İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

DÜNDEN BUGÜNE FİDYE YAZILIMLARIN (RANSOMWARE) GELİŞİMİ VE GELECEĞİ

Çiğdem KILIÇ
113691008

Dr.Öğr.Üyesi Tayfun ACARER

İSTANBUL
2019

Dünden Bugüne Fidye Yazılımların (Ransomware) Gelişimi ve Geleceği

Ransomware from Yesterday to Today Development and Future

Çiğdem Kılıç
113691008

Tez Danışmanı :	**Dr.Öğr.Üyesi Tayfun Acarer** İstanbul Bilgi Üniversitesi	(İmza) .....
Jüri Üyeleri :	**Doç. Dr. Leyla Keser Berber** İstanbul Bilgi Üniversitesi	(İmza) .....
	Dr.Öğr.Üyesi Murat Önok Koç Üniversitesi	(İmza) .....

Tezin Onaylandığı Tarih : 12.06.2019
Toplam Sayfa Sayısı : 98

1) Fidye yazılımları	1) Ransomware
2) Siber güvenlik	2) Cyber security
3) Anti-fidye	3) Anti-malware
4) Siber saldırı	4) Cyber attack
5) Zararlı yazılım	5) Malware

TEŞEKKÜRLER

Başta, tez çalışmam sırasında desteğini hiçbir zaman esirgemeyen çok değerli danışman hocam Dr.Öğr.Üyesi Tayfun Acarer'e, bu konuda beni araştırma yapmaya motive eden Prof.Dr. Ahmet Denker'e, tez sürecinde beni hep destekleyen Doç.Dr.Leyla Berber'e, çalışmanın kapsamlı bir perspektif sunmasına araştırmalarıyla katkıda bulunan ve isimleri metin içerisinde geçen kurum ve derneklere, hummalı hazırlık sürecimde anlayışlarını, yorumlarıyla birlikte katkılarını esirgemeyen başta Ece ve Yener Kılıç olmak üzere aileme ve dostlarıma teşekkürlerimi sunarım.

ÖN SÖZ

Gerek bir ülkenin, gerek bir şirketin, gerekse bir toplumun geleceğini oluşturan unsurlar arasında başta sanayi ve teknoloji üretimi olmak üzere ekonomik dinamikler hayati yer teşkil eder. Ancak güvensiz, korku ve endişe yüklü bir ortamda bu dinamiklerin doğru yönlendirilmesi imkansızdır. Yer altı dünyasının önemli bir enstrümanı haline gelen fidye yazılımı saldırıları, tesis edilmesi arzu edilen gelişim ve huzur ortamının önündeki en ciddi engellerden biri halini almıştır. Yaşanan gelişmeler; kurbanların tuzaklara düşme konusunda yeterince bilinçli olmadıklarının, saldırganların hızına paralel hızda önlemlerin hayata geçirilmesi konusunda geri kalınabildiğinin ve saldırganların bu yolla para kazanmaya devam ettiklerinin kanıtı niteliğindedir. Bu çalışma ile konunun çözüme kavuşturulması için en temel gereklilik olan "farkındalığın" yaratılması hedeflenmiştir.

İÇİNDEKİLER

KISALTMALAR

ABD: Amerika Birleşik Devletleri

AIG: American International Group (Sigorta şirketi)

ATM: Automatic Teller Machine (Otomotik vezne makinesi)

BT: Bilgi teknolojileri

BTK: Bilgi Teknolojileri ve İletişim Kurumu

FBI: Federal Bureau of Investigation (Federal Soruşturma Bürosu)

GSMA: GSM Association (GSM Derneği)

IoT: Internet of Things (Nesnelerin İnterneti)

IP: Internet Protocol (Internet Protokolü)

KOBİ: Küçük ve Orta Büyüklükteki İşletmeler

MBR: Master Boot Record (Ana Kart Kaydı)

MIT: Massachusetts Institute of Technology (Massachusetts Teknoloji Enstitüsü)

NHS: National Health Service (Sağlık Bakanlığı)

PoS: Point Of Sales Terminal (Satış noktaları terminali)

RaaS: Ransomware as a Service (Hizmet Olarak Fidye Yazılımı)

RDP: *Remote Desktop* Connection (Uzak Masaüstü Protokolü)

RSA: Geliştiricilerinin soyadlarının baş harfleri ile adlandırılmış bir şifreleme yöntemi

SMB: Server Message Board (Sunucu İleti Bloğu)

TCK: Türk Ceza Kanunu

TOR: The Oninon Routing (açık kaynak kodlu bir İnternet ağ tarayıcısı)

URL: Uniform Resource Locator (Tekdüzen kaynak bulucu)

US-CERT: United States Computer Emergency Readiness Team (Amerika Birleşik Devletleri Bilgisayar Acil Durum Hazır Ekibi)

USD: United States Dollar (Amerikan Doları)

USOM: Ulusal Siber Olaylara Müdahale Merkezi

VPN: Virtual Private Network (Sanal özel ağ)

Yrd. Doç. Dr.: Yardımcı Doçent Doktor

ŞEKİL LİSTESİ

ÖZET

Fidye yazılımları (ransomware), son yıllarda hem kurumları hem de bireyleri ciddi ölçüde etkileyen ve mağduriyetlerine yol açan küresel bir tehdit olarak karşımıza çıkmaktadır. Şantaj yazılımları da olarak bilinen bu yazılım türü, kurbanlarının makinelerini şifreleme, kilitleme yoluyla ele geçirerek şifreyi çözecek anahtarı belirli bir ücreti ödemeleri karşılığında verebileceğini söyleyen siber saldırganların kullandığı zararlı yazılımlar olarak tanımlanmaktadır. Fidye yazılımları, özellikle uygun güncelleme ve yedekleme prosedürlerini yerine getirmeyen, uygun bir siber güvenlik altyapısı bulunmayan kurbanları etkilemektedir. 30 yıl önce ortaya çıkmasına karşın, son yıllarda gelişen otomasyon seviyesi, bilişime olan bağımlılığın vazgeçilmez hale gelmesi ile birlikte önem derecesini zirveye taşımış ve zirvedeki yerini korumayı sürdürmüştür. Dünya çapında milyarlarca kullanıcıyı etkileyen ve milyarlarca dolarlık kayıp ve hasara neden olan fidye yazılımları, küresel suç örgütleri için silah ya da uyuşturucu ticareti gibi lokomotif iş alanlarından biri haline gelmiştir. Günümüze kadar fidye yazılımı saldırıları halen kayda değer etkisini devam ettirerek gelmiş, gelecek için de ciddi tehdit oluşturacağının sinyallerini vermiştir. Bu yazılımların, kurumlar ve bireyleri potansiyel hedef kitlesi olarak aldığı ve toplam cihaz sayısının milyarlarca olduğu düşünüldüğünde, bu konunun araştırmaların ve yatırımların merkezinde olması yadsınamaz bir gerçeklik olarak karşımıza çıkmaktadır.

Bu tezde, fidye yazılımlarının gelişimi gözetilerek, fidye yazılımlarındaki ortak ve sıra dışı yöntemler incelenerek geleceğin fidye yazılım dünyası için ön analiz gerçekleştirilmiştir. Bu tez, geleceğin teknoloji dünyasında kurumsal şirketlerin, kamu kuruluşlarının ve bireylerin, bu zararlı etkiler nedeniyle nelere dikkat etmeleri ve neleri dikkate alacak şekilde geleceklerini şekillendireceklerine ışık tutmak amacıyla kaleme alınmıştır. Ayrıca, gelecekte yapılacak akademik çalışmalar açısından da literatür ihtiyaçlarını açığa çıkaracaktır. Bunların yanı sıra, bugüne kadar fidye yazılımlarına, kayıtsız kalan bireylerin ve kurumların bu konunun yıkıcı sonuçlarından dolayı dikkatlerini de çekmeyi hedeflemektedir.

Tezde, birinci bölümde fidye yazılımları ile ilgili genel bilgilere, ikinci bölümde etkilerine, üçüncü bölümde fidye yazılımlarının geleceğine, dördüncü bölümde alınabilecek önlemlere ve son bölümde ise genel değerlendirme ve önerilere yer verilmiştir.

ABSTRACT

Ransomware has emerged as a global threat that has significantly affected both institutions and individuals in recent years. This type of software, also known as blackmail software, is defined as malicious software used by cyber intruders who say that they can give their victims in exchange for a certain fee by deciphering their machines by encrypting, locking, and decoding the key. In particular, ransomware affects victims who do not have an appropriate cyber security infrastructure, especially if they are not performing the appropriate update and backup procedures. Although it emerged 30 years ago, the level of automation developed in recent years, with the dependence on cognition becoming indispensable, carried the importance level to the top and continued to maintain its place in the top. Ransomware, which affects billions of users worldwide and causes billions of dollars of loss and damage, has become one of the locomotive business fields for global criminal organizations such as weapons or drug trafficking. Until now, ransomware attacks have continued to have a considerable impact and have signaled that it will pose a serious threat to the future. Considering that these softwares take the institutions and individuals as their potential target audience and the total number of devices is billions, it is an undeniable reality that this issue is at the center of research and investments.

In this thesis, by considering the development of ransomware, common and extraordinary methods in ransomware were examined and preliminary analysis was carried out for the future of the ransomware world. This thesis has been written in order to shed light on what the corporate companies, public institutions and individuals in the future of the future will shape their future by taking into account what these harmful effects are and what they will take into consideration. It will also reveal the needs of literature in terms of future academic studies. In addition to

this, the aim is to draw attention to the ransomware and the indifferent individuals and institutions to the attention of the devastating consequences of this issue.

In the thesis, general information about ransomware in the first section, the effects of the second part, the future of ransomware in the third part, the measures that can be taken in the fourth section and the final evaluations are given in the last section.

GİRİŞ

Fidye yazılımları (İngilizcesi ile ransomware), zararlı yazılım türlerindendir (malware). Şantaj yazılımları ya da fidye virüsü olarak da bilinmektedir. Fidye yazılımları, sürekli gelişmeleri ve yaygınlaşmaları ile beraber günümüzde en sık rastlanan siber tehdit unsurları arasında yer almıştır. Hatta "yüzyılın tehdidi" olarak da nitelendirilmektedir. İşleyiş, saldırganların hedeflerindeki bilgisayar sistemi ya da sistemlerini kilitleyerek ve / ya da dosyaların bazıları ya da tümünü şifreleyerek kullanıcının erişimini engellemek suretiyle kullanıcıdan para koparmaya çalışmaları üzerine kurgulanmaktadır.

1. FİDYE YAZILIMLARINA İLİŞKİN GENEL BİLGİLER

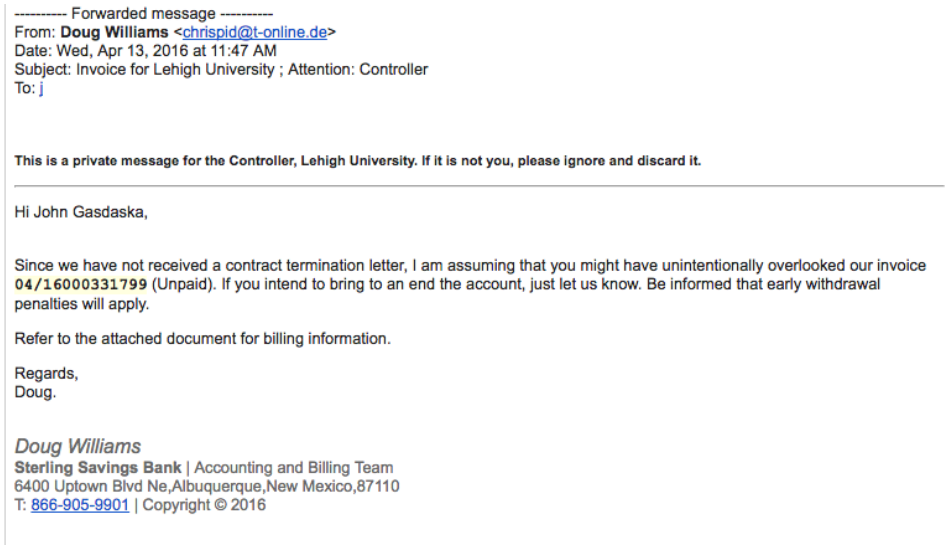
1.1. Fidye Yazılımları Hakkında Temel Bilgiler

Fidye yazılımlarına geçmeden önce "truva atı" (ya da "trojan") kavramının bilinmesinde fayda vardır. Bu kavram, asıl amacını çeşitli metodların ardına gizlenerek gerçekleştirmeyi hedefleyen, meşru yazılım kılığındaki zararlı yazılımları tanımlamaktadır. Mitolojideki Truva Atı'nın bir armağan gibi gösterilip aslında Troya'yı ele geçirecek askerleri içermesine dayanan efsaneye atfen bu isim konmuştur. Nitekim sanal dünyadaki truva atları masum görüntülerinin ardında güvenliği tehdit edici amaçlara hizmet etmektedirler. Truva atları, herhangi bir virüs programının aksine bilgisayar sistemlerinde kendi kendilerine çoğalmaz. Dosyaları ya da sistemi kullanılamaz hale getiren saldırganlar, mağdurlarıyla iletişime geçer ve bu durumun ortadan kaldırılması için para talep ederler. Sonuç olarak fidye yazılımı bir virüs değildir.

Saldırgan önce fidye yazılımını mağdurun cihazına sokarak çalıştırır. Fidye yazılımının bir cihaza girmesini sağlamanın birkaç temel yolu bulunmaktadır. Bunlar:

1- E-posta yoluyla: Fidye yazılımlarını herhangi bir mağdurun bilgisayarına / sistemine yüklemek için en sık kullanılan yolların başına zararlı yazılım içeren e-postalar gönderilmesi gelmektedir. Bu e-postalar çoğunlukla tanınmış şirketlerin adı ve ikna edici içerikler ile gönderilir. Siparişler, telefon faturaları, randevu onayları, kargo haberi gibi masum mesajların ardına gizlenebilirler. Dolayısıyla kullanıcılar bu tip e-postaları genellikle çekinmeden açma ve ekindeki dosyaları inceleme eğiliminde olurlar. Ancak bu sırada farkında olmadan zararlı yazılımı cihazlarına indirme tuzağına düşmüşlerdir; yani fidye yazılımı artık mağdurun cihazına girmiş bulunmaktadır.

Örnek:



---------- Forwarded message ----------
From: **Doug Williams** <chrispid@t-online.de>
Date: Wed, Apr 13, 2016 at 11:47 AM
Subject: Invoice for Lehigh University ; Attention: Controller
To: j

This is a private message for the Controller, Lehigh University. If it is not you, please ignore and discard it.

Hi John Gasdaska,

Since we have not received a contract termination letter, I am assuming that you might have unintentionally overlooked our invoice **04/16000331799** (Unpaid). If you intend to bring to an end the account, just let us know. Be informed that early withdrawal penalties will apply.

Refer to the attached document for billing information.

Regards,
Doug.

Doug Williams
Sterling Savings Bank | Accounting and Billing Team
6400 Uptown Blvd Ne,Albuquerque,New Mexico,87110
T: 866-905-9901 | Copyright © 2016

Şekil 1: E-posta yoluyla fidye yazılımı saldırısı

2- Web yoluyla: Kötü amaçlı yazılımlar, İnternet'te dolaşırken ziyaret edilen herhangi bir web sitesinden de (özellikle de forum siteleri, program indirme siteleri, erotik içerik siteleri, oyun siteleri) bulaşabilmektedir. Bunlar yasal ya da yasadışı siteler olabilmektedir. Kullanıcının siteyi ziyareti sırasında çoğunlukla bilgisayarında güncelleme gerektiği, lisanssız uygulama kullanıldığı, hayvan pornografisi gibi yasadışı içerik bulunduğu, sistemin virüslere karşı taranması gerektiği ve ücretsiz bir virüs tarama programı teklif edildiği gibi sahte iddialar

öne süren mesajlar içeren küçük pencereler (pop-up'lar) açılır. Bazen bu küçük reklam pencerelerinde yasal logolar da kullanılarak bilinçli kullanıcılar bile tuzağa düşürülebilmektedir. Bu tuzağa düşen kullanıcının cihazına artık fidye yazılımı yüklenmiştir.

