarını onları unuttukları anlamına gelmediğini aksine verilerinin satıldığı anlamına geldiğini belirtmektedirler. Bu web sitesinde şirketlerin verileri yüzdeler ile belirtilerek an ve an ifşa edilmektedir[381]. Görüleceği üzere hacker'lar fidye yazılımı saldırılarında çaldıkları verilerle yetinmeyip bu verileri derin ağlarda satışa çıkarmaya bile başlamıştır. Dolayısıyla fidye yazılımı kullanılarak gerçekleştirilen saldırılarda kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu oluşabilecektir.

Kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçunun nitelikli halleri TCK'nın 137-1-a maddesinde suçun kamu görevlisi tarafında ve görevinin verdiği yetkiyi kötüye kullanmak suretiyle işlenmesi ve belli bir meslek ve sanatın sağladığı kolaylıktan yararlanması suretiyle işlenmesi halleri olarak düzenlenmiştir. Bu gibi hallerin varlığında faile verilecek ceza yarı oranında artırılacaktır. TCK'nın 137-1-a maddesindeki nitelikli halden bahsedilebilmek için failin kamu görevlisi olması dışında bu yetkinin kötüye kullanılması gerekmektedir. TCK'nın 137-1-b maddesindeki nitelikli halden açısından için ise kanun koyucu belirli meslek veya sanattan bahsetmediğinden suçu işlemeye elverişli herhangi bir meslek veya sanat nitelikli halin uygulanması için yeterlidir.Fidye zararlı yazılımları gibi güçlü algoritmalara sahip zararlı yazılımların geliştiricileri genellikle bu alanda eğitimli veya uzman kişiler olmaktadır. Dolayısıyla fidye yazılımları kullanılarak gerçekleştirilen saldırılarda hacker'ın kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçunu görevinin verdiği yetkiyi kötüye kullanmak suretiyle işlemesi ve mesleğinin ve sanatının sağladığı kolaylıktan yararlanması suretiyle işlemesi halinde cezası artırılacaktır.

Kişisel verileri hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılacaktır. Fidye yazılımı kullanılarak işlenebilecek kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu bakımından saldırganlar suçta ve cezada kanunilik ilkesi gereğince aynı ceza ile

[381] Bkz: https://continews.click/, E.T. 25.03.2022.

cezalandırılacaktır. Suçun konusunun, Ceza Muhakemesi Kanununun 236'ıncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda ise verilecek ceza bir kat arttırılacaktır.

Kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçunun soruşturma ve kovuşturması re'sen yapılmaktadır. Suç uzlaştırma kapsamında olan suçlardan değildir[382]. Hâkimler Ve Savcılar Kurulu'nun 25.11.2021 tarih ve 1229 sayılı kararı ile bilişim suçlarına bakmakla görevli ihtisas mahkemeleri kurulduğundan görevli mahkeme 15 Aralık 2021 tarihi itibariyle uzman asliye ceza bilişim mahkemeleri olacaktır. Fidye yazılımı kullanarak işlenebilecek kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu bir bilişim sistemi aracılığıyla işlendiğinden ve Hâkimler Ve Savcılar Kurulu'nun 25.11.2021 tarih ve 1229 sayılı kararı ile bilişim suçlarına bakmakla görevli ihtisas mahkemeleri kurulduğundan görevli mahkeme 15 Aralık 2021 tarihi itibariyle uzman asliye ceza bilişim mahkemeleri olacaktır. Lehine haksız yarar sağlanan kişinin tüzel kişi olması durumda ise TCK'nın 246. maddesi gereğince tüzel kişilere özgü güvenlik tedbiri uygulanacaktır[383].

3.4. Bilişim Sistemine Girme Suçu

Bilişim sistemine girme suçu, günümüzde teknolojinin gelişmesiyle birlikte en fazla ihlal eden suç tiplerinden biri olmuştur. Bilişim suçları ülkemizde olduğu gibi birçok ceza hukuk sisteminde tanımı yapılmış olan bir suç tipi değildir[384]. Bilişim suçlarının tanımı yapılırken klasik suçlardan farklı olduğunu belirlemek amacıyla birçok kriter esas alınmıştır[385]. Bu kriterlerden biri de "Suçu İşleyen Faili Esas Alan" kriterdir[386]. Bu kriteri savunan görüşe göre bilişim suçları, bilgisayar becerisine veya bilgisine sahip olan kişilerin işledikleri suçlardır[387].Söz konusu kriter bilişim suçu işleyen faillerin genellikle belirli düzeyde bilgisayar bilgisine sahip olan kişiler olduğu göz önüne alındığında savunulabilir. Ancak bilişim suçlarını tek bu kritere bağlamak doğru olmayacağından genel bir tanımlama yapmak daha doğru olacaktır.

---

382 KANGAL, s. 152.
383 KANGAL, s. 152.
384 AKBULUT, Berrin, Bilişim Alanında Suçlar, Adalet Yayınevi, 2. Baskı, Ankara 2017, s. 55.
385 AKBULUT, s. 55.
386 AKBULUT, s. 65.
387 AKBULUT, s. 65.

Nitekim bir mühendislik alanı[388] olan bilişim kavramının pek çok tanımı bulunmakla birlikte Türk Dil Kurumu sözlüğünde bilişim; *insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik*" şeklinde tanımlanmıştır[389]. 5237 sayılı TCK'da ise salt bilişim kavramı yerine "*daha geniş bir kavram olan*"[390] bilişim sisteminin tanımı yapılmış ve "verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma olanağı veren manyetik sistemler" şeklinde tanımlanmıştır. Dolayısıyla yukarıdaki açıklamalar ışığında; bilişim sistemlerinin ana unsuru bilgisayar olmakla birlikte[391] bilişim sistemi kavramından sadece bilgisayarların değil yapay zekâ teknolojisinin kullanıldığı sistem ve ürünlerinde bu kapsamda değerlendirileceği göz ardı edilmemelidir[392].

5237 sayılı yeni TCK'nın 243. maddesiyle bilişim sistemine girme suçu, TCK'nın topluma karşı suçlar başlıklı üçüncü kısmının "Bilişim Alanında Suçlar" bölümünde düzenlenmiştir. TCK 243.madde;

(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir."

(2) Yukarıdaki fıkrada tanımlanan fillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde verilecek ceza yarı oranına kadar indirilir."

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur."

(4) Ek fıkra= 24/03/2016-6698 S.K./30. Md) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır." şeklindedir.

24/03/2016 tarihli 6698 S.K. ile yapılan değişiklik öncesi5237 sayılı kanunun 243. maddesinin 1. fıkrasında "sisteme girmek ve kalmaya devam etmek" eylemleri

---

388 Wikipedia, https://tr.wikipedia.org/wiki/Bili%C5%9Fim, E.T 12.11.2020.
389 TDK, https://www.tdk.gov.tr/, E.T 12.11.2020.
390 ÖZÇELİK, Büşra, "Bilişim Sistemine Girme Suçu", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2019, s. 10.
391 YILMAZ, Sacit, "*5237 Sayılı TCK'nın 244. Maddesi Alanında Düzenlenen Bilişim Alanındaki Suçlar*", TBBD, C.0, S. 92, 2011, s. 63, https://kutuphane.dogus.edu.tr/mvt/pdf.gif, E.T. 12.11.2020.
392 ÖZÇELİK, s. 10-11.

cezalandırılmışken madde gerekçesinde "sisteme girmek veya kalmaya devam etmek" eylemlerinin cezalandırılacağı hüküm altına alınmıştı[393]. Uygulamada ise madde metni olan sisteme girmek ve kalmaya devam etmek" eylemleri cezalandırılmakla[394] birlikte bu durum çeşitli eleştirilere neden olmakta idi.24/03/2016 tarihli 6698 S.K. ile yapılan değişikle beraber bilişim sistemine girme suçunun oluşması için sisteme girilmesi yeterli görülerek bilişim sisteminde kalma eylemine devam etme şartı kaldırılmıştır[395]. Nitekim benzer düzenleme Avrupa Siber Suç sözleşmesinde görülerek; "*Her bir taraf devlet bir bilgisayar sisteminin tamamı veya herhangi bir bölümüne haksız ve kasıtlı olarak erişilmesini suç kapsamına almak için gerekli kanuni düzenlemeyi yapmalı gerekli önlemleri ihlal edilerek ya da bilgisayar sistemine bağlı diğer bir bilgisayar sistemi aracılığıyla bilgisayar verisini almak ya da başka kötü niyetlerle kullanmak şartına bağlayabilir*" şeklinde hüküm altına alınmıştır[396].

Bilişim suçlarının işlenmesinde ise birçok yol ve yöntem kullanılmaktadır. Bazı bilişim suçlarının işlenmesi için temel bilgisayar bilgisine sahip olmak yeterli iken örneğin; genellikle lamer veya scriptkiddie adı verilen kişiler hazır kod kullanarak sistemleri kırabiliyorken bazılarında örneğin fidye yazılımı saldırısını gerçekleştirmek için ileri düzeyde bilgisayar bilgisine sahip olunması gerekmektedir. Nitekim hacker'ler bilişim suçlarını işlerken truva atı, bilgisayar virüsü veya solucan gibi birçok sayıda zararlı yazılım kullanarak çeşitli yöntemlerle bilişim sistemlerine erişmektedirler. Fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılarda esasen hukuka aykırı bir şekilde bilişim sistemine girme suçunun oluşup oluşmayacağın fidye yazılımının hedef bilişim sistemine yerleşme şekline göre ayrı ayrı değerlendirilmesi gerekecektir[397]. Fidye yazılımlarının oltalama saldırılarıyla gerçekleştirildiği durumlarda fail, mağdurun sistemine hukuka aykırı şekilde girmeyip onu sosyal mühendislik yöntemiyle zararlı yazılımı kendi sistemine yüklettiğinden hukuka aykırı bir erişimden bahsedilmeyecek ve bilişim sistemine girme suçu normal şartlarda oluşmayacaktır[398]. Ancak burada

---

393 ERGÜN, s. 87.
394 ERGÜN, s. 87.
395 APİŞ, Özge, "*Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında Ve Kütüklerinde Arama, Kopyalama Elkoyma Koruma Tedbiri",* Yasama Dergisi, C.0, S. 37, 2018, s. 52, https://dergipark.org.tr/tr/download/article-file/1115263, E.T. 12.11.2020.
396 APİŞ, s. 52.
397 DEĞİRMENCİ, s. 193.
398 DEĞİRMENCİ, Olgun, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi",* s. 193.

dikkat edilmesi gereken husus failin söz konusu erişimi nasıl sağladığıdır. Fidye yazılımın sisteme yerleştirilme şekli veya tekniği bu aşamada suçun oluşması bakımından önemli olacak olup hukuka aykırı olarak mağdurun bilişim sistemine erişim sağlanabildiği hallerde söz konusu suç oluşacaktır[399]. Nitekim fidye yazılımı saldırılarında hedef sisteme göre bulaşma ve sızma yöntemlerinin her geçen gün çeşitlenerek artmasından dolayı fidye zararlı yazılımlarını TCK sistematiğinde bilişim sistemine girme suçu yönünden ele almak da fayda olacaktır.

Öncelikle belirtmek gerekir ki bilişim sistemine girme suçunda korunmak istenen hukuki değerin ne olduğu konusunda doktrinde çeşitli görüşler mevcuttur. ERDOĞAN[400], APAYDIN[401] ve MAHMUTOĞLU'na[402] göre korunan hukuki değer karma nitelikte olup bu suç tipinde birden fazla hukuki değer korunmaktadır. AKBULUT'a[403] göre ise suçla korunan hukuki değer bilişim sistemlerinin güvenliği ve dokunulmazlığıdır. Kanaatimizce de bilişim sistemine girme suçunda korunan hukuki değer karma nitelikte olmakla birlikte esas olanın bilişim sisteminin güvenliğini korumak olduğu söylenebilir[404]. Nitekim fidye yazılımları da esas itibariyle zararlı bir yazılım olduğundan ve bilişim sistemlerine zarar verdiğinden bu tür saldırılarda korunan hukuki yarar öncelikle bilişim sisteminin güvenliği olacaktır.

Kanun koyucu TCK 243.madde açısından suçun failini; "*... giren veya .... kalmaya devam eden kimse*" şeklinde açıkladığından bu suç herkes tarafından işlenmeye elverişlidir[405]. Bilişim sistemine girme suçunun faili herkes olmakla birlikte genellikle fail olarak nitelendirilen kişiler hacker'lardır[406]. Zira daha önce de bahsedildiği üzere özellikle fidye zararlı yazılımları gibi bir kod yazılması gerektiren zararlı yazılım

---

399 DEĞİRMENCİ, Olgun, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi"*, s. 193.

400 ERDOĞAN, Yavuz, "*Bilişim Sistemine Girme Ve Kalma Suçu*", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi C. 12, S. 0, 2010, s. 1369, https://dergipark.org.tr/tr/download/article-file/756750, E.T 03.03.2021.

401 APAYDIN, Cengiz, "Bilişim Sistemine Girme Suçu", Türkiye Adalet Akademisi Dergisi, C. 0, S. 24, 2016, s. 258, https://library.dogus.edu.tr/mvt/pdf.php, E.T 12.11.2020.

402 MAHMUTOĞLU, Fatih Selami, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar Ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 71, S. 1, 2013, s. 859.

403 AKBULUT, s. 118.

404 ÖZSOY, Nevzat, "*Yargıtay Kararları Işığında Doğrudan Bilişim Suçları*", Yaşar Hukuk Dergisi, C.1, S. 2, 2019, s. 305.

405 AKÖZ, Burak Cesur, "Türk Ceza Kanunu Kapsamında Bilişim Suç Ve Cezaları İle Örnek Yargısal Kararların Analizi ve Mevzuat Önerileri", Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri Ve İletişim Kurumu, Yayın No: 0255, Ankara 2018, s. 74.

406 ERDOĞAN, s. 1392; ERCAN, s. 282.

saldırılarını gerçekleştirmek için yeterli seviyede bilişim sistemi bilgisine sahip olunması gerekmektedir. Genel itibariyle bu kişiler de hacker olarak adlandırılmaktadır. Nitekim Kevin MİTNİCK, Kevin POULSEN ve Edward SNOWDEN gibi isimler dünyaca ünlü hacker'lardır. Ancak Türk ceza sistemimizde salt olarak kanun koyucu tarafından böyle bir özellik aranmadığından suçun faili herkes olabilecektir[407]. Bilişim sistemine girilmesi suretiyle yararına lehine haksız yarar sağlanan kişinin tüzel kişi olması durumda ise TCK'nın 246. maddesi gereğince tüzel kişilere özgü güvenlik tedbiri uygulanacaktır[408].Bu suçun mağdur bakımından herhangi bir özellik arz etmemektedir. Hukuka aykırı şekilde girilen veya kalmaya devam edilen bilişim sistemi üzerinde hak sahibi olan veya menfaati tehlikeye giren kişi bu suçun mağduru olacaktır[409]. Öğretide bazı yazarlar tarafından suçun mağdurunun belirli kişiler olamayacağı ileri sürülse de bilişim sistemine girme suçu ile birden fazla kişinin hakkı ihlal edildiyse hakkı ihlal edilen herkes bu suçun mağduru olabilir[410].Tüzel kişilerin ise bu suçun mağduru olup olamayacağı konusunda doktrinde farklı görüşler mevcuttur. Bir görüşe göre tüzel kişiler suçun mağduru olamayacakları için ancak suçtan zarar gören olabileceklerdir[411]. Bizim de katıldığımız diğer görüşe göre ise bu suçu mağduru hem gerçek kişiler hem de tüzel kişilerdir[412]**.** Nitekim özel veya kamu tüzel kişisi hak sahibi olduğu bir bilişim sistemi üzerinde menfaati tehlikeye girerse suçun mağduru olacaktır[413].Bu kapsamda daha çok kurum ve kuruluşları hedef alan fidye yazılım saldırılarının2021 yılında şirketlere verdiği zararın 20 milyar doları aşmış olduğu dikkate alındığında suçun mağduru olabileceği kabul edilmelidir[414]. Siber güvenlik şirketi Sophos tarafından 2021 yılı Ocak- Şubat aylarında yapılan 30 ülkenin yer aldığı ve 5.400 bilgi yöneticisinin katıldığı araştırma raporuna göre Türkiye'de ankete katılanların %48'i son 1 yılda fidye yazılımı saldırısına uğramış ve şirketlerin fidye yazılımının verdiği zararı düzeltmenin bedeli 582 bin 500 dolar olarak kayıtlara

---

407 KURT, Levent, Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları, Seçkin Yayınevi, Ankara 2005, s. 241.

408 ERCAN, s. 282.

409 MAHMUTOĞLU, s. 169.

410 APAYDIN, s. 260; AKBULUT, s. 121.

411 AKÖZ, s. 74.

412 YENİDÜNYA, A. Caner, "*Bilişim Sistemine Hukuka Aykırı Erişim Suçu*", Legal Fikri Ve Sınai Haklar Dergisi, S.4, 2005, s. 1027'den aktaran; EKİCİ ŞAHİN, KORUCUL, s. 596.

413 EKİCİ ŞAHİN, KORUCUL, s. 596.

414 Sigorta Medya, "Fidye Yazılımı Saldırılarının Şirketlere Maliyeti 20 Milyar Doları Aştı", 17 Şubat 2020, https://www.sigortamedya.com.tr/fidye-yazilimi-saldirilarinin-sirketlere-maliyeti-20-milyar-dolari-asti/, E.T. 21.03.2022.

geçmiştir[415]. Yine bu rapora göre 2021 yılında büyük çaptaki kuruluşlar en fazla fidye yazılımı saldırısına maruz kalırken küçük ölçekli şirketler daha az saldırıya maruz kalmıştır.

Fransa'da 8 Şubat 2021'de başlayan ve ertesi güne kadar devam eden fidye yazılımı saldırısında hacker'lar, Dax – Coted'Argent hastanesini hedef almış ve hastane hizmetlerinin büyük ölçüde aksamasına neden olmuştu[416]. Fransız Ceza Kanun'unda "mağdur" ve "suçtan zarar gören" kavramlarının tanımı yapılmamış olmakla beraber bir kişinin suçtan zarar gören olarak kabul edilip davaya katılabilmesi için "zararın doğrudan, kesin, güncel ve tazmin edilebilir" olması gerekmektedir [417]. Ancak işlenen bir suç şans kaybına neden olmuşsa Fransız Yüksek Mahkemesi bunu kesin bir zarar olarak kabul etmekte ve şahsi davaya katılma hakkı vermektedir[418]. Söz konusu şartlar tüzel kişiler içinde geçerli olmakla birlikte bazı hallerde tüzel kişinin doğrudan zararı aranmayarak dolaylı bir şekilde zarar görmüş olması yeterli görülmüştür[419].Fransız Ceza Hukuku doktrininde tüzel kişilerin gerçek anlamda şahsi davaya katılma hakkı olup olmadığı hususu ise tartışmalı olmakla birlikte hâkim olan görüşe göre gerçek kişinin şahsi taraf niteliği gibi tüzel kişinin de şahsi dava açma hakkı vardır[420]. Ancak tüzel kişinin faaliyeti kapsamındaki ortak bir menfaate yönelik bir saldırı gerçekleşmişse bu durumda şahsi davaya katılma hakkı olup olmadığı tüzel kişiye göre farklılık göstermektir[421]. Nitekim Fransız Yüksek Mahkemesine göre kamu kuruluşları ve kamu tüzel kişilikleri mağdur oldukları bir suçtan dolayı şahsi taraf sıfatını alarak dava açabilmektedir[422]. Dolayısıyla Dax – Coted'Argent hastanesine yapılan fidye yazılımı saldırısında hastane yukarıda izah edilen şartları taşıyorsa saldırıdan dolayı tüzel kişilik şahsi taraf sıfatını kazanabilecektir. Nitekim Fransız Ceza Kanun'un 323-1. Maddesi uyarınca bilişim sistemine yönelik gerçekleştirilen fillerde 3 yıl hapis cezası ve 30.000

---

415 TheStateOf Ransomware 2021, https://www.sophos.com/en-us, April 2021, s. 12, E.T. 25.03.2022.

416 BANNİSTER, Adam, "Dax – Coted'ArgentHospital İn France Hit ByRansomwareAttacak", The Daily Swig, 15 February 2021, https://portswigger.net/daily-swig/dax-cote-dargent-hospital-in-france-hit-by-ransomware-attack, E.T. 01.03.2021.

417 PAMUK, s. 63-65.

418 PAMUK, s. 65.

419 PAMUK, s. 92.

420 PAMUK, s. 91.

421 PAMUK, s. 91.

422 PAMUK, s. 107.

Euro para cezası öngörülmüştür[423]. Ancak söz konusu suç devlet tarafından himaye edilen kişisel verilere karşı işlenirse bu durumda nitelikli hal olacak ve fail 5 yıl hapis cezası ve 75.000 Euro para cezası ile cezalandırılacaktır.

TCK'nın 243. maddesindeki suçun konusu bilişim sistemidir[424]. TCK'nın 243. maddesinin gerekçesinde bilişim sistemi verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma olanağı veren manyetik sistemler şeklinde tanımlanmakla beraber bilişim sistemi sadece bilgisayarları değil yapay zekâ teknolojisinin kullanıldığı sistem ve ürünleri de kapsamaktadır. Nitekim bir sistemin bilişim sisteminin olup olmadığı her somut olayda ayrı ayrı değerlendirilerek uzman kişilerce tespit edilmelidir[425]. Bilişim sisteminin bütünü kendisi olmakla birlikte bilişim sisteminin bir kısmı da sistemin bütününü meydana getiren parça veya donanımlardır[426]. TCK'nın 243.maddesi konu bakımından herhangi bir sınırlandırma yapmamakla birlikte bilişim sisteminin güvenlik önlemleriyle korunup korunmaması suçun oluşması için özellik arz etmemektedir[427]. Ancak bazı ülkeler yetkisiz girişin suç teşkil edebilmesi için girilmesi amaçlanan bilişim sisteminin birtakım güvenlik önlemleriyle korunmuş olması şartını aramaktadır[428].Örneğin Norveç Bireysel Ceza Yasasının 145. maddesi; "*Bir kişi hukuka aykırı olarak bir başka kişinin mektubuna ya da diğer kapalı dokümanına veya benzer şekilde içeriklerine erişim sağlarsa ya da bir başka kişinin kilitli bir muhafazasının içindekilere zorla kırarak erişirse…"*[429]şeklinde düzenlenmiştir. Avrupa Siber Suç Sözleşmesinin 2. Maddesinde *"suçun güvenlik önlemlerinin ihlal edilmesi halinde gerçekleşmesi gerekebilir*" şeklinde düzenleme yer aldığından sözleşme taraflarına seçimlik sınırlandırıcı unsur tanımaktadır[430]. Nitekim İngiltere'de bir kişinin bilgisayarına kullanıcısı tarafından güvenlik önlemlerini almamış olması nedeniyle erişim sağlandıysa bu durumun hacker'lar tarafından ileri sürülebilecek bir savunma

---

[423] YAŞAR, Kenan Evren, "*Güncel Değişikliklerle Fransız Ceza Hukukunda Örgüt Kavramı Ve Örgütlenme Suçları*", Ceza Hukuku Ve Kriminoloji Dergisi, C. 3, S. 1, 2015, s. 209, https://dergipark.org.tr/tr/download/article-file/14679, E.T. 01.03.2021.

[424] EKİCİ ŞAHİN, KORUCUL, s. 592, AKBULUT, s. 122.

[425] İHTİYAROĞLU, Uğur, "*Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi*", Hacettepe Hukuk Fakültesi Dergisi, C. 10, S. 2, 2020, s. 416, https://dergipark.org.tr/tr/download/ar ticle-file/1070186, E.T. 01.03.2021.

[426] ÖZÇELİK, s. 51.

[427] ÖZÇELİK, s. 53.

[428] AKBULUT, s. 93.

[429] DÜLGER, "Murat, "*Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı Ve Uygulaması*", dipnot 277, s. 196.

[430] DÜLGER, "Murat, "*Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı Ve Uygulaması*", s. 196.

olarak değerlendirilmesi gerektiği konusunda teklifte bulunulmuş ancak reddedilmiştir[431].

15 Aralık 2017 tarihinde Romanya'nın Bükreş kentinde tutuklanan Rumen asıllı hacker Eveline Cismaru, gerçekleştirdiği fidye yazılımı saldırı sonucu Metropolitian Polis Departmanının gözetim kameralarına ve hükümet bilgisayarlarına erişim sağladığı gerekçesiyle Colombia Bölge Mahkemesi tarafından Bilgisayar Dolandırıcılığı Ve Kötüye Kullanımı Yasasının 18. bölümünün 1030. maddesi alt bölüm (a)(4); *"devlet bilgisayarlarına, banka bilgisayarlarına, uluslar arası veya dış ticaret için kullanılan bilgisayarlara yetkisiz veya verilen yetkinin aşılarak erişilmesi suretiyle dolandırıcılık*", alt bölüm (a)(7); *"bir kişiden para veya başka bir değer sızdırmak amacıyla devlet bilgisayarlarına, devletlerarası veya dış ticarette kullanılan bir bilgisayara zarar verme veya gizliliğini ihlal etme tehdidinde bulunma*"[432] gibi birçok suçtan hakkında 11 maddelik bir iddianame düzenlenerek 25 yıla kadar hapis cezası istemi ile yargılanması talep edilmiştir[433].

Suçu oluşturan fiil, bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı şekilde girmek veya orada kalmaya devam etmektir. Bilişim sistemine girmek; "*bilişim sistemlerinin oluşturduğu soyut sanal alana girmek*"[434], sistemde kalmaya devam etmek ise "*failin sanal ortamda eylemin ciddiliğini ortaya koyabilecek ölçüde kalma*"[435] eylemidir. Bilişim sistemine girme eylemi genellikle herhangi bir yetki olmaksızın uzaktan erişim ile gerçekleşmektedir[436].Fail sisteme erişim sağlamak için truva atı, virüs, solucan gibi birçok zararlı yazılım kullanarak veya sosyal mühendislik yöntemleriyle bilişim sistemine erişim sağlamaktadır. Erişim, bilişim sisteminin bütününe veya bir kısmına girilmesi demektir[437]."Yasadışı Erişim" ise bilişim sisteminin güvenliğine karşı gerçekleştirilen suçları kapsamak için kullanılan bir terimdir[438]. Nitekim ABD Bilgisayar Sahtekârlığı Ve Bilgisayarların Kötüye

---

431 DÜLGER, "Murat, "*Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı Ve Uygulaması*", s. 196-197.
432 ÖZÇELİK, s. 31.
433 Eveline Cismaru'un iddianamesine ulaşmak için bkz.;https://www.justice.gov/usao-dc/pr/romanian-woman-pleads-guilty-federal-charges-hacking-metropolitan-police-department, E.T. 02.03.2021.
434 ERGÜN, s. 89.
435 ERCAN, s. 282.
436 APAYDIN, s. 263.
437 APAYDIN, s. 264.
438 APAYDIN, s. 264.

Kullanılması Yasasında bilgisayara yetkisiz ve izinsiz erişim eylemleri yasaklanmıştır[439]. Yine Danimarka Ceza Kanunu md.236/2, Fransız Ceza Kanunu md. 323-1, Şili Otomatik Bilgi İşlem Suçları Kanunu md.2 ve Belçika Ceza Kanunu md.550' de bilişim sistemlerine yetkisiz erişim yasaklanmıştır[440]. Yine ABD, İngiltere, Hollanda, gibi ülkelerde sisteme yetkisiz girilmiş olması suçun oluşması bakımından yeterli görülmüştür[441]. Fransa, Belçika gibi bazı ülkeler ise bilişim sistemine girme eylemiyle birlikte sistemde kalmaya devam edilmesini seçimlik hareketli suç olarak düzenleyerek yaptırım altına almıştır[442]. Nitekim Türkiye'de 2016 yılında 6698 sayılı kanunla yapılan değişiklikle "*sisteme girilmesi ve sistemde kalmaya devam edilmesi*" ibaresindeki "*ve*" kelimesi *"veya*" olarak değiştirilerek bu unsurlardan birinin gerçekleşmesi suçun oluşması için yeterli görülmüş; sisteme girme ve kalma eylemleri seçimlik hareketli suç tipi olarak düzenlemiştir. Fidye yazılımı kullanılarak gerçekleştirilen saldırılarda saldırgan, mağdurun bilişim sistemine girmek için normal bir şekilde çalışmasına engelleyerek bu eylemini gerçekleştirmekte hatta mağdurun haberi olmaksızın sistemi şifrelemesi bazen saatler almaktadır. Bilişim sistemine girme suçunun oluşması için herhangi bir zararın doğmuş olması gerekmediğinden suç soyut tehlike suçudur ve sistem üzerinde ne kadar süre ile kalındığının da bir önemi de bulunmamaktadır[443].

10 Eylül 2020 tarihinde Almanya'nın Düsseldorf Üniversitesi Kliniğine gerçekleştirilen fidye yazılımı saldırısı sonucu bir kişinin hayatını kaybetmişti. Saldırıyı gerçekleştiren fail veya failler henüz yakalanmamış olsa da savcılık tarafından Alman Ceza Kanun'un (StGB) md. 23 I, 253 şantaja teşebbüs, StGBmd. 222 taksirle öldürme ve StGBmd. 303b bilgisayar sabotaj suçlarından soruşturma başlatılmıştır[444]. Görüleceği üzere Almanya'da gerçekleşen fidye yazılım saldırısında savcılık bilişim suçlarıyla alakalı olarak sadece bilgisayar sabotajı suçundan soruşturma başlatmıştır. Alman Ceza

---

439 TURHAN, s. 84.

440 DEĞİRMENCİ, Olgun, *"Türk Ceza Kanun'unun Bilişim Suçları Bakımından Değerlendirilmesi*", TBBD, S. 58, 2005, s. 204, http://tbbdergisi.barobirlik.org.tr/m2005-58-141, E.T. 06.03.2021., İLBAŞ, s. 10.

441 AKBULUT, s. 92; İLBAŞ, Çığır, "Bilişim Suçlarının Sosyo- Kültürel Seviyelere Göre Algı Analizi", Başkent Üniversitesi Fen Bilimleri Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Ankara 2009, s.11.

442 AKBULUT, s. 93.

443 ÖZSOY, s. 307.