Bazı fidye yazılımları herhangi bir tehdit unsuruna tıklanmasa dahi, masum görünen bir web sayfasının ziyaret edilmesi esnasında arka planda çalışarak mağdurlarının bilgisayarlarına sızabilmektedirler.

Örnek:

Şekil 2: Web yoluyla fidye yazılımı saldırısı

3- Harici donanımlar yoluyla: Fidye yazılımları, taşınabilir bellekler, DVD'ler, CD'ler başta olmak üzere bilgisayara bağlanabilen çeşitli aygıtlar yoluyla da bulaştırılabilmektedir.

Örnek:

Şekil 3: Harici donanımlar yoluyla fidye yazılımı saldırısı

4- Botnet'ler ve sosyal mühendislik yoluyla: Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı, sosyal mühendisliği şöyle tanımlamaktadır: Belirli bir bilgiyi açığa çıkarmak veya meşru olmayan belirli bir eylemi gerçekleştirmek için bir hedefe konuşan tüm teknikler. Bunun yanı sıra bilişim teknolojileri açısından ise şöyle ele almaktadır: Dolandırıcının bir BT sistemine gizlice girerek kötü amaçlarını yerine getirebilmek için psikolojik manipülasyon yöntemleri kullanması. İnsan psikolojisini kullanmanın, siber saldırganların günümüzde sıkça kullanmaya başladıkları bir yöntem olduğu görülmektedir.

Saldırganlar mağdurların duygu sömürüsü (tacize hayır) ya da eğlence güdülerini kullanarak (oyun) ücretsiz yazılımlar indirmelerini sağlar. Bu ücretsiz uygulamalar, ücretsiz yazılım oyunları veya taranan herhangi bir kötü amaçlı yazılımın bulunmadığı ancak yazılımları indirmek için kodun yerleşik olduğu araçlar olarak gelir.[1]

[1] Ransomware Digital Extortion: A Rising New Age Threat; Indian Journal of Science and Technology, Vol 9(14), DOI: 10.17485/ijst/2016/v9i14/82936, Nisan 2016

5- Ransomware as a Service (RaaS; Hizmet Olarak Fidye Yazılımı) yoluyla: Siber suçlular tarafından bulut ortamında çalıştırılan uygulamaların kullanılması yoluyla mağdurların bilgisayarlarına sızılmasına dayanır.[2]

Bilgisayar sistemi ya da sistemlerine fidye yazılımı yüklenmiş olan mağdur kullanıcıyı, artık bu durumdan kurtulmak için teklif edilecek bir fidye tutarı beklemektedir. Özellikle şirketlerde bu durum, iş sürekliliğini ciddi şekilde sekteye uğratmaktadır. 2017 yılında İngiltere NHS'e (National Health Service) yapılan bir saldırıda, hastane ve doktorların hastaları geri çevirerek sağlık hizmeti veremeyecek durumunda kaldıkları basına yansıyan haberler arasındadır.[3]

Son derece tehlikeli olan fidye yazılımlarının mağdurun bilgisayarında yol açabileceği durumlar şöyle özetlenebilir:

1- İş ya da özel yaşama ilişkin belgeler, fotoğraflar, videolar gibi kullanıcı için önemli olan dokümanlar şifrelenerek kullanımı engellenebilmektedir.

2- Aynı dokümanlar ve hatta sistemde yüklü bileşen ve programlar silinebilmekte, değiştirilebilmekte ya da kopyalanabilmektedir.

3- Mağdurun şifreleri, kimlik bilgileri, adres / telefon rehberi gibi hassas verileri çalınabilmektedir.

4- Mağdurun cihazı ve onunla birlikte bağlantılı olduğu sistemdeki diğer cihazlar da kilitlenebilmekte, tüm sistemin işleyişi yavaşlatılabilmekte, hatta durdurulabilmekte ve çökertebilmektedir.

[2] Ransomware Digital Extortion: A Rising New Age Threat; Indian Journal of Science and Technology, Vol 9(14), DOI: 10.17485/ijst/2016/v9i14/82936, Nisan 2016

[3] Chris Graham, The Telegraph, NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history, 20 Mayıs 2017, https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/

5- Fidye yazılımları, bulaştıkları cihazlarda yüklü anti-virüs ve anti-casus yazılımlar gibi güvenlik önemlerini etkisiz hale getirebilmektedir.

Fidye yazılımlarının Macintosh marka cihazlara erişemediği yönündeki yaygın kanı gerçeği yansıtmamaktadır. Fidye yazılımları Mac Os, Windows ve Android de dahil olmak üzere tüm işletim sistemlerini enfekte edebilmektedir.

Fidye yazılımı saldırılarının hemen hemen tamamı para beklentisi ile yapılmaktadır. Nadiren de olsa özellikle bluğ çağındaki gençlerin eğlence adına ya da kimi saldırganların aktivizm adına saldırı düzenledikleri düşünülmektedir.[4] Saldırganlar, mağdurlara istedikleri para miktarının ödenmesi durumunda sistemlerini normale çevirme sözü verirler; ancak her zaman sözlerini tutmaları beklenemez. Ayrıca saldırganlar kimliklerinin deşifre olmaması ve suçlamayla karşı karşıya kalmamaları için ödemelerin çoğunlukla Bitcoin gibi kripto paralarla yapılmasını istemektedirler. Basitçe söylemek gerekirse, Bitcoin herhangi bir banka veya hükümetten bağımsız tamamen dijital bir para birimidir. Bitcoin kullanmak sanal bir cüzdan oluşturmak kadar kolaydır ve özellikle de anonimliği / izinin sürülmesinin zorluğu nedeniyle siber suçlular için son derece caziptir.

1.2. Fidye Yazılımlarının Ortaya Çıkışı ve Tarihi

İlk olarak 1989 yılında, çevrimdışı ortamda ortaya çıkan AIDS Truva Atı ve 2005 yılında çevrimiçi ortamda ilk ortaya çıkan GPCoder örnekleri ilk olmaları açısından incelenmeye değer örneklerdir. Bunlar, çevrimdışı ve çevrimiçi ortamda fidye yazılımlarının kullanılmaya başlanmasına ilişkin ilk örneklerdir. Ardından günümüze dek fidye yazılımları kullanımı yoluyla sayısız şantaj vakası yaşanmıştır. Bazı örnek olayları ilerleyen bölümlerde inceleyeceğimden, bu bölümde fidye yazılımlarının ortaya çıkışına ilişkin ilk iki örneği ele alacağım.

[4] The Future of Ransomware and Social Engineering, 24 Ağustos 2017, sf. 12, 13 https://www.dni.gov/files/PE/Documents/6---2017-AEP_The-Future-of-Ransomware-and-Social-Engineering.pdf

1.2.1. AIDS Truva Atı

Fidye yazılımları, özellikle 2000'li yılların başından beri yaygınlaşmakta ve etkisini günümüze kadar artırarak sürdürmekte ise de bu alanda belgelendirilmiş ilk olay 1989 yılının Aralık ayında meydana gelmiştir. Bu olay AIDS Truva Atı ismiyle anılmaktadır. AIDS hastalığı ile ilgili risk unsurlarını anlatan bilgiler ve kullanıcının yanıtlarına dayanarak AIDS'e yakalanma riskini ölçmeye yarayan etkileşimli (interaktif) bir anket içerdiği iddia edilen binlerce disket, Dünya Sağlık Örgütü'nün toplantısına iştirak eden katılımcılara ve İngiltere'de satılan bir bilgisayar dergisinin hediyesi olarak okuyucularına dağıtıldı. Dağıtım süreci sona erdiğinde zararlı yazılım tetiklendi ve binlerce kullanıcı bu durumdan zarar gördü.[5]

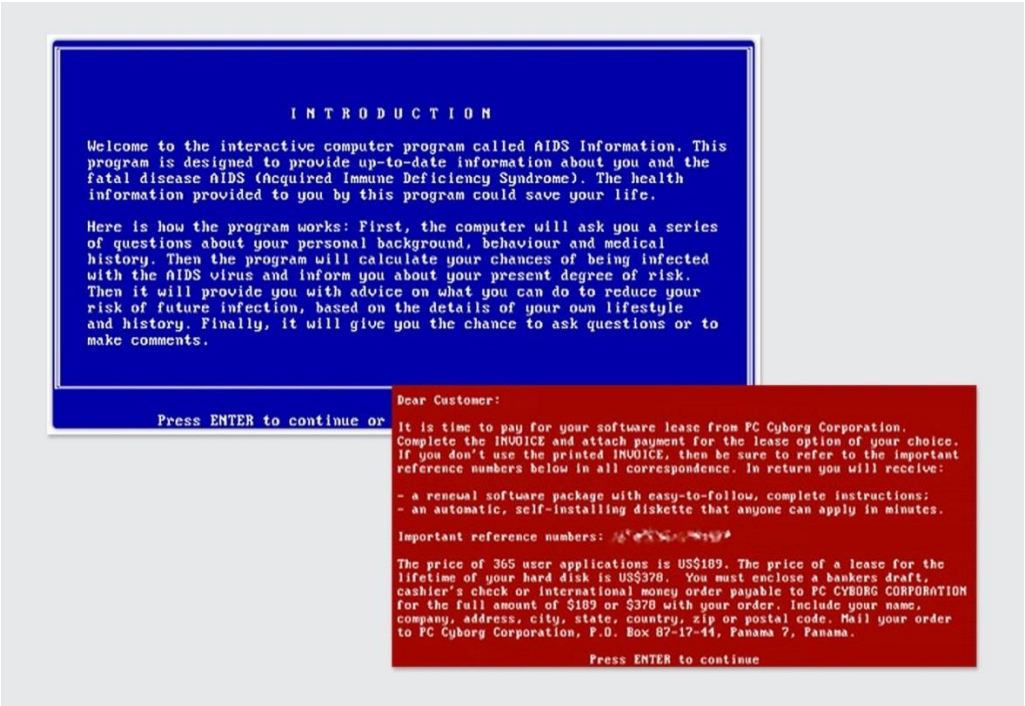
Disketin 90 ülkede 20 bin kullanıcıya dağıtıldığı bilinmektedir.[6] Saldırganlar kendi deyimleriyle "lisans ücreti" olarak addettikleri 189 Dolarlık fidyenin Panama'daki bir posta çeki hesabına gönderilmesini istediler. Disketi bilgisayarına takan mağdurların karşılaştıkları mesaj şöyle özetlenebilir:[7]

"Bu disketi bilgisayarına yükleyenler, PC Cyborg Corporation'a bu programları kiralamanın bedelini tam olarak ödemeyi kabul eder. Bu lisans sözleşmesini ihlal etmeniz durumunda, PC Cyborg, PC Cyborg Corporation'a ödenecek borçları geri almak için gerekli yasal işlemleri yapma ve kullanımınızı sona erdirmek için program mekanizmalarını kullanma hakkını saklı tutar. Bu program mekanizmaları diğer program uygulamalarını olumsuz yönde etkileyecektir. Bu lisans sözleşmesinin şartlarına uymamanız, vicdanınızı ve

[5] Becker's Health IT&CIO Report, First known ransomware attack in 1989, Mayıs 2016, https://www.beckershospitalreview.com/healthcare-information-technology/first-known-ransomware-attack-in-1989-also-targeted-healthcare.html
[6] Alina Simone, 26.3.2015, The Strange History of Ransomware
[7] George Smith, 12.8.2002, The Original Anti-Piracy Hack

hayatınızın geri kalanında sizi rahatsız edebilir ve bilgisayarınız normal şekilde çalışmayı durdurur. Bu ürünü başkalarıyla paylaşmanız kesinlikle yasaktır."

Bu mesaja ilişkin ekran görüntüleri şöyledir:



Şekil 4: AIDS Truva Atı fidye yazılımı saldırısı ekran görüntüsü

Polis, zararlı yazılımın yaratıcısının Amerikalı, Harvard Üniversitesi'nde Biyolog olan Dr. Joseph Popp olduğunu belirledi ve Popp İngiltere'ye şantaj yapmakla suçlanarak tutuklandı. Fakat yetkililer, Popp'un akli dengesinin yerinde olmadığına ve dolayısıyla yargılanmaya uygun olmadığına karar verdiler ve Popp ABD'ye iade edildi.[8]

The Independent gazetesinin, bu olaya ilişkin olarak 1989 yılında yayımladığı bir habere ilişkin kupür şöyledir:[9]

[8] TheAtlantic.com, Kaveh Waddell, 10.5.2016
[9] The Intependent, Aralık, 1989

‘Aids’ disk damages hospital computers

By Tom Wilkie, Science Editor

HOSPITAL computer systems have been damaged by an apparent attempt at computer blackmail which plays on people's fears about Aids.

The Metropolitan Police Fraud Squad confirmed yesterday that it was investigating criminal damage arising from a mysterious "Aids Information" computer disk distributed to users of IBM personal computers across Britain earlier this week. Copies have also turned up in Belgium, California and Zimbabwe.

Police have received complaints from hospitals, universities, banks and other commercial institutions that the disk damaged their computers and rendered them unusable. At least 10 computers are known to have been damaged, but rumours circulating in the computer world put the figure much higher.

Dr Alan Solomon, a leading expert on computer viruses, described the program as "extremely wicked and probably the worst thing that's ever happened in the personal computer world". But he said there was hope for users whose computers had been damaged. "It is a recoverable situation. Panic does more damage than anything else."

The disk was distributed to addresses on a mailing list sold in good faith by the magazine *PC Business World* to a Kenyan businessman, Mr E Ketema. At least 7,000 names appear on the list, including 24 hospitals. Before it sold the list, the magazine asked for a sample of the material to be distributed and was shown only a brochure.

According to Robert Walezy, marketing manager for the magazine's publishers C W Communications, distributing actual disks was therefore unauthorised and in breach of the contract.

Mr Ketema had taken out a short-term subscription with The Business Centre in New Bond Street, London, to receive mail and telephone messages on his behalf while he was in the country from 31 October to 30 November. He described himself as an accountant, but the centre does not know his first name, nor does it have a forwarding address.

The disk is supposed to contain an interactive program that will give users an assessment of their risk of exposure to Aids and recommend measures to reduce the risk. But some computers may crash immediately on loading the disk; in others the damaged is delayed. The program displays messages demanding that the user pay a "licence fee" of $378 to the PC Cyborg Corporation, giving a box number in Panama.

Şekil 5: AIDS Truva Atı fidye yazılımı saldırısına ilişkin 1989 yılında The Independent gazetesinde yayımlanan bir haber kupürü

1.2.2. GPCoder ve benzerleri

Dr. Popp’un çevrimdışı yolla başlattığı fidye yazılımlarının çevrimiçi ortamdaki ilk örneği 2005 yılında tespit edilen GPCoder olmuştur.[10]

GPCoder da bir truva atıdır. Windows sistemlerinde görülmüştür. Saldırganlar önce iş bulma ve kariyer sitesi Monster.com’un üye bilgilerini ele geçirmiş, daha sonra üyelere e-posta yoluyla ulaşarak fidye yazılımlarını mağdurların bilgisayarlarına yüklemişlerdir.[11]

Mağdurun bilgisayarına sızdıktan sonra da dosyalarını 660 ve 1024 bitlik RSA şifreleme yöntemi ile şifrelemiş, böylelikle kullanılamaz hale getirmiştir. Mağdurların bu durumdan kurtulmak için ödeyecekleri fidye miktarları ve ardından da şifreli dosyalarının kilidini nasıl açacakları bilgisayarların ana ekranlarına yönlendirilen bir .txt dosyası ile açıklanmıştır. Olay, iki yıla yakın

[10] Dhanya Thakkar, Preventing Digital Extortion, Birmingham, Sayfa: 39, Mayıs 2017
[11] ITPro, Miya Knights, Rene Millman, 22 Ağustos 2007

süre boyunca Rusya'dan tüm dünyaya yayılan e-postalar yoluyla binlerce İnternet kullanıcısını tehdit etmiştir. [12]

Orijinali Rusça olan e-postada şunlar yazmaktadır:

Merhaba! Job.ru web sitesinde yayınladığınız özgeçmiş ile ilgili olarak size yazıyoruz. Sizin için uygun olabilecek açık bir pozisyonumuz var. ADC Marketing LTD (UK) Moskova'da bir ofis açıyor ve uygun adaylar arıyor. Yakında sizi -karşılıklı uygun bir zamanda- bir mülakata davet edeceğiz.

Teklifimizle ilgileniyorsanız, lütfen ekteki formu doldurun ve bana e-postalayın.

Saygılarımla,
Viktor Pavlov
İK Yöneticisi

Ardından bir siber güvenlik çözüm sağlayıcısı firma tarafından 660 bitlik RSA şifreleme anahtarı kırılarak çözüme kavuşturulmuştur.[13]

GPCoder'ın ardından benzer truva atları –gittikçe karmaşıklaşan, daha kompleks şifreleme yapıları dahilinde- birbiri ardına ortaya çıkmıştır. Bunlar arasında TROJ.RANSOM.A, Archiveus, Krotten, Cryzip ve May Archive gibi örnekleri sıralamak mümkündür.[14]

1.2.3. Fidye Yazılımlarının Tarihine Genel Bakış

[12] VPNmentor.com, Guy Fawkes, 2017

[13] SecureList.com, Denis Nazarov, Olga Emelyanova, Blackmailer: the story of Gpcode, 26.6.2006

[14] GBConcepts Online, 17.9.2009, http://www.gbconcepts.net/blog/tag/troj-ransom-a/#

- **1989 – AIDS Trojan**. Bilinen ilk fidye yazılımıdır. Joseph Popp tarafından yazılmıştır. Çevrimdışı ortamda dağıtılmıştır**.**

- **2005 – GPCoder.** Çevrimiçi ortamda yayılan ilk fidye yazılımıdır.

- **2005 - 2006 – GPCoder, TROJ. RANSOM.A, Arciveus, Krotten, Cryzip ve MayArchive.** Bu yazılımlarda RSA şifreleme algoritması ilk defa kullanılmıştır.

- **2008 – GPCode .A.K**. İlk kez 1024 – bit RSA anahtarı kullanılmıştır.

- **2010 – WinLock** keşfedildi. İlk olarak Rusya'da görüldü. Mağdur, özel bir telefon numarasını arayarak 10 Dolar tutarında telefon görüşmesi yapana kadar bilgisayar ekranında porno görüntüsü çıkarıyordu.

- **2011 –** Bilgisayarı kilitleyen ve yeniden kullanılabilir hale gelmesi için kullanıcıyı sahte telefon listelerine yönlendiren isimsiz bir truva atı keşfedildi.

- **2012 – Reveton**. Kullanıcıya bilgisayarlarının lisanssız yazılım veya çocuk pornosu gibi yasadışı aktiviteler için kullanıldığını söylemekte ve ceza ödemesini istemekteydi. Bir çeşit scareware idi.

- **2013 - CryptoLocker**. En çok bilinen ve kötü nam salan fidye yazılımıdır. Şifrelemeyi artırdı ve önlenmesi en zor olan yazılımdı.

- **2013 - Locker**. Kullanıcıdan 72 saat içerisinde 150 dolar ödeme talep eden bir fidye yazılımı olarak ortaya çıktı.

- **2013 – CryptoLocker 2.0** piyasaya çıktı ve ödemelerde anonimliği artırmak için TOR (The Oninon Routing) ağını kullandı. TOR, kullanıcılara İnternet'te daha gizli gezinti imkanı sağlayan açık kaynak kodlu bir tarayıcı /

ağ olup 6 bini aşkın TOR sunucusu bulunmaktadır. Yani TOR eklentisi bulunan bir bilgisayardan İnternet'e bağlanıldığında, TOR yazılımı bu 6 bini aşkın TOR sunucusundan hedefe ulaşacak şekilde bir yol çizer.[15]

- **2013 – Cryptobit**. Tor kullanan ve şifrelediği her dosyanın ilk 1.024 bitini şifreleyen fidye yazılımı olarak ortaya çıktı.

- **2014 – CTB-Locker (Curve, Tor, Bitcoin)**. Eliptik eğri kriptografiden faydalanır. Anonimlik için Tor, ödeme için Bitcoin kullanır.

- **2014 – CryptoWall**. Bu truva atı, e-postalarla milyarlarca dosya ve kullanıcıyı etkileyen bir başka CryptoLocker sürümü olarak ortaya çıktı.

- **2014 – SynoLocker**. "Synology network attached" (NAS) ağına bağlı depolama (storage) cihazlarını hedef aldı ve buralardaki dosyaları şifreledi.

- **2015 – CryptoWall 2.0 ve CriptoWall 3.0**. Anonimlik için TOR kullandı.

- **2015 – TeslaCrypt and VaultCrypt**. Belirli bilgisayar oyunlarını indirenler hedeflendi

- **2015 – Chimera.** Doxing olarak da anılmaktadır. Talep edilen fidye ödenmezse, kullanıcılar dosyalarının şifrelenmesinin yanında yayılmasıyla da tehdit edildi.

- **2016 – CryptoWall 4.0**. Yalnız dosyaların içerdiği verileri değil, bunun yanı sıra dosya adlarını da şifreledi.

[15] Volkan İnanç, Media Click, Co-Founder, "TOR nedir?"

- **2016 – Locky.** Dosyaları şifrelemekle kalmadı, aynı zamanda bozdu ve .locky uzantısı ile yeniden adlandırdı.

- **2016 – SamSam**. Belirli kuruluşları hedef alarak onların güvenlik açıklarından yararlandı. Özellikle de hastaneler, okullar gibi verilerini geri almak için en çok para ödeyebilecek kuruluşları seçti.

- **2017 – WannaCry**. Windows işletim sisteminin yeni sürümündeki bir güvenlik açığını kullanan saldırganlar, 70'ten fazla ülkede on binlerce kişi ve kurumu etkiledi ve milyarlarca dolarlık hasara neden oldu.

Bu süreçte İngiltere'de sağlık sistemi çöktü, ameliyatlar bir süre yapılamadı, Rusya'da İçişleri Bakanlığı sistemleri etkilendi, pek çok ülkede lojistikten otomotive yüzlerce şirketin işleyişi aksadı

- **2017 – Petya**. Discoder.C adı ile de bilinmektedir. Tek tek dosyalar yerine bilgisayarda yer alan tüm dosyaların konum ve boyut bilgilerinin depolandığı MBR (Master Boot Record) sistemini şifrelemiştir. Böylelikle dosyalara erişim tamamen engellenirken, saldırganlar mağdurlarını dosyalarını imha etmek, satmak ya da yaymakla tehdit etmiştir. Şahısların yanında pek çok küresel şirketi de etkisi altına almıştır.

- **2017 – SynAck**. Geride takip edilecek bir iz bırakmayan Process Doppelgänging isimli yöntemin ilk kez kullanıldığı bu trojan, pek çok ülkede etkili oldu. Yasal işlemlerin içine gizlenerek anti-virüs güvenliğini aşan SynAck, sanal makineler, ofis uygulamaları, kod çeviriciler, veri tabanı uygulamaları, yedekleme sistemleri ve oyun uygulamalarını da hedef aldı.

- **2017 – BadRabbit**. En çok Rusya, Almanya ve Doğu Avrupa ülkelerini etkileyen bu trojan, Odessa Havaalanı, Kiev metro sistemi ve Ukrayna Ulaştırma ve Haberleşme Bakanlığı verilerini de rehin aldı. Yayılması

için herhangi bir güvenlik açığından yararlanmak yerine, sahte bir Adobe Flash yükleme dosyası kullanıldı.

- **2018 – GrandCrab**. Ocak 2018'de yayınlanıp kısa sürede dünyanın yaygın fidye yazılımlarından biri haline gelen GrandCrab'a karşı Bitdefender Antivirüs'ün üretip ücretsiz kullanıma sunduğu şifre çözücü programla Şubat 2019 itibariyle dünya çapında 20 bine yakın mağdurun 18 milyon dolardan fazla kaybı ve sayısız verisinin kurtarıldı açıklandı.

- **2018 – Ryuk**. Özellikle ABD'deki Wall Street Journal, New York Times, Chicago Tribune'ün de aralarında bulunduğu pek çok medyayı etkileyen ve Tribune Publishing ve Los Angeles Times'ın baskı ve dağıtım sürecini sekteye uğratan yönüyle adından söz ettirdi. Saldırganların 640 bin dolarlık Bitcoin geliri elde ettikleri açıklandı.

1.3. Fidye Yazılımlarının Türleri

Fidye yazılımları kilitleyici ve şifreleyici olmak üzere iki kategoride incelenmektedir: Kilitleyici fidye yazılımı ve kripto fidye yazılımı.[16] Bunlardan şifreleyici tür, sızdığı bilgisayar sisteminde yer alan veri ve dokümanları şifreleyerek kullanıcı tarafından açılabilmesini engellemektedir. Kilitleyici türdeki saldırılar ise, dosyaların ötesinde bilgisayar sistemini tamamen kilitleyerek sistemi tümden kullanılamaz hale getirmektedir.

1.3.1. Kilitleyici Fidye Yazılımı (Locker Ransomware)

Kilitleyici fidye yazılımları; kullanıcının bilgisayar ya da akıllı mobil cihazını hedef alarak yazılmıştır. Aynı zamanda "bilgisayar kilitleyici" olarak da adlandırılmaktadır.

[16] Tehdit İstihbaratı ve Analitiği, Deloitte, Sayfa: 6, 12.8.2016

Mağdurun veri ve dosyalarına yönelik bir işlem içermemekte; bunun yerine mağdurun aygıta erişimini sınırlandırmaktadır. Sınırlandırmaktan kasıt, yalnızca saldırgan ile mağdurun iletişim kurmasına, fidye talep etmesine ve ödeme yapmasına imkan tanınmasıdır. Örneğin, saldırgan fareyi kilitlerken, kullanıcının talep edilen fidye bedelini girebilmesi için klavye erişimine izin verebilir. Kullanıcının değerli verilerini temiz tutar ve dokunmaz.

1.3.2. Kripto Fidye Yazılımı (Crypto Ransomware)

Kripto fidye yazılımları; kullanıcının dosyalarını şifreleyen zorlu bir tehdittir. Bilgisayar ortamında saklanan değerli verileri ele geçirmek ve şifrelemek amacıyla kullanılmaktadır. Saldırganlar bu yolla mağdurlarına şifre çözme anahtarını belli bir fidye ödemeleri karşılığında vereceklerini söylemektedirler. Bu şifre ortadan kaldırılmadığı sürece mağdurlar dosyalarını kullanamayacaklardır. Kripto fidye yazılımları, gelişmiş şifreleme algoritmaları içermektedir. Çok sayıda dosya aynı anda şifrelenebilmektedir. Bu tür kötü amaçlı yazılımlar, yıllık milyonlarca dolar haksız kazanç sağlayan siber suçlular için kazançlı bir iş olarak görülmektedir. Bu tip yöntem kullanan saldırganların tipik davranışlarının başında kullanıcı için değerli olabilecek dosyaları ele geçirerek şifrelemeleri gelmektedir.[17] İşleyiş tam olarak şöyledir: İşleme başlayınca, truva atı sistemi tarar ve en değerli dosyaları şifreler. Genelde iş belgeleri, resimler, video dosyaları ve diğer dosyaları arar ve mağdurun bunları açamadığını anladıktan sonra endişelenmesini sağlar. Buna ek olarak kullanıcıyı tehdit ederek dosyalarını sonsuza kadar kaybedeceği uyarısında bulunur.[18] Kullanıcının ekranında verilerin şifrelendiğine ilişkin bir mesaj ortaya çıktığında, saldırgan hedefine çoktan ulaşmış demektir. 2017 yılında dünyanın önde gelen ülkelerini de etkileyen "WannaCry" da şifreleyici fidye yazılımıdır.

[17] Daniel Gonzalez, Thaier Hayajn, IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), Detection and prevention of crypto-ransomware, 2017

[18] Jake Doevan, Fidye Yazılımı Nasıl Temizlenir?, 2016

1.4. Fidye Yazılımlarının İşleyişi

1.4.1. Tipik süreç

Yayılma: Fidye yazılımların bilinen en klasik yayılma yöntemi, e-postadır. Gelen bir e-postanın eki ya da içeriğindeki linke tıklanması ile bilgisayara bulaşabilir. Ayrıca, detayı aşağıdaki maddelerde de açıklanacak olan, "drive-by download", "stratejik web compromise" vb. gibi yöntemler de kullanılmaktadır.

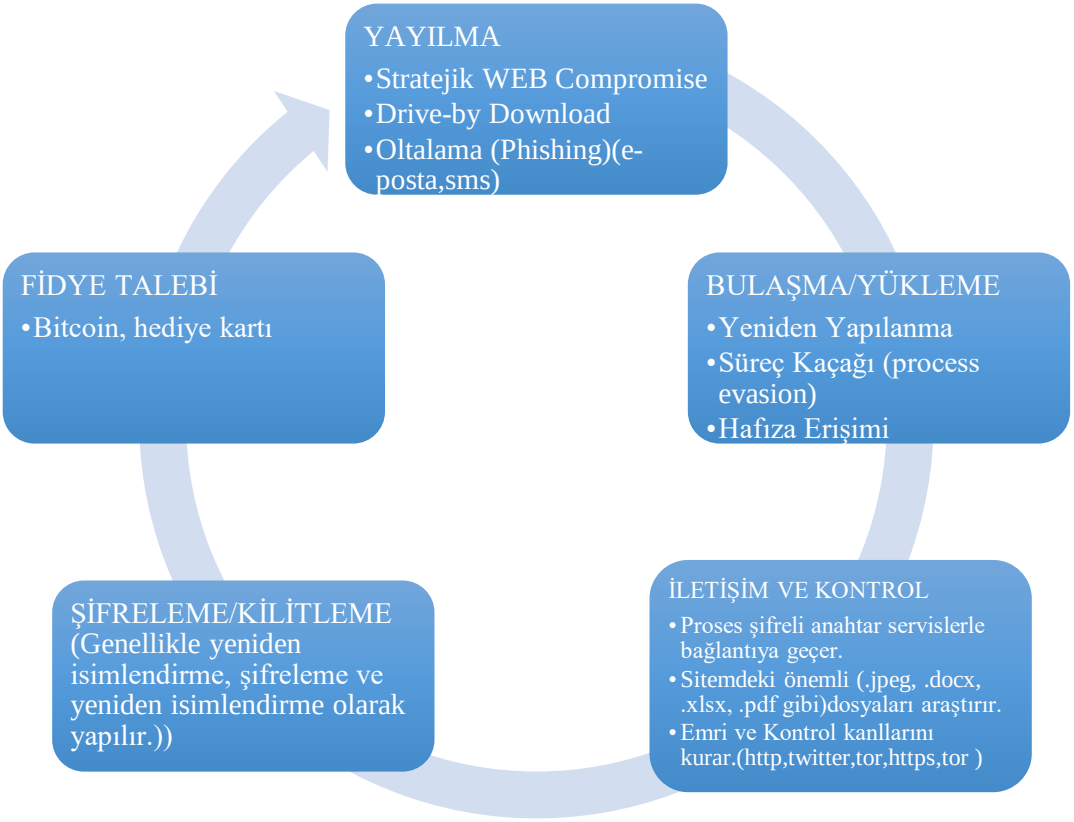
Bulaşma / Yükleme: Fidye yazılımı bilgisayara bulaştıktan sonra öncelikle gömülü kodu yürütecek ve gerçek bir makine ya da sanal alanda olup olmadığını analiz etmeye başlayacaktır. Sonrasında öncelikle Windows koruması ve sistem kurtarma özelliklerini kapatır ve anti-malware ve sistemdeki kayıt fonksiyonlarını devre dışı bırakır.

İletişim ve kontrol: Tüm eylemler, yapılacak sonraki eylemleri etkili bir şekilde belirlemek için bazı komut ve kontrol sistemleri gerektirir. İletişimlerin gerçekleşmesini sağlamak için kurulacak bir iletişim kanalını gerekir. Bu yapı, şifrelemeyi hedeflemesi gereken dosya türlerini tanımlamaktan, sürece başlamak için ne kadar beklemeleri gerektiğine ve sürece başlamadan önce yayılmaya devam etmeleri gerekip gerekmediğine kadar her şeyi içerir.

Şifreleme ve kilitleme: Fidye yazılımın türüne göre, bilgisayarı ve/veya hedef aldığı dosyayı şifreleyerek kilitler ve erişime kapatır ya da sınırlı erişim olanağı tanır.