444 SOLMECKE, Christian, "DüsseldorfUnıklinikGehackt – Patienttot. Mord?", https://www.youtube.com/watch?v=C66ZzCVuobE, E.T. 06.03.2021.

kanununda bahsedilen bilgisayar sabotajı ise TCK'nın 244.maddesine benzer bir düzenleme olmakla birlikte StGBmd. 303b[445];

"(*1) Bir başkası için önemli olan veriye dayalı bir işlemi*

1.303a maddesi birinci fıkrasındaki suçu işlemek

2.202a maddesi ikinci fıkrası anlamındaki verileri, başkasına zarar vermek maksadıyla bilgisayara girmek veya iletmek ya da

3.Bir bilgi işlem sistemini veya işlemciyi bozmak, zarara uğratmak, kullanılmaz hale getirmek, yok etmek veya değiştirmek suretiyle önemli derecede bozan kişi, üç yıla kadar hapis veya adli para cezası ile cezalandırılır…" şeklinde düzenlenmiştir. Nitekim Alman Ceza Kanununda TCK' da olduğu gibi doğrudan bilişim sistemine girme suçuna yer verilmese de 202a maddesinde "veri casusluğu" suçu düzenlenerek hukuka aykırı şekilde veriyi ele geçirme fiili yaptırım altına alınmıştır[446]. Alman Ceza Kanunun "Verilere Yetkisiz Olarak Erişim İmkânı Sağlama" başlıklı 202a maddesinde[447];

"(1) Yetkisiz olarak, kendisine ait olmayan ve haksız erişimlere karşı özel olarak güvenlik altına alınmış bulunan verilere, giriş güvenliğini kırarak kendisi veya bir başkası için erişme imkânı sağlayan kişi, üç yıla kadar hapis veya adli para cezası ile cezalandırılır…"hükmü yer almaktadır.

Hacking eylemlerinin StGB'nın md.202'a kapsamına girip girmediği konusu Alman Ceza doktrininde tartışılmalıdır. Zira Almanya'da 1986 yılından beri salt hacking eylemleri cezalandırılmamaktaydı.[448]. Ancak daha sonra 07.08.2007 tarihinde yapılan değişiklikle verilere erişim suç haline getirilse de[449] hala bazı yazarlarca hacking eylemlerinin StGB'nın md.202'a maddesince cezalandırılmaması gerektiği ileri sürülmektedir[450].Nitekim Düsseldorf Kliniğe gerçekleştirilen fidye yazılımı saldırısında da savcılık StGB'nın md. 202a'dan soruşturma açmamıştır. Kanımızca bunun nedeni Türk Ceza Hukuk sisteminde olduğu gibi Alman Ceza Hukukunda da içtima hükümleri gereğince daha özel bir düzenleme olan StGB md.303b'nin tercih edilerek uygulama

---

445 ERDAĞ, s. 293.
446 ÖZÇELİK, s. 33.
447 ERDAĞ, s. 286.
448 TRÖNDLE, Herbert, FİSCHER, Thomas, StrafgesetzbuchUndNebengesetze, C.H BeckVerlag, 52. Auflage, 2004, s. 1301.
449 AKBULUT, s. 93.
450 TRÖNDLE, FİSCHER, s. 1301.

alanı bulması ve bu nedenle soruşturma açılmadığı akla gelebilir. Ayrıca StGBmd.202'a uyarınca veriye erişmek veya ele geçirmek için bir şekilde sisteme girilmesi veya kalınması gerektiğinden esasen TCK' 243.maddesi ile benzerlik gösterdiği söylenebilir[451]. Zira daha öncede belirtildiği üzere Alman Ceza kanununda 2007 yılında yapılan değişiklikle verilere erişim sağlanamasa bile sisteme girilmesi de suç olarak kabul edilmişti[452].

Bilişim sistemine girme suçu kasten işlenebilen bir suçtur[453]. Türkiye'nin 02.04.2014 tarihinde taraf olduğu Sanal Ortamda İşlenen Suçlar Sözleşmesine göre taraf devletler suçun gerçekleşmesini "*verileri elde etmek amacıyla veya başka bir sahtekârlık amacıyla işlenmesi şartına*" bağlayabileceklerini düzenlemiştir[454]. Ancak TCK'nın md. 243 bakımından böyle bir şart aranmamış olup failin hangi amaç ile hareket ettiği önemli değildir[455]. Hukuka aykırı bir şekilde kasten sisteme girilmiş olması yeterlidir[456]. Suçun oluşması için hukuka aykırı olarak sisteme girilmiş olması gerektiğinden bu suçun olası kastla işlenmesi de mümkün değildir[457]. Yine suçun taksirle işlenebileceği düzenlenmediğinden suç taksirle işlenemez[458]. Ancak yanlışlıkla bir bilişim sistemine girdikten sonra bilerek veya isteyerek sistemde kalmaya devam kişi bilişim sistemine girme suçunu işlemiş sayılacaktır[459]. Bu doğrultu da fidye zararlı yazılımı kullanarak işlenebilecek bilişim sistemine girme suçunun olası kastla veya taksirle işlenmesi de mümkün olmayacaktır.Suçun oluşması için bilişim sistemine girme veya kalma eyleminin hukuka aykırı şekilde gerçekleşmesi gerekmektedir[460]. Daha öncede izah edildiği üzere fidye yazılımın sisteme yerleştirilme şekli veya tekniği bu aşamada suçun oluşması bakımından önemli olacak olup hukuka aykırı olarak mağdurun bilişim sistemine erişim sağlanabildiği hallerde bilişim sistemine girme suçu oluşacaktır. Örneğin drive- bydowlands yöntemiyle mağdur, herhangi bir linki tıklamasa veya bir eklenti açmasa dahi fidye yazılımı güncel olmayan tarayıcılardan faydalanarak web

---

451 ERDAĞ, Ali İhsan, "*Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda),* Gazi Üniversitesi Hukuk Fakültesi Dergisi, C. 14, S. 2, 2010, s. 284, https://dergipark.org.tr/tr/download/article-file/789484, E.T. 06.03.2021.

452 ERDAĞ, s. 287.

453 ERCAN, s. 283; AKBULUT, s. 139.

454 AKBULUT, s. 139.

455 ERCAN, s. 283.

456 ERCAN, s. 283.

457 AKBULUT, s. 139

458 EKİCİ ŞAHİN, KORUCULU, s. 608.

459 AKBULUT, s. 139

460 ERGÜN, s. 90.

sitesinde gezerken arka planda sessizce kendini yükleyebilir ve mağdurun sistemine hukuka aykırı bir şekilde girebilir. Böyle durumlarda bilişim sistemine girme suçunun oluştuğu söylenebilecektir

Failde bilişim sistemine hukuka aykırı olarak girdiği bilincinin olması ve fiilinin hukuka aykırı olduğunu bilmesi gerekir[461]. TCK md. 24 'de düzenlenen "görevin ifası", md. 25'de düzenlenen "meşru savunma", md. 26'da düzenlenen "hakkın kullanılması" ve md. 26/2 'de düzenlenen "ilgilinin rızası" gibi haller hukuka uygunluk nedenlerinden biri olmakla birlikte bilişim sistemine girme suçu bakımında ayrı ayrı değerlendirilmesi gerekmektedir. Nitekim ilgilinin rızası veya görevin ifası gibi hallerde bilişim sistemine girilmesi halinde suç oluşmaz[462]. Yine daha önce de izah edildiği üzere suçun oluşması için sistem üzerinde gerekli güvenlik önlemlerinin alınması da şart olmadığından sistemin şifre ile korunmaması rıza anlamına gelmeyecek ve hukuka uygunluk nedeni olarak kabul edilmeyecektir[463]. Ancak verilen rıza sadece kişinin bilişim sistemine girmekten ibaretse ve fail sisteme girdikten sonra kalmaya devam etmişse bu durumda yine suç oluşacaktır. Ayrıca rızanın bilişim sistemi üzerinde hak sahibi tarafından verilmiş olması gerekmektedir[464]. Aksi halde bir rızadan bahsedilemeyecektir. Yine somut olaya göre kusurluluğu etkileyen hallerin gündeme gelmesinden bahsedilebilecektir

CMK'nın "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma" başlıklı TCK'nın 134'üncü maddesi, "İletişimim Tespiti, Dinlenmesi ve Kayda Alınması" başlıklı TCK'nın 135'inci maddesi ve "Teknik Araçlarla İzleme" başlıklı TCK'nın 140'ıncı maddesinin uygulandığı durumlarda suç oluşmayacaktır[465].

Son zamanlarda fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılara karşı koruma sağlamak için uzman kişilerce pek çok sayıda yazılım ve uygulama programları geliştirilmiştir. Beyaz şapkalı hacker olarak da adlandırılan bu kişiler çalıştıkları veya hizmet verdikleri kurum veya kuruluşların sistemleri üzerindeki güvenlik zafiyetlerini tespit edebilmek adına sızma testini (Penetration) gerçekleştirirler. Sızma testi sırasında

461 ERCAN, s. 283.
462 ERCAN, s. 283.
463 ERGÜN, s. 90.
464 ERDOĞAN, s. 1408.
465 ÖZCAN, s. 427.

saldırgan gibi davranarak sistemi test ederler ve buldukları açıkları raporlarlar ve söz konusu sızma işlemini yazılı izinle yaparlar. Dolayısıyla sızma testi sırasında hacker'lar sistem üzerindeki güvenlik açıklarının kontrolü amacıyla çeşitli yöntemlerle saldırgan gibi davransa da aslında burada hukuka uygun şekilde verilmiş bir rızadan bahsedileceğinden bilişim sistemine girme suçu oluşmayacaktır. Ancak sızma testi için verilen rızanın dışına çıkılması veya devam edilmesi halinde TCK'nın 243'üncü maddesi kapsamında suç oluşacaktır.

Bilişim sistemine girme suçunda girme ve kalma şeklinde seçimlik hareket söz konusu olduğundan teşebbüs hükümlerini ayrı ayrı değerlendirmek gerekecektir[466]. Zira suçun teşebbüse elverişli olup olmadığı doktrinde tartışmalıdır. Bilişim sistemine girme suçuna teşebbüsün mümkün olmadığını savunan görüşe göre bu suç tehlike suçudur ve dolayısıyla teşebbüs mümkün değildir[467]. Bilişim sistemine girme suçuna teşebbüsün mümkün olduğunu kabul eden ve bizim de katıldığımız görüşe göre fail icra hareketlerine başlamasına rağmen elinde olmayan sebeplerle bilişim sistemine girememişse teşebbüs gerçekleşecektir[468]. Ancak hukuka aykırı şekilde bilişim sistemine girdikten sonra suç oluşacağından kalma eylemi için teşebbüsten bahsedilemeyecektir[469]. Nitekim TCK'nın 243/3'üncü fıkrasında düzenlenen suçun neticesi sebebiyle ağırlaşmış hali ancak taksirle işlenebileceğinden ve taksirli suça teşebbüs mümkün olmayacağından söz konusu fıkra bakımından da teşebbüs hükümleri uygulanamayacaktır[470]. Suçun 243/4'üncü fıkrasında düzenlenen halinde ise suç mütemadiyen bir suç olduğundan ve fail icra hareketlerine başlamasına rağmen elinde olmayan sebeplerle devam edememişse teşebbüs mümkün olacaktır[471]. ABD' de ise yetkisiz erişimi yasaklayan ve 7 ayrı suç tipini düzenleyen Bilgisayar Dolandırıcılığı Ve Kötüye Kullanımı Yasasının 18. bölümünün 1030. Maddesinin b fıkrasına göre bu suça teşebbüs etmenin de suç oluşturduğu ve bu suça teşebbüs edenlerin de cezalandırılacağı

---

466 AKBULUT, s. 150.
467 YILMAZ, Sacit, Türk Ceza Hukuku Sisteminde Siber Suçlar, 1. Basım, Adalet Yayınevi, Ankara 2016, s. 190.
468 ERDOĞAN, s. 1413; AKBULUT, S. 150.
469 AKBULUT, s. 151.
470 AKBULUT, s. 151; ERDOĞAN, s. 145; İHTİYAROĞLU, s. 430.
471 İHTİYAROĞLU, s. 430

hüküm altına alınmıştır[472]. Yine İsveç Hukukunda bilişim sistemine yetkisiz erişim sağlamakla birlikte bu suça teşebbüs edenlerinde cezalandırılacağı düzenlenmiştir[473] .

Fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılarında ise bilişim sistemine girme suçu bakımından teşebbüs mümkün olabilecektir. Örneğin fail malvertising yöntemiyle fidye yazılımı bulaştırmak için mağdurun sistemine hukuka aykırı şekilde erişim sağlayacakken mağdurun reklam alanından çıkması nedeniyle zararlı yazılımın yüklenememesi nedeniyle suç tamamlanamamışsa teşebbüs aşamasında kalacaktır. Suç iştirak bakımından herhangi bir özellik göstermemektedir[474]. Dolayısıyla TCK'nın md.37- md.40 maddelerinde düzenlenen iştirake ilişkin hükümler uygulanacaktır[475]. Fidye yazılımı kullanılarak gerçekleştirilebilecek saldırılarında suç iştirak açısından herhangi bir özellik arz etmediğinden genel hükümlere göre faillik ve şeriklikten bahsedilecektir. Yine suçun zincirleme suç olarak işlenmesi mümkündür. Zira TCK md. 243/1 ve 243/3 fıkraları bir suç işleme kararıyla değişik zamanlarda aynı kişiye karşı zincirleme şeklinde işlenebilir[476]. Doktrinde TCK'nın 243. maddesi ile 244. maddesi arasındaki içtima ilişkisi tartışmalıdır[477]. Bir görüşe göre TCK'nın 243.maddesi ile 244. maddesi arasında geçitli suç ilişkisinden bahsedileceğinden faile yalnızca final suç olan TCK'nın 244.maddesince ceza verilmesi gerekmektedir[478]. Diğer bir görüşe göre ise TCK'nın 244/1-2fıkralarındaki suçun gerçekleşmesi için mutlaka TCK'nın 243.maddesindeki suçun işlenmesi gerekmediğinden ve zorunlu unsuru olmadığından gerçek içtima hükümleri uygulanarak faile her birinden ayrı ayrı ceza verilmesi gerekmektedir[479]. Diğer bir görüşe göre fail TCK'nın 243.maddesindeki suçu işlerken aynı zamanda TCK'nın 244. maddesindeki suçları da işlerse bir fiil ile birden fazla suçun oluşmasına sebep vereceğinden fikri içtima hükümleri gereğince en ağır ceza olan 244. maddesince ceza verilmesi gerekmektedir[480]. Keza, Yargıtay 8. Ceza Dairesi 18.02.2016 gün, 2015/9713 E.2016/1868 K sayılı kararında TCK md. 243/1 ve TCK

---

472 ÖZÇELİK, s. 31-32.
473 İLBAŞ, s. 14.
474 ERDOĞAN, s. 1416
475 AKBULUT, s. 151.
476 İHTİYAROĞLU, s. 431.
477 AKBULUT, s. 152
478 ARTUK/GÖKÇEN/YENİDÜNYA, s. 4664'den aktaran; APAYDIN, s. 291.
479 KARAKEHYA, Hakan, "Türk Ceza Kanun'unda Bilişim Sistemine Girme Suçu", TBBD, S. 81, 2009, s. 22, http://tbbdergisi.barobirlik.org.tr/m2009-81-498, E.T. 06.03.2021.
480 AKBULUT, s. 152; ERDOĞAN, s. 141; APAYDIN, s. 292.

md. 244/2'nin oluştuğu bir olaya ilişkin davada faile yalnızca TCK md. 244/2 maddesince ceza vermiştir[481].

Fidye yazılımı kullanılarak gerçekleştirilen saldırılarda TCK md. 243 ile md.244 arasındaki içtima ilişkisinde söylediklerimiz geçerli olacaktır. Fail, mağdurun bilişim sistemine drive-bydowlands yöntemiyle bilişim sistemine girip fidye yazılımını yüklediğinde artık sistemin normal şekilde çalışmasını engelleyerek bozmaktadır. Böyle bir olayın varlığı halinde fail TCK'nın 243.maddesindeki suçu işlerken aynı zamanda TCK'nın 244. maddesindeki suçları da işlerse bir fiil ile birden fazla suçun oluşmasına sebep vereceğinden fikri içtima hükümleri gereğince en ağır ceza olan 244. maddesince ceza verilmesi gerekmektedir. Ancak fidye yazılımlarının oltalama saldırılarıyla gerçekleştirildiği durumlarda fail, mağdurun sistemine hukuka aykırı şekilde girmeyip onu sosyal mühendislik yöntemiyle zararlı yazılımı kendi sistemine yüklettiğinden TCK md.243'den bahsedilemeyecek ve fail bu durumda TCK md.244'den cezalandırılacaktır.

TCK md. 243/2'de ise suçun daha az ceza verilmesini gerektiren nitelikli hali düzenlenmiştir. Söz konusu fıkra; *"Yukarıda tanımlanan fillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir*" şeklinde düzenlenmiştir. Maddenin gerekçesinde suçun bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde neden daha az ceza verileceğine ilişkin bir açıklama yapılmadığından söz konusu suçun indirim sebebi olarak düzenlenmesi doktrinde tartışmalara neden olmuştur[482]. Kanaatimizce TCK md. 243/3 ile sistem sahibinin veya hak sahibinin malvarlığı değerleri de ihlal edileceğinden suçun indirimli hal olarak değil nitelikli hal olarak düzenlenmesi gerekmektedir[483]. TCK'nın 243. maddesinin gerekçesinde "bedeli karşılığı yararlanılabilen sistemler" kavramına ilişkin herhangi bir açıklama yapılmadığından bu kavramdan ne anlaşılması gerektiği de doktrinde tartışmalıdır[484].Bir görüşe göre internet cafe ve benzeri mekânlarda verilen

[481] AKBULUT, dipnot:433, s. 153.
[482]ÖZÇELİK, s. 99.
[483] DÜLGER, Murat, Bilişim Suçları Ve İnternet İletişim Hukuku, s. 353'den aktaran; APAYDIN, s. 271; Bazı yazarlara göre ise böyle bir indirim halinin düzenlenmesi doğru değildir. Bkz; ERDOĞAN, s. 1400; Bir kısım yazarlarsa TCK'nın 243/1 maddesiyle ihlal edilen hukuki yararın, bedeli karşılığı yararlanılabilen sistemlere girmek veya kalmak suretiyle ihlal edilen hukuki yarardan daha fazla korunması gerektiğini dolayısıyla daha az cezaya hükmedilmesinin yerinde olduğunu ileri sürmektedirler. Bkz; APAYDIN, s. 272; EKİCİ Ş., KORUCULU, s. 615.
[484]ERDOĞAN, s. 1397; APAYDIN, s. 270.

hizmetler 243/3 fıkrası kapsamına girmektedir[485]. Bizimde katıldığımız görüşe göre ise internet cafe gibi yerler bu kapsama girmemektedir[486]. Zira 243/3 fıkrası ile kastedilenin sistemin kullanıldığı mekân olmayıp bedeli karşılığı yararlanılabilen sistemlerden anlaşılması gerekenin sistem içinde elektronik yapıda sunulan hizmetlerin olduğudur[487]. Dolayısıyla ücret karşılığında yararlanılan veya hizmet alınan web sitelerinin, yazılım programlarının ve uygulamalarının bedel karşılığı yararlanabilen sistemler olduğu söylenebilecektir[488]. Ücretli uygulamalar üzerinden bulaştırılan fidye yazılımı saldırılarında suçun bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hali söz konusu olacak ve TCK'daki düzenlemeye bakıldığında faile verilecek ceza yarı oranına kadar indirilecektir. Ancak böyle bir indirimden bahsedilmesi bile fidye yazılımı geliştiricileri tarafından cazip hale getirilerek kötüye kullanılacaktır. Bu bakımdan TCK md.243/3 fıkrası oldukça tehlikeli bir hal olarak karşımıza çıkacaktır.

TCK md. 243/3'de suçun netice sebebiyle ağırlaşmış hali düzenlenmiştir. Söz konusu fıkra; *"Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur"* şeklinde düzenlenmiştir. Söz konusu ağırlaşmış halden bahsedebilmek için failin taksirinin bulunması gerekir[489]. Şayet fail verilerin yok edilmesinde veya değiştirilmesinde kastla hareket etmemişse neticesi sebebiyle ağırlaşmış halden sorumlu olmayacaktır[490]. Fidye yazılımları doğası gereği hedef sistemi kilitleyip /şifrelemekte ve hatta bazı türdeki fidye yazılımları sistemdeki verileri otomatik olarak silecek şekilde yüklenmektedir. Böyle bir durumun varlığı halinde fail hakkında altı aydan iki yıla kadar hapis cezasına hükmolunacaktır.

Bilişim sistemine girme suçunun birinci fıkrasında düzenlenen hali için bir yıla kadar hapis veya adli para cezası öngörülmüştür. Suçun alt sınırı belirtilmediği için TCK'nın 49.'uncu maddesi uyarınca alt sınır 1 ay olarak kabul edilecektir[491]. TCK'nın 243/2. maddesinde düzenlenen suçun işlenmesi halinde verilecek ceza yarı oranında indirilecektir. TCK md.243/ 3.fıkrada düzenlenen fiil nedeniyle verilerin yok olması veya değişmesi halinde altı aydan iki yıla kadar hapis cezası,yine 243/4. Fıkrasında

[485] DÜLGER, Murat, Bilişim Suçları Ve İnternet İletişim Hukuku, s. 374'den aktaran; EKİCİ Ş., KORUCULU, s. 614.
[486] AKBULUT, s. 144.
[487] ERDOĞAN, s. 1399.
[488] AKBULUT, s. 144.
[489] AKBULUT, s. 149.
[490] AKBULUT, s. 149.
[491] AKBULUT, s. 153-154.

düzenlenen hali için ise bir yıldan üç yıla kadar hapis cezasına hükmolunacaktır. Fidye yazılımı kullanılarak işlenebilecek bilişim sistemine girme suçu bakımından saldırganlar suçta ve cezada kanunilik ilkesi gereğince aynı ceza ile cezalandırılacaktır.

Terörle Mücadele Kanun'un Terör Amacıyla İşlenen Suçlar başlıklı 4. maddesine göre bilişim sistemine girme suçu, suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti kapsamında işlendiği takdirde terör suçu olarak kabul edilecek ve verilecek ceza yarı oranında artırılacaktır [492] . Lehine haksız yarar sağlanan kişinin tüzel kişi olması durumda ise TCK'nın 246. maddesi gereğince tüzel kişilere özgü güvenlik tedbiri uygulanacaktır.

Terör faaliyetlerin gerçekleştirilmesi için bilişim araçlarının kullanıldığı siber terörizm saldırıları son zamanlarda en etkili terör eylemi olarak karşımıza çıkmaktadır[493]. Nitekim 2017 yılında bütün dünyayı etkisi altına alan WannaCry fidye yazılımı saldırısı siber terörizm saldırısı olarak nitelendirilmişti[494]. Bu bakımdan fidye yazılım saldırılarının terörizm amaçlarıyla işlenmesi halinde eylem terör suçu sayılacak faile verilecek ceza yarı oranında artırılacaktır.

Bilişim sistemine girme suçunun soruşturma ve kovuşturması re'sen yapılmaktadır. Ancak bu suçun yurt dışında işlenmesi halinde TCK'nın 11 ve 12. maddelerinde belirtilen hallerde TCK'nın 14. maddesi gereğince Türkiye'de soruşturma ve kovuşturma yapılamayacaktır[495]. TCK md 243/3 bakımından ise fail Türk vatandaşı olup suçu yurt dışında işlemişse ve fail Türkiye'de ise suçun soruşturulması ve kovuşturulması şikâyete tabi olacaktır ve bu durumda Türk kanunlarına göre yargılaması yapılacaktır[496]. Şikâyete bağlı bir suç olmadığından uzlaştırma kapsamında değildir.

Hindistan ve Bangladeş gibi ülkelerde bilişim suçlarına bakmakla görevli özel mahkemeler kurulmuş iken[497]; Türkiye'de de Hâkimler Ve Savcılar Kurulu'nun 25.11.2021 tarih ve 1229 sayılı kararı ile bilişim suçlarına bakmakla görevli ihtisas mahkemeleri kurulmuştur. Bilişim suçlarında15 Aralık 2021 tarihi itibariyle görevli

---

492 AKBULUT, s. 154.

493 YALMAN, Yıldıray, "Siber Terör, Terörizm ve Mücadele", Siber Güvenlik ve Savunma Kitap Serisi 1, SAĞIROĞLU, Şeref, ALKAN, Mustafa, (Ed), Grafiker Yayınları, 1. Baskı, Ankara 2018, s. 260.

494 YALMAN, "Siber Terör, Terörizm ve Mücadele", s. 267.

495 AKBULUT, s. 155.

496 AKBULUT, s. 155.

497 DÜLGER, s. 168.

mahkeme uzman asliye ceza bilişim mahkemeleri olacaktır. Fidye yazılımı kullanılarak işlenebilecek bilişim sistemine girme suçu bir bilişim sistemi aracılığıyla işlendiğinden ve Hâkimler Ve Savcılar Kurulu'nun 25.11.2021 tarih ve 1229 sayılı kararı ile görevli mahkeme 15 Aralık 2021 tarihi itibariyle uzman asliye ceza bilişim mahkemeleri olacaktır. Lehine haksız yarar sağlanan kişinin tüzel kişi olması durumda ise TCK'nın 246. maddesi gereğince tüzel kişilere özgü güvenlik tedbiri uygulanacaktır.

Bilişim sistemine girme suçunda yetkili mahkeme suçun işlendiği yer mahkemesi olmakla birlikte genellikle suçun sisteme uzaktan erişim sağlanarak işlenmesi ya da dinamik IP adreslerinin kullanılması suçun tam olarak nerede işlendiği konusunda tespit sağlayamamaktadır. Ancak bilişim sistemine giren kişinin bulunduğu yer ile girilmek istenen sistemin bulunduğu her iki yerde hareketin gerçekleştirildiği yer olarak kabul edileceğinden bu hareketlerden birinin Türkiye'de gerçekleştirilmiş olması yetkili mahkemenin Türkiye olmasına neden olacaktır[498].

3.5. Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme

Bilgi ve teknolojinin birbirine paralel şekilde geliştiği bu son dönemde bilişim sistemlerinin güvenliği de büyük ölçüde tehlike altına girmiştir. Bilişim sistemine zarar veren yazılımlar genellikle "virüs" şeklinde ifade edilse de doğurdukları ve yarattıkları etkileri bakımından zamanla alt gruplara ayrılarak isimlendirilmiştir[499]. Fidye yazılımı, Trojan, worm, botnet ve keylogger'lar gibi birçok sayıda zararlı yazılımlar bulunmaktadır. Bu zararlı yazılımlardan olan fidye yazılımlarının sisteme bulaştığı anda bilgisayara veya donanımlarına zarar vermeden temizlenmesi oldukça zor hatta imkânsızdır. "Görev yükünün" diğer zararlı yazılımlarından farklı çalışması birçok bilişim sisteminin fidye yazılımı karşısında güçsüz hale getirmesine sebep olmuştur[500]. Öyle ki fidye yazılımları karşısında antivirüs programları dahi başarılı olamamaktadır. Fidye yazılımları bulaştıkları sistemdeki verileri şifreleyerek bilgisayarın normal şekilde

[498] AKBULUT, s. 156.

[499]HENKELOĞLU, Türkay, Adli Bilişim: Dijital Delillerin Elde Edilmesi Ve Analizi, Pusula Yayıncılık, 2. Baskı, İstanbul 2014, s. 187.

[500]GÜNGÖR, Abdülkadir, Linux İşletim Sisteminde Malware Analizi, Abdülkadir Güngör Yayıncılık, 2021, s. 16.

çalışmasını engelleyip kullanılamaz hale getirmektedir.[501] Dolayısıyla doğrudan doğruya bilişim sistemini verileri korumaya yönelik olarak düzenleme TCK'nın 244. maddesi konumuz olan fidye yazılım saldırıları açısından oldukça önem arz etmektedir.

Türk Ceza Kanun'un ikinci kitap üçüncü kısmında yer alan "Topluma Karşı Suçlar" kısmının "Bilişim Alanında Suçlar" bölümünde düzenlenen TCK md. 244' e göre;

"(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıda fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur."

TCK'nın 244. maddesinin Adalet Komisyonunda düzenlenen halinde suç üç fıkradan oluşmaktayken ilk fıkrada suç oluşturan eylemler tek tek sayılmış, devamı fıkralarında ise suçun nitelikli hallerine yer verilmiştir[502]. Ancak 5237 sayılı TCK'da 244. maddeyi düzenleyen hükümde söz konusu fiillerin farklı şekillerde dört fıkra halinde düzenlendiği görülmüştür[503].Nitekim madde metninde görüleceği üzere md 244/1-2-4. fıkralarında üç ayrı suç tipi düzenlenmiş, md 244/3 'de ise suçun nitelikli haline yer verilmiştir[504].

Türkiye'nin de 2014 yılında taraf olduğu Avrupa Siber Suçlar Sözleşmesinin "verilere müdahale" ve "sistemlere müdahale" başlığını taşıyan 4. ve 5. maddeleri uyarınca 5237

---

501 VpnMentor, "*Fidye Yazılım Tehdidinin Tarihi: Geçmişi, Bugünü ve Geleceği*", https://tr.vpnmentor.com/blog/fidye-yazilim-tehdidinin-tarihi-gecmisi-bugunu-ve-gelecegi/, E.T 03.03.2021.

502 KARAGÖZ, Mehmet Can, Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme Suçu, On İki Levha Yayıncılık, 1. Baskı, İstanbul 2020, s. 151.

503 KARAGÖZ, s. 151.

504 AKBULUT, s. 173.

sayılı TCK'da benzer bir düzenlemeye gidilerek söz konusu filler TCK md. 244/1-2 maddelerince yaptırım altına alınmıştır[505].