Fidye talebi: Dosyalar şifrelendikten sonra, mağdurlara nasıl ele

geçirildiklerini anlatan bir ekran gösterilir. Ve fidye miktarı ve nasıl ödeneceği konusunda mağdur yönlendirilir.[19]



Şekil 6: Fidye yazılımı saldırılarının tipik işleyiş süreci

1.4.2. Hedef kitlesi ve hedefi ele geçirme yöntemleri

"Fidye yazılımların hedef kitlesi kimlerdir?" sorusunun kısa cevabı "herkes" iken uzun cevabı daha da karmaşıktır. Fidye yazılım saldırısına karşı savunmasızlığınız, verilerinizin korsanlar için cazibesi, bir fidye talebine hızlı bir şekilde yanıt vermenin ne kadar kritik olduğu, güvenliğinizin ne kadar

[19] Liska, Allan; Gallo, Timothy. Ransomware: Defending Against Digital Extortion (Kindle Locations 154-156). O'Reilly Media. Kindle Edition.

savunmasız olduğu ve çalışanlarınızın kimlik avı e-postaları konusunda ne kadar güçlü bir şekilde eğitim aldığı gibi faktörler öne çıkmaktadır. Yapılan saldırılar göz önüne alındığında, eğitim, devlet, sağlık, enerji, finans sektörleri, insan kaynağı departmanlarının ön plana çıktığı görülmektedir. [20]

Saldırganların hedef kitle belirlemelerinde etkili olan birkaç unsurdan söz edilebilir. Örneğin üniversiteleri hedefleyebilirler, çünkü daha küçük güvenlik ekipleri ve çok fazla dosya paylaşımı yapan ve savunmayı zorlaştıran farklı bir kullanıcı tabanlarını göz önüne alarak "kolay lokma" olarak görebilirler. Öte yandan, bazı kuruluşlar saldırganlar açısından daha caziptir. Örneğin havaalanları ve hastaneler genellikle dosyalarına derhal erişime ihtiyaç duyacaklarından daha yüksek meblağlar ödeyebilecek mağdurlar olarak görülebilmektedir. duyarlar. Hukuk ofisleri, siyasi kurumlar gibi hassas veriye sahip hedef kitleler de, sessizce uzlaşmaya ve ödeme yapmaya yanaşabilecek potansiyelde görülebilmektedir.

Ele geçirme yöntemlerine baktığımızda ise, genellikle benzer yöntemler ile web tabanlı anlık mesajlaşma uygulamaları ile yayılır/yayılmıştır. Bu yöntemleri kısaca şöyle açıklayabiliriz:[21]

Oltalama (Phishing): Genellikle, web sitesini ziyaret etme ve/veya ekli dosyayı açmaya yönelik e-postalar gönderilmesi ile gerçekleştirilir.

Pretexting: Özel bilgi almak için kendini başkası olarak sunmaya (sahte domain ile e-posta adresi alınarak bilgi alınmasına) dayanmaktadır.

---

[20] James A. Martin, Who is a target for ransomware attacks? 14 Temmuz 2017, https://www.csoonline.com/article/3208111/security/who-is-a-target-for-ransomware-attacks.html

[21] US-CERT, Crypto Ransomware, Alert (TA14-295A), 30 Eylül 2016, https://www.us-cert.gov/ncas/alerts/TA14-295A

Typosquating: Saldırganın benzer bir alan adıyla bir web sitesi kurması ve bekleyerek kullanıcının bilgilerini alması yoluyla hayata geçirilmektedir.

Drive-by Download: Sistem, son kullanıcının bilgisi olmadan bir kötü amaçlı yazılım veya casus yazılım parçasını otomatik olarak indirdiğinde ortaya çıkar.[22]

Stratejik Web Compromise: Belirli bir hedef veya hedef demografisi seçildiğinde en sık kullanılan yöntemdir. Bunlar son kullanıcıların stratejik geri bildirimine dayanır ve genellikle daha özel hedefli saldırılar için ayrılır. "Watering Hole Attack" de denir. [23]

Vulnerability Exploitation: Özetle, mevcut güvenlik açığından faydalanmak için geliştirilen bir yöntemdir. Güvenlik açığı bulmak için ağları taranır. Önceki yöntemlerde olduğu gibi kullanıcı tarafından başlatılan eylemlerin sonucudur. [24]

1.5. Siber Güvenlik Kavramı İçinde Fidye Yazılımlarının Yeri

Günümüzde bilgi sistemleri ile paralel olarak gelişen siber tehdit ve saldırılar, gerek bireyler, gerek şirketler, gerekse devlet kurumlarını giderek daha yenilikçi, gelişmiş tehditlerle karşı karşıya bırakmaktadır. Ne yazık ki yukarıda pek çok örneği verdiğimiz olayların da gösterdiği üzere, siber güvenlik tehdit ve saldırıları arasında fidye yazılımları en yaygın ve sık karşılaşılan risk unsurlarından biridir. Bazen bir bilgisayarı, bazen de tüm ağı rehin alabilen fidye yazılımları, aynı zamanda bugünün bilgisayar korsanları tarafından kullanılan en agresif taktiklerden biridir. Bilgi teknolojileri alanında evrensel boyutta bir tehdit unsuru

[22] Liska, Allan; Gallo, Timothy. Ransomware: Defending Against Digital Extortion (Kindle Locations 154-156). O'Reilly Media. Kindle Edition.
[23] Liska, Allan; Gallo, Timothy. Ransomware: Defending Against Digital Extortion (Kindle Locations 154-156). O'Reilly Media. Kindle Edition.
[24] Liska, Allan; Gallo, Timothy. Ransomware: Defending Against Digital Extortion (Kindle Locations 154-156). O'Reilly Media. Kindle Edition.

olan fidye yazılımları, en korkulan siber saldırılar arasında yer almaktadır. Massachusetts Institute of Technology'nin Ocak 2018'de yayınladığı MIT Technology Review'a göre, fidye yazılımları dünya çapındaki en büyük altı siber tehdit arasında gösterilmektedir.

Güney Afrika menşeili uluslararası bilişim şirketi Dimention Data'nın açıkladığı verilere göre, 2018 itibariyle dünya çapındaki toplam zararları yazılımların içinde fidye yazılımlarının oranı yüzde 7'dir. Bu oran bir önceki yıl ise, yüzde 1 olarak tespit edilmiştir.[25]

Çok uluslu teknoloji şirketi Cisco Systems'in açıkladığı 2019 Siber Tehrit Raporu'na göre ise, fidye yazılımı saldırıları yılda yüzde 350'den fazla artış göstermektedir. [26]

Küresel antivirüs şirketi ESET, 2018'de İstanbul'da yaptığı bir toplantıda da günümüzde işletmelere yönelik en popüler siber saldırı şeklinin fidye yazılımları olduğu açıklanmıştır.

Öte yandan uluslararası siber güvenlik şirketi Symantec tarafından Şubat 2019'da açıklanan "Internet Security Threat Report"a göre, fidye yazılımı saldırılarından 2017 yılına kadar en çok bireyler etkilenirken, 2017 yılı itibariyle işletmelere ve bireylere yönelik saldırılar eşitlenmiş, 2018 ve sonrasında ise işletmelere yönelik saldırılar ağırlık kazanmıştır. Aynı rapor, 2018 yılında dünya genelindeki işletmelerin yüzde 81'inin bir fidye yazılımı olayına maruz kaldıklarını ortaya koymaktadır.[27]

Şüphesiz mağdur profilindeki bu değişiklik, elde edilmek istenen kazanç miktarına ilişkin beklentinin artışıyla ilişkili olarak meydana gelmiştir.

[25] Dimension Data, NTT Security 2018 Global Threat Intelligence Report, Ocak 2019, sf. 18
[26] Cisco Systems, 2019 Threat Report, Ocak 2019, sf. 5
[27] Symantec Internet Security Threat Report, Volume 24, Şubat 2019, sf. 16

Bu siber zorbalık olayı, haber manşetlerine giderek daha fazla taşınmaya başlanmaktadır. Dünyanın çeşitli yerlerindeki en yüksek tirajlara sahip ulusal gazetelerde manşetlere yansıyan bazı örnekler şöyledir:

Protect yourself from ransomware

As malicious software holds computer systems hostage worldwide, here's what you need to know to keep your data safe

Ransomware has been making headlines after cybercriminals hijacked hundreds of thousands of computers in India and around the world. Ransomware, which is often transmitted by email or web pop-ups, involves locking up people's data and threatening to destroy it if a ransom is not paid. The global cyber-attack has affected 2,00,000 Windows computers in more than 150 countries, including China, Japan, South Korea, Germany, India and Britain.

"Not only individuals, but even governments and big companies with so much to lose fail to secure their systems and train their employees about necessary security practices," says Marty P Kamden, a marketing executive for the private network service provider NordVPN. "Cautious online behaviour would probably have prevented the malware from infecting the network in the first place."

What can businesses and individuals do to protect themselves from ransomware? Here are some tips from security experts:

Update your software
Security experts indicate the malware that spurred this global attack, called WannaCry, have infected machines by getting people to download it through email. If people had simply stayed on top of security updates, their machines would not have been infected, says Chris Wysopal, CTO of Veracode, an application security company. Consumers can remedy this by configuring their PCs to install the latest software updates.

Install antivirus software
In addition to keeping Windows up-to-date with the latest security enhancements, antivirus software can prevent malware from infecting your computer. Kamden of NordVPN said 30 per cent of popular antivirus systems were capable of detecting and neutralising the ransomware.

Be wary of suspicious emails and pop-ups
Security experts believe WannaCry may have initially infected machines via email attachments. The lesson: Avoid clicking links inside dubious emails, Kamden said. How do you spot a fishy email? Look carefully at the email address of the sender to see if it is coming from a legitimate address. Also, ransomware developers often use pop-up windows that advertise software products that remove malware. Do not click on anything through these pop-ups.

Create backups of your valuable data
In the event that a hacker successfully hijacks your computer, you could rescue yourself with a backup of your data stored somewhere, like on a physical hard drive. That way, if a hacker locked down your computer, you could simply erase all the data from the machine and restore it from the backup.

Create a security plan for your business
For larger businesses, applying security updates organisation-wide can be difficult. If one employee's machine lacks the latest security software, it can infect other machines across the network. IT professionals should regularly educate and test employees on spotting suspicious emails, said Matt Ahrens, vice-president of Crypsis, a cybersecurity firm.

What to do if already infected
If you are already a victim of ransomware, the first thing to do is disconnect your computer from the internet so it does not infect other machines. Then report the crime to law enforcement and seek help from a technology professional who specialises in data recovery to see what your options might be. If there are none, don't lose hope: There may be new security tools to unlock your files in the future.

— NEW YORK TIMES

Şekil 7: Times Of India, Hindistan, 21 Mayıs 2017

Şekil 8: The Epoch Times, New York, 19 Mayıs 2017

facebook.com/nationnews @nationnews @suthichai

A NEW BUZZ FOR DENGUE >> 8B

THE NATION

INSIGHTFUL, IN TREND, INDEPENDENT

nationmultimedia.com TUESDAY, May 16, 2017 20 PAGES, 2 SECTIONS, VOLUME 42, NO 55135 / Bt30

About 300 nurses gather in the yard in front of Phumin Temple in Nan province yesterday to press their demand that the government recruit more nurses as permanent civil servants.

Prayut tells nurses to stop protesting, ministry must stick to hiring regulations

PRATCH RUJIVANAROM
THE NATION

PRIME MINISTER General Prayut Chan-o-cha responded yesterday to ongoing protests by nurses, saying the allocation of civil service posts that they are demanding must comply with the workforce reformation plan every five to 10 years.

Prayut said every ministry had to follow the rules in enrolling new workers and had to manage their vacant positions first before asking for more staff.

He also urged the nurses not to protest and make the issue political.

Nurses have pledged to continue their protest amid complaints about understaffing, tough working conditions and unfair salaries. The Public Health Ministry has asked them to be patient, stating that nursing positions are being allocated.

Hundreds of nurses in Nan demonstrated yesterday to show solidarity with government-employed nurses campaigning for more permanent civil servant positions and fairer benefits.

Pattanaphong Wongbunyanuwej, a representative of the Nan nurses, said the group gathered in a symbolic gesture to raise their voices to the government, urging it to allocate more civil servant positions and improve the working conditions and benefits for nurses. "We want the government to understand the hardship of nurses, as we are working extraordinarily long hours with unfair remuneration, so we gather today to show our demands," Pattanaphong said.

Meanwhile, the Temporary Employee Professional Nurse Network fan page on Facebook invited temporary nurses to fill in a questionnaire to survey the number who intend to resign if the proposal to increase civil servant position for nurses is rejected by the government.

Dr Tassana Boontong, president of the Thailand Nursing and Midwifery Council, stressed that the civil servant position is very important for a nurse, as it can guarantee career stability and provide proper health benefits for their family.

"This problem [the nurses unable to be enrolled as civil servants] causes 48 per cent of new nurses to resign after the first year at work. In the second year, 25 per cent of those remaining follow suit. How can we have enough nurses in the system, as we cannot save them in the system in the first place?" Tassana said.

"Our research showed that the nurses worked up to 37 shifts per month, but their payment is low compared to the doctors. There is also not enough welfare for the nurses if they are injured or die due to their work."

She said that the performance-based pay for nurses was almost 28 times lower than for doctors, even though they work harder. In case of an accident, nurses receive very little benefits to compensate for their loss. "This is a good time for the policy makers to understand nurses' hardship. They give up their energy, time and personal lives to take care of the patients and look after our health, so they should have job security and better welfare in return," she said.

Tassana said the Nursing and Midwifery Council had proposed 10,992 civil servant positions for nurses over three years. This meant that only 3,864 positions were sought from the government per year, which was not a large amount.

However, she said she understood that the Public Health Ministry was working hard to manage the vacant positions for nurses to meet the proposed positions and asked fellow nurses to be patient during this allocation.

All 200 Thai computers hit by WannaCry fixed: expert

RESPONSE CENTRE PLANS TO SPEND BT400M TO TRAIN IT STAFF TO DEFEND AGAINST ATTACKS

THE NATION

A digital advertising hoarding on Wireless Road infected with WannaCry displays hackers' demand for ransom money.

TWO hundred computers in Thailand were hit by the global ransomware attack but all had been fixed and could be used normally again, an official from a computer emergency response team said yesterday.

Surangkana Wayuparb, chief executive officer of the Electronic Transactions Development Agency (ETDA) and head of the Thailand Computer Emergency Response Team (ThaiCERT), said owners of the 200 computers infected by the WannaCry bug had not paid ransoms demanded to decode data encrypted by the hackers.

The basic problem on all the infected computers had been fixed and all were functioning normally after technicians followed the advice provided by ThaiCERT, she said, without elaborating on details.

On Sunday, Europol revealed that the WannaCry ransomware had affected 200,000 victims in 150 countries and described the cyberattack as "unprecedented".

Pol Maj-General Siripong Timula, commander of the IT Support Division at the Office of Information and Communication Technology, advised people hit by WannaCry to not pay the ransoms demanded but instead collect evidence and file a complaint with the Technology Crime Suppression Division (TCSD).

Prime Minister Prayut Chan-o-cha said yesterday government agencies had not been affected by the malware but a few big companies had.

Following the reported cyberattack, Prayut said a lack of control could be dangerous.

"It's necessary that we keep things under control but I don't mean that we are going to restrict people's access to information," he said. He also ordered all government agencies to be vigilant about the cyberattack, check for loopholes, update cybersecurity tools and educate officials.

The Bank of Thailand has been alerted to watch for signs of WannaCry infections but there were not any reports yesterday that bank computers in Thailand had been affected.

Surangkana said as a long-term strategy, the ETDA would prepare computer users to deal with cyber threats. This year, the agency will spend Bt400 million to help ThaiCERT develop skills and technology to deal with cybersecurity issues.

She said a cybersecurity bill was being debated by the National Reform Steering Assembly, but in her view the bill was not as important as training skilled IT workers who could deal with cyber threats.

Somsak Khaosuwan, deputy permanent secretary of the Ministry of Digital Economy and Society, said if government computers were infected, the ministry would advise them to immediately shut down their systems and alert ThaiCERT.

State agencies had already backed up information on computer systems, so problems should not affect services if government computers become infected, Somsak said.

Organisations with infected computers can contact the Online Complaint Centre on 1212 or directly inform ThaiCERT at 02-123-1212, which is taking calls 24 hours a day.

Meanwhile, Twitter users shared photos on Sunday showing two digital advertising boards infected with the ransomware, which displayed a message from the hackers instead of the normal advertisements as Bangkok traffic passed by, the Thaivisa website reported.

One photo, shared by Twitter user ALiCE6TY9 on Saturday, showed one infected ad board located on Wireless Road. There were also reports of another board infected in the Vibhavadi area in northern Bangkok.

Meanwhile, Chanwit Kaewkasi, a lecturer at the Computer Engineering Department at the Suranaree University of Technology in Nakhon Ratchasim province, yesterday demonstrated the Block Wannacry program, which was developed by university lecturers to protect computers from the malware.

The program is now available for free download with more than 1 million visits at the host webpage and tens of thousands of downloads.

Royal Thai Police deputy spokesman Colonel Krisana Pattanacharoen said national police chief Pol General Chakthip Chaijinda had ordered agencies to be careful in downloading data from the Internet and vigilant in safeguarding data on government PCs as the ransomware spread.

Interpol had warned Thai police about the attack and also urged vigilance but so far police systems had not been affected, he said.

Meanwhile, a Microsoft spokesperson released a statement that said people who installed free anti-virus software or Windows updates would be protected.

Given the serious potential impact on Microsoft customers and their businesses, the company has released updates for Windows XP, Windows 8 and Windows Server 2003.

Şekil 9: The Nation, Tayland, 15 Mayıs 2017

Şekil 10: The Daily Telegraph, İngiltere, 22 Mayıs 2017

1.6. Fidye Yazılımlarına İlişkin İstatistikler

Özellikle son 10 yılda giderek artan çok sayıda yüksek profilli fidye yazılımı saldırıları; bireyleri, şirketleri ve kamu kurumlarını tehdit etmeye hız kesmeksizin devam etmektedir. Bu önemli siber güvenlik sorunu, önemli bir mücadele alanı yaratmıştır.

Konuyla ilgili kurumların ve siber güvenlik şirketlerinin birbiri ardına yayınladıkları raporlar da bu artışı rakamlarla ortaya koymaktadır. Örneğin Güney Afrika menşeili uluslararası bilişim şirketi Dimention Data'nın açıkladığı verilere göre, fidye yazılımı saldırıları 2017 yılında bir önceki yıla oranla yüzde 350 artış göstermiştir.[28]

Journal of Health Care Compliance'ın Ekim 2018 sayısında yayımlanan bir makale, 2018'in ilk altı ayında, 2017'nin aynı dönemine oranla yüzde 229'luk bir artışa işaret eden 181,5 milyon fidye saldırısı olduğunu bildirmektedir. Buna göre, şifrelenmiş tehditler bir yılda yüzde 275 oranında artmıştır. [29]

Fidye yazılımı saldırılarının en sık yaşandığı ülkelerden biri Amerika'dır. Amerikan istihbarat ve güvenlik örgütü FBI'ın İnternet üzerinden gerçekleştirilen dolandırıcılık faaliyetleri ile ilgilenen birimi İnternet Suçları Şikayet Merkezi'nin (IC3) 7 Mayıs 2018'de açıkladığı rakamlar, 2017 yılında kuruma bin 783 fidye yazılımı şikayetinin ulaştığını göstermektedir. Bu siber saldırılar, mağdurlarını 2.3 milyon doların üzerinde zarara uğratmıştır.[30]

2018 yılının Aralık ayı itibariyle Türkiye, dünyada en çok fidye yazılımı saldırısına uğrayan ülkeler arasında dünyada altıncılığı, Avrupa'da ise birinciliği göğüsledi. Trend Micro Smart Protection Network'ün yayınladığı rapora

[28] Dimension Data, NTT Security 2018 Global Threat Intelligence Report, Ocak 2019
[29] A New Wave of Ransomware Is Coming This Fall; Marcus Chung is Chief Executive Officer (CEO) at BoldCloud, Journal of Health Care Compliance, Ekim 2018
[30] FBI Releases the IC3 2017 Internet Crime Report and Calls for Increased Public Awareness, Mayıs 2018

göre, Aralık 2018'de meydana gelen fidye yazılımı saldırılarında en çok saldırıya uğrayan ülkeler arasında Amerika, Brezilya, Hindistan, Vietnam ve Meksika'dan sonra Türkiye altıncı sırada yer aldı. Aynı rapor Türkiye'nin bu açıdan Avrupa'da birinci sırada bulunduğunu ortaya koydu. Öte yandan Türkiye'de tespit edilen saldırıların, Orta Doğu'daki diğer ülkelerde saptanan saldırıların toplamına yakın olduğu belirlendi.[31]

Tüm bunlar, fidye yazılımının siber suçlular için son derece kazançlı bir girişim olmaya devam ettiğinin kanıtıdır.

Son yıllarda yaşanan fidye yazılımları saldırılarına bağlı olarak ortaya çıkan istatistikler olayın hayret verici boyutlarını gözler önüne sermektedir:

- **Fidye yazılımı saldırılarının sıklığı ve ödemeler artması beklenmektedir**. Veri güvenliği alanındaki araştırmalarıyla ön plana çıkan uluslararası bağımsız araştırma kuruluşu Ponemon Institute, Amerika, Avrupa, Orta Doğu ve Kuzey Afrika bölgesindeki bin 100'den fazla bilişim profesyonelinin katıldığı bir anket düzenlemiştir. 2017 yılının sonlarında gerçekleştirilen "2018 Study on Global Megatrends in Cybersecurity" başlıklı bu ankete katılanların yüzde 67'si fidye yazılımı saldırılarının sıklığı ve talep edilen ödeme miktarlarının artacağına inanmaktadır.

- **Şirketlerin yarısından çoğu fidye yazılımı saldırılarına karşı korunmamaktadır.** Küresel siber güvenlik şirketi Sophos ABD, Kanada, Meksika, Fransa, Almanya, İngiltere, Avustralya, Japonya, Hindistan ve Güney Afrika'nın aralarında bulunduğu 10 ülkedeki 3 bine yakın bilişim profesyonelinden topladığı bilgilerle "The State of Endpoint Security Today" [32] başlıklı rapor oluşturdu. 2018 yılında açıklanan bu rapora göre:

[31] TrendMicro TrendLabs Security Roundups and Predictions Report, Mart 2019, sf: 22
[32] A Sophos Guide, 2018, https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/endpoint-survey-report.pdf

- Ankete katılan şirketlerin yüzde 54'ü, 2017'de bir fidye yazılımı saldırısı sonucu etkilendiğini bildirmiştir.

- Bu şirketlerin yüzde 31'i, yakın gelecekte bu tür bir saldırının gerçekleşmesinin beklendiğini belirtmiştir.

- Araştırmaya katılan kuruluşların yüzde 54'ünün fidye yazılımı saldırılarına karşı spesifik bir "anti-ransomware" güvenlik kalkanı bulunmamaktadır.

- Aynı yıl, kuruluş başına ortalama iki fidye yazılımı saldırısı gerçekleşmiştir.

- Saldırılardan etkilenen kuruluş başına maliyet 133 bin ABD Doları olarak tespit edilmiştir.

- Öte yandan ankete katılanların yüzde 5'i toplam maliyet olarak 1.3 milyon dolar ile 6.6 milyon dolar arasında rakamlar bildirmiştir. Bu maliyete ödenen fidyenin yanı sıra kapalı kalma süresi, insan gücü, cihaz maliyeti, ağ maliyeti ve kaybedilen fırsatlar da dahil edilmiştir.

- Fidye yazılımı saldırılarına en çok maruz kalan sektörlerin başında sağlık gelmekte; onu enerji, hizmet ve perakende sektörleri izlemektedir.

- Fidye yazılımı saldırılarına en çok maruz kalan ülkelerin başını ise Hindistan çekmekte; onu Meksika, ABD ve Kanada takip etmektedir.

- **Fidye yazılımı saldırıları, Amerikalı küçük ölçekli şirketlere bir yılda 75 milyar dolar kaybettirmiştir.** Bir Amerikan siber güvenlik ve veri yedekleme şirketi olan Datto ise, fidye yazılımı saldırılarıyla başa çıkmak için çalışan BT

hizmet sağlayıcı kuruluşlardaki bini aşkın profesyonelle bir anket yapmıştır. 2018 yılının sonunda yayınlanan anket sonuçlarına göre:

- Fidye yazılımlarının ABD'deki yalnızca küçük ölçekli şirketlere yıllık maliyeti 75 milyar doları aşmıştır.

- Ankete katılanların yüzde 97'si işletmelere yönelik saldırıların artmasını öngörmektedir.

- Küçük işletme sahipleri maruz kaldıkları fidye yazılımı saldırıları karşısında BT hizmet sağlayıcılarını aramaktan kaçınmazken, ancak dört olaydan birini resmi mercilere rapor etmektedir.

- BT hizmet sağlayıcılarının yüzde 46'sı yaşanan fidye yazılımı saldırılarının sorumlusu olarak kimlik avı e-postalarını göstermektedir. Yüzde 36'sı ise, şirketlerde çalışanlara yeterince siber güvenlik eğitimi verilmediğini savunmaktadır.

- Saldırıya uğrayan küçük işletmelerin yüzde 48'i saldırı sonucunda kritik öneme sahip verilerini kaybetmişlerdir.

- KOBİ'lere yönelik fidye yazılımı saldırılarının yılda 1 ila 5 kez gerçekleşme oranı yüzde 60 olarak tespit edilirken, bu saldırılara yılda altı defadan fazla maruz kalanların oranı ise yüzde 40 olarak açıklanmıştır.

- **Fidye yazılımları mobil cihazları da etkilemektedir.** Uluslararası anti-virüs ve İnternet güvenliği şirketi Kaspersky, 5 Mart 2019'da yayınladığı "Mobile Malware Evolution 2018" isimli raporda şunları açıklamaktadır:

- 2018 yılında 151 bin 359 yeni mobil bankacılık truva atı, 60 bin 176 yeni mobil fidye truva atı keşfedilmiştir.

- 2018’de mobil fidye yazılımına en fazla maruz kalan ülkeler şöyle sıralanmaktadır: Amerika, Kazakistan, İtalya, Polonya, Belçika, İrlanda, Avusturya, Romanya, Almanya, İsviçre.

- **Fidye yazılımlarının yol açtığı hasarın maliyetinin 2021'de 2015'e kıyasla 57 kat daha fazla olması beklenmektedir.** [33] Siber güvenlik pazarına ilişkin araştırma ve raporlar sunan, Kaliforniya, New York ve İsrail’de ofisleri bulunan CyberSecurity Ventures’in 6 Şubat 2019’da yayınladığı verilere göre:

  - Fidye yazılımlarının yol açtığı hasarın maliyetinin 2021'de 2015'e kıyasla 57 kat daha fazla olması beklenmektedir. Bu veri, fidye yazılımlarının en hızlı büyüyen siber suç türü olduğunu göstermektedir. ABD Adalet Bakanlığı, fidye yazılımını siber suç için yeni bir iş modeli ve küresel bir fenomen olarak tanımlamıştır.

  - 2016’da dünya çapında her 40 saniyede bir fidye yazılımı saldırısı gerçekleşirken, bu sürenin 2019'da 14 saniyeye, 2021'de 11 saniyeye inmesi beklenmektedir.

  - Başarılı saldırıların ve veri ihlallerinin yüzde 90'ından fazlasının kimlik avı dolandırıcılığından, alıcılarına bir bağlantıyı tıklatması, bir belge açması veya istememesi gereken bilgileri iletmesi için hazırlanmış e-postalardan kaynaklandığı bildirilmektedir.

- **Bireylerin yarısından fazlası fidye ödemeye razı olduğunu beyan etmektedir.** Çok uluslu bilişim şirketi IBM, 2016 yılında “Ransomware: How Consumers and Businesses Value Their Data” [34] başlıklı bir anket yapmıştır. Bu

[33] Steve Morgan, 2019 Cybersecurity Almanac: 100 Fact,s, Figures, Predictions and Statistics,2019, https://cybersecurityventures.com/cybersecurity-almanac-2019/

[34] Limmor Kessem, Ransomware: How Consumers and Businesses Value Their Data, 2016, https://www.triscal.com.br/wp-content/uploads/2018/08/seguranca-ransomware_how_consumers_businesses_value_their_data-2016.pdf

kapsamda ABD'deki 600 iş insanı ve bini aşkın tüketiciye sorular yöneltilmiştir. Buna göre:

- Ankete katılan tüketicilerin yarısından fazlası başlangıçta fidye ödemeyeceklerini belirtirken, belirli veri türleri hakkında soru sorulduğunda yüzde 54'ü finansal veriyi geri almak için büyük olasılıkla ödeme yapacaklarını belirtmiştir.

- Ankete katılan ebeveynlerin yarısından fazlası (yüzde 55), dijital aile fotoğraflarına erişim için fidye ücretini ödemeye razı olacaklarını belirtmiştir. Bu oran, çocuksuz katılımcılarda yüzde 39'da kalmıştır. Bu da ebevynler siber saldırganlar için etkili bir hedef kitle olduğunu ortaya koymaktadır.

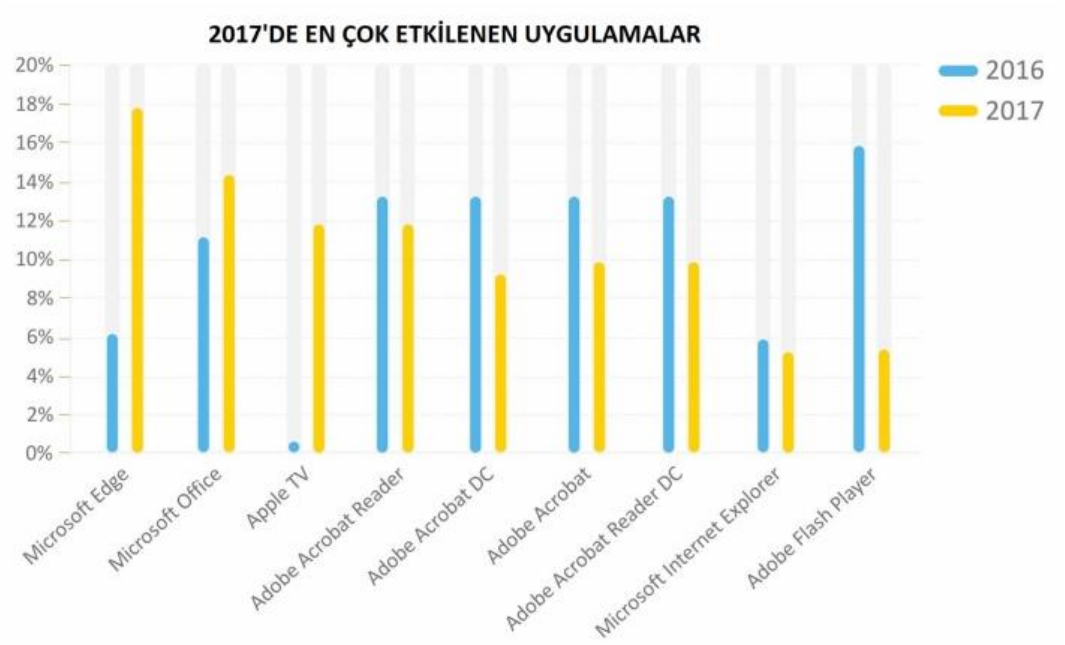
- Ankete katılan her iki şirket yöneticisinden bir tanesi daha önce bir fidye yazılımı saldırısına maruz kalmıştı. Çalışma, bu yöneticilerin yüzde 70'inin sorunu çözmek için fidye ödediğini; bu katılımcıların yarısının 10 bin doların üzerinde ve yüzde 20'sinin 40 bin doların üzerinde ödeme yaptığını ortaya koymuştur.

- Tüm şirket yöneticilerinin yaklaşık yüzde 60'ı verilerini kurtarmak için fidye ödemeye razı olduklarını belirtmiştir. Bu veriler arasında en kritik olanları şöyle sıralamışlardır: Finansal kayıtlar, müşteri kayıtları, fikri mülkiyet hakkı içeren dosyalar ve iş planları.