Suçla korunan hukuki yararın ne olduğu konusunda doktrinde fikir birliği bulunmamaktadır. Bir görüşe göre TCK md. 244/1 ve 244/2'de düzenlenen suçlarda korunan hukuki yarar "mülkiyettir"[506]. Zira bu suçun konusunu oluşturan veriler mal kapsamına girmediğinden kanun koyucu bu suç ile birlikte mala zarar verme suçunun özel bir görünüş şeklini oluşturarak boşluğu doldurmak istemiştir[507]. Bir görüşe göre TCK md. 244/1 ve md. 244/2' de 2 farklı suç düzenlendiğinden korunan hukuki yararda bu kapsamda ayrı ayrı ele alınmalıdır[508]. Buna göre md. 244/1'de; bilişim sistemi sahiplerinin, işletmecilerin veya kullanıcıların sistemin sorunsuz şekilde çalışmasındaki yararı korunurken, md. 244/2' de tasarruf yetkisine sahip kişilerin verilerin bozulmadan, engellenmeden ve müdahale olmaksızın kullanılmasındaki yarar korunmaktadır[509]. Bir görüşe göre suçla koruna hukuki yarar karma niteliktedir[510]. Zira TCK'nın 244. Maddesinde düzenlenen suç mala zarar vermenin elektronik bir çeşidi olup koruna hukuki yararda bilgisayarın dokunulmazlığı ve sistemin istenildiği şekilde hizmet etmesidir[511]. Sanal Ortamda İşlenen Suçlar Sözleşmesinin raporunda ise koruna hukuki değer olarak veri ve bilgisayar programlarının bütünlüğü gösterilmiştir[512]. Diğer bir görüşe göre ise bilişim sistemleri birçok alana hizmet ettiğinden bilişim sistemi ve güvenliği dışındaki diğer menfaatler veya değerlerin suçla korunan hukuki değer olarak ayrıca belirtilmesine gerek yoktur[513]. Zira bir hastanedeki bilişim sisteminde bir hastanın hayatı yani yaşam hakkı korunurken bir bankanın bilişim sisteminde kişinin maddi değerleri korunduğundan bu gibi değerler dolaylı hukuki değer olup esas olanın bilişim sistemi ve güvenliği yani mülkiyet hakkıdır[514]. Nitekim Almanya'da Düesseldorf Üniversitesi Kliniğine yapılan fidye yazılım saldırısında hastane bilgisayarları çalışamaz hale geldiğinden hastaya müdahale edilememiş ve başka bir

505 AKBULUT, s. 177, ALP, s. 75.
506 TEZCAN/ERDEM/ÖNOK, s. 846.
507 TEZCAN/ERDEM/ÖNOK, s. 846.
508 AKBULUT, s. 181.
509 AKBULUT, s. 181
510 ERDAĞ, s. 281.
511 ERDAĞ, s. 280.
512 KARAGÖZ, s. 154.
513 PALLI, Hayati, "Türk Hukukunda VeMukaseyeli Hukukta Bilişim Suçları", Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Kayseri 2008, s. 164.
514 PALLI, s. 164.

hastaneye nakli sağlanırken hasta hayatını kaybetmişti. Bu saldırı da hastanın yaşam hakkı ihlal edilmekle birlikte fidye zararlı yazılımları bilişim sistemlerine zarar verdiğinden bu saldırılarda korunan hukuki yarar öncelikle bilişim sistemi ve güvenliği olacaktır. Dolayısıyla bu kapsamda dar ve geniş anlamda olmak üzere 2 farklı hukuki yararın korunduğu, dar anlamda korunmak istenen hukuki yararın mülkiyet hakkı olduğu geniş anlamda korunmak istenen hukuki yararın ise bilişim sisteminin bütünlüğü ve veri güvenliği olduğu söylenebilir[515].

Suçun faili herkes olabilir. Bilişim suçlarının tanımlanmasında fail kriterini esas alan görüş bugün hala geçerli olsaydı suç beyaz yaka suçu[516] olarak kabul edilecek ve özgü suç niteliğinde olacaktı. Ancak günümüzde böyle bir sınırlandırma yapılmamakla birlikte TCK'nın 244. maddesinde de faile ilişkin bir kriter aranmadığından suç herkes tarafından işlenebilecektir. Tüzel kişiler ise suçun faili olamayacağı için lehine haksız yarar sağlanan kişinin tüzel kişi olması durumda ise TCK'nın 146. maddesi gereğince tüzel kişilere özgü güvenlik tedbiri uygulanacaktır[517]. Saldırganların sahte e-posta veya web adresler kullandığı mağduru yanıltıp zararlı yazılımı kendilerinin tıklamasını sağladıkları saldırılarda zararlı yazılımı indirme fiillerini bizzat mağdurun kendisine yaptırmış olduklarından böyle durumlarda TCK md.244/2 bakımından dolaylı faillikten söz edilebilecektir[518]. Suçun mağduru sistem veya veriler üzerinde tasarruf yetkisine sahip olan kişi olmakla birlikte bilişim sisteminin maliki veya zilyedi olmasına gerek yoktur[519]. Dolayısıyla suçun mağduru herkes olabilir. Tüzel kişilerin ise bu suçun mağduru olup olamayacağı doktrinde tartışmalıdır. Bir görüşe göre bu suçun mağduru ancak gerçek kişiler olup tüzel kişiler suçtan zarar görendir[520]. Bir görüşe göre ise suçun mağduru kamu idaresi olup suç kişilere karşı suçlar bölümünde düzenlenmediğinden

---

515 KARAGÜLMEZ, s. 155.

516 ABD Adalet Bakanlığı beyaz yaka suçlarını şu şekilde tanımlamıştır*; " Girişimci, profesyonel veya yarı profesyonel veya yarı profesyonel mesleki statüye sahip bireyler tarafından aldatma teknikleri kullanmak suretiyle finansal kazanç sağlamak amacıyla işlenen şiddet içermeyen suçlardır; bu kişiler özel mesleki bilgi ve fırsatlara sahiplerdir, özel teknik ve profesyonel iş bilgisine sahip bireylerin gerçekleştirdikleri eylemlerdir".* Nakden*;* ŞENTÜRK, Fatih*, " Beyaz Yaka Suçları Ve Yolsuzluklar",* Çankırı Karatekin Üniversitesi İktisadi İdari Bilimler Fakültesi Dergisi, C. 3, S. 2, 2013, s. 151, https://dergipark.org.tr/tr/download/article-file/382278, E.T. 12.02.2020.

517 TEZCAN/ERDEM/ÖNOK, s. 846.

518 DEĞİRMENCİ, Olgun, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi",* s. 194.

519 ALP, s. 80.

520 AKBULUT, s. 185.

gerçek kişiler ancak suçtan zarar gören olarak kabul edilecektir[521]. Bizim de katıldığımız görüşe göre ise bu suçu mağduru hem gerçek kişiler hem de tüzel kişilerdir. Daha önceki bölümlerde izah edildiği üzere fidye yazılımı saldırıları çoğunlukla tüzel kişilere karşı gerçekleştirildiğinden suçun mağduru olarak kabul edilmeleri büyük önem arz edecektir.

Suçun konusu TCK md. 244/1-2 fıkraları bakımından farklılık göstermektedir Buna göre md. 244/1'deki suçun konusu bilişim sistemi iken md. 244/2'deki suçun konusu ise bilişim sistemindeki verilerdir[522]. TCK md. 244/3 fıkrasında düzenlenen suçun konusunun ise malvarlığı olmakla birlikte öğretide suçun konusunun bilişim sistemi ve sistemdeki verilerin olduğu ifade edilmektedir. Veri, TDK sözlüğünde[523]; "bilgi, data" olarak tanımlanmakla birlikte TCK'nın 243. maddesinin gerekçesinde verinin sistem üzerinde bütün soyut unsurları kapsadığı belirtilmiştir[524].Nitekim öğretide verinin mutlaka bir bilişim sisteminin içinde yer alması gerektiği ifade edilmektedir[525].

3.5.1. Bilişim Sisteminin Engellenmesi veya Bozulması Fıkrasına Göre Fiil

Sistemin engellenmesi veya bozulması filleri suçun netice unsurunu meydana getireceğinden neticeli bir suçtur[526]. TCK'nın 244. maddesinin ilk 2 fıkrasında farklı iki suç tipi düzenlenmekle birlikte bu suçlar serbest hareketli suçlardır[527]. Bu suç genellikle birden fazla seçimlik hareketin aynı anda gerçekleşmesiyle oluşsa da fail tek suç işlemiş gibi kabul edilerek ceza belirlemesi yapılırken alt sınırdan uzaklaşılacaktır[528] .

Bilişim Sisteminin Engellenmesi; sistemin akışına uygun şekilde çalışmasına müdahale edilerek aksatılmasıdır[529]. Veriler üzerinde işlem yapılması, kullanılması, kaydedilmesi gibi veri işleyişine engel olan hareketler bilişim sisteminin engellenmesidir[530].

---

521 HAFIZOĞULLARI, Z., ÖZEN, M., Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, Usa Yayınları, Ankara 2012, s. 48'den aktaran; ALP, s. 80-81.
522 TEZCAN/ERDEM/ÖNOK, s. 846.
523 Türk Dil Kurumu, https://sozluk.gov.tr/
524 ALP, s. 81.
525 AKBULUT, s. 189; ALP, s. 81.
526 AKBULUT, s. 191.
527 ALP, s. 83.
528 ALP, s. 84.
529 ALP, s. 85.
530 AKBULUT, s. 190.

Bilişim Sisteminin Bozulması; sistemin normalden daha farklı çalışmasıdır[531]. Bozulma herhangi bir şekilde olabilir[532]. Suçun işlenmesi bakımından özellik arz etmemektedir[533].Zararlı yazılımlar ile sistemin çalışması bozulacağı gibi fiziksel müdahale ile de bozulabilir[534]. Doktrinde bazı yazarlara göre sistemin donanımlarına zarar verme eylemi TCK'nın 244. Maddesindeki suçu değil 151. maddesinde ki mala zarar verme suçunu oluşturmaktadır. Ancak TCK'nın 244. maddesinde böyle bir sınırlandırma yapılmadığından fiziki unsurlara yapılan müdahale halinde bu suç oluşacaktır[535].

Sistemi Engelleme ve Bozma eylemlerinin farkını belirleyebilmek için şu ölçütten yararlanılabilir; Şayet sisteme yapılan müdahale sonunda sistem hala eskisi gibi çalışıyorsa engelleme, eski halinde çalışmayıp bunun için sistem üzerinde bir takım değişiklikler yapılması gerekiyorsa bozulma fiilinden bahsedilebilir[536]. Nitekim DDOS saldırısı sonucunda sistem olması gerektiği gibi çalışmaktaysa sistemin engellendiğinden bahsedilebilir[537].

2- Verileri Bozma, Yok Etme, Değiştirme, Erişilmez Kılma, Veri Yerleştirme, Verileri Başka Yere Gönderme Fıkrasına Göre Fiil

Suç seçimlik hareketli olduğundan suçun tamamlanması için sayılan fiillerden birinin gerçekleştirilmesi yeterli olacak olup ceza belirlemesi yapılırken alt sınırdan uzaklaşılacaktır[538].

Verileri Bozmak; verinin elverişli bir şekilde kullanılmasına zarar verilmesi[539], kalıcı olarak zarara uğratılmasıdır[540]. Verilerin nasıl bozulacağı konusunda kanunda sınırlandırma yapılmadığı için bu suç serbest hareketli suçtur[541]. Uygulamada failin

---

531 AKBULUT, s. 194.
532 AKBULUT, s. 194.
533 ALP, s. 89.
534 ALP, s. 89.
535 AKBULUT, s. 191-192.
536 KARAGÖZ, s. 166.
537 KARAGÖZ, s. 166.
538 KARAGÖZ, s. 168.
539 AKBULUT, s. 195.
540 KARAGÖZ, s. 170.
541 ALP, s. 90.

kastının 244/1 mi yoksa 244/2'ye mi yönelik olduğunun tespiti zor olduğundan somut olaya ve failin yöneldiği eyleme göre vasıflandırma yapmak gerekecektir[542].

Verilerin Yok Edilmesi; verinin mevcudiyetinin ortadan kaldırılmasıdır[543]. Bilişim sistemindeki veriler bazen birtakım program veya işlemlerle geri döndürülebilmektedir[544].Sistemdeki verilerin geri dönüşüm klasörüne taşınması durumunda verilerin yok edilip edilmediği hususu doktrinde tartışmalıdır. Bir görüşe göre geri dönüşümü mümkün olan verilerin yok edilmesinden bahsedilemeyeceğinden böyle bir durumda TCK 244. Maddesindeki diğer seçimlik hareketlerden bahsedilecektir[545]. Bir görüşe göre verilerin silinerek geri dönüşüm kutusuna gönderilmesi halinde verinin yapısı bozulmadığından verilerin yok edilmesi suçu oluşmayacaktır[546]. Bir görüşe göre ise verinin silinmesi ile yok edilmesi aynı anlama geleceğinden verilerin böyle bir durumda verilerin yok edilmesi suçu oluşacaktır[547].Sistemdeki verilerin fiziksel müdahale veya çeşitli yöntemlerle yok edilmesi mümkün olup ne şekilde yok edildiği veya edileceği önemli değildir[548].

Verilerin Değiştirilmesi; "*Yeni bilginin oluşmasını sağlayan her tür hareket*" verilerin değiştirilmesidir[549]. Verilerin kopyalanması verinin değiştirilmesi kapsamında olmayıp verilerin orijinalinde değiştirmenin yapılması gerekmektedir[550].

Erişilmez Kılma; Herhangi bir şekilde veriler erişilmez kılınabilir[551]. Hak sahibi veya yetkili olan kişi sistemdeki verilere ulaşamıyorsa veriler erişilmez kılınmıştır[552]. Erişilmez kılmanın geçici süreyle mi yoksa sürekli mi olması gerektiği noktasında doktrinde fikir ayrılığı bulunsa da genel kabule göre geçici süre ile sistemdeki verilere erişilmeme halinde suç oluşacaktır[553]. Keza sistemin erişilmez kılınması halinde veriler

542 TEZCAN/ERDEM/ÖNOK, s. 846; ALP, s. 91.
543 AKBULUT, s. 196.
544 ALP, s. 92.
545 AKBULUT, s. 197.
546 KARAGÖZ, s. 174.
547 ALP, s. 93.
548 ALP, s. 93.
549 AKBULUT, s. 198.
550 AKBULUT, s. 198.
551 AKBULUT, s. 199.
552 AKBULUT, s. 200.
553 AKBULUT, s. 200.

hala sistemde mevcut olduğundan diğer seçimlik hareketlerden bu noktada ayrılmaktadır[554].

Veri Yerleştirme; Veri yerleştirmeden bahsedilmek için sistem üzerinden herhangi bir veri eksiltmeksizin yeni bir verinin dâhil edilmesidir[555]. Suçun oluşması için sisteme girişin hukuka aykırı olup olmaması değildir[556].

Verileri Başka Bir Yere Gönderme; sistem içerisindeki verilerin başka bir sisteme gönderilmesidir[557].

Bu suç genel kastla işlenebilen suçlardan olup taksirle işlenmesi mümkün değildir[558].Suçun taksirle işlenmesi halinde faile herhangi bir ceza verilmeyecektir[559]. Suçun işlenmesi için özel kast aranmadığı gibi suç doğrudan kast veya olası kastla işlenebilir[560]. Fidye yazılımı saldırıları kapsamında işlenecek olan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu da taksirle işlenemeyecek olup fail başkasının bilişim sistemini engellediğini, bozduğunu ya da sistemdeki verileribozduğunu, değiştirdiğini, başka bir yere gönderdiğini ve bu filleri işlemek suretiyle kendisi veya başkası için haksız yarar elde ettiğini bilmelidir.

TCK'nın 244. maddesi bakımından hukuka uygunluk nedeni olarak ilgilinin rızasından bahsedilebilir[561]. Bu durumda hukuka aykırılık unsuru ortadan kalkacağı için suç oluşmayacaktır. Yine 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun çerçevesinde yetkinin kullanıldığı hallerde hukuka uygunluk nedeninden bahsedilecek TCK'nın 244. maddesinde düzenlenen suç oluşmayacaktır[562].Fidye zararlı yazılımını kullanıldığı saldırılarda hukuka aykırılık unsuru bakımından *"*Bilişim Sistemine Girme Suçu" için ifade ettiğimiz hususlar burada da aynen geçerli olduğundan sızma testlerinde güvenlik açıklarının kontrolü amacıyla gerçekleştirilen testlerde ilgili kişi tarafından hukuka uygun şekilde verilmiş bir rızadan bahsedileceğinden sistemi

554 KARAGÖZ, s. 174.
555 KARAGÖZ, s. 174.
556 ALP, s. 98.
557 AKBULUT, s. 202.
558 TEZCAN/ERDEM/ÖNOK, s. 848; MAHMUTOĞLU, s. 868.
559 KARAGÖZ, s 185.
560 ÖZSOY, s. 335.
561 TEZCAN/ERDEM/ÖNOK, s. 849.
562 TEZCAN/ERDEM/ÖNOK, s. 849.

engelleme, bozma, verileri yok etme veya değiştirme suçu oluşmayacaktır. Ayrıca yine somut olayın özelliklerine göre ve kanundaki düzenlemeler çerçevesinde kusurluluğu etkileyen hallerin gündeme gelmesinden bahsedilebilecektir. Örneğin bir başkasının bilişim sistemini bozmak amacıyla hacker tutulması veya benzeri bir sebeple sisteme zarar verilmesi halinde karşı saldırı olarak fidye zararlı yazılımı saldırısının gerçekleştirilmesi halinde diğer şartlarında varlığı halinde kişinin haksız tahrik etkisi altında suçu işlediği sebebiyle kanaatimizce haksız tahrik hükümleri gündeme gelebilecektir.

TCK'nın 244/1-2-4 fıkraları bakımından düzenlenen suçlara teşebbüs mümkündür[563]. TCK'nın 244.maddesinde düzenlenen suç seçimlik hareketli suç olduğundan failin eyleminin bir kısmının teşebbüs aşamasında kaldığı bir kısmının ise tamamlandığı durumlarda ne olacağı sorunu gündeme gelmektedir[564]. Böyle bir durumda önemli olan husus birden fazla hareket aynı anda gerçekleşse de tek bir suç oluşacağından failin eylemlerden birini tamamlaması halinde diğer seçimlik hareketler teşebbüs aşamasında kalsa da tamamlanmış tek bir suçtan bahsedilecektir[565]. Öte yandan TCK'nın 244/4 fıkrası bakımından failin kastı haksız yarar sağlama olduğundan söz konusu suçun birinci ve ikinci fıkradaki eylemleri gerçekleştirmesine rağmen haksız çıkar elde edemediyse failin sorumluluğunu belirleyebilmek için failin kastının ortaya konması gerekecektir[566]. Şayet failin kastı haksız yarar elde etmeye yönelik değilse ve birinci ve ikinci fıkradaki filleri işlemişse 244/4. fıkradaki suça teşebbüsten değil 244/1 veya 244/-2. Fıkralarındaki tamamlanmış suçtan sorumlu olacaktır[567].

Fidye zararlı yazılımları kullanılarak gerçekleştirilen saldırılarda ise olan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu bakımından teşebbüs mümkün olabilecektir. Örneğin fail hukuka aykırı bir şekilde girmiş olduğu bilişim sistemine fidye yazılımını bulaştırıp sistemi bozacakken elde olmayan nedenler ile tamamlayamamışsa suç teşebbüs aşamasında kalacaktır.

563 ÖZSOY, s. 335; TEZCAN/ERDEM/ÖNOK, s. 849.
564 MAHMUTOĞLU, s. 868.
565 MAHMUTOĞLU, s. 868
566 ÖZSOY, s. 336.
567 AÇIKGÖZ, s. 110.

Suç iştirak bakımından herhangi bir özellik göstermemekte olup TCK'nın md.37-md.40 maddelerinde düzenlenen iştirake ilişkin genel hükümler uygulanacaktır[568]. Hackerler bilişim suçunu işlerken kimliklerini deşifre etmemek veya yakalanmamak için dinamik IP adresleri kullandıkları gibi zombi bilgisayarlarda kullanarak hiçbir şeyden haberi olmayan başka bir bilgisayar kullanıcısı üzerinden suç işlemektedirler[569]. Nitekim bu şekilde bir hacker tarafından ele geçirilerek yönetilen zombi bilgisayarlar ile sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunun işlenmesi halinde zombi bilgisayar sahiplerinin ancak fail ile ilişkisinin tespiti halinde somut olaya göre iştirak hükümleri gündeme gelebilecektir[570].

TCK'nın 244. maddesinde düzenlenen suçlar için içtima hükümlerinin her halinin uygulanması mümkündür[571]. Suç zincirleme suç şeklinde işlenebileceği gibi[572] aynı fille birden fazla kişiye karşı da işlenebilir[573]. Bu durumda aynı neviden içtima hükümlerinden bahsedilecektir. TCK'nın md. 244/1 ve md. 224/2 fıkralarında yer alan suçların aynı anda işlenmesi mümkün olmakla birlikte böyle bir durumda farklı neviden içtima hükümleri gereğince failin daha ağır olan md. 244/1'den cezalandırılması gerekecektir[574]. Yine fail md. 244/1 ile md. 244/2 fıkralarında yer alan suçları işlerken aynı zamanda md. 244/4'de yer alan suçu da işlerse bu durumda fail bileşik suç hükümleri gereğince md. 244/4'den cezalandırılacaktır[575]. TCK'nın 136. Maddesinde yer alan kişisel verileri verme veya ele geçirme suçu ile TCK'nın 244. Maddesinde yer alan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları arasındaki ilişki bakımından ise fikri içtima ilişkisinin varlığından söz edilecek olursa fail daha ağır ceza olan TCK md. 244/4'den cezalandırılacak[576]; görünüşte fikri içtima ilişkisinin varlığından söz edilecek olursa da TCK md. 136 'dan hüküm kurulması gerekecektir[577]. TCK md. 244 ile md. 243 arasındaki içtima ilişkisi açısından ise bilişim sistemine girme suçunda bahsedilmiş olunduğundan ayrıca burada değinilmeyecektir.

---

568 MAHMUTOĞLU, s. 869.
569 "Zombi Bilgisayarlar Ve Bilişim Suçu", https://www.sertels.av.tr/avukat/hukuk/bilisim-hukuku/zombi-bilgisayarlar-ve-biliim-sucu.html, E.T. 05.02.2021.
570 KARAGÖZ, s. 196.
571 KARAGÖZ, s. 197.
572 AKBULUT, s. 209.
573 KARAGÖZ, s. 197.
574 KARAGÖZ, s. 198.
575 AKBULUT, s. 210; ALP, s. 109.
576 AKBULUT, s. 212.
577 KARAGÖZ, s. 200.

TCK'nın md. 244/4 düzenlenen; "Yukarıda fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur" maddesi fidye yazılımı saldırıları bakımından önem arz etmektedir. Zira fidye yazılımları haksız bir kazanç elde etme amacıyla programlandıklarından dolayı bu kapsamda bir fiil suçun konusunu oluşturduğu takdirde içtima hükümleri çerçevesinde değerlendirmek gerekecektir. Fail fidye yazılımı saldırısı ile sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunun birinci ve ikinci fıkralarında düzenlenen suçu işlerken aynı zamanda bu fiillerin işlerken kendisinin veya başkasının yararına haksız bir çıkar sağlaması durumunda fail bileşik suç hükümleri gereğince md. 244/4'den cezalandırılacaktır. TCK'nın 244. maddesinde yer alan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları arasındaki ilişki bakımından ise fikri içtima ilişkisinin varlığından söz edilecek olursa fail daha ağır ceza olan TCK md. 244/4'den cezalandırılacak ve fail hakkında iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunacaktır. Ancak görünüşte fikri içtima ilişkisinin varlığından söz edilecek olursak ise de TCK md. 136 'dan hüküm kurulması gerekecek , fail iki yıldan dört yıla kadar hapis cezası ile cezalandırılacaktır..

TCK md. 244/3'de suçun nitelikli hali düzenlenmiştir. Söz konusu fıkra; "*Bu fillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır"* şeklinde düzenlenmiştir. Söz konusu nitelikli halin uygulanması bakımından kanunda yalnızca banka veya kredi kurum ve kuruluşlarıyla sınırlandırma yapılması doğru olmamıştır[578]. Zira bu niteliğe haiz olmayan şirket veya kuruluşlar içinde sistemlerinin engellenmesi, bozulması, verileri yok edilmesi veya değiştirilmesi de önem arz etmektedir[579]. Nitekim fidye yazılım saldırılarında daha çok şirketlerin hedef olduğu hususu da göz önüne alındığında nitelikli, hali düzenleyen maddenin yetersiz kaldığı gözlemlenecektir. Kamu kurum veya kuruluşlarından maksat tüzel kişiliğe haiz olan ve olmayan bütün kuruluşlar olmakla birlikte banka kavramından ise 5411 sayılı Bankacılık Kanunun 3.

[578] AKBULUT, s. 205.
[579] AKBULUT, s. 205.

Maddesindeki tanıma uygun şekilde yer alan mevduat bankaları ve katılım bankaları ile kalkınma ve yatırım bankaları kastedilmektedir[580].

TCK'nın md. 244/4 düzenlenen; "*Yukarıda fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur"* fıkrasının nitelikli hal olup olmadığı hususu tartışmalıdır. Doktrinde bir görüşe göre bilişim sistemi aracılığıyla haksız yarar sağlama suçu 244. maddenin nitelikli hali olmayıp ayrı bir suç niteliğindedir[581]. Diğer bir görüşe göre ise bilişim sistemi aracılığıyla haksız yarar sağlama suçu bağımsız bir suç olmayıp 244. madde de düzenlenen suçun nitelikli halidir[582].Biz ise doktrindeki tartışma argümanlarına yer vermeden söz konusu suçun TCK sistematiğinde 244. madde de düzenlenmiş olması sebebiyle nitelikli hal kapsamında değerlendirerek bu başlık altında yer verdik.

Yine suçun bir diğer nitelikli hali Terörle Mücadele Kanunun da düzenlenmiştir. Terörle Mücadele Kanun'un Terör Amacıyla İşlenen Suçlar başlıklı 4. maddesine göre sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu, suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti kapsamında işlendiği takdirde terör suçu olarak kabul edilecek ve verilecek ceza yarı oranında artırılacaktır[583].

Bilişim sistemlerinin işleyişini engelleyen ya da bozan kişi 1 yıldan 5 yıla kadar hapis cezası ile; bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi ise altı aydan üç yıla kadar hapis cezası ile cezalandırılacaktır. Bu fillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılacaktır. Yine bu fillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunacaktır. Fidye yazılımı kullanılarak işlenebilecek sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu bakımından saldırganlar suçta ve cezada kanunilik ilkesi gereğince aynı ceza ile cezalandırılacaktır. Lehine haksız yarar sağlanan

580 AKBULUT, s. 205.
581 TEZCAN/ERDEM/ÖNOK, s. 849; AKBULUT, s. 217.
582 KARAGÖZ, s. 181.
583 AKBULUT, s. 208.

kişinin tüzel kişi olması durumda ise TCK'nın 246. maddesi gereğince tüzel kişilere özgü güvenlik tedbiri uygulanacaktır.

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunun soruşturma ve kovuşturması re'sen yapılmaktadır. Ancak bu suçun yurt dışında işlenmesi halinde TCK'nın 11 ve 12. maddelerinde belirtilen hallerde TCK'nın 14. maddesi gereğince Türkiye'de soruşturma ve kovuşturma yapılamayacaktır[584]. TCK md 243/3 bakımından ise fail Türk vatandaşı olup suçu yurt dışında işlemişse ve fail Türkiye'de ise suçun soruşturulması ve kovuşturulması şikâyete tabi olacaktır ve bu durumda Türk kanunlarına göre yargılaması yapılacaktır[585]. Hâkimler VeSavcılar Kurulu'nun 25.11.2021 tarih ve 1229 sayılı kararı ile bilişim suçlarına bakmakla görevli ihtisas mahkemeleri kurulmuştur. Fidye yazılımı kullanılarak işlenebilecek sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu bir bilişim sistemi aracılığıyla işlendiğinden ve Hâkimler Ve Savcılar Kurulu'nun 25.11.2021 tarih ve 1229 sayılı kararı ile görevli mahkeme 15 Aralık 2021 tarihi itibariyle uzman asliye ceza bilişim mahkemeleri olacaktır.

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunda yetkili mahkeme CMK'nın 12.maddesi gereği suçun işlendiği yer mahkemesidir[586]. Söz konusu suçlarda genellikle suçun tam olarak nerede işlendiği konusunda tespit sağlanamamaktadır. Böyle bir durumda suçun işlendiği yer tespit edilemezse CMK'nın 13.maddesi gereği şüpheli veya sanığın yakalandığı yer, şayet yakalanamamışsa yerleşim yeri mahkemesi yetkilidir[587]. Suç uzlaştırma kapsamında olmamakla birlikte 5271 sayılı CMK'nın ek 24/11/2016-6763/34 maddesine eklenen hükümle suça sürüklenen çocuklar TCK'nın 244/2 maddesince uzlaşma kapsamına alınmıştır[588].

3.6. Yasak Cihaz Veya Programlar

Son yıllarda internet kullanımının artmasıyla birlikte siber saldırıların sayısında da ciddi artışlar yaşanmıştır. Özellikle pandemi ile birlikte gerçekleştirilen siber saldırılar durumun ciddiyetini ortaya koymuştur. Hacker'lar tarafından yeni tür ve sayıda zararlı

584 AKBULUT, s. 215.
585 AKBULUT, s. 215.
586 ALP, s. 116.
587 AKBULUT, s. 216.
588 ALP, s. 117.

yazılımlar geliştirilmekle birlikte yeni bulaşma ve sızma yöntemleri de ortaya çıkmaktadır[589]. Nitekim İçişleri Bakanlığının "Covid – 19 Pandemisi Döneminde Siber Suç Riskleri Ve Güvenliğe Etkileri" isimli raporunda internetin yoğun kullanılması nedeniyle yeni suç imkânlarının oluştuğu ve vatandaşların en fazla siber suç türünden zararlı yazılım bulaşmasına maruz kaldığı tespit edilmiştir[590]. Dolayısıyla bir zararlı yazılım çeşidi olan fidye yazılımları yasak cihaz veya programlar suçu açısından oldukça önem arz etmektedir.

24.03.2016 tarihli 6698 sayılı Kişisel Verileri Koruma Kanunun 30. maddesinin 5. Fıkrası ile 5237 sayılı Türk Ceza Kanun'umuza "Yasak Cihaz Veya Programlar" başlıklı yeni bir suç tipi eklenmiştir[591]. 5237 sayılı TCK'nın 245/A maddesinde düzenlenen Yasak Cihaz Veya Programlar Suçu;

"(1)Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır" şeklinde düzenlenmiştir.