- Ankete katılan küçük işletmelerin yalnızca yüzde 29'u, orta büyüklükteki işletmelerin yüzde 57'sine kıyasla fidye yazılımı saldırılarına maruz kalmıştı. Bu da henüz ne yapmaları gerektiği konusunda kapsamlı bir fikir sahibi olmayan küçük işletmelerin, saldırganların önemli hedefleri arasında yer almalarını tetikleyecektir.

- **Sigorta şirketlerine başvurular artmaktadır.** Küresel bir sigorta şirketi olan American International Group (AIG), sigortalıları tarafından 2017'de siber güvenlik alanında alınan taleplerin dörtte birinden fazlasının (yüzde 26) birincil nedeni olarak fidye yazılımlarının bulunduğunu açıklamıştır. Oysa bu oran, 2013 - 2016 yıllarında taleplerin yüzde 16'sını teşkil etmiştir.

- **Fidye yazılımları gelişmekte, hedeflenen uygulamalar değişmektedir.** Ağ güvenliğine yönelik çeşitli İnternet cihazları üreten küresel bir şirket olan SonicWall, 2018 yılında bir "Siber Tehdit Raporu" yayınladı. Verileri SonicWall Capture Labs Tehdit Ağı üzerinden toplanan raporda, yaklaşık 200 ülkedeki 1 milyondan fazla güvenlik sensörü kaynak alındı. Raporda yer alan iki önemli istatistik bize hem artan benzersiz fidye yazılım imzaları ile saldırıların yeni çeşitler kazandığını, hem de en çok etkilenen uygulamalarda Microsoft Edge ve Apple TV gibi yenilikçi uygulamaların başı çektiğini göstermektedir: [35]



Şekil 11: Fidye yazılımı saldırılarından en çok etkilenen uygulamalar, 2016-2017

[35] SonicWall Siber Tehdit Raporu 2018, sf. 10, http://www.m2s.com.tr/bulten/2018_Sonicwall_siber_tehdit_raporu-TR.pdf

Şekil 12: Benzersiz fidye yazılım imzaları, 2015, 2016 - 2017

1.7. Fidye Yazılımlarından Korunma Yolları

Hem kişisel, hem de kurumsal olarak sahip olunan bilgilerin ve sistemin sağlıklı işleyişinin güvence altına alınması için *fidye* saldırılarından *korunmak* gerekmektedir.

Fidye yazılımlarının istenmeyen sonuçlarından korunmak için şirketlerin ilk başta siber güvenlik ve risk değerlendirme önlemlerine yatırım yapmaları önemlidir. Aynı şekilde bireylerin de kullandıkları bilgisayarlarda güvenlik programlarına yer vermeleri önemlidir. Birden çok bilgisayarın yer aldığı yapılarda, her kullanıcının bilgisayarında anti-fidye ve firewall yazılımlarının ayrı ayrı yüklenmiş, güncel ve çalışır durumda bulundurulması, anlamlı bir güvenlik kalkanı olacaktır. Anti-virüs programları fidye yazılımlarına karşı dirençli olmayabilir; bu nedenle özellikle anti-fidye uygulamalarından faydalanılması kritik öneme sahiptir.

Ancak her türlü güvenlik önleminin alınması ancak riski azaltır, yine de sıfırlamaz. Bu nedenle verilerin yedeklenmesi, bu yedeklerin İnternet'e ve yedekleme yapılan bilgisayarlara bağlı olmayan harici cihazlara kaydedilmesi,

yedeklemenin günlük olarak yapılması, en az bir yedeklemenin ayrı bir fiziksel ortamda saklanması önem taşımaktadır.

Öte yandan şirketlerin bir fidye yazılımı saldırısı olasılığına karşılık kriz eylem planlarının da hazır olması gerekmektedir. Bu planda kimin ne zaman bilgilendirileceği, talep edilen fidyeyi ödeyip ödememeye karar verme yetkisine kimin sahip olacağı, adli mercilerle koordinasyondan kimin sorumlu olacağı gibi bilgileri kapsamalıdır.

Kullanılan bilgisayar sistemlerinin güncellenmesi de en az veri yedekleme kadar önem taşımaktadır. Fidye yazılımlarının bilgisayarların işletim sistemi ve uygulamalarındaki açıkları ve hataları tespit ederek bu noktadan saldırıda bulunma eğilimi göstermelerinden hareketle, işletim sistemi ve uygulamaların düzenli olarak güncellenmesi de olası saldırılara karşı önemli bir savunma üstünlüğü teşkil edecektir. Bununla birlikte İnternet tarayıcılarında istenmeyen kodların çalıştırılması da engellenmelidir.

Kötü amaçlı yazılımın neden olduğu tehlike, bilgisayar sistemleri ve programlarının düzenli olarak güncellenmesi ve bilgilerin gün be gün yedeklenmesi ile kolayca azaltılabilir. Yazılım güncellemeleri, fidye yazılımının girilmesine izin veren dijital delikleri kapatır ve yedekler, kullanıcıların bilgileri zorlamadan kurtarmasını sağlamaktadır. Bununla birlikte, birçok bireysel ve kurumsal kullanıcı bu temel önlemleri almak konusunda halen yetersiz vaziyettedir.

Şüphesiz bu konuda bilinçlenmek, eğitim olanaklarından yararlanmak da etkin tedbirlerden bir başkası olacaktır. Böylelikle kullanıcı hatalarının en aza indirgenmesi mümkün olabilecektir. Bu konuda bilinçli bir kullanıcının bilinmeyen linklere tıklarken ya da e-posta eklerini açarken daha dikkatli davranacağı, indirdiği her dosyanın güvenlik taramasından geçmesine özen göstereceği şüphe götürmez bir durumdur.

Bireysel kullanıcıların fidye yazılımlara karşı savunmasını önemli ölçüde artırmak için yapabileceklerini şu şekilde üç maddede toplayabiliriz:

1- Amazon, Google, Microsoft ve diğer bulut depolama alanı sağlayıcılarının, kullanıcılarını siber saldırılardan korumak için her yıl yüz milyonlarca dolar harcadığı bilinmektedir. Bireysel kullanıcıların en önemli bilgilerini bulut depolamaya taşıyarak (ve tabi yedeklemeyi unutmayarak) bu imkanlardan yararlanması yerinde bir davranış olacaktır. Microsoft, Apple ve diğerleri ayrıca, yazılım güncelleştirmelerini yayınlandıkça bireysel bilgisayarlarda otomatik olarak uygulanmasına izin veren ayarlara sahiptir.

2- Daha fazla koruma için İnternet tarayıcısının güvenlik ve gizlilik ayarları düzenlenmelidir. Google Chrome, Apple Safari ve Mozilla Firefox gibi tarayıcılar kullanıcılarını bu konuda yönlendirmektedir. Ayrıca, şüpheli e-postalar asla açılmamalı, şüpheli e-postaların ekleri indirilmemeli veya şüpheli e-postalardaki bağlantılara tıklanmamalıdır.

3- Anti-fidye çözümleri kullanılmalıdır. Bu bireysel kullanıcılara ilk etapta pahalı gelebilir, ancak bunları kullanmanın maliyetinin kullanmamanın getirebileceği maliyetlerden çok daha az olduğu göz ardı edilmemelidir.

Konuyla ilgili olarak ülkemizdeki yetkili merciler de harekete geçmiş, buna bağlı olarak 2011 yılında Bakanlar Kurulu kararı ile Emniyet Genel Müdürlüğü bünyesinde Siber Suçlarla Mücadele Daire Başkanlığı kurulmuştur. Kuruma http://www.siber.pol.tr/Sayfalar/default.aspx adresinden erişim sağlanabilmektedir. Ayrıca 2014 yılında Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından fidye yazılımlarının da aralarında bulunduğu siber olaylarla ilgili çalışma yapmak üzere Ulusal Siber Olaylara Müdahale Merkezi (USOM)

kurulmuştur. USOM'un İnternet sitesinde zararlı yazılımların listesi güncel olarak yayınlanmaktadır: https://www.usom.gov.tr/zararli-baglantilar/1.html

Siber suçlara bağlı olarak siber güvenlik şirketleri ve sundukları çözüm sayıları da artış göstermektedir. Bilgisayar sistemlerinin fidye yazılımlarından korunması için özel olarak geliştirilmiş "anti-fidye" uygulamaları bulunmaktadır. Bunların bazıları ücretsiz olarak da temin edilebilmektedir. Dünya çapında en çok tanınan siber güvenlik çözüm sağlayıcıları arasında BitDefender, Eset, KasperSky, McAfee, Symantec, TrendMicro gibi örnekler sıralanabilir. Ücretsiz temin edilebilen anti-fidye uygulamalarına birkaç örnek vermek gerekirse şunları sıralayabiliriz: Acronis, Avast, Cybereason, RansomBuster… Bu alandaki gelişmiş çözümler, e-posta yoluyla girmeye çalışan herhangi bir saldırının tespit edilmesine bilişsel zeka ve gerçek zamanlı algılama sistemi kullanarak yardımcı olabilmektedir.

Bir fidye yazılımı saldırısına uğrayan mağdurun önünde iki seçenek bulunmaktadır:

1- İstenen fidyeyi ödemek.
2- İstenen fidyeyi ödemeyi reddetmek.

Şimdi bu iki seçeneğin etkilerini ayrıntılı olarak inceleyelim.

1- İstenen fidyeyi ödemek.

Fidye saldırganlarının talep ettikleri fidye miktarlarının giderek artmakta olduğunu söylemek yanlış olmayacaktır. Ancak çok yüksek oranlardaki fidye miktarları siber sigorta kapsamında karşılanması da umulmamalıdır. Düşük fidye miktarları ise saldırganlar açısından çabaya değer görülmeyecektir. Gerçekte, fidye yazılımı mağduru olan herhangi bir şirketi

bekleyen yüklü bir maliyet var demektir. Bireylerde ise bu durum ele geçirilen belgelerin manevi önemine bağlı olarak değişkenlik gösterecektir.

İstenen fidye miktarının yüksek ya da düşük olmasının işletme tarafından şu bakış açısıyla değerlendirilmesi muhtemeldir: Şirketin işlerinin kesintiye uğraması, bilgisayar kullanmadan yapılabilecek işlemlerin kısıtlı olması, ele geçirilen verilerin taşıdığı önem ve yaşanacak olası itibar kaybı.

İş kesintisinin maliyetinin genellikle siber sigorta tarafından karşılanması olağandır. Kayıp verileri yeniden oluşturabilen güvenilir bir yedekleme sistemine sahip olsalar bile, saldırıya uğrayan şirketlerin veri gizliliği idari para cezalarına tabi olabilir ve ayrıca verileri çalınan tüm muhataplara bildirim gönderme ile ilgili bazı maliyetler de söz konusu olacaktır. Bu maliyetlerin her ikisi de bir sigorta poliçesi tarafından karşılanabilir.
Ancak yukarıda sıralanan diğer olası etkiler konusunda maliyeti paylaşmak mümkün görülmemektedir.

Üstelik fidyenin ödenmesi durumunda erişimi engellenen dosyalara yeniden erişim sağlanabileceğinin bir garantisi yoktur. Ancak bu noktada rahatlatıcı bir durum şudur ki: Saldırganlar, fidye ödemesinden sonra belirli bir süre içerisinde bir şifre çözme algoritması sağlamazlarsa, bir şirkete bir daha saldırdıklarında fidye alamayacaklarını bilirler.

Ayrıca mağdur konumdaki şirketin çalınan verilerinin açığa çıkması durumunda ne kadar daha büyük bir risk altında olduğu da değerlendirilmelidir. Bu konuda da bir garanti söz konusu değildir.

Fidyeyi ödemeye razı olmanın bir başka riski daha vardır: Bu onlara ilgili şirkete ya da başka şirketlere yeni saldırılar gerçekleştirmek konusunda cesaretlendirecektir.

Tüm bu riskler göz önüne alındığında ilk olarak yetkili adli merciler ile irtibata geçerek saldırganların tutumu, karakteristiği ve taşıdığı risklerin uzmanlarca incelenmesi sağlanmalıdır.

2- İstenen fidyeyi ödemeyi reddetmek.

İstenen fidyeyi ödemeyi reddetmenin de ekonomik bir maliyeti vardır. En başta yedek verilere geçme maliyeti vardır ki bu pek çok faktöre bağlı olarak değişkenlik gösterecektir. Şirketler verilerini günlük olarak yedeklerse, maliyet ve kesinti önemsiz olabilir. Ancak veri farkı, belirli günlük işlemleri kapsayamayacak kadar fazlaysa, iş kaybı ve verimlilik kaybı önemli olabilir. Başka bir konu, yedekleme verilerine geçmek için gereken zamandır. Operasyonel kayıp siber sigorta şirketi için belirleyici bir faktör olacaktır.

Fidye ödemeyi reddeden şirketlerin de tekrar saldırıya uğrama ihtimali vardır. Orijinal veriler ve sistemler saldırganlar tarafından şifrelendiğinde, saldırganların sisteme nasıl sızdığını anlamak için kapsamlı bir adli soruşturma yürütülmesi zorunluluk halini alır. Mağdur, yedekleme verilerine geçerken siber güvenlik önlemlerini yükseltip sıkılaştırsa bile, hedeflenen şirketin sistemine zaten başarılı bir şekilde sızan saldırganların başka bir yol bulabilmesi mümkündür.

Saldırganların şirketi uzlaştırmaya ikna etmenin çeşitli yollarını belirleyerek keşif araştırması yapabilecekleri de göz önüne alınmalıdır. Hedeflenen şirketin sistemlerine tekrar girmek için yararlanabilecekleri üçüncü taraf güvenlik açıklarına odaklanabilirler.

Sonuç olarak bir fidye yazılımı operasyonu ile ilgili karar vermenin en temel yolu, saldırının finansal etkisinin ne olacağını iyi anlamak ve adli mercilerle iş birliği yapmaktır. Bu durumda masaya yatırılması gereken noktaların

başında finansal etkinin yanı sıra şirketin potansiyel siber risk duruşunu saldırganın bakış açısından görmek gerekmektedir.

Ek olarak Amerika Birleşik Devletleri Bilgisayar Acil Durum Hazır Ekibi (United States Computer Emergency Readiness Team; US-CERT) tarafından önerilen son derece kapsamlı koruyucu önlemler şöyle listelenmektedir:

- Anti-virüs ve anti-fidye programları kullanın ve bunları düzenli olarak güncelleyin.
- İşletim sisteminize gelen güncelleme eklentilerini takip edin ve sisteminizi bu doğrultuda güncel tutun.
- Dosya ve yazıcı (printer) paylaşım hizmetlerini devre dışı bırakın. Bu hizmetler gerekliyse, güçlü şifreler veya Active Directory kimlik doğrulaması kullanın.
- İstenmeyen yazılım uygulamaları yüklemek ve çalıştırmak için kullanıcıların yetkilerini (izinlerini) kısıtlayın. Gerekmedikçe, kullanıcıları yerel yöneticiler grubuna eklemeyin.
- Güçlü bir şifre politikası uygulayın ve şifrelerinizi düzenli olarak değiştirmeyi ihmal etmeyin.
- E-posta eklerini açarken, göndereni tanıyor ve ekli bir e-posta bekliyor olsanız bile dikkatli olun.
- İstenmeyen bağlantı isteklerini reddetmek üzere yapılandırılmış bir güvenlik duvarı kullanın.
- Sunuculardaki gereksiz servisleri devre dışı bırakın.
- Şüpheli e-posta eklerini tarayın ve kaldırın; taranan ekin "gerçek dosya türü" olduğundan (yani, uzantının dosya başlığına uyduğundan) emin olun.
- Kullanıcıların web tarama alışkanlıklarını izleyin; riskli içeriğe sahip sitelere erişimi kısıtlayın.

- Çıkarılabilir medya kullanırken dikkatli olun (örneğin USB flaş sürücüler, harici sürücüler, CD'ler vb.).
- Bilgisayarınızda başlatmadan önce İnternet'ten indirilen tüm yazılımları tarayın.
- En son siber tehditlerle ilgili kurumsal farkındalığı artırın.

1.8. Fidye Yazılımlarının Hukuksal Boyutu

Bilgi Teknolojileri Kurumu'nun (BTK) sitesinde Bilişim Suçları Yapısı / Ortak Özellikleri aşağıdaki şekilde belirtilmiştir:[36]

- Bilişim suçunun işlenmesinde bilgisayar sistemleri ve teknolojilerinin kullanılması.
- Bilişim suçunun sonucunda çok yüksek kazancın kolay ve daha az riskle temin edilmesi.
- Yeni suçlar olması nedeniyle gerekli kanun ve düzenlemelerin eksik ve yetersiz olması.
- Yeterli mevzuat olsa bile uygulamanın eksik bilgi veya yeteneğe sahip olma ihtimalinin yüksek olması.
- Diğer suç türlerine gore daha ağır maddi ve manevi sonuçlar doğurması.
- Suç mağdurlarının genelde bilinçsiz kullanıcılar ile ekonomi ve finans sektöründen olması.
- Ekonomik kaybın büyük olması nedeniyle, genelde basit suçlar haricinde güvenlik güçlerine bildirilmemesi.
- Normal kişiler yönüyle de bu tür suçun mağduru olunması durumunda genellikle takip edilmesi gereken prosedüre tam olarak hakim olunmaması.
- Zarara uğrayan mağdurların büyük kuruluş ve işletmeler olması durumunda itibar ve prestij kaybetme korkusunun baskın gelmesi.

[36] BTK, Bilişim Hukuku ve Bilişim Suçu, 11 Kasım 2016, http://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu-detay-58.html

- Bilişim suçunu işleyenlerin genelde 17-35 yaş arasındaki gençlerden oluşması.
- Bilişim suçu mağdurlarının genellikle ticari faaliyette bulunan kurumlar olması.
- Suçluların çoğunluğu, bazen fiillerinin deşifre olunmaması için ihbar edilmeyeceğinden, bazen ise, bu fiilleri karşılayacak ceza normunun bulunmamasından cesaretle, eylemlerinin yaptırımsız kalacağına güvenle hareket etmektedir.
- Suçlular adi ve münferit olabileceği gibi organize de olabilmektedir.
- Bilişim suçu, bilgi teknolojilerinden sonra ortaya çıkan yeni bir suç çeşididir.
- Bilişim suçu ile bilişim yoluyla işlenen suç ayrılmaktadır.
- Bilişim suçu ile mücadele bilinçlendirme ayağı da olan komplike bir süreçtir.
- Suçlu ve suç yontemi hızlı bir şekilde gelişebilmektedir.
- Genellikle uluslararası boyutu bulunmaktadır.

Bu maddeler, fidye yazılımlarının bir bilişim suçu olduğunu açıkça ortaya koymanın ötesinde neredeyse fidye yazılımlarını tarif etmektedir. Zira bilgisayar sistemleri kullanılarak işlenmekte, kolay ve az riskle yüksek kazanç kapısı olarak görülmekte, mevzuat ve uygulamalarına ilişkin eksikler bulunmakta, ağır maddi ve manevi sonuçlar doğurmakta, genelde güvenlik güçlerine bildirilmemekte ve uluslararası boyuta sahip olmaktadır. Tüm maddeler adeta fidye yazılımları için özel olarak hazırlanmış gibi durmaktadır. Bu maddelerin önemli bir tanesi de "Suç mağdurlarının genelde bilinçsiz kullanıcılar ile ekonomi ve finans sektöründen olması" tarifinin yapıldığı maddedir.

Fidye yazılımlarının kendine has özelliklerine karşılık gelen maddelere Türk Ceza Kanunu'nda da yer verilmiştir

2016 yılında yürürlüğe giren KVKK (Kişisel verilerin Korunması Kanunu) gerçek kişilere ait kişisel verilerin sınırsız biçimde ve gelişigüzel toplanması, yetkisiz

kişilerin erişimine açılması, ifşası veya amaç dışı ya da kötüye kullanımı sonucu kişilik haklarının ihlal edilmesinin önüne geçilmesi amaçlanmaktadır.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın hazırladığı "Siber Güvenlik Yasa Tasarısı"na göre Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile SOME'lerin işlevinin yasa ile daha da artırılması öngörülürken, etkin denetim, sır saklama yükümlülüğü, siber olaylara müdahale ekiplerinin görevleri, operasyon merkezleriyle Kamu-Net uygulamalarına ilişkin usul ve esasları barındırmakta ve siber saldırılara karşı güvenlik açıklarını kapatmayan şirketlere de çeşitli yaptırımlar uygulanacağı belirtilmektedir.[37]

1.9. Fidye Yazılımları Ödeme Yöntemleri

Nadir bir kısmının tarihte geleneksel yöntemlerle ödendiği bilinse de saldırganlar açısından Bitcoin'in en güvenli ödeme yöntemi olarak görüldüğü anlaşılmıştır. Nitekim yasal olmayan porno siteleri, ilaç satış siteleri gibi pek çok yasadışı faaliyet için Bitcoin'in bir ödeme yöntemi olarak benimsendiği bilinmektedir. Bu bölümde fidye yazılımlarının gelir akışında, Bitcoin ile yapılan ödemeler anlatılacaktır.

Bitcoin ile yapılan ödemeler incelendiğinde, fidyelerin gönderildiği anahtar adreslerde toplandığı (toplayıcı), sonrasında bu adreslerden alındığı ya da başka adreslere aktarıldığı görülmektedir. Anahtar adres, bilinen bir kümeye aitse, fidye yazılım ödemelerinin izlenmesi için son yol olarak kabul edilebilir. Anahtar adres ve bunlara karşılık gelen kümelenmelerin, Bitcoin ticareti yapan siteler ve / veya çevrimiçi (online) bahis / kumar siteleri ile bağlantılı olduğu ya da farklı aktörlerin paralarını ve işlemlerini karıştıran ve böylece kripto-para birimi işlemlerinin dijital izlerini kamufle eden aracı servislerle bağlantılı olduğu görülmektedir. "Mixing Services" karıştırıcı siteler kara para aklama ve siber

[37] Milliyet.com.tr, Zorunluluk geliyor! Tüm şirketler çalıştıracak, 20 Eylül 2017, http://www.milliyet.com.tr/zorunluluk-geliyor-tum-sirketler-ekonomi-2522944/

suçlarla ilgili faaliyetlerde, ödeme yöntemleri olarak kripto para birimlerine dayanan merkezi bir rol oynamaktadırlar. [38]

Bitcoin ile fidye yazılımlarının güçlü ilişkisini şu korelasyonla da ortaya koymak mümkün olabilir:

- Bitcoin'in en yüksek seviyeye ulaştığı yıl 2017 olmuştu. 2017 yılında Bitcoin'in değeri yüzde 1579 oranında devasa şekilde artmıştı.[39]

- Fidye yazılımı saldırılarının en yoğun yaşandığı yıllar arasında da 2017 ön plana çıkmıştır. WannaCry, Petya, BadRabbit gibi tarihin en büyük fidye yazılımı saldırıları 2017 yılında ortaya çıkmıştı. Küresel arenada aynı anda pek çok ülkeye fidye yazılımı saldırıları gerçekleştirilen 2017, uzmanlarca "fidye zararlısı yılı" olarak nitelendirildi.[40]

Bu tezimizi doğrulayan ve kripto para odaklı fidye yazılımlarının son dönemin artış yaşayan trendlerinden birisi olduğunu göz önüne seren bir takım bilgiler de Moskova, New York, Londra ve Dubai'de temsilcilikleri bulunan çok uluslu siber güvenlik şirketi Group IB'nin "Yüksek Teknoloji Suç Trendleri" isimli raporunda yer almaktadır. 2017 ve 2018 yıllarındaki gerçekleştirilen saldırıları mercek altına alan rapor, Kuzey Kore'nin finanse ettiği söylentileriyle gündeme gelen siber saldırgan grubu Lazarus'u çevrimiçi borsalardan çalınan 882 milyon dolar değerindeki kripto paranın tek başına 571 milyon dolarlık kısmından sorumlu tutmuştur.[41]

[38] Masarah Paquet-Clouston GoSecure Research, Kanada, Bernhard Haslhofer Austrian Institute of Technology, Austria, Benoît Dupont Université de Montréal, Canada, Ransomware Payments in the Bitcoin Ecosystem, sf. 3, https://arxiv.org/pdf/1804.04080.pdf
[39] CNNTürk.com.tr, 2017'nin sanal para şampiyonu Ripple: 1 yılda değeri yüzde 36 bin arttı, 4 Ocak 2018, https://www.cnnturk.com/ekonomi/kripto-para/2017nin-sanal-para-sampiyonu-ripple-1-yilda-degeri-yuzde-36-bin-artti
[40] HaberTurk.com, Fidye saldırıları 2017'ye damgasını vurdu, 17 Ocak 2018, https://www.haberturk.com/fidye-saldirilari-2017ye-damgasini-vurdu-1799490-ekonomi
[41] Group IB, Hi-Tech Crime Trends 2018, https://www.group-ib.com/resources/threat-research/2018-report.html

Şimdi bir de Bitcoin'in fidye yazılımı saldırganları açısından kullanışlı olmasının en önemli gerekçelerine yakından bakalım:

- **Anonimlik**: Diğer sanal para birimlerinin aksine Bitcoin cüzdanları oluşturmak için herhangi bir kimlik ibrazı gerekmez. Bu, siber suçluların arkalarına iz bırakmamasını sağlamakla birlikte Bitcoin'i onlar için en cazip kılan unsurdur.

- **Tam otomatikleştirilebilir**: Fidye ödemelerinin tüm yönlerini, cüzdan oluşturmadan ödeme izlemeye, para aktarmaya kadar tüm işlemleri otomatikleştirmek kolaydır. Saldırganlar, her mağdur için özel bir ödeme adresi tanımlayabilmekte ve süreci otomatikleştirebilmektedirler. Üstelik otomatik ödeme talep edebilecek yazılım yazmak son derece kolaydır. Ödemelerin otomatik olarak talebi, saldırganlar açısından süreci hızlandırmaktadır.

- **Para iade edilemez**: Bitcoin'i saldırganlar nezdinde kullanışlı kılan en önemli etkenlerden biri de işlemlerin iptal edilememesi, yani ödeme alındıktan sonra herhangi bir şekilde geri istenememesidir. Bir Bitcoin işlemi geri alınamaz, yalnızca para alan kişi tarafından iade edilebilir. [42] Bu, fidye ödendikten sonra, kredi kartı işlemlerinden farklı olarak paranın geri ödenmeyeceğini garanti eder.

- **Eşdeğeri yoktur**: Başka hiçbir para birimi, siber suçluların yasadışı faaliyetlerinden doğan kazançlarını (on milyonlarca dolar) bu kadar kolay kazanmasına olanak sağlamaz.

- **İzlenebilirlik**: Bitcoin cüzdanlarının oluşturulması kadar izlenmesi / takibi de kolaydır. Saldırganlar her saldırı için ayrı bir cüzdan oluşturarak her mağdurlarına farklı bir ödeme atayabilirler. Böylece hangi mağdurlarının para ödediklerini kolayca bulup takip edebilirler.

[42] Bitcoin.org, Some things you need to know, https://bitcoin.org/en/you-need-to-know

Saldırganlar açısından tüm bu avantajlarının yanında Bitcoin'in bir dezavantajı da vardır ki bu da güvenlik güçlerinin yararlanabileceği en etkili noktayı teşkil eder: Bitcoin hareketlerini izlemek zor olsa da mümkündür. Bitcoin işlemleri halka açıktır ve hangi cüzdanlara bakılacağı bilindiği sürece, fidye ödemelerini takip etmek için ihtiyaç duyulan tüm bilgilere ulaşılabilmektedir.

Ödemelerinin izlenebilmesini önlemek için çoğu kez saldırganların Bitcoin'lerini birden fazla cüzdan arasında aktardığı, hatta bazılarının ödemeleri takip etmeyi zorlaştırmak için Bitcoin mikserlerini kullandığı bilinmektedir. Ancak bu da aşılamaz bir durum değildir; zira Bitcoinler'in kaç kez taşındığı önemli değildir, nihayetinde değişim noktaları izlenebilir ve sonuçta tek bir ödeme cüzdanına ulaşılacaktır. Bu noktaya ulaşana kadar izlemeye devam etmek gerekmektedir. [43]

2. FİDYE YAZILIMLARININ ETKİLERİ

Bu bölümde fidye yazılımlarının bireysel ve kurumsal kullanıcılara yönelik etkileri ele alınacaktır.

Fidye yazılım saldırılarının fidyenin ötesinde bir maliyeti vardır. Kesinti süresi, bu süredeki kayıp satışlar, müşteri memnuniyetsizliği, saldırıyı hafifletme ve kurtarma masrafları, marka repütasyonunun uğradığı zarar, karşılanamayan sözleşme yükümlülükleri, uyumsuzluk için para cezaları dikkate alındığında saldırının maliyeti oldukça artmaktadır.

Fidye yazılımı saldırılarının türlerini aktarmıştık:

[43] Danny Yuxing Huang1 , Maxwell Matthaios Aliapoulios2 , Vector Guo Li3 Luca Invernizzi4 , Kylie McRoberts4, Elie Bursztein4 , Jonathan Levin5 Kirill Levchenko3, Alex C. Snoeren3, Damon McCoy2,Tracking Ransomware End-to-end.

- Fidye yazılımı sızdığı bilgisayarın, akıllı mobil cihazın ya da bilgisayar ağının içindeki dosyaları şifreleyerek erişilemez hale getirir.

- Kimi fidye yazılımı saldırganları dosyaları şifrelemek yerine bilgisayar ya da diğer cihazlara erişimi tamamen engeller ve hiçbir işlem yapılamaz hale getirir.

Bu durumların kullanıcılara etkileri şöyle olabilmektedir:

- Bilgisayarda yer alan değerli verilerin çalınması (örneğin bireylerin hesap şifrelerinin ya da kurumların müşteri veri tabanlarının ele geçirilmesi).

- Çalınan değerli verilerin üçüncü taraflarla paylaşılması (örneğin bireylerin telefon rehberlerindeki kayıtların arkadaşlık sitelerine ya da kurumlarının pazarlama stratejilerinin rakip kuruluşlara iletilmesi).

- Mağdurların verilerine ya da sistemlerine erişimlerini kaybetmesinin iş ve özel yaşamlarındaki olağan süreci sekteye uğratması, iş kesintisine yol açması (örneğin bireylerin özel yazışmalarını yapamaması ya da bir havayolu şirketinin uçuşlarının aksaması).

- İş kesintisine uğrayan kurumların verimliliği, itibarı ve motivasyonunun düşüşe geçmesi (örneğin bir bankanın işlem yapamaması, bir e-ticaret sitesinin müşteri kaybı ya da bir hastanenin muayene kabul edememesi).

- İzlenmesi gereken adımlar konusunda kararsız kalınması ile sürecin uzaması.

- Sorunu çözmek için harcanan zamanın yanı sıra sistemleri ve dosyaları geri yüklemek için oluşan zaman kaybı.

- Müşteri memnuniyetsizliği.