Bu suçun TCK'ya eklenmesinin Türkiye'nin Avrupa Konseyi Siber Suç sözleşmesine taraf olmasının gerektirdiği yükümlülükten kaynaklandığı belirtilmektedir[592]. Nitekim TCK'nın 245/A maddesinin gerekçesinde Sanal Ortamda İşlenen Suçlar Sözleşmesinin 6. maddesinde düzenlenen hükmüyle sözleşmeye taraf devletlere bilişim suçlarının işlenmesini kolaylaştıran cihazların kötüye kullanımının yaptırım altına alma yükümlülüğünün getirildiği belirtilmiştir[593]. Avrupa Siber Suç Sözleşmesinin "Cihazların Kötüye Kullanımı" başlıklı 6. Maddesinde yer alan düzenleme ile TCK md. 245/A 'da düzenlenen suç genel olarak birbirine uygun olmakla birlikte birtakım

[589] ÇUBUKÇU, Fatih, Bilgi Güvenliği Yönetim Sistemi, Pusula Yayıncılık, 1. Basım, İstanbul 2018, s. 11.
[590] "Salgın Döneminde En Fazla Maruz Kalınan Siber Suç Zararlı Yazılım Bulaşması Oldu", https://www. aa.com.tr/tr/bilim-teknoloji/salgin-doneminde-en-fazla-maruz-kalinan-siber-suc-zararli-yazilim-bulasmasi-oldu/2084757, E.T 15.03.2021.
[591] KOCA, Mahmut, ÜZÜLMEZ, Mahmut, "Türk Ceza Hukuku Özel Hükümler, Adalet Yayınevi, 5. Baskı, Ankara 2018, s. 912.
[592] KOCA, ÜZÜLMEZ, s 912.
[593] AKBULUT, s. 345.

farklılıklar mevcuttur. Avrupa Siber Suç Sözleşmesi bu maddeye uygulanacak suçları yasadışı erişim, yasadışı araya girme, verilere müdahale ve sisteme müdahale ile sınırlamışken TCK md. 245/A için böyle bir sınırlandırılma yapılmayarak bilişim alanında suçlar bölümünde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçlar da kapsam altına alınmıştır[594]. Avrupa Siber Suç Sözleşmesinin 6. maddesinde taraf devletlerin cezai sorumluluğunun doğması için 1. fıkranın a bendinin i ve ii bölümlerinde söz konusu unsurlardan belli sayıda bulundurulmasını şart olarak koyabileceklerini belirtmişken TCK md. 245/A için böyle bir düzenleme getirilmemiştir[595]. Yine sözleşmenin 6. maddesi şifre, erişim kodu veya benzeri veriyi, bir bilgisayar sisteminin tamamına veya herhangi bir kısmına erişimi mümkün kılan ifadeleriyle belirtmişken TCK md. 245/A için böyle bir sınırlandırılma yapılmamıştır[596].

TCK md. 245/A maddesinin "Yasak Cihaz Veya Programlar "başlığı şeklinde düzenlenmiş olması doktrinde birtakım eleştirilere neden olmuştur. Zira madde başlığı suçun konusu oluşturup madde içeriğini yansıtmadığından "Suçta Kullanılacak Cihaz Veya Programların Üretilmesi, Yayılması Veya Bulundurulması" başlığı daha doğru olacaktır[597]. TCK md. 245/A maddesindeki benzer düzenlemenin Birleşik Krallık hukuk sisteminde de olduğu söylenebilir[598]. Nitekim TCK' da olduğu gibi İngiliz Hukukunda da benzer düzenleme ile hazırlık hareketi niteliğindeki bu eylemler bağımsız bir suç olarak düzenlenmiştir[599]. Yine Rusya Federasyonu Ceza Kanunun da bilişim suçları kapsamında zararlı yazılım üretme gibi suçlar düzenlenerek yaptırım altına alınmıştır[600].

Suçla korunan hukuki değerin ne olduğu konusunda doktrinde farklı görüşler mevcut olmakla birlikte bizimde katıldığımız görüşe göre suçla korunan hukuki değer bilişim

---

[594] AKBULUT, s. 345.
[595] AKBULUT, s. 345.
[596] AKBULUT, s. 345.
[597] ÖZBEK, Veli Özer, DOĞAN, Koray, BACAKSIZ, Pınar, TEPE, İlker, "Türk Ceza Hukuku Özel Hükümler", Seçkin Yayıncılık 13. Baskı, Ankara 2018, s.1034; AKBULUT, s. 348. Akbulut'a göre ise "Yasak Cihaz veya Programların Kötüye Kullanılması" başlığının daha doğru bir düzenleme olacağı ifade edilmiştir: s. 348.
[598] DÜLGER, "*Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı Ve Uygulaması*", s. 165- 166.
[599] DÜLGER, "*Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı Ve Uygulaması*", s. 166.
[600] EHLİZ, Hakan, "Bilişim Suçlarının Ulusal Ve Uluslararası Düzeyde Değişen Güvenlik Algısı Üzerinde Etkisi", İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul 2019, s. 81.

sistemlerinin güvenliği, güvenirliği ve kamu düzenidir[601]. Fidye yazılımları esas itibariyle zararlı bir yazılım olduğundan fidye yazılımı ile işlenebilecek olan yasak cihaz veya programlar suçu ile korunan hukuki değer bilişim sisteminin güvenliği ve güvenirliği olacaktır.

Bu suçun faili herkes olabilir. Belirli bir meslek grubundan olmak suçun faili bakımından ağırlatıcı neden olarak öngörülmemiştir[602]. Faile ilişkin hacker olmak gibi bir kriter aranmadığından suç herkes tarafından işlenebilecektir. Ancak esasen kod yazmak veya bir yazılım geliştirmek herkesin yapabileceği bir iş değildir. Özellikle fidye yazılımı gibi güçlü algoritmalarla şifrelenen bir yazılımı yazmak hiç kolay değildir. Fidye yazılımlarının antivirüs programından gizlenebilmesi ve fidye yazılımlarına karşı hala bir çözüm anahtarı oluşturulamaması fidye yazılımlarını hem zor hem de daha da cazip hale getirmektedir. Zira fidye yazılımcısı eğer kodlamada bir hata yaparsa kendini deşifre edebilir yada mağdur bu konuda uzman kimselerden yardım alarak şifreyi çözebilir. Dolayısıyla bu da hacker'lar için istenmeyen riskli ve zor bir durum olarak karşılarına çıkabilir.

TCK'nın. 245/A maddesiyle hazırlık hareketi niteliğindeki filler yaptırım altına alındığı için suçun işlenmesi ile birlikte belirli bir kişinin hakkına yönelik saldırıdan da bahsedilemeyeceğinden bu suçun mağduru toplumu oluşturan herkes olacaktır[603].Bu bakımdan fidye yazılımı saldırısı ile işlenebilecek olan yasak cihaz veya programlar suçunun mağduru herkes olabilecektir.

Zararlı yazılımların bir suçu oluşturup oluşturmayacağı sorunu doktrinde uzun yıllar tartışılagelen bir konu olmuş, zararlı yazılımların faydalı amaçlar içinde kullanabileceği ve bunun tespitinin oluşum evresinde belirlenmesinin mümkün olmadığı dolayısıyla zararlı yazılımlarının başlı başına cezalandırılmaması gerektiği görüşü ileri sürülmüştür[604]. Avrupa Siber Suç Sözleşmesinin "Cihazların Kötüye Kullanımı" başlıklı 6. maddesinde bilişim suçlarının işlenmesini kolaylaştıran cihazların kötüye kullanımı

---

601 AKBULUT, s. 349; aksi görüşe göre iseTCKmd. 245/A ile yasaklanan cihaz veya programların üretilmesi ve sıklıkla tedavül etmesi bilişim sistemlerinin hukuka aykırı amaçlar için kullanıldığına ilişkin toplumda kanaat oluşturacağından ve kanun koyucu söz konusu düzenlemeyle kanunda belirtilen filleri yasaklayarak toplumsal inancı korumak istediğinden suçla korunan hukuki yarar kamunun bilişim sistemlerine yönelik güvenidir; bkz; KOCA / ÜZÜLMEZ, s. 913.

602 YILMAZ, s. 375.

603 KOCA/ÜZÜLMEZ, s. 913.

604 DEĞİRMENCİ, Olgun, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi",* s. 188.

cezalandırılmıştır. Açıklayıcı raporuna göre ise hem suç teşkil edebilecek hem de yasal amaçlarla kullanılabilecek ("dateuse") yazılımların ilgili maddeye dâhil olup olmadığı tartışılmış ve nihayetinde hem sübjektif hem de objektif olarak söz konusu cihazın suçu işlemek biçimde oluşturulması gerektiği kabul edilmiştir[605]. Bu kapsamda "test yazılımlar (website load capacity testing)" gibi ilgili kişisine hem siteyi verimli kullandırma imkânı sağlayan hem de DDoS saldırı ataklarında kullanılabilen yazılımlar dateuse yazılımlarına örnek olarak gösterilebilir[606]. TCK'nın. 245/A maddesindeki suçun konusu her türlü program, cihaz, şifre ve sair güvenlik kodudur[607].Bilgisayar programı ile suç işlemek için kullanılan programlar kastedilmektedir[608]. Bilgisayar virüsü olarak da adlandırılan zararlı yazılımlar bilgisayar kullanıcısının veya sahibinin rızası dışında bilgisayar sistemine zarar vermek için tasarlanan kötü amaçlı yazılımlardır[609]. Bilgisayar virüsleri sistemdeki dosya veya verileri silmek şeklinde programlanabileceği gibi sistemi yavaşlatarak gereği gibi kullanılmasını engelleyecek şekilde programlanabilir[610]. Virüsler, solucanlar, Truva atları, rootkitler, RAT, Botnet, keylogger ve fidye yazılımı gibi yazılımlar zararlı yazılımlardandır[611].

Cihaz, fiziksel varlığı ve donanım unsuru olan şeyler için kullanılmakta olup söz konusu cihazın mutlaka ileri teknoloji bir cihaz olması zorunlu değildir[612].Örneğin bir gizli kameranın ATM'ler de kart sahibinin şifresini kaydetmek için tasarlanması halinde kanunda belirtilen cihaz olarak kabulü mümkün olacaktır[613].

Şifre, kelime anlamı olarak "*gizli haberleşmeye yarayan işaretlerin tümü, kod"*[614]demektir. Şifrelendirme işlemini programlama olarak kabul etmek mümkün olmakla birlikte doktrinde şifre ile neyin kastedildiği kanunda belirtilmediğinden bu husus eleştirilmiştir[615].

---

605 DEĞİRMENCİ, Olgun, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi",* s. 191.
606 DEĞİRMENCİ, Olgun, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi",* s. 191.
607 KOCA/ÜZÜLMEZ, s. 914; ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1035.
608 AKBULUT, s. 351.
609 BÜLBÜL/BİNGÖL, s. 32.
610 BÜLBÜL/BİNGÖL, s. 39.
611 BAŞARAN, s. 15-16.
612 ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1035.
613 ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1035.
614 https://sozluk.gov.tr/, E.T. 25.03.2021.
615 ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1037.

Sair güvenlik kodu ise bilişim teknolojilerindeki güvenlikleri ifade etmek için kullanılmaktadır[616]. Güvenlik kodları farklı alan ve hizmetlerde kullanıldığından kanunda sair güvenlik kodu denilerek esasen tüm kodlar dâhil edilmek istenmiştir[617]. Yine doktrinde sair güvenlik kodunun "belirlilik" ilkesine aykırı olduğu sair kavramının "şifre veya sair" ifadesiyle değerlendirilmesi gerektiği ileri sürülmektedir[618].

TCK'nın. 245/A maddesindeki suçun konusu her türlü program, cihaz, şifre ve sair güvenlik kodunun bilişim alanında suçlar bölümünde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçları işlemek için yapılması veya oluşturulması gerekmektedir[619]. Bu bakımdan örneğin birçok bilişim firmasının kullandığı "pentest" adı verilen sızma testlerinde suç işlemek amacıyla değil de test ve güvenlik açıklarını tespiti amacıyla oluşturulduğu hallerde TCK md. 245/A kapsamında suç oluşmayacaktır[620].

Suçu oluşturan fiiller; bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun imal edilmesi, ithal edilmesi sevk edilmesi, nakledilmesi, depolanması, kabul edilmesi, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulmasıdır[621]. Bu bakımdan suç seçimlik hareketli suçlardan olup sayılan fillerden birinin gerçekleşmesiyle suç oluşacaktır[622]. Sevk etme, nakletme, depolama ve bulundurma eylemleri anlama geldiğinden kanunda bu kavramların hepsine yer verilmesi doktrinde eleştirilmiştir[623]. Suçun nasıl işleneceği noktasında kanunda sınırlandırılmaya gidildiğinden bağlı hareketli suç niteliğindedir[624]. Suçun oluşumu bakımından zarar unsuru aranmadığından suç soyut tehlike suçudur[625]. Seçimlik hareketlerden birden fazlasının gerçekleşmesi eylemi tek suç olmaktan çıkarmayacağından temel cezanın belirlenmesinde alt sınırdan uzaklaşılarak ceza tayin edilecektir[626].

---

616 AKBULUT, s. 353.
617 AKBULUT, s. 353.
618 KOCA/ÜZÜLMEZ, s. 914
619 AKBULUT, s. 354.
620 AKBULUT, s. 354.
621 ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1037.
622 KOCA/ÜZÜLMEZ, s. 914; ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1037
623 KOCA/ÜZÜLMEZ, s. 914
624 ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1037; AKBULUT, s. 355.
625 AKBULUT, s. 355.
626 YILMAZ, s. 378; [626] KOCA/ÜZÜLMEZ, s. 914

Bu bakımdan fidye yazılımı kullanılarak gerçekleştirilen saldırılarda bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun imal edilmesi, ithal edilmesi sevk edilmesi, nakledilmesi, depolanması, kabul edilmesi, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulması eylemleri suçu oluşturan fillerdir.

Suçun manevi unsuru fiilin kasten işlenmesi olup suçun taksirle işlenmesi mümkün değildir[627]. Failin imal ettiği, ithal ettiği sevk ettiği, naklettiği, depoladığı, kabul ettiği, satışa arz ettiği, satın aldığı, başkalarına verdiği veya bulundurduğu şeyin cihaz, şifre ve sair güvenlik kodu olduğunu bilmelidir. Ancak suçun oluşması için failin kasti yeterli değildir[628]. Failin imal ettiği, ithal ettiği sevk ettiği, naklettiği, depoladığı, kabul ettiği, satışa arz ettiği, satın aldığı, başkalarına verdiği veya bulundurduğu şeyin cihaz, şifre ve sair güvenlik kodu olduğunu bilmesi gerekip ayrıca bu filleri bilişim alanında suçlar bölümünde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçları işlemek amacıyla oluşturulduğunu bilmesi gerekir[629]. Ancak amacını oluşturan suçları işlemesi şart değildir[630]. Failin bu amacı tespit edilemiyorsa bu suçtan dolayı cezalandırılmayacaktır[631]. Suçun olası kastla işlenmesi mümkündür[632].

Dünyanın en büyük fidye yazılım saldırısı olan WannaCry'ı durduran ve kahraman ilan edilen İngiliz hacker Marcus Hutchins, saldırıyı durdurduktan kısa bir süre sonra "Kronos" adında yazılımı üretmekle suçlanarak 2017 yılında FBI tarafından tutuklanmıştı[633]. Wisconsin Eyaleti Federal mahkemesine sunulan iddianame de Federal Temel Yasanın 18. md.1030 (a) (5) (A) başta olmak üzere 6 farklı suçtan yargılanan Marcus Hutchins ifadesinde, amacının kötü amaçlı bir yazılım yazmak olmadığını ve yalnızca bir hata yapıp kodu başka birine sattığını ve bu kodun sonrasında başka birinin bankacılık trojanını oluşturmak için başka kötü amaçlı yazılıma dahil edildiğini belirtmiş[634] ve yargılama sonucunda mahkeme tarafından WannaCry saldırısını

---

627 SOYASLAN, Doğan, "Ceza Hukuku Özel Hükümler", Yetkin Yayınları, 12. Baskı, Ankara 2018, s. 688; YILMAZ, s. 378.
628 KOCA/ÜZÜLMEZ, s. 915.
629 AKBULUT, s. 358; KOCA/ÜZÜLMEZ, s. 915.
630 KOCA/ÜZÜLMEZ, s. 915.
631 KOCA/ÜZÜLMEZ, s. 915.
632 AKBULUT, s. 358; ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1040.
633 "Küresel Saldırıyı Engelleyen Hacker ABD'de Gözaltına Alındı", https://www.aa.com.tr/tr/dunya/kuresel-siber-saldiriyi-engelleyen-hacker-abdde-gozaltina-alindi/876188, E.T. 25.03.2021.
634 TomorrowUnlocked, "Hacker: Hunter- WannaCry: TheMarcusHutchinsStory- All 3 Chapters", https://www.youtube.com/watch?v=vveLaA-z3-o&t=10s, 2019, (13:32 - 14:50), E.T. 25.03.2021.

durdurmayı başaran Marcus'un toplum için tehdit oluşturmadığını belirterek Marcus'un WannaCry saldırısındaki katkılarından dolayı serbest bırakılmasına karar verilmiştir[635]. Söz konusu olayda hacker Marcus, ABD yasalarına göre kötü amaçlı yazılım ürettiği gerekçesiyle yargılanmışsa da başka bir fidye yazılım saldırısını durdurduğu için serbest bırakılmıştır. Türk Ceza Hukuk sistemi açısından bu olay değerlendirildiğinde ise Marcus Hutchins'in imal ettiği, ithal ettiği sevk ettiği, naklettiği, depoladığı, kabul ettiği, satışa arz ettiği, satın aldığı, başkalarına verdiği veya bulundurduğu şeyin cihaz, şifre ve sair güvenlik kodu olduğunu bilmesi gerekip ayrıca bu filleri bilişim alanında suçlar bölümünde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçları işlemek amacıyla oluşturması gerektiğinden sırf bu nitelikte cihaz veya programların oluşturulması Türk Ceza Kanuna göre suç oluşturmadığından Marcus Hutchins'in eylemi TCK'ya göre cezalandırılması mümkün olmayacaktı.

Bu suç için hangi hukuka uygunluk nedenlerinin olduğu konusunda doktrinde farklı görüşler mevcuttur. Bazı yazarlara göre bu suç için hukuka uygunluk nedeni bulunmamaktadır[636]. Bazı yazarlara göre bu suç için TCK md. 24/1 'de yer alan kanun hükmünün yerine getirilmesi ve TCK md 25/2' de yer alan ilgilinin rızası olmak üzere iki tane hukuka uygunluk nedeni vardır[637]. Bazı yazarlara göre ise ilgilinin rızası kişinin mutlak şekilde tasarruf edebileceği hak üzerinde bulunacağından bu suç için ilgilinin rızası hukuka uygunluk nedeni kabul edilemeyecek olup görevin ifası ve hakkın kullanılması hallerinde hukuka uygunluk nedenlerinin varlığından bahsedilecektir[638].

Fidye yazılımları ise zararlı bir yazılım olmakla birlikte (Penetration) sızma testiyle sistem üzerindeki güvenlik açıklarının kontrolü amacıyla oluşturulan yazılım programların varlığı halinde ilgilinin rızasından bahsedileceğinden yasak cihaz veya programlar suçu oluşmayacaktır.

Suç sırf hareket suçu olup seçimlik hareketlerden birinin yapılması suç gerçekleşeceğinden teorik olarak hareketlerin kısımlara bölünebildiği hallerde suça teşebbüsten söz edilebilir[639]. Örneğin fail fidye yazılımının cihaz veya programın

635 Tomorrow Unlocked, (20:56 – 23:25)
636 YILMAZ, s. 378.
637 ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1039- 1040.
638 AKBULUT, s. 358
639 KOCA/ÜZÜLMEZ, s. 915.

imalatına başlamakla beraber cihaz veya programın üretimini tamamlayamadan yakalanırsa suç teşebbüs aşamasında kalmış olacaktır[640]. Suç iştirak bakımından herhangi bir özellik göstermemekte olup fidye yazılımının kullanıldığı saldırılarda TCK'nın md.37- md.40 maddelerinde düzenlenen iştirake ilişkin genel hükümler uygulanacaktır[641].

Suç zincirleme suç şeklinde işlenebilir[642]. Bu suç hazırlık hareketi niteliğindeki filleri cezalandırdığından failin gerek amaçladığı suç açısından gerekse de TCK md. 245/A 'da düzenlenen suç açısından ayrı ayrı cezalandırılmaları gerekecektir[643]. Ayrıca TCK 245/A maddesinde yer alan suç özel ve ayrı bir düzenleme olduğundan TCK'nın 244. maddesinde düzenlenen fikri içtima hükümleri uygulanmayarak iki ayrı suç varmış gibi hareket edilip ayrı ayrı suçlardan ceza verilmelidir[644]. Yine içtima ilişkisi bakımından FSEK'nın 72. Maddesinde düzenlenen suç ile Elektronik İmza Kanunun 16. Maddesinde düzenlenen suç, TCK md. 245/A'ya göre özel hüküm niteliğinde olduğundan bu suçların varlığı halinde TCK md. 245/A maddesi uygulama alanı bulmayacaktır[645].

Fidye zararlı yazılımı saldırıları açısından da yasak cihaz veya programlar suçu özel ve ayrı bir düzenleme olduğundan TCK'nın 244. maddesinde düzenlenen fikri içtima hükümleri uygulanmayarak faile amaçladığı ve TCK md. 245/A 'da düzenlenen suç açısından ayrı ayrı ceza verilecektir

TCK'da 245/A maddesinde düzenlenen suçu işleyenler hakkında bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası öngörülmüştür. Kanun koyucu tarafından genellikle ekonomik kazancın elde edildiği suçlarda hapis ve adli para cezası birlikte öngörüldüğünden TCK'da 245/A maddesinde düzenlenen suç açısından da kanun koyucu ekonomik kazancın sağlandığını kabul ederek hapis cezası ve adli para cezasının birlikte verilmesini öngörmüştür[646]. Adli para cezasının alt sınırı TCK md. 52/1 gereğince beş gün olarak kabul edilecektir[647].Fidye zararlı yazılımı kullanılarak

---

640 AKBULUT, s. 360.
641 YILM AZ, s. 379; KOCA/ÜZÜLMEZ, s. 915.
642 YILMAZ, s. 380; AKBULUT, s. 360.
643 KOCA/ÜZÜLMEZ, s. 916.
644 YILMAZ, s. 379.
645 AKBULUT, s. 361; KOCA/ÜZÜLMEZ, s. 916.
646 AKBULUT, s. 362; KOCA/ÜZÜLMEZ, s. 916.
647 YILMAZ, s. 380.

işlenebilecek yasak cihaz veya programlar suçu bakımından saldırganlar suçta ve cezada kanunilik ilkesi gereğince aynı ceza ile cezalandırılacaktır. Lehine haksız yarar sağlanan kişinin tüzel kişi olması durumda ise TCK'nın 246. maddesi gereğince tüzel kişilere özgü güvenlik tedbiri uygulanacaktır[648].

TCK'da 245/A maddesinde düzenlenen suçun soruşturma ve kovuşturması re'sen yapılmaktadır[649]. Suç sırf hareket suçu olduğundan hareketin kısmen veya tamamen gerçekleştirildiği mahkeme yetkili mahkeme olacaktır[650]

Hâkimler Ve Savcılar Kurulu'nun 25.11.2021 tarih ve 1229 sayılı kararı ile bilişim suçlarına bakmakla görevli ihtisas mahkemeleri kurulmuştur. Fidye zararlı yazılımı kullanılarak işlenebilecek yasak cihaz veya programlar suçu bir bilişim sistemi aracılığıyla işlendiğinden Hâkimler Ve Savcılar Kurulu'nun 25.11.2021 tarih ve 1229 sayılı kararı ile görevli mahkeme 15 Aralık 2021 tarihi itibariyle uzman asliye ceza bilişim mahkemeleri olacaktır.Suç uzlaştırma kapsamında olmamakla birlikte 5271 sayılı CMK'nın ek 24/11/2016-6763/34 maddesine eklenen hükümle mağduru veya suçtan zarar görenin gerçek veya özel hukuk tüzel kişisi olması şartıyla suça sürüklenen çocuklar bakımından üst sınırı üç yılı geçmeyen TCK'nın 245/ A maddesi uzlaşma kapsamına alınmıştır.

3.7. Yağma

Fidye zararlı yazılımı saldırılarında gerçekleştirilen hukuka aykırı eylemler siber yağma olarak da adlandırılmaktadır. Zira fidye yazılımı saldırılarında esasen mağdur gasp edilmekte ve fail bunu bir bilişim sistemi üzerinden gerçekleştirmektedir. Bu anlamda fidye zararlı yazılımlarını yağma suçu açısından incelemek faydalı olacaktır. Şöyle ki; Yağma suçu 5237 sayılı TCK'nın "Malvarlığına Karşı Suçlar" başlıklı ikinci kısmının onuncu bölümünde düzenlenmiştir. TCK' nın 148. maddesinde basit hâli, 149. maddesinde nitelikli hâli ve 150. maddesinde daha az cezayı gerektiren hâller başlığı altında düzenlenmiştir.

Buna göre basit yağma suçu TCK'nın 148. maddesinde;

---

[648] AKBULUT, s. 362.
[649] KOCA/ÜZÜLMEZ, s. 916.
[650] AKBULUT, s. 362.

(1) Bir başkasını, kendisinin veya yakınının hayatına, vücut ve cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğinden ya da malvarlığı itibariyle büyük bir zarara uğratacağından bahisle tehdit ederek veya cebir kullanarak, bir malı teslime veya malın alınmamasına karşı koymamaya mecbur kılan kişi, altı yıldan on yıla kadar hapis cezası ile cezalandırılır.

(2) Cebir ve tehdit kullanılarak mağdurun, kendisini veya başkasını borç altına sokabilecek bir senedi veya var olan bir senedi hükümsüz kaldığını açıklayan bir vesikayı vermeye, böyle bir senedin alınmasına karşı koymamaya, ileride böyle bir senet haline getirilebilecek bir kâğıdı imzalamaya veya varolan bir senedi imha etmeye veya imhasına karşı koymamaya mecbur edilmesi halinde aynı ceza verilir.

(3) *Mağdurun, herhangi bir vasıta ile kendisini bilmeyecek ve savunulamayacak hale getirilmesi de yağma suçunda cebir sayılır*." şeklinde düzenlenmiştir.

Yağma suçunun nitelikli hali ise TCK'nın 149. maddesinde;

"(1) Yağma suçunun;

a) Silahla,

b) Kişinin kendisini tanınmayacak bir hale koyması suretiyle,

c) Birden fazla kişi tarafından birlikte,

d) Yol kesmek suretiyle ya da konutta, işyerinde veya bunların eklentilerinde,

e) Beden veya ruh bakımından kendisini savunmayacak durumda bulunan kişiye karşı,

f) Var olan veya var sayılan suç örgütlerinin oluşturdukları korkutucu güçten yararlanılarak

g) Suç örgütüne yarar sağlamak maksadıyla,

h) Gece vaktinde işlenmesi halinde, fail hakkında on beş yıla kadar hapis cezasına hükmolunur.

(3) *Yağma suçunun işlenmesi sırasında kasten yaralama suçunun neticesi sebebiyle ağırlaşmış hallerinin gerçekleşmesi durumunda, ayrıca kasten yaralama suçuna ilişkin hükümler uygulanır"* şeklinde düzenlenmiştir.

Yağma suçunun daha az cezayı gerektiren hali ise 150. maddede;

(1) Kişinin bir hukuki ilişkiye dayanan alacağını tahsil amacıyla tehdit ve cebir kullanması halinde, ancak tehdit ve kasten yaralama suçuna ilişkin hükümler uygulanır.

(2) *Yağma suçunun konusunu oluşturan malın değerinin azlığı nedeniyle, verilecek ceza üçte birden yarıya kadar indirilebilir"* şeklinde düzenlenmiştir.

Uygulamada genellikle gasp terimi olarak kullanılan yağma suçu, ceza hukuku anlamında kişilere karşı cebir veya tehdit kullanarak mallarının alınması anlamına gelmektedir[651] . Eski Türk Ceza Kanun'unda da "gasp" olarak ifade edilen yağma aslında cebir veya tehdit kullanılarak yapılan bir hırsızlık suçudur[652]. Yağma suçunu hırsızlık suçundan ayıran en önemli unsur ise kullanılan cebir veya tehdittir[653]. Nitekim öğretide "cebri hırsızlık" şeklinde de adlandırılmaktadır[654]. Yağma suçu, cebir tehdit ve hırsızlık suçlarının bir araya gelmesiyle oluşan bir suç tipi olduğundan suçla korunmak istenen hukuki değerde birden fazladır[655]. Bu kapsamda suçla korunan hukuki değerin kişinin hürriyeti, vücut dokunulmazlığı, zilyetliği ve mülkiyeti olduğu söylenebilir[656]. Ancak suç malvarlığına karşı işlenen suçlar bölümünde düzenlendiğinden ağırlıklı olarak mülkiyet hakkının korunmak istendiği ifade edilebilir[657].

Fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırıların yağma suçuna konu olup olmayacağını değerlendirirken ise temelde 2 hususa değinmek gerekecektir. Öncelikle fidye yazılımı saldırılarındaki verilerin erişilmez kılınması tehdidinin mağdurun malvarlığı açısından büyük bir zarar oluşturup oluşturmayacağı ele alınmalı, ardından fidye yazılımlarında fidye ödeme yöntemi olarak kullanılan kripto paraların bir malı teslime veya malın alınmamasına karşı koymama kapsamında mal olarak kabul edilip edilemeyeceği değerlendirilmelidir[658].

---

651 AYDIN, Devrim, Türk Ceza Hukukunda Yağma Suçu, Yetkin Yayınları, 1. Baskı, Ankara 2020, s. 18.

652 Türkiye Adalet Akademisi, ALTUĞ, Şahin (Editör), Yargıtay Ceza Daireleri Uygulamasında Sıklıkla Rastlanan Bozma Sebepleri, Ankara Açık Ceza İnfaz Kurumu İş yurdu Müdürlüğü Matbaası, 2. Baskı, Ankara 2018, s. 664.

653 Türkiye Adalet Akademisi, s. 664.

654 NOYAN, Erdal, Hırsızlık Suçları, Adalet Yayınevi, 2. Baskı, Ankara 2007, s. 421.

655 ARSLANTÜRK, s. 37.

656 ARSLANTÜRK, s. 37.

657 M.DİNÇ, RUHİ, "*Türk Ceza Kanunu'nda Yağma Suçu"*, s. 88.

658 DEĞİRMENCİ, Olgun, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi",* s. 195.

Malvarlığı, maddi değeri olan, para ile ölçülebilen ve başkalarına devredilebilen tüm hak ve borçları ifade etmekte birlikte ceza hukuku kapsamında daha geniş bir yelpazede kullanılmaktadır [659]. Yine TCK md. 148'de belirtilen tehdidin büyük bir zarara uğratacak nitelik ve ağırlıkta olması gerekmektedir[660]. Fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılarda fail mağdurun bilişim sistemindeki dosya ve klasörlerini şifreleyerek erişimsiz hale getirmekle tehdit etmektedir. Bilişim sistemindeki veriler malvarlığı değeri olarak kabul edilebilmektedir[661]. Fidye yazılımı saldırılarında erişimsiz kılmakla tehdit edilen veriler mağdur için "malvarlığı açısından büyük bir zarar" oluşturabilecektir[662]. Zira hastane, belediye ve üniversitelere gerçekleştirilen fidye yazılımı saldırılarında saldırıya uğrayan şirketlerin saldırı nedeniyle hizmet verememekten kaynaklı zarara uğraması malvarlığı açısından büyük bir zarara neden olmaktadır. Nitekim Almanya Düesseldorf Üniversitesi Kliniğine fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırıda hastanenin sağlık hizmetleri sekteye uğradığından yetkililer hastaya müdahale edemedikleri için bir kişi hayatını kaybetmiştir. Yine Şili'nin tek kamu bankası olan Banko Estado'nın veri ve bilgisayar sistemlerine karşı gerçekleştirilen fidye yazılımı saldırısında banka ülkedeki bütün işlemlerini durdurmak zorunda kalarak milyonlarca zarara uğramıştır. Görüleceği üzere verilere erişim sağlayamama kişilerin yaşam bütünlüklerini tehlikeye attığı gibi malvarlığı itibariyle büyük bir zarara da uğratılmaktadır.

Yağma suçunun konusunu "mal" oluşturmaktadır. Suçun tanımında malın taşınabilir olduğuna ilişkin bir ifade yer almasa da doktrinde ve 5237 sayılı TCK'nın gerekçesinde malın taşınılabilir olduğu kabul edilmektedir[663]. Yağma suçunda kastedilen mal ile "*üzerinde ayni ve şahsi haklar kurulabilen tüm haklar*" anlaşılmalıdır[664]. Manevi değer taşıyan şeyler de suçun konusunu oluşturmakla birlikte somutlaştırılmamış şeyler suçun konusunu oluşturmamaktadır[665]. Fidye zararlı yazılımı kullanılarak gerçekleştirilen

---

659 S. BAKLACI, Sevim, Yağma Suçu, Yaşar Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İzmir 2020, s. 12.

660 S. BAKLACI, s. 45.

661 DEĞİRMENCİ, Olgun, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi",* s. 195.

662 DEĞİRMENCİ, Olgun, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi",* s. 195.

663 NOYAN, s. 432.

664 ARSLANTÜRK, Mustafa, İcrasından İnfazına Bütün Yönleriyle Yağma Suçu, Adalet Yayınevi, 3. Baskı, Ankara 2021, s. 45

665 ARSLANTÜRK, s. 46.

saldırılarda fidye ödemesi olarak kabul edilen kripto paralar bu kapsamda ekonomik bir değere sahip olmakla birlikte kripto paraların maddi bir varlık olup olmadığı irdelenmelidir[666]. Kripto paralar bilişim sistemi üzerinde tutulan veri parçaları online ve offline olarak bulunabilmektedir[667]. Offline olarak kripto paranın tutulması halinde bir maldan bahsedilecek ve fail kripto parayı teslime zorlaması halinde fidye yazılımları yağma suçunun konusunu oluşturabilecektir[668].

Suçun faili cebir ve tehdit kullanarak taşınır malı alan gerçek kişidir[669]. Dolayısıyla suçun faili herkes olabilecektir. Fidye zararlı yazılımı kullanılarak işlenebilecek yağma suçunun faili herkes olabilmektedir. Zira kanun koyucu herhangi bir ayrıma gitmemiştir

Bu suçun mağduru zilyet olduğu taşınır malı elinden cebir veya tehditle alınan kişidir. Dolayısıyla suçun mağduru herkes olabilir[670].Suç tanımında cebir veya tehdidin kullanılması gibi birden fazla harekete yer verildiğinden seçimlik hareketli bir suçtur.

Suç kasten işlenebilecek bir suç olup taksirle işlenmesi mümkün değildir. Suçun oluşması için kanunda özel bir amaç aranmadığından genel kast yeterli olacaktır[671]. Dolayısıyla fidye zararlı yazılımı kullanılarak işlenebilecek yağma suçunu da taksirle işlenmesi mümkün olmayacaktır

Cebir veya tehdit kullanmak suretiyle hırsızlık suçundan ayrılan yağma suçunda hırsızlık suçunun aksine suçun tamamlanması için failin taşınır mal üzerindeki tasarrufun varlığı aranmamakta olup taşınır malı almış olması yeterli görülmektedir[672]. Zira yağma suçunda mağdur failin cebir veya tehdidinden dolayı zilyetliğinden çıkmasına engel olamamaktadır[673]. Bu bakımdan yağma suçu sırf hareket suçu olup taşınır mal zilyedin tasarrufundan çıkınca tamamlanmış olacağından normal şartlarda

---

666 DEĞİRMENCİ, Olgun, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi",* s. 197.
667 DEĞİRMENCİ, Olgun, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi",* s. 197.
668 DEĞİRMENCİ, Olgun, "*Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi",* s. 197.
669 NOYAN, s. 431.
670 M.DİNÇ, RUHİ, "*Türk Ceza Kanununda Yağma Suçu"*, s. 88.
671 NOYAN, s. 435.
672 NOYAN, s. 440.
673 NOYAN, s. 440.

suça teşebbüs mümkün olmayacaktır[674]. Ancak fail cebir veya tehdit kullandığı halde mal failin zilyetliğine geçemediği durumlarda suç teşebbüs aşamasında kalacaktır[675].

Yağma suçunda zilyetliği başkasına ait olan bir taşınır malın zilyedin rızası olmadan cebir veya tehdit kullanılarak alınması söz konusu olduğundan burada bahsedilen zilyetliğin hukuka uygun olması zorunlu değildir[676]. Dolayısıyla fidye yazılımı saldırılarında failin hukuka aykırı bir şekilde erişim sağladığı bilişim sistemi üzerinde zilyetliğinden bahsedilebilecektir.

Konumuz bakımından fidye zararlı yazılımları kullanılarak işlenebilecek yağma suçunun nitelikli hali olarak işlenmesi en muhtemel suç örgütüne yarar sağlamak maksadıyla işlenmesi olacaktır. Nitekim fidye yazılımları saldırılarını gerçekleştiren kişiler örgüt üyesi mensubu olmaktadırlar ve elde ettikleri haksız kazancı örgütleri için kullanmaktadırlar. Revil, NetWalker, Egregor gibi fidye yazılım hacker grupları başlı başına bir örgüttür. Dolayısıyla fidye zararlı yazılımları kullanılaraksuç örgütüne yarar sağlamak maksadıyla yağma suçunun işlenmesi halinde failler hakkında on beş yıla kadar hapis cezasına hükmolunacaktır.

Fidye zararlı yazılımları kullanılarak işlenebilecek yağma suçunda failin bir hukuki ilişkiye dayanan alacağını tahsil etmek amacıyla fidye yazılımı kullanarak yağma suçunu gerçekleştirmesi halinde, ancak tehdit suçuna ilişkin hükümler uygulanabilecektir. Fakat suçun daha az cezayı gerektiren ikinci fıkranın gerçekleşmesi pek mümkün görünmemektedir. Malın değerinin azlığının belirlenmesinde bir kıstas öngörülmemiş olup oluşan her somut olaya göre değerlendirme yapılması gerekecektir[677]. Dolayısıyla fidye yazılımı saldırılarında hacker'ların hedef sistemli saldırılar düzenlemesi ve fidye ödeme aracı olarak kripto paralar kullanıyor olması suçun konusunu oluşturan malın değerinin azlığı şartını oluşturmayacak ve suçun daha az ceza gerektiren halinden bahsedilemeyecektir.

TCK md. 43/3 'de suçun zincirleme suç şeklinde işlenmeyeceği özellikle belirtildiğinden zincirleme suç hükümleri uygulanamayacak olup mağdura karşı yapılan

---

674 M.DİNÇ, RUHİ, "*Türk Ceza Kanununda Yağma Suçu,"*s. 91.

675 M.DİNÇ, RUHİ, "*Türk Ceza Kanununda Yağma Suçu"*, s. 91

676 ARSLANTÜRK, s. 46.

677 M. DİNÇ, Yasemin, RUHİ, M.EMİN, "*Türk Ceza Kanununda Yağma Suçu*", Erzincan Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, C. 11, S. 2, 2018, s. 96, https://dergipark.org.tr/tr/download/article-file/614261, E.T. 25.03.2022.

her fiil yağma suçunu oluşturacaktır. İştirakin her türlüsü mümkün olup fidye zararlı yazılımı kullanılarak işlenebilecek yağma suçunda bakımından da iştirake ilişkin genel hükümler uygulanacaktır.Konumuz itibariyle fidye zararlı yazılımı kullanılarak işlenebilecek yağma suçunda hukuka uygunluk hallerinin tatbiki mümkün olmadığından hukuka uygunluk sebebi bulunmamaktadır.

Yağma suçunun soruşturma ve kovuşturması re'sen yapılmaktadır. Suç sırf hareket suçu olduğundan hareketin kısmen veya tamamen gerçekleştirildiği mahkeme yetkili mahkeme olacaktır. Suç re'sen soruşturulan bir suç olup Ceza Muhakemeleri Kanun'unun 253. maddesinde sayılan suçlardan olmadığından uzlaşma kapsamında değildir[678].

Yağma suçunun basit halini işleyenler hakkında altı yıldan on yıla kadar hapis cezası ön görülmüştür. Yağma suçunun nitelikli halini işleyen fail hakkında ise on beş yıla kadar hapis cezasına hükmolunacaktır. Terörle Mücadele Kanun'un Terör Amacıyla İşlenen Suçlar başlıklı 4. maddesine göre yağma suçu, suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti kapsamında işlendiği takdirde terör suçu olarak kabul edilip verilecek ceza yarı oranında arttırılacağından fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırıların terör örgütünün faaliyeti çerçevesinde işlenmesi halinde eylem terör suçu sayılacak faile verilecek ceza yarı oranında arttırılacaktır. Ayrıca yağma suçunun konusunu oluşturan malın değerinin azlığı nedeniyle, verilecek ceza üçte birden yarıya kadar indirilebilecektir. Fidye yazılımı kullanılarak işlenebilecek yağma suçu bakımından saldırganlar suçta ve cezada kanunilik ilkesi gereğince aynı ceza ile cezalandırılacaktır. Lehine haksız yarar sağlanan kişinin tüzel kişi olması durumda ise TCK'nın 246. maddesi gereğince tüzel kişilere özgü güvenlik tedbiri uygulanacaktır

Hâkimler Ve Savcılar Kurulu'nun 25.11.2021 tarih ve 1229 sayılı kararı ile bilişim suçlarına bakmakla görevli ihtisas mahkemeleri kurulmuştur. Fidye yazılımı saldırılarında yağma suçu bir bilişim sistemi aracılığıyla işleneceğinden Hâkimler Ve Savcılar Kurulu'nun 25.11.2021 tarih ve 1229 sayılı kararı ile görevli mahkeme 15 Aralık 2021 tarihi itibariyle uzman asliye ceza bilişim mahkemeleri olacaktır.

[678]M.DİNÇ, RUHİ, ""*Türk Ceza Kanununda Yağma Suçu"*, s. 98.

4. DÜNYA'DA FİDYE ZARARLI YAZILIMI SALDIRILARI, AMERİKA BİRLEŞİK DEVLETLERİNDE FİDYE ZARARLI YAZILIMI SALDIRILARINA KARŞI ALINAN TEDBİRLER VE TÜRK CEZA HUKUKUNDA YAPILMASI ÖNERİLEN DEĞİŞİKLİKLER

4.1. Genel Olarak

Son zamanlarda gittikçe artan fidye zararlı yazılımı saldırıları gelecekte öngörülen kötü senaryolar durumun ne kadar ciddi olduğunu ortaya koymaktadır. Fidye yazılımları ilk olarak 2017 yılında WannaCry saldırısı ile küresel çapta etkisini doğurmuş ve bu durum 2021 yılında küresel alanını daha da genişleterek etkisini artırmaya devam etmiştir. İnternet ve teknolojinin merkezi sayılan ABD bundan en fazla etkilenen ülke olmuştur. Dolayısıyla da bu saldırılara karşı önlemlerini alan ülkelerden de biri olmuştur.

Fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılarda dünyada ilk 5 sırada yer alan Türkiye hala fidye yazılım saldırılarına karşı önlem almaya başlamamıştır. Konunun yargıya intikal etmemesi kurbanların saldırganlara fidye taleplerini ödedikleri sonucunu doğurmaktadır. Yine KVKK'nın resmi sitesinde yayınlanan veri ihlallerinde birçok şirketin fidye yazılımı saldırısına maruz kaldığı gerçeğini ortaya çıkarmaktadır.

Bu bölümde, şimdiye kadar yapılan açıklamalar ışığında dünyada gerçekleştirilen fidye yazılımı saldırılarına ve ABD'de alınan önlem ve tedbirlere yer verilerek Türk Ceza hukuk sisteminde fidye yazılımı saldırılarına karşı yapılması önerilen değişiklikler anlatılacaktır.

4.2. Dünya'da Fidye Yazılımı Saldırıları

4.2.1. Grubman Shire Meiselas & Sack Hukuk Bürosu

Lady Gaga, Madonna, MariahCarey, Christina Aquilera, Bruce Springstean ve Nicki Minaj'ın da müvekkil olarak bulunduğu Grubman Shire Meiselas & Sack Hukuk Bürosu geçtiğimiz yıl Revil hacker grubu tarafından fidye yazılım saldırısına uğramıştı[679]. Saldırıda birçok ünlünün de yer aldığı 756 GB boyutundaki kişisel verileri

[679] "Fidyeci Hackerler Ünlü İsimlerin Bilgilerini Çaldı", https://www.sonhaberler.com/fidyeci-hackerlar-unlu-isimlerin-bilgilerini-caldi-haber-810745, E.T. 11.04. 2021.

ele geçirilerek 42 Milyon dolar fidye talep edilmiş ve saldırganlar fidyenin ödenmemesi halinde ele geçirdikleri verileri açık arttırma usulü ile satacaklarını açıklamışlardı[680].

4.2.2. Transform Hospital Group

2020 yılının Aralık ayında fidye yazılım çetesi olarak bilinen REvil hacker grubu İngiltere'deki birçok ünlü oyuncu ve sanatçılarında bulunduğu Transform Hospital Group'a fidye yazılım saldırısı gerçekleştirmiş, darknet web sayfasında "*müşterilerin samimi fotoğraflarının tamamen hoş bir manzara olmadığını* "söyleyerek basına sızdırmakla tehdit etmiş ve yüklü miktarda bitcoin talep etmişlerdi[681].

4.2.3. Pakistan Enerji Tedarik Şirketi

Geçtiğimiz ocak ayında Pakistan'ın enerji tedarik şirketine yapılan fidye yazılım saldırısında Pakistan tarihin en büyük elektrik kesintisini yaşamış ve hacker'ler tarafından 7, 7 milyon değerinde bitcoin talep edilerek ödenmediği takdirde şirketin hassas verilerini yayınlamakla tehdit etmişlerdi[682].

4.2.4. California Üniversitesi

1 Haziran 2020 tarihinde Netwalker hacker grubu California Üniversitesine fidye yazılım saldırısı gerçekleştirmiş ve hacker'ler üniversitenin verilerini şifreleyerek hasta kayıtları karşılığında 1, 14 milyon dolar talep etmişlerdi[683].

4.2.5. Brno Üniversite Hastanesi

12 Mart 2020 tarihinde Çek Cumhuriyetinin en büyük COVID-19 hastanesi olan Brno Üniversite hastanesine fidye yazılım saldırısı gerçekleştirilmiş ve hastane yaşanılan

---

680 "Siber Saldırganlar 42 Milyon Dolar Fidye İstiyor", http://blog.isr.com.tr/2020/06/siber-guvenlik-bulteni-mays-2020.html, E.T. 11.04. 2021.

681 https://www.1mh.org/bilgisayar-korsanlari-estetik-ameliyat-fotograflarini-sizdirmakla-tehdit-ediyor/, E.T. 15.01.2021.

682 https://muhabbit.com/pakistanin-en-buyuk-guc-saglayicisi-netwalker-tarafindan-hacklendi/, 01.01.2021.

683 BAYLANÇİÇEK, Berk, "*Kaliforniya Üniversitesi Hackerlara 1. 14 Milyon Dolar Fidye Ödediğini Açıkladı*", https://www.webtekno.com/kaliforniya-universitesi-hackerlara-fidye-odedi-h95936.html, E.T. 25.01.2021.

aksaklık nedeniyle birçok ameliyatı iptal ederek hastalarını başka bir hastaneye sevk etmek zorunda kalmıştı[684].

4.2.6. Almanya Düesseldorf Üniversite Hastanesi

10 Eylül 2020 tarihinde Almanya'nın Düsseldorf Üniversitesi Kliniğine gerçekleştirilen fidye yazılım saldırısında hastanenin sağlık hizmetleri sekteye uğramış ve hastane yetkilileri hastaya müdahale edemedikleri için bir kişi hayatını kaybetmişti[685].

4.2.7. BancoEstado

7 Eylül 2020 tarihinde Şili'nin tek kamu bankası olan Banko Estado'nın bankan veri ve bilgisayar sistemlerine karşı Revil hacker grubu tarafından gerçekleştirilen fidye yazılım saldırısı sonucunda banka ülkedeki bütün işlemlerini durdurmak zorunda kalmıştı[686].

4.2.8. İsrail Sigorta Şirketi Shirtbit

İsrail'de Black Shadow isimli hacker grubu İsrailli sigorta şirketi Shirtbit'e fidye yazılım saldırısı gerçekleştirerek müşterilerin verilerini çalıp bunların ekran görüntüsünü bir forumda paylaşarak şirketi 1 milyon dolar zarara uğratmıştı[687].

4.2.9. New Orleans Belediyesi

ABD'de 13 Aralık 2019 tarihinde hacker'ler New Orleans belediyesine fidye yazılım saldırısı gerçekleştirerek belediyeyi 7 milyon dolar zarara uğratmıştı[688]

---

684 https://www.healthcareitnews.com/news/emea/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak, E.T 15.01.2021.

685 https://www.yenisafak.com/teknoloji/fidye-yazilimi-ilk-defa-bir-olume-neden-oldu-3568434, E.T. 05.01.2021.

686 "Fidye Saldırısından Sonra Ünlü Banka Tüm Şubelerini Kapattı", https://tr.investing.com/news/crypto currency-news/fidye-saldrsndan-sonra-nlu-banka-tum-ubelerini-kapatt-2006411, E.T. 12.12.2020.

687 https://www.star.com.tr/dunya/musteri-verileri-sizdirildi-israilli-sirketten-fidye-istiyorlar-haber-1592037/, 25.03.2021

688 ROBİNSON, Teri, "RansomwareAttackCost New Orleans $7 MillionAndCounting", https://zephyrnet.com/tr/ransomware-attack-cost-new-orleans-7-million-and-counting/, 25. 03. 2021.

4.2.10. Dax- Cote'dArgent

Fransa'da 8 Şubat 2021 tarihinde hacker'lerDax – Coted'Argent hastanesine fidye yazılım saldırısı gerçekleştirerek hastane hizmetlerinin büyük ölçüde aksamasına neden olmuştu[689].

4.2.11. Washington DC Metropolitian Polis Departmanı

ABD'de geçtiğimiz aylarda Babuk isimli hacker grubu Washington DC Metropolitian Polis Departmanına fidye yazılım saldırısı gerçekleştirerek polis merkezine ait 250 GB boyutunda veriyi ele geçirip bu verilerin ekran görüntülerini DeepWeb'de paylaşmışlardı[690].

4.2.12. İrlanda Sağlık Hizmet Grubu (HSE)

14 Mayıs Cuma günü İrlanda'da sağlık hizmetleri servisi fidye yazılım saldırısına uğrayarak hastane acil servis hizmetleri dışında bütün bilişim sistemlerini kapatmak zorunda kalmış ve saldırı hastanenin işleyişini ciddi oranda yavaşlamasına sebep olmuştu[691].

4.2.13. Yeni Zelanda Sağlık Kuruluşu Waikato

Geçtiğimiz mayıs ayında Yeni Zelanda Waikato bölgesi sağlık kuruluşuna gerçekleştirilen fidye yazılımı saldırısı Yeni Zelanda tarihinin en büyük siber saldırısı olarak kabul edilmiş ve saldırı nedeniyle randevuların tamamı ve ameliyatların birçoğu iptal edilmiş, hasta ve personellerin verileri çalınarak medyaya sızdırılmıştı[692].

---

689 BANNİSTER, Adam, "Dax – Coted'ArgentHospital İn France Hit ByRansomwareAttacak", TheDailySwig, https://portswigger.net/daily-swig/dax-cote-dargent-hospital-in-france-hit-by-ransomware-attack, E.T. 01.03.2021.

690 ÇALIŞKAN, Oğuzhan, Secloot, " Washington DC Polis Departmanı Fidye Yazılımı Saldırısına Uğradı", https://www.secloot.com/washington-dc-polis-departmani-fidye-yazilimi-saldirisina-ugradi/, E.T. 12.05.2021.

691 TRT Haber, "İrlanda Sağlık Servisi Siber Saldırıya Uğradı", https://www.trthaber.com/haber/dunya/irlanda-saglik-servisi-siber-saldiriya-ugradi-580851.html, E. T. 24.06.2021.

692 "Fidye Yazılım Saldırganları Hasta Bilgilerini Sızdırdı", https://www.savunmatr.com/siber-guvenlik/fidye-yazilimi-saldirganlari-hasta-bilgilerini-sizdirdi-h12091.html, E.T. 24.06.2021.

4.2.14. Dünyanın En Büyük Et Üreticisi JBS SA

30 Mayıs 2021 tarihinde Brezilya merkezli dünyanın en büyük et üreticisi olan JBS SA'ya gerçekleştirilen fidye yazılım saldırısında şirket, ülkedeki bilişim sistemlerini askıya alarak üretimleri durdurmuş ve veri kaybı yaşamamak adına 11milyon dolar fidye ödediğini duyurmuştu[693].

4.2.15. ABD Petrol Şirketi ColonialPipeline

7 Mayıs 2021 tarihinde DarkSide isimli hacker grubu ABD'nin en büyük boru hattına fidye yazılımı saldırısı gerçekleştirerek akaryakıt transferlerinin aksamasına sebep olmuş ve şirket yetkilileri daha fazla risk almamak adına 5 milyon dolar tutarında fidye ödediklerinin açıklamışlardı[694].

4.2.16. Daelim – Limak – SK – Yapı Merkezi Ortak Girişimi

27 Nisan 2021 tarihinde KVKK tarafından yapılan veri ihlalleri bildirim duyurusunda DLSY adi ortaklığının 24 Nisan 2021 tarihinde fidye yazılım saldırısına maruz kaldığı ve saldırıda tahmini 20.000 kişiye ait verinin ihlalden etkilendiğini duyurmuştur[695].

4.3. Amerika Birleşik Devletlerinde Fidye Yazılımı Saldırılarına Karşı Alınan Tedbirler

4.3.1. ABD'de Fidye Zararlı Yazılımı Saldırıları

Bilgisayarın anavatanı ve dünyada teknolojinin merkezi olan ABD, teknolojinin ve internetin olumsuz sonucundan en fazla etkilenen ülkelerden biri olmuştur. Özellikle son yılda büyük bir tehdit haline gelen fidye yazılım saldırılarında ciddi anlamda kayıplar yaşamaya başlayan ABD, bu konuda önlemlerini almaya başlamıştır. ABD'de mali bir suç olarak kabul edilen fidye yazılımları petrol şirketi Colonial Pipeline

---

693 "JBS SA Bilgisayar Korsanlarına 11 Milyon Dolar Fidye Ödedi", https://www.trthaber.com/haber/dunya/jbs-sa-bilgisayar-korsanlarina-11-milyon-dolar-fidye-odedi-587730.html, E.T. 24.06.2021.

694 "ABD'li Petrol Şirketi Fidye Ödediğini Doğruladı", https://www.trthaber.com/haber/dunya/abdli-petrol-sirketi-fidye-odedigini-dogruladi-582039.html, E.T. 24.06.2021.

695 Kişisel Verileri Koruma Kurumu, https://www.kvkk.gov.tr/Icerik/6961/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-DLSY-Adi-Ortakligi, E.T. 24.06.2021.

Company'e yapılan saldırı sonrasında jeopolitik sorun haline gelmiş ve nihayetinde 16 haziran2021'deCenevre'de görüşme yapan ABD başkanı Joe Biden ve Rusya Cumhurbaşkanı Vladimir Putin fidye yazılımı saldırılarına karşı işbirliği yapmak üzere anlaşmışlardır[696]. Nitekim yakın bir zaman önce de eski siyah şapkalı hacker Hector Xavier Monsegur'de ABD'ye karşı siber saldırılarının katlanarak daha da artacağını ve ABD'nin bu konuda yetersiz kalacağını dile getirmişti[697] .

4.3.2. Fidye Zararlı Yazılımı Saldırılarına Karşı Alınan Önlemler

4.3.2.1. Fidye Yazılım Kılavuzu

ABD, petrol şirketi Colonial Pipeline Company'e yapılan saldırı sonrasında fidye yazılımı saldırılarını gerçekleştiren hacker'ları terörist olarak kabul etme kararı almıştır[698]. Nitekim saldırı sonrası ülke genelinde savcılıklara gönderilen kılavuzda fidye yazılımına ilişkin soruşturmanın terörizm ile aynı önceliğe sahip olacağı ifadesi yer almıştır[699]. Dolayısıyla ABD'de fidye yazılım saldırıları tıpkı terör suçu gibi öncelik görecek ve bu kapsamda soruşturma yürütülecektir.

4.3.2.2. Avrupa Birliği Ortak Siber Birimi

Avrupa Komisyonu ABD ve İrlanda'da yaşanan fidye yazılımı saldırısından sonra siber saldırıları önlemek için AB ve üye ülkelerin uzmanlarından oluşan ve en geç 30 Haziran 2023' kadar geçmesi amaçlanan "Ortak Siber Birim" kurulmasını içeren teklifini 23 Haziran 2021 tarihinde yayınlamıştır[700]

---

696 "Rusya Kaynaklı Fidye Yazılımı Saldırıları Hakkında Ne Biliniyor?", https://www.amerikaninsesi.com/ a/biden-putin-zirvesindeki-gundem-fidye-yazdilimi/5931043.html, E.T. 24.06.2021.

697 "Eski Siyah Şapkalı Hacker Üyesi: "ABD'ye Yönelik Siber Saldırılar Katlanarak Daha Kötü Bir Hale Gelecek", 20 Haziran 2021, https://www.savunmatr.com/siber-guvenlik/eski-siyah-sapkali-hackerlar-uyesi-abd-ye-yonelik-siber-h12718.html, E.T. 25.06.2021.

698 KILIÇ, Zeynep, "ABD Fidye Yazılım Saldırılarını Terörizmle Eş Tuttu", https://siberbulten.com/diji tal-guvenlik/abdden-fidye-yazilimcilara-terorist-muamelesi/, E.T. 26.06.2021.

699 https://siberbulten.com/dijital-guvenlik/abdden-fidye-yazilimcilara-terorist-muamelesi/, E.T. 26.06.2021.

700 "AB'den Siber Saldırılara Karşı "Ortak Birim" Hareketi, "https://www.savunmatr.com/siber-guvenlik/ab-den-siber-saldirilara-karsi-ortak-birim-hareketi-h12780.html,

4.3.2.3. Başkanlık Kararnamesi

Colonial Pipeline Company'e yapılan fidye yazılımı saldırısından sonra ABD başkanı Joe Biden 12 Mayıs 2021 tarihinde siber güvenliği artırmak için 34 sayfadan oluşan "Siber Güvenlik İnceleme Kurulu" kurulmasını öngören başkanlık kararnamesini imzalamıştır[701]. "Ulusal Siber Güvenliğin Geliştirilmesi" isimli kararname[702] federal hükümet ile özel sektör arasında iletişimi geliştirmek ve ABD'nin siber saldırılara karşı müdahale gücünü artırmak için hazırlanmıştır[703].

4.3.2.4. Fidye Ödemelerini Kolaylaştırmaya Yönelik Olası Yaptırım Riskleri Hakkında Tavsiye

ABD Hazine Bakanlığı 1 Ekim 2020 tarihinde "Fidye Ödemelerini Kolaylaştırmaya Yönelik Olası Yaptırım Riskleri Hakkında Tavsiye" yayınlayarak fidye yazılım saldırısına maruz kalan ve fidye ödeyen kişi veya kurumlara yaptırım uygulanabileceğini hüküm altına almıştır[704].

4.4. Türk Ceza Hukukunda Yapılması Önerilen Değişiklikler

4.4.1. Genel Olarak

Fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırıların son yıllardaki artışı gelecekte daha büyük siber saldırılarının gerçekleşeceği gerçeğini ortaya koymaktadır. 2018 yılında SonıcWall tarafından hazırlanan rapora[705]göre 2017 yılında fidye yazılımların kullanımı %101, 2 oranında artmışken 2021 yılı siber tehdit raporuna göre

---

[701] YILMAZ, Mehmet Sait, "Beyaz Saray, ABD Siber Güvenlik Savunmasını Artırmak İçin Krtik Kararlar Aldı", 14 Mayıs 2021, https://www.cozumpark.com/beyaz-saray-abd-siber-guvenlik-savunmasini-arttirmak-icin-kritik-kararlar-aldi/, E.T. 26.06.2021

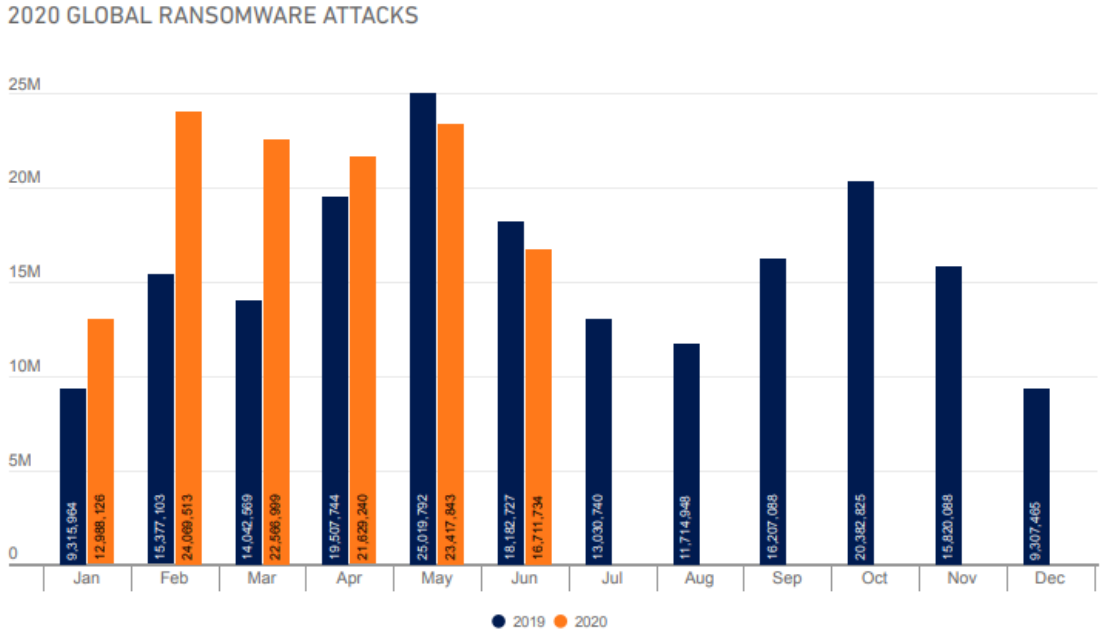
[702] Kararname için bkz: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, E.T. 26.06.2021

[703] "NSA, Biden'ın İmzaladığı Siber Güvenlik Emrinde Önemli Rol Oynayacak", https://www.savunmatr.com/siber-guvenlik/nsa-bidenin-imzaladigi-siber-guvenlik-emrinde-onemli-bir-rol-h12066.html, E.T. 26.06.2021.

[704] https://www.darkreading.com/risk/us-treasurys-ofac-ransomware-advisory-navigating-the-gray-areas/a/d id/1339394, 01.01.2021.

[705] 2018 SonicWall Siber Tehdit Raporu, s. 3, https://www.sonicwalldestek.com/wp-content/uploads/2018/ 04/2018-Sonicwall-siber-tehdit-raporu-TR.pdf, E.T. 07.03.2021

ise bu oran 2020 yılında 2019 yılına kıyasla %62 oranında artmıştır[706]. SonıcWall tarafından yapılan araştırmaya göre hukuki yaptırımlar siber saldırıların çeşitlenmesinde ve başarılarında düşüş sağlamaktadır[707]. Türkiye'nin fidye yazılımı saldırılarına uğrayan ülkeler arasında ilk sırada gelmesi ve bu saldırıların gücü karşısında hukuki yaptırımların etkili olabilmesi nedeniyle birtakım önlemler alınması gerekmektedir.



Şekil 4. 2020 Yılı Global Fidye Yazılımı Saldırı İstatistikleri

4.4.2. Fidye Zararlı Yazılımı Saldırıları İstatistiklerinde Türkiye

Siber saldırıların son yıllardaki sayılarında ciddi artış diğer ülkelerde olduğu gibi Türkiye içinde büyük sorun ve tehdit oluşturmaktadır. Saldırganların fidye ödeme yöntemi olarak bitcoin gibi kripto paralar talep etmesi tespit edilmelerini zorlaştırmaktadır. Son araştırmalara göre Türk şirketleri fidye yazılımlarından büyük

[706] 2020 yılı fidye yazılım saldırı istatistikleri tablosu için bkz: Sonicwall, 2020 SonicwallCyberThreat Report, July 2020, s. 17, https://www.sonicwall.com/resources/2020-cyber-threat-report-mid-year-update-pdf/, E.T. 01.07.2021.

[707] SonicWall Siber Tehdit Raporu, s. 10, https://www.sonicwalldestek.com/wp-content/uploads/2018/04/2018-Sonicwall-siber-tehdit-raporu-TR.pdf, E.T. 07.07.2021

kayıplar yaşamakta ve çareyi fidye miktarlarını ödemekte bulmaktadırlar[708]. Türkiye özellikle 2020 yılında fidye yazılımı saldırıları çok daha fazla maruz kalmıştır. Nitekim siber güvenlik araştırma şirketleri tarafından yapılan araştırma ve istatistikler bu durumu göz önüne sermektedir. Şöyle ki;

Dünyaca ünlü küresel çözümler sağlayıcısı Trend Micro'nun veri güvenliği olaylarını araştırdığı 2020 yılı haziran ayı küresel siber tehdit raporuna göre Türkiye dünyada en fazla fidye yazılım saldırısına uğrayan birinci sıradaki ülke olmuştur[709]. Rapora göre haziran ayında tespit edilen fidye yazılım saldırılarının %26.4'ü Türkiye'de gerçekleşti.

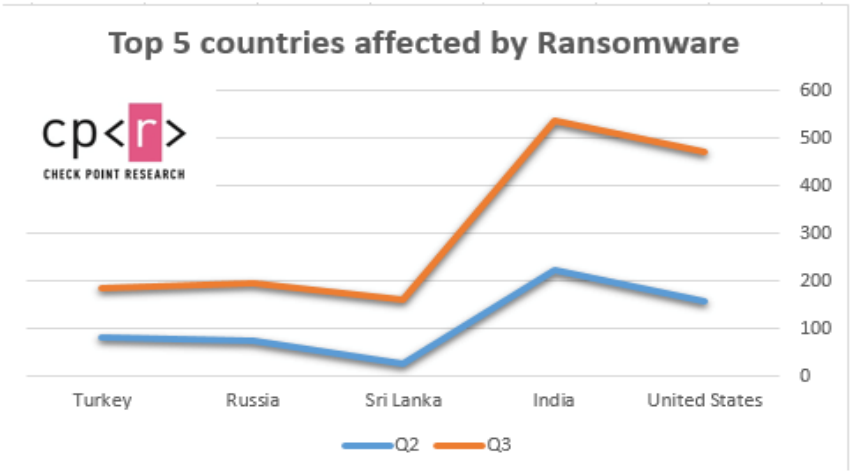
Şekil 5. Trend Micro2020 Yılı Haziran Ayı Küresel Siber Tehdit Raporu Mayıs ve Haziran Aylarında En Fazla Fidye Yazılımı Saldırısına Maruz Kalan Ülkeler

Check Point Software şirketinin küresel fidye yazılım saldırıları araştırmasına göre 2020 yılında Türkiye fidye yazılım saldırılarına maruz kalan ilk 5 ülkeden biri olmuştur[710] .

[708] "Türk Şirketleri Artan Fidye Yazılımı Saldırıları Nedeniyle Büyük Maddi Kayıplar Yaşıyor", 22 Haziran 2021, https://bitdefender.com.tr/turk-sirketleri-artan-fidye-yazilimi-saldirilari-nedeniyle-buyuk-maddi-kayiplar-yasiyor/, E.T. 07.07.2021.

[709] Trend Micro Haziran ayı küresel siber saldırı raporu istatistikleri için bkz: Trend Mıcro, "FastFactsRegıonal Data, June 2020, s.6 https://resources.trendmicro.com/rs/945-CXD-062/images/Fast_Facts_ Regional_Data_2020_06.pdf, E.T. 07.07.2021.

[710] Check Point Software şirketininistatistikleri tablosu için bkz:GlobalSurges in RansomwareAttacaks, https://blog.checkpoint.com/2020/10/06/study-global-rise-in-ransomware-attacks/, E.T. 01.07.2021.



Şekil6 .Check Point Software Şirketi Küresel Fidye Yazılım Saldırıları Araştırması 2020 Yılında Fidye Yazılımı Saldırısına Uğrayan Ülkeler

Safety Detectives'in 2020 yılı fidye yazılım saldırı raporuna göre ise Türkiye 2020 yılında fidye yazılım saldırısın uğrayan dünyada ikinci ülke olmuştur[711].

Şekil 7. SafetyDetectives 2020 yılı Fidye Yazılımı Saldırı Rapor İstatistiği

[711] SafetyDetectives'in 2020 yılı fidye yazılım saldırı araştırma istatistikleri tablosu için bkz: RansomwareFacts, Trends&Statisticsfor 2021, https://www.safetydetectives.com/blog/ransomware-statistics/, E.T. 01.07.2021.

4.4.3. Önerilen Değişiklikler

4.4.3.1. TCK md. 107 Şantaj Suçu Yönünden

Saldırganın bulaştığı sistemdeki veri dosyalarını şifreleyerek mağdurun tekrardan dosyalarına erişmek için karşılığında fidye istediği zararlı yazılım türü olan fidye yazılımı TCK'da ki düzenleme alanına bakıldığında bazı hallerde şantaj suçunu oluşturabilecektir. Ancak bu anlamda henüz kanuni düzenleme yokken ABD fidye yazılımlarına karşı hukuki önlemler almaya başlamıştır. Nitekim ABD, 2020 yılının mayıs ayında REvil hacker grubu tarafından New York hukuk firması Grubman Shire Meiselas & Sack' e yapılan fidye yazılım saldırısını terör suçu olarak kabul etmiş ve 1 Ekim 2020 tarihinde OFAC fidye yazılım ödemelerini kolaylaştırmaya yönelik tavsiye yayınlayarak fidye yazılım taleplerini kabul eden kuruluşların Uluslararası Acil Durum Ekonomik Güçler Yasası (IEEPA) kapsamında yaptırımlara tabi olunacağı konusunda uyarıda bulunmuştur. Zira ABD' de OFAC tarafından belirlenen terörist gruplarına yapılan fidye ödemeleri federal yasanın 18. bölümün 2339B kapsamında maddi destek olarak kabul edilmekte olup yasaya aykırılık teşkil etmektedir. Keza ABD Hazine Bakanlığı 1 Ekim 2020 tarihinde "Fidye Ödemelerini Kolaylaştırmaya Yönelik Olası Yaptırım Riskleri Hakkında Tavsiye" yayınlayarak fidye yazılım saldırısına maruz kalan ve fidye ödeyen kişi veya kurumlara yaptırım uygulanabileceğini hüküm altına almış ve 23 Ekim 2020 tarihinde OFAC, "triton" isimli kötülümcül yazılım geliştirerek ABD'nin siber güvenliğini hedef alan Rus hükümetine bağlı bir kuruma ABD Düşmanlarına Yaptırım Yoluyla Mücadele Yasasının 244. maddesi uyarınca yaptırım kararı aldığını açıklamıştır. Görüleceği üzere ABD artan fidye yazılım saldırı vakalarına karşı yasa düzenlemelerine gitmişken Türkiye'nin fidye yazılımı kullanılarak gerçekleştirilen saldırılarda açık hedefte olması nedeniyle şantaj suçunu düzenleyen md. 107'de değişiklikler yapılması gerekecektir.

Terörle Mücadele Kanun'un Terör Amacıyla İşlenen Suçlar başlıklı 4. maddesine göre şantaj suçunun suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti kapsamında işlenmesi halinde terör suçu olarak kabul edilerek faile verilecek ceza yarı oranında artırılmaktadır. Bu kapsamda fidye yazılımı saldırılarının terör örgütünün faaliyeti kapsamında işlenmesi halinde faile verilecek ceza yarı oranında artacak olmakla birlikte ABD'de olduğu gibi Türkiye'de de fidye ödemelerinin terör suçu olarak kabul edilmesi

ve ceza kanununda bu doğrultuda değişiklik yapılması kanaatimizce zaten mağdur olan kişi ikinci kez mağdur edecek ve bu da ceza ve ceza muhakemesi hukuku bakımından önemli sonuçlara sebep olacaktır.

Fidye yazılımı saldırılarında hacker'ların dinamik IP adres kullanmaları ve özellikle ödeme yöntemi olarak sanal para kullanmaları bu saldırganların tespiti zorlaştırmakta ve soruşturma aşamaları uzun sürmektedir. Bu nedenle uluslararası bir tehdit unsuru olan fidye yazılımı saldırılarında Türk Ceza Kanun'unda yeni düzenlemeler yapılarak sürecin hızlanması adına soruşturma ve kovuşturma aşamalarına ilişkin özel usuller uygulanmalıdır.

4.4.3.2. TCK md. 135 Kişisel Verileri Kaydetme – TCK md. 136 Kişisel Verilerin Hukuka Aykırı Olarak Verilmesi Veya Ele Geçirilmesi Suçu Yönünden

Fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılarda gelinen son noktaya bakıldığında verilerimiz hedef haline gelmeye başlamış ve 2020 yılında COVID-19pandemisi ile birlikte saldırganların hedeflerinde kurbanlarının kişisel verileri, sağlık hizmetleri ve hasta verileri yer almıştır. Fidye yazılım saldırılarında ele geçirilen veriler hacker'lar tarafından Deep Web'te satışa çıkarılmaya başlanarak büyük veri ihlalleri yaşanmaya başlanmıştır Nitekim Amerikan Tıbbi Tahsilât şirketinin açıkladığı istatistiklere göre hacker'lar 12 milyon hastanın verilerini çalıp bunları "dark web" te satışa çıkarmışlardır.

Kişisel verinin ihlalline ilişkin suçlarda Avrupa Birliği Genel Veri Koruma Tüzüğünde 20.000, 000 Euro'ya kadar ciddi yaptırımlar düzenlenmişken 6698 sayılı Kişisel Verileri Koruma Kanunu'nda bu sınırlar çok daha düşüktür. Bu anlamda fidye yazılımı saldırısı ile kişisel verilerin ihlallerinde öngörülen hapis ve ceza miktarlarının arttırılması yönünde değişiklik yapılmalıdır.

4.4.3.3. Bilişim Sistemine Yönelik Suçlar Yönünden

Birçok zararlı yazılım saldırılarında olduğu gibi fidye yazılımı saldırılarında da bilişim sistemine girme suçu oluşacaktır. Nitekim fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılarda ilk olarak hacker'ın hedef bilgisayara erişerek bilişim sistemine hukuka aykırı giriş yapması suretiyle işlediğinden bilişim alanında işlenen

suçlar bakımından önem taşımaktadır. Hacker tarafından kullanılan virüs, solucan veya trojenler gibi zararlı yazılımlar bilişim sisteminin düzgün şekilde çalışmasını engellendiğinden bu kötü amaçlı yazılımların sisteme bulaştığı anda bilgisayara veya donanımlarına zarar vermeden temizlenmesi oldukça zordur. Fidye yazılımları da bulaştıkları sistemdeki verileri şifreleyerek bilgisayarın normal şekilde çalışmasını engelleyip kullanılamaz hale getirmektedir. Nitekim her geçen gün farklı tür ve isimde bilişim sistemi üzerindeki verileri veya dosyaları şifrelemek üzere programlanan fidye yazılımları geliştirilmektedir. Ülkemizde de TCK'ya 2016 yılında eklenen madde ile "Yasak Cihaz Ve Programlar" suç haline getirilerek zararlı yazılım ve programların kullanılması engellenmek istenmiştir. Ancak bilişim alanına yönelik suçlara ilişkin yaptırımlar şuan Türkiye için ciddi tehdit ve tehlike olan fidye yazılımları bakımında yetersiz kalabilecektir. Bilişim sistemine girme suçunun birinci fıkrasında düzenlenen halinde suçun alt sınırı belirtilmediği için TCK'nın 49.'uncu maddesi uyarınca alt sınır 1 ay olarak kabul edilecektir. Yine TCK'da 245/A maddesinde düzenlenen halinde adli para cezasının alt sınırı belirtilmediği için alt sınır TCK md. 52/1 gereğince beş gün olarak kabul edilecektir. Bu düzenleme ise fidye zararlı yazılımları bakımından oldukça eksik bir düzenleme olarak karşımıza çıkmaktadır. Bu suçlarda alt sınırları daha yüksek belirlenmelidir. Terörle Mücadele Kanun'un Terör Amacıyla İşlenen Suçlar başlıklı 4. maddesine göre bilişim sistemine girme suçu, suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti kapsamında işlendiği takdirde terör suçu olarak kabul edilip verilecek ceza yarı oranında arttırılacağından fidye zararlı yazılımıkullanılarak gerçekleştirilen saldırıların terörizm amaçlarıyla işlenmesi halinde eylem terör suçu sayılacak faile verilecek ceza yarı oranında arttırılacaktır. Yine Terörle Mücadele Kanun'un Terör Amacıyla İşlenen Suçlar başlıklı 4. maddesine göre sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu, suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti kapsamında işlendiği takdirde terör suçu olarak kabul edilecek ve verilecek ceza yarı oranında artırılacaktır. Ancak daha önce bahsedildiği üzere ABD'de olduğu gibi Türkiye'de fidye ödemelerinin terör suçu olarak kabul edilmesi ve ceza kanununda bu doğrultuda değişiklik yapılması kanaatimizce zaten mağdur olan kişi ikinci kez mağdur edecek ve bu da ceza ve ceza muhakemesi hukuku bakımından önemli sonuçlara sebep olacaktır

TCK md. 244/3'de suçun nitelikli halinde suçun banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır" şeklinde düzenlenmiştir. Söz konusu nitelikli halin uygulanması bakımından kanunda yalnızca banka veya kredi kurum ve kuruluşlarıyla sınırlandırma yapılmıştır. Ancak bu nitelikte olmayan şirket veya kuruluşlar içinde sistemlerinin engellenmesi, bozulması, verileri yok edilmesi veya değiştirilmesi de önemli olduğundan ve fidye yazılımı saldırılarında daha çok şirketlerin hedef olduğu hususu da göz önüne alındığında nitelikli hali düzenleyen maddenin yetersiz kalıp yalnızca banka veya kredi kurum ve kuruluşlarıyla sınırlandırma yapılmaması gerekmektedir.

4.4.3.4. Yağma Suçu Yönünden

Bilişim sistemimizin, verilerimizin yağmalandığı siber yağma- dijital yağma olarak adlandırılan fidye zararlı yazılımı saldırıları yağma suçu açısından da büyük önem arz etmektedir. Nitelikli yağma suçunu düzenleyen TCK md.149 'a göre suç örgütüne yarar sağlamak maksadıyla yağma suçunu işlenmesi halinde ceza miktarının on beş yıla kadar artırılacağı hükme bağlanmıştır. Bu bağlamda Revil, Conti, Anonymous gibi fidye yazılımı çetelerinin suç örgütüne yarar sağlamak maksadıyla işlenmesi halinde suçun nitelikli halinden bahsedilecektir. Ancak burada kanımızca yapılması öngörülen değişiklik fidye zararlı yazılımı saldırılarında bu tespitinin her zaman mümkün olabileceği kabul edilerek suçun caydırıcılığına etkisi bakımından karine olarak kabul edilmeli ve fidye zararlı yazılımı kullanarak işlenebilecek şantaj suçunda faile verilecek ceza suçun temel hali olarak düzenlenmesi gerekmekte ve fidye yazılımı kullanarak işlenebilecek yağma suçu için öngörülen hapis ve ceza miktarlarının arttırılması yönünde değişiklik yapılmalıdır.

5. SONUÇ

Son yıllarda internetin ve bilişim sistemlerinin hayatımızdaki önemi artarken birçok sorunu da beraberinde getirmiştir. Bu gelişmeler neticesinde "hacker'lık" sanal dünyanın tehditleri olarak hayatımıza girmiştir. 2017 yılında hacker'lar tarafından bütün dünyayı sarsan fidye yazılımı ile yeni bir siber saldırı geliştirilmiştir. Dünya'da başta ABD ve Rusya olmak üzere birçok önemli devlet banka ve hastaneler bu saldırıdan etkilenmiş ve hacker'lar büyük bir kaosa neden olmuşlardır. Tüm bu gelişmeler neticesinde birçok ülke hukuk ve güvenlik sistemlerinde değişikliklere giderek önlemler almaya başlamıştır. Küresel çapta en büyük fidye yazılımı saldırısını 12 Mayıs 2017 tarihinde gerçekleştiren siyah şapkalı hacker'lar 2020 yılında pandeminin de etkisiyle birlikte fidye yazılımlarının çeşitli varyantlarını geliştirerek güçlerini daha da artırmış; çok sayıda önemli kurum ve kuruluşlara zarar vermişlerdir. Türkiye'nin de maruz kaldığı bu saldırının gelecekte daha ciddi zararlara neden olacağı tahmin edilmektedir. Bu sebeple global çapta olan siber tehdit için birtakım önlemler alınması gerekmektedir.

İngilizce ransomware kelimesinden fidye yazılımı olarak Türkçeye çevrilen ve şantaj yazılımı olarak da adlandırılan bu zararlı yazılım siyah şapkalı hacker'lar tarafından şantaj şeklinde programlanmıştır. Zararlı bir yazılım türü olan fidye yazılımı tarihte ilk kez 1989 yılında karşımıza çıkmıştır. Joseph Popp, AIDS hastalığına yakalanma riskini tespit eden uygulamanın olduğu 20.000 disketi doksan ülkedeki araştırmacılara göndermiş ve içindeki zararlı yazılımın devreye girmesiyle birlikte kullanıcılardan lisans bedeli adında fidye talep eden zararlı yazılım geliştirmiştir. Bu zararlı yazılım ise Joseph Popp'un kurduğu bu hayali şirket "PC Cyborg Corporation" tarafından dağıtılmıştır. Uzun bir süre sessizliğini koruyan fidye yazılımları 2013 yılında tekrar kendini göstermiş ve CryptoLocker adıyla Gameover Zeus Botnet üzerinden Windows işletim sistemlerine bulaşan fidye yazılım türü ortaya çıkmış ve milyonlarca zarara sebep olmuştur. Yine 2014 yılında Windows işletim sistemine bulaşan CryptoWall ve 2015 TeslaCrpyt adıyla ortaya çıkan oyun dosyaları ve kullanıcılar hedef alan fidye yazılımları çıkmıştır. 2017 tarihine gelindiğinde ise fidye yazılımları küresel krize neden olan ilk saldırısını gerçekleştirmiş ve WannaCry fidye yazılımını 150 den fazla ülkedeki büyük ve önemli kuruluşlara verdiği zararla dünya çapındaki en büyük siber saldırı olarak tarihe geçmiştir. WannaCry fidye yazılımı saldırısından hemen sonra ise

Ukrayna'da başlayan ve hızla dünyaya yayılan Petya isimli fidye yazılım saldırısı meydana gelmiştir. WannaCry saldırısını gerçekleştiren siyah şapkalı hacker'lar 24 saatte 30.000 dolar ele geçirmişken Petya saldırısında siyah şapkalı hacker'ların 10.000 dolar haksız kazanç sağlamışlardır. 2019 ve 2020 yıllarında ise fidye yazılımı saldırılarından sağlanan haksız kazançların milyon dolarla ulaşması, kripto paraların kullanımının yaygınlaşması ve pandeminin etkisiyle birlikte fidye yazılımı saldırıları siyah şapkalı hacker'lar tarafından cazip hale gelmiş ve yeni varyantlarda fidye yazılımları geliştirilmeye başlanmıştır. Bunlardan biri de 2018 yılında ortaya çıkan ve 2019-2020 yıllarında daha da güçlü hale gelen Ryuk fidye yazılımıdır. Hedef odaklı olarak en fazla miktarda fidye alabileceği büyük ölçekli şirketlere saldıran Ryuk fidye yazılımı yazılımı en tehlikeli fidye yazılımlardan biri olmakla beraber pandeminin etkisiyle birlikte birçok sağlık kuruluşu hedef almış ve milyonlarca dolar fidye toplamıştır. 2020 yılıyla birlikte fidye yazılımı saldırıları kendini duyurmaya başlamış ve geleceğin en büyük siber tehdidi olarak görülmeye başlanmıştır. 2022 yılına gelindiğinde ise fidye yazılımları sürekli kendini geliştirmeye devam etmekte ve fidye yazılımları familyasına her gün bir yenisi daha eklenmektedir. Fidye yazılımlarında saldırganlar çeşitli sızma yöntemleri ile hedef bilgisayara bulaşmaktadırlar. Siyah şapkalı hacker'lar tarafından en sık kullanılan yöntemlerin başında ise insan faktörünün etkili olduğu sosyal mühendislik yöntemiyle oltalama saldırısı, kötü amaçlı reklam anlamına gelen malvertisement ve güvenlik zafiyetleri en sık kullanılan yöntemlerdir. Bunun haricinde fidye yazılımlarının çeşitleri varyantlarıyla birlikte her geçen gün yeni bulaşma yöntemleri ve saldırı mekanizmaları güçlendirilmektedir. Fidye zararlı yazılımları diğer zararlı yazılımlardan farklı olarak sisteme bulaştıktan sonra yazılımcısının yardımı olmadan kurbanın sisteme erişmesi veya dosyalarının şifresini çözmesi oldukça zordur. Yine fidye zararlı yazılımlarında çok güçlü şifreleme algoritmalar kullanılması ve yine kripto paralarla finanse edilmesi de fidye yazılımı saldırılarını odak noktası haline getirmektedir. Fidye yazılımlarının çalışma şeklini 5 ana başlık altında inceleyebiliriz. Fidye yazılım saldırılarının ilk evresi olan yayılma aşamasında saldırganlar çeşitli yöntemlerle veya en sık kullanılan yöntem olan kurbanın mailine banka ekstresi, telefon faturası veya anket göndererek kurbanın dikkati çeker ve linki tıklamasını sağlar. Kullanıcı linki tıkladıktan sonra fidye yazılımı sisteme yayılmış olur. Bazen de saldırganlar kullanıcının haberi olmaksızın sisteme zararlı

yazılımı otomatik olarak (drivebydowland) indirilmesini sağlayarak fidye yazılımını yayarlar. Fidye yazılımı bilgisayara bulaştıktan sonra öncelikle gerçek bir sistemde olup olmadığını tespit etmeye başlar ve bu aşamada saldırgan fidye yazılımının hangi sistemlere bulaştığını belirlemek için genellikle bilgisayar sistem adını MD5 özet fonksiyonunu veya Mac adresini kullanarak kendisini benzersiz hale getirir. Daha sonra antivürüs programlarının kendisini tespit etmesine izin vermeden saldırganın komuta kontrol sistemi ile iletişimini kurmasını küçük bir kod parçası sisteme yerleştirilir ve ardından komutlar alarak kendini bilgisayara indirirve sistem kurtarma özelliklerini kapatarak Windows korumaları devre dışı bırakılır.Fidye yazılımının bulaştığı sistemde hangi dosyaları şifreleyeceği, ne zaman şifrelemeye başlayacağı ya da ne kadar süre virüsün sistemde kalması gerektiği gibi hususlarının fidye yazılımına istek olarak gönderilmesi gerekir. Fidye yazılımlarında komut dosyaları kurbanın sistemine fidye yazılımını indirip yüklenmek için tasarlanmış olup bulaştığı kurban sistemdeki verilere ulaşmak için komuta ve kontrol sunucuyla iletişiminin sağlanması gerekmektedir. Komuta ve kontrol aşamasının fidye yazılımı bulaştığı sistemin tespitini, güvenirliğini ve verinin değerini belirlemek gibi önemli amaçları bulunmaktadır. Komuta kontrol aşamasında belirlenen her türlü dosya biçimleri ise malcode (zararlı yazılım kodu) ile şifrelenmektedir ve şifreleme fidye yazılımı saldırılarında en önemli safhalardan biridir. Zira fidye zararlı yazılımının anatomisi gereği saldırgan tarafından şifrelenen dosyaların açılmaması ve bu anahtarın sadece saldırganda olması gerekmektedir. İlk fidye yazılımları ancak belirli türdeki “, jpg, .pdf, .zip, ve .doc” gibi dosyaları şifreliyorken artık bu tür sınırlamalar olmaksızın her türlü dosyalar şifrelenebilmektedir. Fidye yazılımı saldırılarında fidye ödemesi olarak bitcoin tercih edilmektedir. Zira bitcoin dünyanın en gizli para transfer olarak görüldüğünden ve hesap sahiplerinin isim ve kimlik bilgileri bulunmadığından fidye ödeme aracı olarak saldırganlar tarafından en fazla tercih edilen fidye ödeme biçimi olmuştur.

Fidye yazılımlar diğer zararlı yazılım türlerinden farkı olarak “şantaj” şeklinde programlanmaktadır. Fidye yazılımı bilgisayara veya sisteme bulaştığında başta belgeler olmak üzere, resimler, filmler, veri tabanları ve birçok türdeki dosyayı şifrelemekte ve bu dosyalara mağdurun veya kurbanın erişebilmesi için para talep etmektedir. Şantaj suçunun kanundaki düzenleme alanına bakıldığında ise fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılarda şantaj suçunun işlenmesi bazı hallerde mümkün

olabilecektir. Suçun 107. maddesinin 1. fıkrası bakımından "Hakkı olan veya yükümlü olduğu bir şeyi yapacağından veya yapmayacağından bahisle bir kimseyi kanuna aykırı veya yükümlü olmadığı bir şeyi yapmaya ve yapmamaya ya da haksız çıkar sağlamaya zorlamak" şantaj suçunun ilk halini oluşturmakta ve maddenin 1. fıkrasında var olan yasal hak ve yükümlülük kötüye kullanılmaktadır. Fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılarda saldırganların hakkı olan veya yükümlü olduğu bir durum olmadığından şantaj suçunun fidye yazılımı saldırıları bakımından suç teşkil etmeyeceği öğretide kabul edilmekle birlikte kanımızca da bu madde bakımından fidye yazılım saldırısının şantaj suçunun Suçun 107. maddesinin 1. fıkrası bakımından işlenmesi mümkün olmayacaktır. Suçun 107. maddesinin 2. fıkrası bakımından ise söz konusu fiil "Kendisine veya başkasına yarar sağlamak maksadıyla bir kişinin şeref ve saygınlığına zarar verecek nitelikteki hususların açıklanacağı veya isnat edileceği tehdidinde bulunulmasıdır. Fidye yazılımı saldırılarının 107. maddenin 2. fıkrası bakımından da suç teşkil edip etmeyeceği öğretide tartışmalı olmakla birlikte daha önce de açıklandığı üzere fidye yazılım saldırılarında saldırganlar açıklayacakları bilgi, belge veya görüntülerle mağdurların itibar veya saygınlıklarına zarar vermekle tehdit etmektedirler. Dolayısıyla şantaj suçunun 107. maddesinin 2. fıkrası bakımından şantaj suçu işlenmesi mümkün olacaktır.

Fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılarda başlangıçta bilişim sistemleri üzerindeki verileri şifrelemekteyken 2019 'un sonlarına doğru siyah şapkalı hacker'lar bilişim sistemi üzerindeki kişisel ve hassas verileri de şifreleyerek tehdit unsuru haline getirmişlerdir. Dolayısıyla fidye yazılımı saldırılarında kaydedilen bir veriden bahsedilecektir. Burada kaydetme fiili dijital bir ortamda gerçekleşmektedir. Zira fidye yazılımı bulaştığı sistem üzerindeki dosya ve klasörleri şifrelediği için suçu oluşturan fiil kişisel verilerin elektronik veri tabanına, CD'ye veya USB belleğe kaydedilmesidir. Fidye zararlı yazılımları bulaştığı sistem üzerindeki dosya ve klasörleri otomatik olarak şifrelediğinden veya bunu kilit altına alarak kaydettiğinden fidye yazılımı kurbanın bilgisayara bulaştığı anda kişisel verilerin kaydedilmesi suçundan bahsedilebilecektir.

Fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılarda ele geçirilen veriler hacker'lar tarafından kamuoyuna ifşa edilerek veya Deep Web'te satışa çıkarılarak büyük veri ihlalleri neden olmuş ve gün geçtikçe de fidye yazılımı saldırıları nedeniyle

ciddi veri kayıpları yaşanmaya başlanmıştır. Bu bakımdan fidye yazılımı saldırılarında kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu önem arz etmektedir. Öğretide, fidye zararlı yazılımları herhangi bir veriyi ele geçirip ifşa etmeğinden dolayı TCK md.135 ve md. 136'daki suçları oluşturmayacağı görüşü ileri sürülmüşse de fidye zararlı yazılım saldırılarında gelinen son noktaya bakıldığında başta kişisel veriler olmak üzere verilerin hacker'ların hedefinde olması, bu verilerin derin ağlarda satışa çıkarılması ve fidye zararlı yazılımlarının amacına bakıldığında ilgili suçun oluşması bakımından yeterli olacağından bu görüşe katılmadığımızı belirtmek isteriz. Dolayısıyla fidye zararlı yazılımı kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçuna konu olabilecektir.

Fidye zararlı yazılımı saldırısı bir bilişim sistemine girilmesi suretiyle işlenmektedir. Zira siyah saldırgan hedef bilgisayara erişerek sisteme hukuka aykırı giriş yapmaktadır. Fidye yazılımı saldırısı genellikle kullanıcıya gönderilen sahte e-posta bağlantısına tıklamasıyla meydana gelmektedir. Bilişim sistemine girilmesiyle birlikte fidye yazılımında kullanılan şifreleme yöntemi ile mağdurun sisteme girilmesi engellenmektedir. Fidye yazılımları fiil itibariyle saldırgan mağdurun sistemine hukuka aykırı şekilde girmeyip sosyal mühendislik gibi çeşitli yöntemlerle zararlı yazılımı bulaştırtıp mağdurun sistemine erişim sağladığından hukuka aykırı bir erişimden bahsedilmeyecek ve bilişim sistemine girme suçu normal şartlarda oluşmayacaktır. Ancak burada dikkat edilmesi gereken husus failin söz konusu erişimi nasıl sağladığıdır. Fidye yazılımın sisteme yerleştirilme şekli veya tekniği bu aşamada suçun oluşması bakımından önemli olacak olup hukuka aykırı olarak mağdurun bilişim sistemine erişim sağlanabildiği hallerde bilişim sistemine girme suçundan bahsedilebilecektir.

Fidye yazılımları bulaştıkları sistemdeki verileri şifreleyerek bilgisayarın normal şekilde çalışmasını engelleyip kullanılamaz hale getirmektedir. Hatta öyle ki saldırgan tarafından şifre anahtarı olmadan sistemi açmaya çalışmak kişinin yıllarını alabilmektedir. Saldırganların sahte e-posta veya web adresler kullanarak gerçekleştirdikleri fidye yazılımı saldırılarında mağduru yanıltarak zararlı yazılımı kendilerinin tıklamasını sağladıkları saldırılarda saldırganlar, zararlı yazılımı indirme fiillerini bizzat mağdurun kendisine yaptırmış olduklarından böyle durumlarda sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunda bakımından TCK md.244/2 dolaylı faillikten söz edilebilecektir. Yine TCK'nın md. 244/4 düzenlenen;

“Yukarıda fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur” maddesi fidye yazılımı saldırıları bakımından önem arz etmektedir. Zira fidye yazılımları haksız bir kazanç elde etme amacıyla programlandıklarından dolayı bu kapsamda bir fiil suçun konusunu oluşturduğu takdirde içtima hükümleri çerçevesinde değerlendirmek gerekecektir. Fail fidye yazılımı saldırısı ile sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunun birinci ve ikinci fıkralarında düzenlenen suçu işlerken aynı zamanda bu fiillerin işlerken kendisinin veya başkasının yararına haksız bir çıkar sağlaması durumunda fail bileşik suç hükümleri gereğince md. 244/4’den cezalandırılacaktır. TCK’nın 244. maddesinde yer alan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları arasındaki ilişki bakımından ise fikri içtima ilişkisinin varlığından söz edilecek olursa fail daha ağır ceza olan TCK md. 244/4’den cezalandırılacak ve fail hakkında iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunacaktır. Ancak görünüşte fikri içtima ilişkisinin varlığından söz edilecek olursak ise de TCK md. 136 ‘dan hüküm kurulması gerekecek , fail iki yıldan dört yıla kadar hapis cezası ile cezalandırılacaktır..

Fidye yazılımları sistem üzerindeki verileri veya dosyaları şifrelemek üzere programlanmıştır. Söz konusu programlar çok güçlü algoritmalarla hukuka aykırı şekilde tasarlanmakta olup her geçen gün farklı tür ve sayıda fidye yazılımları geliştirilmektedir. Ülkemizde de TCK’ya 2016 yılında eklenen madde ile “Yasak Cihaz Ve Programlar” suç haline getirilerek zararlı yazılım ve programların kullanılması yasaklanmıştır. Bu kapsamda fidye yazılımı saldırılarında bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun imal edilmesi, ithal edilmesi sevk edilmesi, nakledilmesi, depolanması, kabul edilmesi, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulması eylemleri Yasak Cihaz Ve Programlar suçunu oluşturacaktır.

Fidye yazılımı saldırılarının yağma suçuna konu olup olmayacağını değerlendirirken ise temelde 2 hususdan bahsedilmesi gerekmektedir. Öncelikle fidye zararlı yazılımı saldırılarındaki verilerin erişilmez kılınması tehdidinin mağdurun malvarlığı açısından büyük bir zarar oluşturup oluşturmayacağı ele alınmalıdır. Daha sonra ise fidye yazılımlarında fidye ödeme yöntemi olarak kullanılan kripto paraların bir malı teslime

veya malın alınmamasına karşı koymama kapsamında mal olarak kabul edilip edilemeyeceği ele alınmalıdır. Fidye zararlı yazılımı kullanılarak gerçekleştirilen saldırılarda fidye ödemesi olarak kabul edilen kripto paralar bu kapsamda ekonomik bir değere sahip olmakla birlikte kripto paralar bilişim sistemi üzerinde tutulan veri parçaları online ve offline olarak bulunabilmektedir. Offline olarak kripto paranın tutulması halinde bir maldan bahsedilecek ve fail kripto parayı teslime zorlaması halinde fidye yazılımları yağma suçunun konusunu oluşturabilecektir. Bu şartların varlığı halinde fidye zararlı yazılımı kullanılarak yağma suçu işlenebilecektir.

Fidye yazılımı saldırılarında dünyada ilk 5 sırada yer alan Türkiye hala fidye yazılım saldırılarına karşı hukuki önlemler almaya başlamamıştır. Konunun yargıya intikal etmemesi kurbanların saldırganlara fidye taleplerini ödedikleri sonucunu doğurmaktadır. KVKK'nın resmi sitesinde yayınlanan veri ihlallerinde birçok şirketin fidye yazılımı saldırısına maruz kaldığı gerçeğini ortaya çıkarmaktadır. Büyük bir tehlike arz eden ve Türkiye için de ciddi tehlike oluşturan fidye yazılımlarına karşı önlemler alınması gerekmektedir. Kanımızca bilişim alanına yönelik suçlara ilişkin yaptırımlar fidye yazılımları bakımında yetersiz kalmaktadır

Yapılan tüm açıklamalar çerçevesinde fidye yazılımları kullanılarak gerçekleştirilen saldırılarının ciddi bir siber tehdit olmasına karşın Türk Ceza Hukuku sistematiğinde cezalandırılmasının yetersiz kalması, gerekli önlemlerin henüz alınmaması, fidye yazılımlarının her geçen gün etkisel verimliliğini artırması, finansal olarak hacker'lara daha fazla kar sağlaması ve saldırıları vazgeçilmez hale getirmesi durumun ciddiyetini ortaya koymaktadır. Nitekim tüm bu gelişmeler neticesinde artık fidye zararlı yazılımı saldırılarının çağının başladığını ve bu kapsamda kritik dönemler yaşanacağını söylemek yanlış olmayacaktır.

KAYNAKÇA

" Phobas Fidye Yazılımı", https://www.enigmasoftware.com/tr/phobosfidyeyazilimi-cikarma/, E.T 12.12.2021.

" Salgın Döneminde En Fazla Maruz Kalınan Siber Suç Zararlı Yazılım Bulaşması Oldu", 22 Aralık 2020, https://www.aa.com.tr/tr/bilim-teknoloji/salgin-doneminde-en-fazla-maruz-kalinan-siber-suc-zararli-yazilim-bulasmasi-oldu/2084757, E.T 15.03.2021.

"132 Ülkeden Binlerce Hacker HackIstanbul 2018 Yarışmasında Bir Araya Gelecek", https://www.sondakika.com/haber/haber-132-ulkeden-binlerce-hacker-hackistanbul-2018-11153525/, E.T 18.11.2019.

"AB'den Siber Saldırılara Karşı "Ortak Birim" Hareketi, "https://www.savunmatr.com/siber-guvenlik/ab-den-siber-saldirilara-karsi-ortak-birim-hareketi-h12780.html, E.T. 05.01.2021.

"ABD Hastaneleri Sanal Fidyecilerin Saldırısı Altında", 29 Ekim, 2020, https://www.amerikaninsesi.com/a/abd-hastaneleri-sanal-fidyecilerin-saldirisi-altinda/5640544.html, E.T. 05.01.2021.

"ABD Savunma Bakanlığından Türk Hacker'e Teşekkür", 30 Haziran 2017, http://www.haber7.com/, E.T. 11.11.2019

"ABD'de 12 Milyon Hastanın Bilgileri 'darkweb'te Satışa Çıkarıldı", 18 Haziran, 2019, https://www.bloomberght.com/abd-de-12-milyon-hastanin-bilgileri-dark-web-te-satisa-cikarildi-2225734, E.T. 05.01.2021.

"ABD'li Petrol Şirketi Fidye Ödediğini Doğruladı", https://www.trthaber.com/haber/dunya/abdli-petrol-sirketi-fidye-odedigini-dogruladi-582039.html, E. T 24.06.2021.

"AdrianLamoCv", https://www.tarihiolaylar.com/biyografiler/adrian-lamo-cv-239, E.T 18.11.2019.

"Beyaz Şapkalı Hacker Nedir?", 8 Temmuz 2016, ,https://sibertehdit.com/beyaz-sapkali-hacker-nedir/, E.T 11.11.2019.

"Beyaz Şapkalı Hacker'ler", 14 Şubat 2016, https://www.bizimsakarya.com.tr/haberler/beyaz-sapkali-hackerler-h23855.html, E.T 18.11.2019.

"Bilgisayar Korsanları Estetik Ameliyat Fotoğraflarını Sızdırmakla Tehdit Ediyor", A 24 Aralık 2020, https://www.1mh.org/bilgisayar-korsanlari-estetik-ameliyat-fotograflarini-sizdirmakla-tehdit-ediyor/, E.T 15.01.2021.

"Canı Sıkıldı NASA'yı Hackledi", Türkiye Gazetesi, 27 Nisan 2019, https://www.turkiye gazetesi.com.tr/, E.T 15.12.2019.

"Eski Siyah Şapkalı Hacker Üyesi: "ABD'ye Yönelik Siber Saldırılar Katlanarak Daha Kötü Bir Hale Gelecek", 20 Haziran 2021, https://www.savunmatr.com/siber-guvenlik/eski-siyah-sapkali-hackerlar-uyesi-abd-ye-yonelik-siber-h12718.html, E. T 25.06.2021.

"FBI Tarafından Aranan 10 Hacker", https://www.webtekno.com/sektorel/fbi-tarafindan-aranan-10-hacker-h12346.html, E.T 18.11.2019.

"Fidye Saldırısından Sonra Ünlü Banka Tüm Şubelerini Kapattı", 8 Eylül, 2020, https://tr.investing.com/news/cryptocurrency-news/fidye-saldrsndan-sonra-nlu-banka-tum-ubelerini-kapatt-2006411, E.T 12.12.2020.

"Fidye Yazılım Saldırganları Hasta Bilgilerini Sızdırdı", 27 Mayıs 2021, https://www.savunmatr.com/siber-guvenlik/fidye-yazilimi-saldirganlari-hasta-bilgilerini-sizdirdi-h12091.html, E. T 24.06.2021.

"Fidye Yazılım Tehdidinin Tarihi: Geçmişi, Bugünü ve Geleceği", https://tr.vpnmentor.com/blog/fidye-yazilim-tehdidinin-tarihi-gecmisi-bugunu-ve-gelecegi/, E.T 03.03.2021.

"Fidye Yazılımcılar "BabukLocker" İle 2021'e Merhaba! Dedi!", 1 Ocak 2021, https://www.siber.care/blog/fidye-yazilimcilar-babuk-locker-ile-2021e-merhaba-dedi, 25.03.2021.

"Fidye Yazılımı Kurbanlarının Yarısından Fazlası Fidyeyi Ödüyor, Yalnızca Dörtte Biri Tüm Verileri Geri Alabiliyor", 7 Nisan 2021, https://www.cybermagonline.com/ fidye-yazilimi-kurbanlarinin-yarisindan-fazlasi-fidyeyi-oduyor-yalnizca-dortte-biri-tum-verileri-geri-alabiliyor, E.T. 12.04.2021.

"Fidyeci Hackerler Ünlü İsimlerin Bilgilerini Çaldı", 14 Mayıs 2020, https://www.sonhaberler.com/fidyeci-hackerlar-unlu-isimlerin-bilgilerini-caldi-haber-810745, E.T 11.04. 2021.

"Hacker Gibi Düşünerek Saldırılardan Korunun", Sonsöz Gazetesi, Nisan 2019), https://sonsoz.com.tr/, E.T 11.11.2019

"Hacker'ların Tarihi", http://arsiv.ntv.com.tr/news/119212.asp, E.T 18.11.2019.

"Hacking Nedir?", http://siberguvenlikhaberleri.blogspot.com/2014/05/hacking-nedir.html,E.T 10.11.2019.

"Hastane Siber Saldırıya Uğradı: Bir Hasta Hayatını Kaybetti", 24 Eylül, 2020, https://www.yenisafak.com/teknoloji/fidye-yazilimi-ilk-defa-bir-olume-neden-oldu-3568434, E.T 05.01.2021.

"JBS SA Bilgisayar Korsanlarına 11 Milyon Dolar Fidye Ödedi", https://www.trthaber.com/haber/dunya/jbs-sa-bilgisayar-korsanlarina-11-milyon-dolar-fidye-odedi-587730.html, E. T 24.06.2021.

"KelihosBotnet'ini İşleten Rus Siber Korsan Suçunu Kabul Etti", 16 Eylül 2018, https://bilgiguvende.com/kelihos-botnetini-isleten-rus-siber-korsan-sucunu-kabul-etti/, E.T 12.12.2020.

"Küresel Saldırıyı Engelleyen Hacker ABD'de Gözaltına Alındı", https://www.aa.com.tr/tr/dunya/kuresel-siber-saldiriyi-engelleyen-hacker-abdde-gozaltina-alindi/876188, E.T 25.03.2021.

"Lady Gaga'ya Siber Saldırı: 42 Milyon Dolar İstediler", 18 Mayıs, 2020, https://www.gazeteduvar.com.tr/dunya/2020/05/18/lady-gagaya-siber-saldiri-42-milyon-dolar-istediler, E.T 12.02.2020.

"LockBit2.0 Fidye Yazılımı Tarafından Kullanılan Teknikler", 2021, https://cyberartspro.com/-locbit-yazilimi-kullanilan-teknikler/, E.T. 15.02.2022.

"MountLockerRansomware, Hackerlara Çifte Gasp İmkanı Sunuyor", 13 Aralık 2020, https://www.sibermagazin.com/mount-locker-ransomware-hackerlara-cifte-gasp-imkani-sunuyor/, E.T 25.03.2021

"Müşteri Verileri Sızdırıldı! İsrailli Şirketten Fidye İstiyorlar", 3 Aralık 2020, https://www.star.com.tr/dunya/musteri-verileri-sizdirildi-israilli-sirketten-fidye-istiyorlar-haber-1592037/, 25.03.2021

"NSA, Biden'ın İmzaladığı Siber Güvenlik Emrinde Önemli Rol Oynayacak", https://www.savunmatr.com/siber-guvenlik/nsa-bidenin-imzaladigi-siber-guvenlik-emrinde-onemli-bir-rol-h12066.html, E. T 26.06.2021.

"Phreakar Nedir?", https://phreaker.nedir.org/, E.T. 11.11.2021.

"Ransomware Teknikleri Ve Analizleri", https://www.infinitumit.com.tr/ransomware-trendleri-ve-analizler/, E.T. 27.03.2022.

"RDP Bağlantısı Nasıl Yapılır?", https://bidb.amasya.edu.tr/media/4594/rdp-4.pdf, E.T. 27.03.2022

"Rusya Kaynaklı Fidye Yazılımı Saldırıları Hakkında Ne Biliniyor?", https://www.ameri kaninsesi.com/a/biden-putin-zirvesindeki-gundem-fidye-yazdilimi/5931043.html, E.T. 24.06.2021.

"Ryuk Fidye Yazılımı Nedir?", TrendMicro, https://www.trendmicro.com/tr_/what-is/ransomware/ryuk-ransomware.html, E.T. 02.03.2022.

"ScriptKiddie Nedir", http://www.dijitalteknoloji.net/internet/script-kiddie-nedir.html, E.T. 07.12.2021.

"Siber Saldırganlar 42 Milyon Dolar Fidye İstiyor", http://blog.isr.com.tr/2020/06/siber-guvenlik-bulteni-mays-2020.html, E.T 11.04. 2021.

"Siyah Şapkalı Hacker Kimdir?", http://www.dijitalteknoloji.net/internet/siyah-sapkali-hacker-kimdir.html, E.T 18.11.2019.

"TeslaCrpyt Nedir Ve Nasıl Kaldırılır?", 2016, https://blog.360totalsecurity.com/tr/, E.T 15.01.2020.

"Vvv Uzantılı Virüs Nasıl Temizlenir?", https://uzmanim.net/soru/vvv-uzantili-virus-nasil-temizlenir/63219, E.T. 15.01.2020.

"Wikileaks ABD'ye ait Şimdiye Kadarki En Büyük Casusluk Dosyalarını Yayınladı", https://siyasihaber4.org/e/wikileaks, E.T. 15.12.2019.

"Zombi Bilgisayarlar Ve Bilişim Suçu", https://www.sertels.av.tr/avukat/hukuk/bilisim-hukuku/zombi-bilgisayarlar-ve-biliim-sucu.html, E.T 05.02.2021.

ADAKLI, Gülsen, "KRONİK: Hâkim Güçlere Ve Hakim Gazeteciliğe Meydan Okuyan Bir Girişim: Wikileaks, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi, C. 66, S. 1, 2011, s. 189-182, https://dergipark.org.tr/tr/download/article-file/35885, E.T. 18.11.2019.

AİDAN, J.S, VERMA, H.K, AWASTHİ, L.K, "ComprehensiveSurvey On PetyaRansomware Attack", 2017 İnternational Conference On NextGeneration Computing AndInformatıonSystems, Jammu 2017, s.122, doi:10.1109/ICNGCIS.2017.30

AİDAN, J.S, VERMA, H.K, AWASTHİ, L.K, "ComprehensiveSurvey On PetyaRansomware Attack", 2017 İnternational Conference On NextGeneration Computing AndİnformatıonSystems, Jammu 2017, doi:10.1109/ICNGCIS.2017.30.

AKALIN, Şükrü Haluk, CEBECİ, Zeynel, BADA, Erdoğan, MITIŞ, Bülent, ACAR, Levent, TAN, Ali, Bilgisayar Terimleri Karşılıklar Kılavuzu, Türk Dil Kurumu Yayınları, 3. Baskı, Ankara 2013.

AKBULUT, Berrin, Bilişim Alanında Suçlar, Adalet Yayınevi, 2. Baskı, Ankara 2017.

AKINCI, Ayşe Nur, "Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti", Uzmanlık Tezi, T.C Cumhurbaşkanlığı Strateji Ve Bütçe Başkanlığı, Yayın No: 001.

AKÖZ, Burak Cesur, "Türk Ceza Kanunu Kapsamında Bilişim Suç Ve Cezaları İle Örnek Yargısal Kararların Analizi ve Mevzuat Önerileri", Bilişim Uzmanlığı Tezi, Bilgi Teknolojileri Ve İletişim Kurumu, Yayın No: 0255, Ankara 2018.

ALP, Barış Emre, Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme Suçu, Adalet Yayınevi, 1. Baskı, Ankara 2019.

ALP, Özgür, "*Akıllı Şehirlerde Siber Güvenlik*", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2018.

ALSHAİKH, Hesham, RAMADAN, Nagy, Ahmet H., HEFNY, "RansomwarePreventionandMitigationTechniques", İnternationalJournal Of ComputerApplacations, V. 77, N. 40, 2020, https://www.researchgate.net/publication/339326833_Ransomware_Prevention_and_Mitigation_Techniques, E.T 05.02.2022.

ALTINDERE, Murat, Kişisel Verilerin Korunması Hukuku ve Uygulaması, Adalet Yayınevi, 1. Baskı, Ankara 2020.

ALTUNTAŞ, Abdülaziz, KalıLınux, Kodlab Yayınevi, 11. Baskı, İstanbul 2019.

APAYDIN, Cengiz, "Bilişim Sistemine Girme Suçu", Türkiye Adalet Akademisi Dergisi, C. 0, S. 7, 2016, s. 245-308, https://library.dogus.edu.tr/mvt/pdf.php, E.T 12.11.2020.

APİŞ, Özge, "Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında Ve Kütüklerinde Arama, Kopyalama Elkoyma Koruma Tedbiri", Yasama Dergisi, C.0, S. 37, 2018, s. 49-86, https://dergipark.org.tr/tr/download/article-file/1115263, E.T 12.11.2020.

ARİFOĞLU, Ali, DEMİRER, Mehmet, Şengül, Gökhan, Öz, Osman, Bilişim Terimleri Sözlüğü, Türk Standartları Enstitüsü Yayınları, 1.Baskı, Ankara 2006.

ARSLAN, Rengin "Türkiye'ye Siber Saldırının 10 Günü: Ne Oldu?", 24 Aralık 2015, https://www.bbc.com/turkce/haberler/2015/12/151224_siber_saldiri_arslan, E.T 25.12.2019.

ARSLANTÜRK, Mustafa, İcrasından İnfazına Bütün Yönleriyle Yağma Suçu, Adalet Yayınevi, 3. Baskı, Ankara 2021.

AYDIN, Devrim, Türk Ceza Hukukunda Yağma Suçu, Yetkin Yayınları, 1. Baskı, Ankara 2020.

AYDIN, Sedat Erdem Aydın, AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, On İki Levha Yayıncılık, 1. Baskı, İstanbul 2015.

BANNİSTER, Adam, "Dax – Coted'ArgentHospital İn France Hit ByRansomwareAttacak", The Daily Swig, 15 February 2021, https://portswigger.net/daily-swig/dax-cote-dargent-hospital-in-france-hit-by-ransomware-attack, E.T 01.03.2021.

BANNİSTER, Adam, "Dax – Coted'ArgentHospital İn France Hit ByRansomwareAttacak", The Daily Swig, 15 February 2021, https://portswigger.net/daily-swig/dax-cote-dargent-hospital-in-france-hit-by-ransomware-attack, E.T 01.03.2021.

Barış Taşkın, Be[IN]Crypto, "İşler Karışabilir: Kripto Para Fidyecileri Donald Trump'ı Tehdit Etti", 16 Mayıs 2020, https://beincrypto.com.tr/isler-karisabilir-kripto-para-fidyecileri-donald-trumpi-tehdit-etti/, E.T 15.01.2021.

BAŞARAN, Alper, Siber Kıyamet, Arıon Yayınevi, 1. Baskı, İstanbul 2017.

BAŞARAN, Alperen, Zararlı Yazılımlar, Arıon Yayınevi, 1. Baskı, İstanbul 2019.

BAYLANÇİÇEK, Berk, Webtekno, "Kaliforniya Üniversitesi Hackerlara 1. 14 Milyon Dolar Fidye Ödediğini Açıkladı", https://www.webtekno.com/kaliforniya-universitesi-hackerlara-fidye-odedi-h95936.html, E.T 25.01.2021.

BAYRAKTAR ve diğerleri, Hürriyete, Şerefe, Özel Hayata, Hayatın Gizli Alanına Karşı Suçlar, On İki Levha Yayıncılık, 1. Baskı, C.III, İstanbul 2018.

BAYRAKTUTAN, Serhat, "Hürriyet Aleyhine İşlenen Bir Suç Olarak Hürriyet Suçu, Yayımlanmamış Doktora Tezi, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli 2016.

BGA Security Blog, "Ransomware Saldırılarını Nasıl Tespit Edebilirsiniz", 5 Kasım 2021, https://www.bgasecurity.com/2021/11/ransomware-saldirilarini-nasil-tespit-edebilirsiniz/,E.T. 27.03.2022.

BHATTACHARYYA, S., HASSANİEN, A.E, GUPTA, D., KHANNA, A., PAN, I., (Ed.), İnternationalConference OnInnovative Computing andCommunations, Proceedings of ICICC 2018, Volume 2, SpringerPuplisher, 2018.

BIÇAKCI, Salih, "*NATO'nun Gelişen Tehdit Algısı: 21 Yüzyılda Siber Güvenlik*", Uluslararası İlişkiler Dergisi, C. 10, S. 40, 2014, s. 101-130, https://dergipark.org.tr/tr/download/article-file/540269, E.T. 11.11.2021.

BİLGE, Burak, "*Şantaj Suçu*", İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi C.6, S.1, 2019, s. 131-160, https://dergipark.org.tr/tr/download/article-file/1102151, E.T. 15.01.2021.

BONCUK, İsmail, "Türk Ceza Hukukunda Teşebbüs", İstanbul Kültür Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul 2018.

BÜYÜKGÖZE, Selma, EL, Çağrı, Kendi Siteni Kendin Koru, Kodlab Yayınevi, 1. Baskı, İstanbul 2018.

Charlıe Gere, Dijital Kültür, (Çev: AYDOĞDU, Akın), İstanbul 2019.

Coin Türk, "Yeni Başlayanlar İçin 12 Maddelik Kripto Para Başlangıç Rehberi*",* 2 Ocak 2020, https://coin-turk.com/yeni-baslayanlar-icin-13-maddelik-bitcoin-rehberi, E.T 03.01.2020.

ÇAKIR, Hüseyin, Nursel, YALÇIN, KILIÇ, Mehmet Serkan, "İnternet Sitelerine Yapılan Siber Saldırılar: 2015 yılı Türk Kamu Siteleri İncelemesi", Güvenlik Stratejileri Dergisi, C. 13, S. 25, 2017, s. 149-192, https://dergipark.org.tr/tr/download/article-file/298060, E.T. 18.11.2019.

ÇALIŞKAN, "Behlül, Ağ Toplumunda Bilgi Sızıntılarının Gazeteciliğe Etkisi: Redhack Örneği", Yayımlanmamış Doktora Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2016.

ÇALIŞKAN, Oğuzhan, Secloot, " Washington DC Polis Departmanı Fidye Yazılımı Saldırısına Uğradı", 30 Nisan 2021, https://www.secloot.com/washington-dc-polis-departmani-fidye-yazilimi-saldirisina-ugradi/, E.T 12.05.2021.

ÇELİK, Soner, ÇELİKTAŞ, Barış, *"Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar",* CyberpolitikJournal, C. 3, S. 5, 2018, s. 105-132, https://dergipark.org.tr/tr/download/article-file/536201, , E.T. 08.01.2020.

ÇOBAN, Serhat, "Hackerlık Kavramı, Modeller ve Medyada Hackerlığın Sunumu", Bilişim Teknolojileri Online Dergisi, C. 11, S.40, s.40-43, 2020, https://dergipark.org.tr/en/download/article-file/1096412, E.T 28.01.2022.

ÇOTAK, Alper, "Sigortacılık Sektöründe Siber Güvenliği, Dünyada Ve Türkiye'deki Gelişmelerin İncelenmesi", Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Bankacılık Ve Sigortacılık Enstitüsü, İstanbul 2019.

ÇUBUKÇU, Fatih, Bilgi Güvenliği Yönetim Sistemi, Pusula Yayıncılık, 1. Basım, İstanbul 2018.

DARKReading, "US Treasury's OFAC RansomwareAdvisory: NavigatingTheGrayAreas", 11/24/2020, https://www.darkreading.com/risk/us-treasurys-ofac-ransom ware-advisory-navigating-the-gray-areas/a/d-id/1339394, 01.01.2021.

DEĞİRMENCİ, Olgun, "*2004 Türk Ceza Kanun'un Bilişim Suçları Bakımından Değerlendirilmesi*", TBBD, S. 58, 2005, s. 195-208, http://tbbdergisi.barobirlik.org.tr/m2005-58-141, E.T. 06.03.2021.

DEĞİRMENCİ, Olgun, "Cryptolocker; Bir Fidye Virüsünün Ceza Hukuku Açısından Analizi", Yaşar Hukuk Dergisi, C. 1, S. 2, 2019, s. 175-204. https://dergipark.org.tr/en/download/article-file/1335226, E.T. 15.01.2020.

DEMİRKOL, Neslihan, "Türk Ceza Hukukunda Şantaj Suçu", Yayımlanmamış Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi, Isparta 2017.

DOĞU, Ali Haydar, "*Kişisel Verilerin Korunmasına Genel Bir Bakış*", 34. Bilişim Kurultayı, s. 175-181, 2017, http://ceur-ws.org/Vol-2045/34_Bilisim_2017_paper_23.pdf, E.T. 09.02.2021

DÜLGER, Murat Volkan, "Kişisel Verilerin Korunması Kanunu Ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması", İstanbul MedipolÜniversitesi Hukuk Fakültesi Dergisi C.3, S. 2, 2016, s. 101-168, https://dergipark.org.tr/tr/download/article-file/1102227, E.T. 09.02.2021.

DÜLGER, Murat, "*Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı Ve Uygulaması*", Türkiye Adalet Akademisi Dergisi, C. 0, S. 31, 2017, s. 141-258, https://dergipark.org.tr/tr/download/article-file/981531, E.T. 14.02.2021.

DÜLGER, Murat, Bilişim Suçları Ve İnternet İletişim Hukuku, 4. Baskı, Seçkin Yayınevi, Ankara 2014.

Edward Roche, RAC monitör, "Federal Authorities May ImposeCivilPenaltiesAgainstHospitalsPayingRansomwareDemands", October 28, 2020, https://www.racmonitor.com/federal-authorities-may-impose-civil-penalties-against-hospitals-paying-ransomware-demands, E.T 15.01.2021.

EGEMENOĞLU, Alaaddin, "*Yargıtay Kararları Işığında 5237 Sayılı Türk Ceza Kanunu'nda Tehdit Suçu*", İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, C.4, S.1, 2017, s. 59-102, https://dergipark.org.tr/tr/download/article-file/1102238, E.T. 01.02.2021.

EHLİZ, Hakan, "Bilişim Suçlarının Ulusal Ve Uluslararası Düzeyde Değişen Güvenlik Algısı Üzerinde Etkisi", İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul 2019.

EKİCİ ŞAHİN, Meral, KORUCUL, Irmak, "*Bilişim Sistemine Girme Suçu- Suçun Kamu Personeline Ve Özel Sektör Çalışanlarına Tahsis Edilen Bilgisayarlarla İşlenmesine İlişkin Bir Değerlendirme*", Dokuz Eylül Üniversitesi, Prof. Dr Durmuş TEZCAN'a Armağan, C. 21, Özel S., 2019, s. 585-626, https://hukuk.deu.edu.tr/wp-content/uploads/2019/09/MERAL-EKICI-SAHIN-IRMAK-KORUCULU.pdf, E.T 12.11.2020.

ELBAHADIR, Hamza, Hacking İnterface: Bilişimin Yer altı Dünyası, Kodlab Yayıncılık, 12. Baskı, İstanbul 2016.

EMRE KAYA, Ayşe Elif, "*Enformasyon Toplumunun Suçluları: Hacker'lar*", Marmara İletişim Dergisi, C. 0, S. 16, 2010, s. 46-56, https://dergipark.org.tr/tr/download/article-file/233521, E.T. 25.12.2019.

ERCAN, İsmail, Ceza Hukuku Özel Hükümler, On İkiLevha Yayıncılık, 15. Baskı, İstanbul 2019.

ERDAĞ, Ali İhsan, "*Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda*), Gazi Üniversitesi Hukuk Fakültesi Dergisi, C. 14, S. 2, 2010, s. 275-303, https://dergipark.org.tr/tr/download/article-file/789484, E.T. 06.03.2021.

ERDOĞAN, Yavuz, "*Bilişim Sistemine Girme Ve Kalma Suçu*", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi C. 12, S. 0, 2010, s. 1363-1433, https://dergipark.org.tr/tr/download/article-file/756750, E.T. 03.03.2021.

ERGİN, Toprak, Elif, KÜPELİ, B. Gökay, Siber Kırılma, Altıkırkbeş Yayınları, 1. Baskı, İstanbul 2018.

ERGÜN, İsmail, Siber Suçların Cezalandırılması Ve Türkiye'de Durum, Adalet Yayınevi, Ankara 2008.

ERİŞ, Ufuk, Türkiye'de Kırıcı (Hacker) Kültürü, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, Eskişehir 2009.

Eset, GORETSKY, Aryeh, "RDP'yi İnternetten Ayırma Zamanı Geldi", 23 Aralık 2019, https://www.eset.com/tr/blog/rdpyi-internetten-ayirmanin-zamani-geldi/, E.T. 27.03.2022.

Fidye Yazılımı(Ransomware) Nasıl Bulaşır?, https://sparta.com.tr/makaleler/fidye-yazilimi-nasil-bulasir/, E.T 14.02.2021.

GRİMES, A. Roger, RansomwareProtectionPlaybook, Wiley Publisher, 1st.Edition 2021..

GÜLTEKİN, Melek Nil, "Kişisel Verilerin Ceza Hukuku Yönünden Korunması", Yayımlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2012.

GÜNGÖR, Abdülkadir, Linux İşletim Sisteminde Malware Analizi, Abdülkadir Güngör Yayıncılık, 2021.

GÜNGÖR, Murat, "Ulusal Bilgi Güvenliği: Strateji Ve Kurumsal Yapılanma", Uzmanlık Tezi, T.C Kalkınma Bakanlığı-Bilgi Dairesi Toplumu Başkanlığı, Ankara 2015, s. 40.

Habertürk, "Ece Üner'le 1 Gün", 2017, https://www.youtube.com/watch?v=WjcsHbA, E.T 12.01.2020.

HAFIZOĞULLARI, Zeki, ÖZEN, Muharrem, "*Özel Hayata Ve Hayatın Gizli Alanına Karşı Suçlar*", Ankara Barosu Dergisi, C. 0, S.4, 2009, s. 9- 20, https://dergipark.org.tr/tr/download/article-file/397650, E.T. 02.12.2020.

HAFIZOĞULLARI, Zeki, ÖZEN, Muharrem, Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar, 3. Basım, Ankara 2013.

HENKELOĞLU, Türkay, Adli Bilişim: Dijital Delillerin Elde Edilmesi Ve Analizi, Pusula Yayıncılık, 2. Baskı, İstanbul 2014.

https://muhabbit.com/pakistanin-en-buyuk-guc-saglayicisi-netwalker-tarafindan-hacklendi/, E.T. 01.01.2021.

https://www.1mh.org/bilgisayar-korsanlari-estetik-ameliyat-fotograflarini-sizdirmakla-tehdit-ediyor/, E.T. 15.01.2021.

https://www.darkreading.com/risk/us-treasurys-ofac-ransomware-advisory-navigating-the-gray-areas/a/d id/1339394, E.T. 01.01.2021.

https://www.healthcareitnews.com/news/emea/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak, E.T. 15.01.2021.

https://www.star.com.tr/dunya/musteri-verileri-sizdirildi-israilli-sirketten-fidye-istiyorlar-haber-1592037/, E.T. 25.03.2021

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, E. T 26.06.2021

https://www.yenisafak.com/teknoloji/fidye-yazilimi-ilk-defa-bir-olume-neden-oldu-3568434, E.T. 05.01.2021.

Huobi, BullTrader, "Pakista'nın En Büyük Güç Sağlayıcısı, NetWalker Tarafından Hacklendi", 12 Eylül, 2020, https://muhabbit.com/pakistanin-en-buyuk-guc-saglayicisi-netwalker-tarafindan-hacklendi/, E.T 01.01.2021.

Hürriyet, "Fidye Yazılımı Saldırılarında Büyük Artış", https://www.hurriyet.com.tr/teknoloji/fidye-yazilimi-saldirilarinda-buyuk-artis-41783058, E.T 25.03.2021.

Hürriyet, "Fidye Yazılımı Saldırılarında Büyük Artış", https://www.hurriyet.com.tr/teknoloji/fidye-yazilimi-saldirilarinda-buyuk-artis-41783058, E.T. 25.03.2021.

Hürriyet, "Hacker'lar, California Üniversitesi'nden 1, 1 milyon Dolar Fidye Aldı", 30 Haziran, 2020, https://www.hurriyet.com.tr/teknoloji/hackerlar-california-universitesinden-1-1-milyon-dolar-fidye-aldi-41553360, E.T 14.02.2021.

Investing.com, "Fidye Saldırısından Sonra Ünlü Banka Tüm Şubelerini Kapattı", 8 Eylül, 2020, https://tr.investing.com/news/cryptocurrency-news/fidye-saldrsndan-sonra-nlu-banka-tum-ubelerini-kapatt-2006411, E.T 12.12.2020.

İÇEL, Kayıhan, "*Görünüşte Birleşme (İçtima) ilkeleri Ve Yeni Türk Ceza Kanunu*", İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, S. 14, 2008, s. 35-49, https://kutuphane.dogus.edu.tr/mvt/pdf.php, E.T. 12.12.2020.

İHTİYAROĞLU, Uğur, "*Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi"*, Hacettepe Hukuk Fakültesi Dergisi, C. 10, S. 2, 2020, s. 406-440, https://dergipark.org.tr/tr/download/article-file/1070186, E.T. 01.03.2021.

İLBAŞ, Çığır, "Bilişim Suçlarının Sosyo- Kültürel Seviyelere Göre Algı Analizi", Başkent Üniversitesi Fen Bilimleri Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Ankara 2009.

JDSUPRA, "JonesDay Global Privacy&Cybersecurity Update", January 8, 2021, https://www.jdsupra.com/legalnews/jones-day-global-privacy-cybersecurity-3823733/, E.T 02.05.2021.

JELEN, Sara, "Hacker Vs Cracker: Main DifferencesExplained", https://securitytrails.com/blog/hacker-vs-cracker, E.T. 11.11.2021

KANGAL, Zeynel T.,Kişisel Verilerin Ceza Ve Kabahatler Hukukunda Korunması, On İki Levha Yayıncılık, 1. Baskı, İstanbul 2019.

KARA, İlker *"TeslaCrypt Fidye Yazılım Virüsünün Tespiti, Teknik Analiz Ve Çözümü*", Uluslararası Yönetim Bilişim Sistemleri Ve Bilgisayar Bilimleri Dergisi, C. 2, S. 2, 2018 s.87-94, https://dergipark.org.tr/tr/download/article-file/918843, E.T. 03.01.2020.

KARA, Mahruze, "Siber Saldırılar – Siber Savaşlar Ve Etkileri", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2013.

KARAGÖZ, Mehmet Can, Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme Suçu, On İki Levha Yayıncılık, 1. Baskı, İstanbul 2020.

KARAKAŞ, Ezgi, "Türk Ceza Hukukunda Şantaj Suçu", Yeditepe Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul 2015.

KARAKEHYA, Hakan, "*Türk Ceza Kanun'unda Bilişim Sistemine Girme Suçu*", TBBD, S. 81, 2009, s. 87-94, http://tbbdergisi.barobirlik.org.tr/m2009-81-498, E.T. 06.03.2021.

KILIÇ, Çiğdem, "Dünden Bugüne Fidye Yazılımların (Ransomware) Gelişimi Ve Geleceği", Yayımlanmamış Yüksek Lisans Tezi, Bilgi Üniversitesi Lisansüstü Programlar Enstitüsü, İstanbul 2019.

KILIÇ, Zeynep, Siber Bülten, "ABD Fidye Yazılım Saldırılarını Terörizmle Eş Tuttu", https://siberbulten.com/dijital-guvenlik/abdden-fidye-yazilimcilara-terorist-muamelesi/, E. T 26.06.2021.

Kişisel Verileri Koruma Kurumu, 100 Soruda Kişisel Verileri Korunması Kanunu, KVKK Yayınları, Ankara 2018.

Kişisel Verileri Koruma Kurumu, https://www.kvkk.gov.tr/Icerik/6961/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-DLSY-Adi-Ortakligi, E.T 24.06.2021.

KOCA, Mahmut, ÜZÜLMEZ, İlhan, "*Kişisel Verilerin Kaydedilmesi Suçu*", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr Durmuş TEZCAN'a Armağan, C. 21, Özel S. 2019, s. 69-93, https://hukuk.deu.edu.tr/wp-content/uploads/2019/09/ MAHMUT-KOCA-ILHAN-UZULMEZ.pdf, E.T. 02.12.2020.

KOCA, Mahmut, ÜZÜLMEZ, Mahmut, "Türk Ceza Hukuku Özel Hükümler, Adalet Yayınevi, 5. Baskı, Ankara 2018.

KODAZ, Halife, BOTSALI, M. Fatih, "Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması", Selçuk Teknik Dergisi", C. 9, S. 1, 2010, s.11- 14.

KONUKSEVEN, Saadettin, ÖZEN, Tuna, 50 Yıllık Hayal Bitcoin, MediaCat Yayıncılık, 1. Baskı, İstanbul 2018.

KORKMAZ, Ali " *İnsan Hakları Bağlamında Özel Hayatın Gizliliği Ve Korunması",* Karamanoğlu Mehmet Bey Üniversitesi Sosyal Ve Ekonomik Araştırmalar Dergisi 16, S. 1, 2014, s. 99-103, https://dergipark.org.tr/tr/download/article-file/107205, E.T. 09.02.2021.

KUMAR, R., QUANG,N.H, KUMAR SOLANKI, V., CORDANA, M., KUMAR PATTNAİK (Ed.), ResearchInİntelligentAnd Computing İn Engineering: Select Proceedings Of Rıce 2020, SpringerPuplisher, 1.st.ed., 2021.

KURT, Levent, Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları, Seçkin Yayınevi, Ankara 2005.

LİSKA, Allan, GALLO, Timothy, RansomwareDefendingAgainistDigitalExtortion, O'Relly Publisher, ABD 2017.

M. DİNÇ, Yasemin, RUHİ, M.EMİN, "*Türk Ceza Kanununda Yağma Suçu*", Erzincan Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, C. 11, S. 2, 2018, s. 96, https://dergipark.org.tr/tr/download/article-file/614261, E.T. 25.03.2022.

MAHMUTOĞLU, Fatih Selami, "*Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar Ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 71, S. 1, 2013, s. 859.

Marmara Belediyeler Birliği, Belediyelerde Veri Yönetiminde Kişisel Verilerin Korunması Kanuna Uyum Süreci Raporu, 2018, s. 9. https://marmara.gov.tr/

UserFiles/Attachments/2018/06/08/7d98853e-8dea-4b52-ad86-978f7f1604fb.pdf, E.T. 09.02.2021.

Milliyet, "2016'nın En Büyük Siber Saldırıları Nerelere Yapıldı?" 29 Aralık, 2016, https://www.milliyet.com.tr/galeri/2016-nin-en-buyuk-siber-saldirilari-nerelere-yapildi-2369865/1, E.T 09.02.2021.

Mühendislik Teknoloji Danışmanlık, 2016 Ekim- Aralık Dönemi Siber Tehdit Durum Raporu,https://afyonluoglu.org/PublicWebFiles/Reports-TR-SG/2016%20T%C3%BCrkiye%20Siber%20Tehdit%20Durum%20Raporu-STM.pdf, E.T. 12.01.2020.

Mühendislik Teknoloji Danışmanlık, 2017 Nisan-Haziran Dönemi Siber Tehdit Durum Raporu, 2017, s. 9, https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-nisan-haziran-2017, E.T. 12.01.2020.

NEBİL, Füsun Sarp, BitcoinVe Kripto Paralar, Pusula Yayıncılık, 1. Baskı, İstanbul, 2018.

NOYAN, Erdal, Hırsızlık Suçları, Adalet Yayınevi, 2. Baskı, Ankara 2007..

NTV, "Bilgileri Çalınan Yahoo Kullanıcıları Ne Yapmalı?", 23 Eylül 2016, https://www.ntv.com.tr/galeri/teknoloji/bilgilericalinanyahookullanicilarineyapmali, IAVLacY7MUaokX95-v1CLg/VxQFBonBo0i5JnQCl7QZ4g, E.T 09.02.2021.

OLSON, Parmy, Biz Anonsymous'uz, (Çev.AĞIRNASLI, Suphi Nejat), Paloma Yayınevi, 1. Baskı, İstanbul 2014.

ÖZBEK, Veli Özer, DOĞAN, Koray, BACAKSIZ, Pınar, TEPE, İlker, "Türk Ceza Hukuku Özel Hükümler", Seçkin Yayıncılık 13. Baskı, Ankara 2018.

ÖZBEK, Veli Özer, DOĞAN, Koray, BACAKSIZ, Pınar, TEPE, İlker, "Türk Ceza Hukuku Özel Hükümler", Seçkin Yayıncılık 13. Baskı, Ankara 2018.

ÖZCAN, Fethi Feyyaz, "Yeni Medya Ve Dijital Aktivizm", Yayımlanmamış Yüksek Lisans Tezi, Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2012.

ÖZÇAKMAK, Burak, "Fidye Yazılımları Analizleri Ve Korunma Yöntemleri", Gazi Üniversitesi Fen Bilimleri Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Ankara 2018, s. 72.

ÖZÇELİK, Büşra, "Bilişim Sistemine Girme Suçu", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2019.

ÖZÇOBAN, Cuma, "21. Yüzyılda Ulusal Güvenliğin Sağlanmasında Siber İstihbaratın Rolü", Yayımlanmamış Yüksek Lisans Tezi, Milli Savunma Üniversitesi Harp Akademileri Stratejik Araştırmalar Enstitüsü, İstanbul 2014, s. 55

ÖZKAN, Asaf, TAŞDELEN, Esra, *"Türkiye'de Kişi Hak Ve Özgürlüklerinin Gelişimi Bağlamında Hürriyet-i Şahsiye Kanunu*", Atatürk Dergisi, C.8, S. 1, 2019, s. 53-78, https://dergipark.org.tr/tr/download/article-file/767525, E.T. 15.01.2021.

ÖZKAN, İbrahim, "Siber Saldırıların Ekonomik Boyutu", Yayımlanmamış Yüksek Lisans Tezi, Bilecik Şehy Edebali Üniversitesi Sosyal Bilimler Enstitüsü, , Bilecik 2019.

ÖZSOY, Nevzat, "Yargıtay Kararları Işığında Doğrudan Bilişim Suçları", Yaşar Hukuk Dergisi, C.1, S. 2, 2019, s. 295-352.

ÖZÜNALDIM, Anıl, "2020 Yılının En Büyük Faaliyetleri", https://www.tamindir.com/haber/2020-en-buyuk-hackler_64127/, E.T 02.12.2020.

PALLI, Hayati, "Türk Hukukunda Ve Mukayeseli Hukukta Bilişim Suçları", Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Kayseri 2008.

PARLAR, Ali, ÇOBANOĞLU, Yekta, Uygulamada Özel Hayata Ve Hayatın Gizli Alanına Karşı Suçlar, Aristo Yayınevi, 1. Baskı, İstanbul 2018, s. 303.

ROBİNSON, Teri, " Ransomware Attack Cost New Orleans $7 MillionAndCounting", 17 January 2020, https://zephyrnet.com/tr/ransomware-attack-cost-new-orleans-7-million-and-counting/, E.T. 25. 03. 2021.

ROBİNSON, Teri, " Ransomware Attack Cost New Orleans $7 MillionAndCounting", 17 January 2020, https://zephyrnet.com/tr/ransomware-attack-cost-new-orleans-7-million-and-counting/, 25. 03. 2021.

S. BAKLACI, Sevim, Yağma Suçu, Yaşar Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İzmir 2020.

SANDILAÇ, Nurullah, "Siber Dünyada Hacker Kültürü, HacktivizmVe Bilişim Suçları", Yayımlanmamış Yüksek Lisans Tezi, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sakarya 2021.

SARAN, A.Nurdan, "Fidye Yazılımlar", Siber Güvenlik ve Savunma Kitap Serisi 3, SAĞIROĞLU, Şeref,(Editör), Grafiker Yayınları, 1. Baskı, Ankara 2019.

SARIUSTA, Kader, "Kişisel Verilerin Ceza Hukuku Yoluyla Korunması", Yayımlanmamış Yüksek Lisans Tezi, Gaziantep Üniversitesi Sosyal Bilimler Enstitüsü, Gaziantep 2018.

SCOTT, James, SPANIEL, "Drew, TheIcıtRansomware Rapor", InsututeforCrıtıcıalInfrastructureTechnology, 2016, s. 10., https://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report2.pdf, E.T 08.02.2022.

SEALS, Tara, "RyukRansomware: NowWithWorming Self- Propagation", Threat Post, 2021, https://threatpost.com/ryuk-ransomware-worming-self-propagation/164412/, E.T. 15.02.2022.

SELİMOĞLU, Seval, ALTUNEL, Mehtap, "*Siber Güvenlik Risklerinden Korunmada Köprü Ve Katalizör Olarak İç Denetim",* Denetişim Dergisi, C. 0, S 19, 2019, s. 5-16, https://dergipark.org.tr/tr/download/article-file/750860, E.T.03.01.2020

Sigorta Medya, "Fidye Yazılımı Saldırılarının Şirketlere Maliyeti 20 Milyar Doları Aştı", 17 Şubat 2020, https://www.sigortamedya.com.tr/fidye-yazilimi-saldirilarinin-sirketlere-maliyeti-20-milyar-dolari-asti/, E.T. 21.03.2022.

SOLMECKE, Christian, "DüsseldorfUnıklinikGehackt – Patienttot. Mord?", 3 November 2020, https://www.youtube.com/watch?v=C66ZzCVuobE, E.T 06.03.2021.

Sözcü, "Yemek Sepetine Veri İhlalinden Ceza Kesildi", 7 Şubat 2022, https://www.sozcu.com.tr/2022/ekonomi/yemek-sepetine-veri-ihlalinden-ceza-kesildi, E.T. 25.03.2022.

SPIN Media LLC, C. 9, S. 10, 1994, s. 63-92.

STARK, John Reed, "*RansomwarePayment: Legality, Logistics, andProof Of Life*", NasdaqGovernanceClearinghouse, 2017, https://listingcenter.nasdaq.com/assets/Ransomware_White_Paper_2.pdf, E.T. 12.02.2020.

STARK, John Reed, Kevin M. LaCroix (By), "RansomwarePayment: Legality, Logistics, Mitigation, AndInsurance", July 12, 2017, https://www.dandodiary.com/2017/07/articles/uncategorized/guest-post-ransomware-payment-legality-logistics-mitigation-insurance/, E.T 11.02.2021.

STEFENKO, Lukas, "Android Fidye Yazılımı Geri Döndü", https://www.eset.com/tr/blog/android-fidye-yazilimi-geri-dondu/, E.T 10.12.2021.

ŞAHİN, Tamer, Hacker'ın Aklı, Doğan Yayıncılık, 3. Baskı, İstanbul 2012.

ŞENTÜRK, Fatih, " *Beyaz Yaka Suçları Ve Yolsuzluklar*", Çankırı Karatekin Üniversitesi İktisadi İdari Bilimler Fakültesi Dergisi, C. 3, S. 2, 2013, s. 143-167, https://dergipark.org.tr/tr/download/article-file/382278, E.T. 12.02.2020

TheStateOf Ransomware 2021, https://www.sophos.com/en-us, April 2021, s. 12, E.T. 25.03.2022.

TomorrowUnlocked, "Hacker: Hunter- WannaCry: TheMarcusHutchinsStory- All 3 Chapters", https://www.youtube.com/watch?v=vveLaA-z3-o&t=10s, (2019), (13:32 - 14:50), E.T. 25.03.2021.

TRÖNDLE, Herbert, FİSCHER, Thomas, StrafgesetzbuchUndNebengesetze, C.H BeckVerlag, 52. Auflage, 2004.

TRT Haber, "İngiltere'de Hastaneye Siber Saldırı: Ünlülerin Estetik Fotoğrafı Yayılabilir", 25 Aralık, 2020, https://www.trthaber.com/haber/dunya/ingilterede-hastaneye-siber-saldiri-unlulerin-estetik-fotograflari-yayilabilir-541036.html, E.T 12.02.2020.

TRT Haber, "İrlanda Sağlık Servisi Siber Saldırıya Uğradı", 14 Mayıs 2021, https://www.trthaber.com/haber/dunya/irlanda-saglik-servisi-siber-saldiriya-ugradi-580851.html, E.T. 24.06.2021.

TURHAN, Oğuz, "Bilgisayar Ağları İle İlgili Suçlar(Siber Suçlar), Planlama Uzmanlığı Tezi, T.C Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Ankara, 2006.

Turner Wright, Cointelegraph Türkçe, "Donald Trump'a Hacker Tuzağı- 42 MilyonDolarlık XMR İstiyorlar", 15 Mayıs, 2020, https://tr.cointelegraph.com/news/ ransomware-gang-demands-42m-or-it-releases-trumps-dirty-laundry, E.T 15.01.2021.

Türkiye Adalet Akademisi, ALTUĞ, Şahin (Editör), Yargıtay Ceza Daireleri Uygulamasında Sıklıkla Rastlanan Bozma Sebepleri, Ankara Açık Ceza İnfaz Kurumu İş yurdu Müdürlüğü Matbaası, 2. Baskı, Ankara 2018, s. 664.

United StatesDepartment of Justıce, "United States Peter Levashov", https://www.justice.gov/usao-ct/us-v-peter-levashov, E.T 02.03.2021.

United StatesDepartment of Justıce, "United StatesYevgenyNikulin, https://www.justice.gov/usao-ndca/pr/russian-hacker-sentenced-over-7-years-prison-hacking-three-bay-area-tech-companies, E.T 16.03.2021.

ÜZÜLMEZ, İlhan, Tehdit, Şantaj Ve Cebir Kullanma Suçları, Turhan Kitabevi, 1. Bası, Ankara 2007.

Wikipedia, https://tr.wikipedia.org/wiki/Bili%C5%9Fim, E.T 12.11.2020

YALMAN, Yıldıray, Siber Terör, Terörizm ve Mücadele, Siber Güvenlik ve Savunma, SAĞIROĞLU, Şeref, ALKAN, Mustafa, (Ed), Grafiker Yayınları, 1. Baskı, Ankara 2018.

YANAR, , Yasin, Ceza Hukuku Ve Bağlamında Hukuku Bağlamında Tck Md. 245/A Yasak Cihaz Veya Programlar Suçu, Yayımlanmamış Yüksek Lisans Tezi, İstanbul 2019.

YAŞAR, Kenan Evren, "*Güncel Değişikliklerle Fransız Ceza Hukukunda Örgüt Kavramı Ve Örgütlenme Suçları*", Ceza Hukuku Ve Kriminoloji Dergisi, C. 3, S. 1, 2015, s. 191-237, https://dergipark.org.tr/tr/download/article-file/14679, E.T. 01.03.2021.

YILDIZ, Eyyüp, BARAN, Ahmet, ASLAY, Fulya, "Ransomware Tehdidinin Evrimi, Bilişim Sistemlerinin Korunması Ve Zarar Hafifletme Stratejileri", Mühendislik Alanında Araştırma Ve Değerlendirmeler, HASDEMİR, Zehra, TURHAN, Mahmut, (Ed.), Gece Kitaplığı, C.1, 1.Basım, Ankara 2021.

YILMAZ, Mehmet Sait, "Beyaz Saray, ABD Siber Güvenlik Savunmasını Artırmak İçin Krtik Kararlar Aldı", 14 Mayıs 2021, https://www.cozumpark.com/beyaz-saray-abd-siber-guvenlik-savunmasini-arttirmak-icin-kritik-kararlar-aldi/, E.T. 26.06.2021.

YILMAZ, Sacit, "*5237 Sayılı TCK'nın 244. Maddesi Alanında Düzenlenen Bilişim Alanındaki Suçlar*", TBBD, C.0, S. 92, 2011, s. 62-100, ,https://kutuphane.dogus.edu.tr/mvt/pdf.gif, E.T. 12.11.2020.

YILMAZ, Sacit, Türk Ceza Hukuku Sisteminde Siber Suçlar, 1. Basım, Adalet Yayınevi, Ankara 2016.

YILMAZ, Seda, "Siber Güvenliğin Sağlanmasında Yazılım Kalite Süreçlerinin Önemi", Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara 2015.

YURTCAN, Erdener, Hürriyete Karşı Suçlar, Adalet Yayınevi, 3. Baskı, Ankara 2012.

YÜKSEL, Yavuz Sultan Selim, "Bilgisayar Korsanlarından "SextortionİIe Şantaj", 12 Ağustos, 2020, https://www.hurriyet.com.tr/gundem/bilgisayar-korsanlarindan-sextortion-ile-santaj-40926096, E.T.15.01.2021.

İNTERNET KAYNAKLARI

https://dergipark.org.tr/tr/

https://www.hsk.gov.tr/

https://www.enigmasoftware.com/

https://sozluk.gov.tr/,

https://www.eset.com/tr/

https://www.savunmatr.com/

https://www.webtekno.com/

https://www.nedir.org/

https://sibermagazin.com/

https://tr.wikipedia.org/wiki/Anasayfa

http://tbbdergisi.barobirlik.org.tr/

https://www.kvkk.gov.tr/veri-ihlali-bildirimi/

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı-Soyadı : Cansu ADAM

Doğum Yeri ve Tarihi :

Elektronik Posta Adresi :

Eğitim Durumu

Lisans Öğrenimi : 2016, KTO Karatay Üniversitesi, Hukuk Fakültesi

Yüksek Lisans Öğrenimi : 2022, KTO Karatay Üniversitesi, Kamu Hukuku Anabilim Dalı (Tezli Yüksek Lisans)

Bildiği Yabancı Diller : İngilizce, Almanca

İş Deneyimi

Stajlar : 2016, Avukatlık Stajı

Avukatlık Stajı

Çalıştığı Kurumlar : Konya Barosu, Avukat

Tarih: 20 Nisan 2020