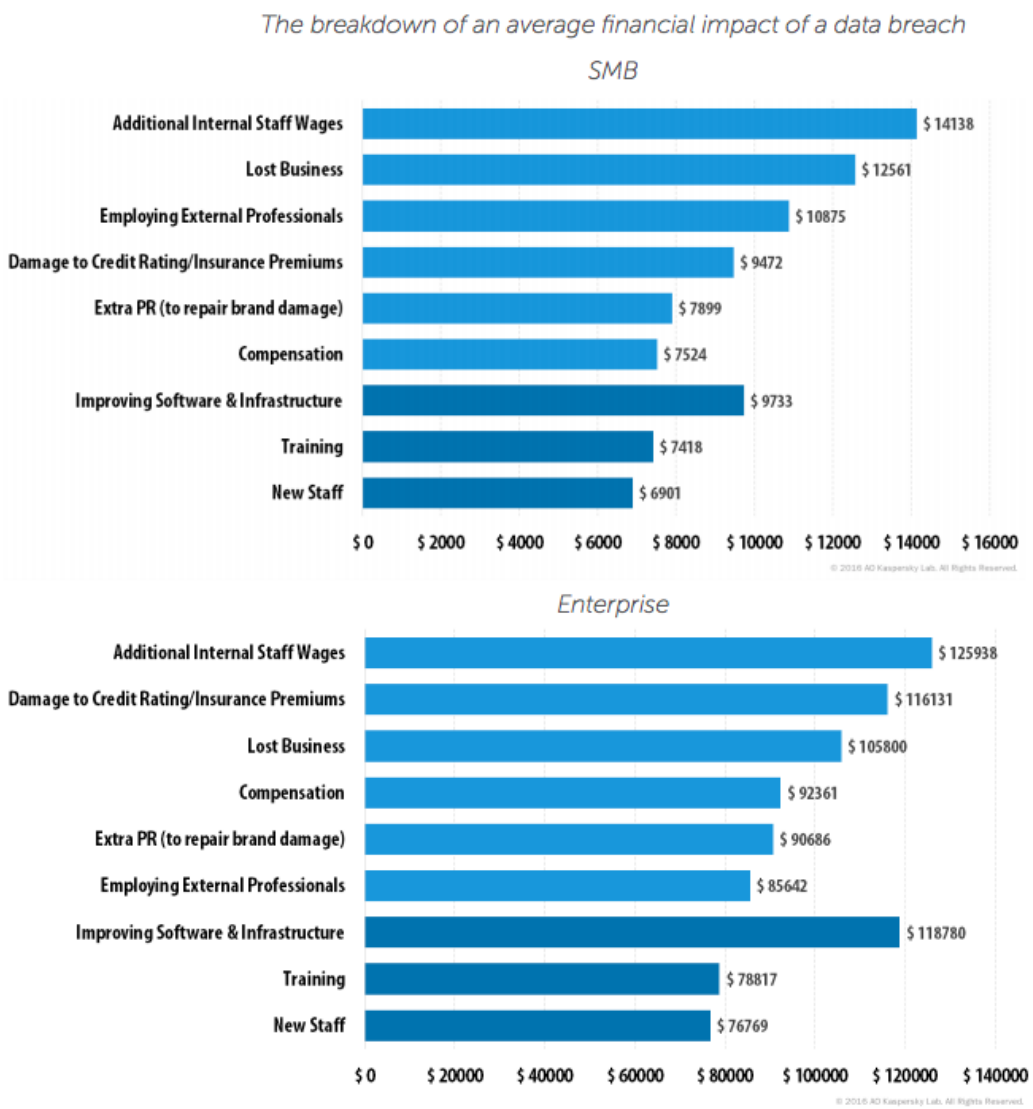
- Saldırıyı hafifletme ve kurtarma maliyeti.

- Tehdit altındaki cihazların yerine koyma maliyeti.

- Para cezası, hapis cezası gibi hukuki yaptırımlara yol açabilecek veri ihlallerinin yaşanması (örneğin bir eleman bulma şirketinin aday havuzundaki özgeçmişlerin ya da bir telekom operatörü şirketin müşterilerinin -mesela kredi kartı bilgilerinin de aralarında bulunduğu- özel bilgilerinin ele geçirilmesi.)

Kaspersky'ın raporuna göre; ABD'de KOBİ'lerin maruz kalacağı bir fidye yazılımı saldırısının maliyeti 86 bin dolar civarında olurken, daha büyük bir firmada bu maliyetin 861 bin seviyesine çıktığı belirtilmektedir. Bu saldırıların birden fazla olabileceği dikkate alındığında, uğranacak zarar daha da artacaktır.[44]

[44]Kaspersky Security Spotlight, A Guide to Avoiding Financial Losses in Cybersecurity, sf. 8, https://go.kaspersky.com/rs/802-IJN-240/images/Follow_the_Money_eBook.pdf?aliId=330210897



Şekil 13: Veri ihlallerinin yol açtığı finansal etkiler

Amerikan menşeili çok uluslu risk yönetim kuruluşu Gallagher'e göre, 2018 yılında rapor edilen fidye yazılımı saldırılarının yüzde 38'i hizmet sektörüne yönelik olmuştur. Günümüzde hizmet sektörü fidye yazılımı saldırılarından en fazla etkilenen sektör olarak bilinmektedir.[45] Bununla birlikte, hastane, toplu

[45] What is ransomware and how does it affect your business?, Bella Wilkinson, Gallagher Recruitment Insurance

taşıma ve polis departmanlarının da dahil olduğu birçok sektör bu zararlı yazılımdan etkilenmiştir.[46]

Fidye yazılımı saldırılarından en çok etkilenen sektörlerden bir tanesi sağlık sektörüdür. Bilişim alanında dünya çapında gerçekleştirdiği araştırma, yayıncılık, etkinlik ve pazar analizi çalışmalarıyla tanınan IDG'nin tahminlerine göre, en fazla fidye yazılımı saldırısına maruz kalan sektörlerin başında gelen sağlık sektöründe bu tip saldırıların 2017'den 2020'ye dört misli artacaktır.[47] Özellikle saldırı alan hastaneler için durum pek çok şirketten farklı olarak insan yaşamını tehlikeye atacak boyutlara ulaşabilmekte ve tam anlamıyla bir ölüm kalım meselesi olabilmektedir. Burada hayati olan konu, saldırganların hastane sisteminde kayıtlı olan hastaların sosyal güvenlik numarası, kredi kartı verileri, tıbbi geçmiş, istihdam bilgileri, adres ve e-posta adresi gibi en kişisel bilgilerini almasıdır. Bu veriler dolandırıcılık, kimlik hırsızlığı ve kimlik avı saldırısından daha fazlası için kullanılabilmektedir. Hastanelerin stok kayıtları değiştirildiğinde ya da bazı hastaları hayatta tutmak için gerekli verilerine ulaşılamadığında bu durum yaşamsal risk arz edebilmektedir.

Bu nedenle saldırıya uğrayan hastanelerin güvenlik güçleri ile iletişime geçmeyi bile beklemeden istenen fidyeyi ödemeyi kabul etme olasılıkları yüksektir; bu da saldırganları daha bu sektöre karşı daha iştahlı hale getirmektedir. Örneğin, Los Angeles Times'ta yer alan bir habere göre, Hollywood Presbyterian Medical Center, 2016 yılında uğradığı fidye yazılımı saldırısının akabinde kolluk kuvvetlerine ulaşmadan önce saldırganların talep ettiği yaklaşık 17 bin dolara tutarındaki 40 Bitcoin'i ödemiştir.[48]

[46]Jesper B. S. Christensen Niels Beuschau, , Ransomware detection and mitigation tool, sf. 5, http://www2.imm.dtu.dk/pubdb/views/edoc_download.php/7039/pdf/imm7039.pdf

[47] Cybersecurity Business Report, Steve Morgan, Cybersecurity Ventures CEO'su, CSO from IDG, Kasım 2017

[48] "Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating" Los Angeles Times, 18 Şubat 2016

Hizmet sektöründen bir başka örnek verecek olursak, uluslararası kargo dağıtım hizmeti veren FedEx'i ele alabiliriz. FedEx'ten Eylül 2017'de uluslararası haber ajansı Reuters'e yapılan açıklamada, şirketin Hollanda temsilciliğine yapılan NotPetya isimli fidye yazılımı saldırısı sonucunda üç aylık karının 300 milyon dolar azaldığı ve bu durumun şirketin tüm yıllık kazanç tahminlerini de olumsuz yönde değiştirdiği belirtildi. Şirketin bildirdiğine göre siber güvenlik sigortası bulunmamaktaydı.[49]

2.1. Örnek Olaylar ve Etkileri

Bilinen birkaç saldırı örneğini etkileri açısından inceleyelim.

2.1.1. WannaCry

Siber güvenlik, kötü amaçlı yazılım, gizlilik ve dijital haklar üzerine, İnternet'in derin köşelerinden haberler ve bilgiler sunan bir kaynak olan The Threat Report'a (Tehdit Raporu) göre, ilk olarak 12 Mayıs 2017'de ortaya çıkan WannaCry zararlı yazılımı, bugüne değin İngiltere ve İskoçya başta olmak üzere 150 ülkedeki yüz binlerce (230 bini aşkın) bilgisayarı etkilemiştir. [50] Bu ülkelerdeki Ulusal Sağlık Hizmetleri de dahil olmak üzere pek çok alanda işler durma noktasına gelmiştir. Örneğin doktorlar hasta kayıtlarına erişemediklerinden acil servise gelen çok sayıda hastayı ambulansla başka bir hastaneye yönlendirmek zorunda kalmıştır.

Ayrıca Almanya, Rusya, İspanya, Çin ve Amerika gibi ülkelerde telekom, ulaşım, güvenlik, finans sektöründen firmalar bu zararlı yazılımın saldırılarından etkilenmiştir.[51]

---

[49] https://www.reuters.com/article/us-fedex-results/cyber-attack-hurricane-weigh-on-fedex-quarterly-profit-idUSKCN1BU2RG,19 Eylül 2017

[50] Martinez Athena, Safe Computing Habits In The "Post Ransomware" Era,2019, https://www.thethreatreport.com/safe-computing-habits-in-the-post-ransomware-era/

[51] Jackie Wattles ve Jill Disis, money.cnn.com, Ransomware attack: Who's been hit, 15 Mayıs 2017, http://money.cnn.com/2017/05/15/technology/ransomware-whos-been-hit/index.html

Saldırının arkasında “The Shadow Brokers” isimli hacker grubu bulunmaktadır. Windows işletim sistemindeki güvenlik açıklarından yararlanan bu grup, Sunucu İleti Bloğu (SMB) protokolünün eski sürümünü kullanarak Windows bilgisayarlarını hedeflemiştir. Bir solucan olarak bilgisayar ağlarında yayılan WannaCry, kimlik avı veya diğer sosyal mühendislik yöntemleriyle yayılan fidye yazılımında olduğu gibi mağdur katılımı olmadan da otomatik olarak yayılımını sürdürebilmiştir.

Windows işletim sistemi bulunan bilgisayarların sabit disklerindeki dosyaları şifreleyerek kullanıcıların bunlara erişimini engellemeye dayanan saldırıda, saldırganlar kullanıcılardan dosyaların şifresini çözmek için üç gün içinde bitcoin cinsinden 300 ila 600 dolar arasında bir fidye ödemelerini talep etmiştir. Ancak ödeme yapıldıktan sonra bile, sınırlı sayıda mağdura şifre çözme anahtarı verilmiştir.

Microsoft’un hamlesi ise, Windows XP ve Windows Vista dahil olmak üzere, Windows'un kullanım ömrünün sonuna gelen sürümleri için güvenlik açığını azaltmaya yönelik eklentiler yayınlamak olmuştur. Aslında söz konusu güvenlik açığı Microsoft tarafından saldırıdan yaklaşık iki ay önce tespit edilmişti. Microsoft, ilk olarak Mart 2017'de yayımlanan Windows MS17-010 düzeltme ekinde CVE-2017-0144 olarak izlenen güvenlik açığını bulmuştu ve bunu düzeltmek için bir eklenti yayınlamıştı. Buna rağmen, birçok şirket Windows sistemlerini güncellememiş ve bu nedenle WannaCry solucanına maruz kalmıştır. Güncelleme yapmayan kuruluşların pek çoğu yeni eklentilerden olumsuz etkilenebilecek eski sistemleri kullanmaktaydılar.

Siber güvenlik şirketlerinin araştırmacıları, WannaCry solucanı için geçici olarak Kuzey Kore hükümetiyle bağları olan Lazarus Group'u suçlamıştır. Aralık 2017’de, Beyaz Saray resmen WannaCry’ın Kuzey Kore’den yayıldığını duyurmuştur.

Kuzey Kore ile WannaCry arasında çeşitli ilişkiler kurulmuştur. Saldırıların IP adresinin Kuzey Kore bağlantılı olduğu öne sürülmüş; aynı zamanda yapılan tersine mühendislik çalışmalarında Kuzey Kore kodlama yapısı ile WannaCry arasında ciddi bir bağlantı kurulmuştur.

Dünya çapında binlerce bilgisayarı hedef alan WannaCry zararlı yazılımı, her bir bilgisayar için benzersiz bir Bitcoin cüzdan adresi oluşturmak üzere yapılandırılmıştır. Ancak, kodun doğru bir şekilde çalışmaması sebebiyle, mağduru ödemeler için üç adede sabit kodlu adrese yönlendirmiştir. Bu durum, saldırganların, hangi mağdurun sabit kodlu adresleri kullanarak ödeme yaptığını belirleyemediğini göstermektedir.[52]

WannaCry solucanının küresel maliyetinin 8 milyar dolar olduğu tahmin edilmektedir.[53]

Şekil 14: WannaCry saldırganlarının yolladığı ekran mesajı örneği

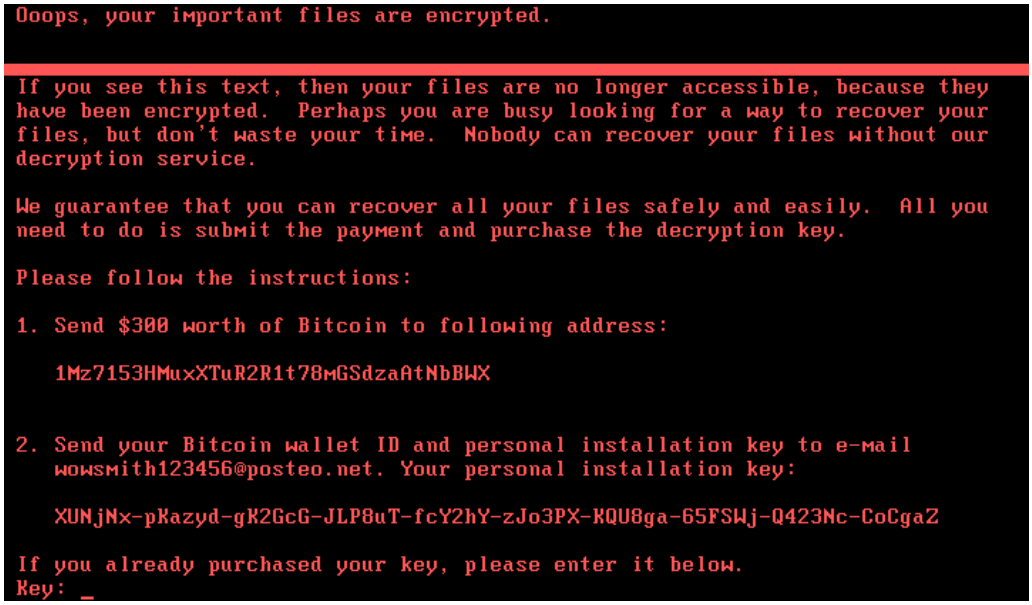
[52] Symantec Corporation, What you need to know about the WannaCry ransomware, 23 Ekim 2017, https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack
[53] James R. Slabay, Understanding the true hiding costs of ransomware attacks on the business, https://www.acronis.com/en-us/articles/costs-of-ransomware-attacks/

Şirketlerin kendilerini bu durumdan korumak için ilk etapta kullanmakta oldukları Microsoft Windows işletim sistemlerinin güncellemelerini kontrol edip 14 Mart 2017 günü yayınlanan MS17-010 kodlu eklentiyi yüklemeleri gerekmekteydi. Ayrıca görünen o ki şirketler çalışanlarını siber saldırılara karşı bilinçli hale gelecekleri eğitim programlarına tabi tutulmamışlar, kurumsal ağlardaki güvenlik zafiyetlerinin keşfedilmesi ve erken önlem alınması için gerekli sızma testlerini yapmamışlar ve düzenli olarak da yedek almamışlardı. WannaCry'ın bu denli yayılmasında, tüm bu ihmalkarlıkların büyük önem arz ettiği görülmektedir.

2.1.2. Petya

İnsanların siber güvenlik konularında daha fazla bilgi edinmelerine yardımcı olan bir proje olarak başlatılan ve https://www.2-spyware.com/ adresi üzerinden yayın yapan 2SpyWare'da yer alan bilgilere göre Petya, ilk olarak 2016 yılında keşfedilen bir dosya şifreleme truva atıdır. Günümüze değin birkaç farklı güncelleme ile çeşitli varyantları karşımıza çıkmayı sürdürmüştür. Türevleri arasında PetrWrap, GoldenEye, Mamba virüsü, Mischa, Diskcoder.D ve Bad Rabbit de sıralanmaktadır.

Petya, mağdurların bilgisayarlarındaki dosyaların şifrelenerek erişilemez hale getirilmesi ve ardından şifre anahtarının verilmesi için fidye talep edilmesi yönündeki klasik fidye yazılımı saldırılarından biri olmuştur. Fidyeler de tipik olarak BitCoin cinsinden talep edilmiştir. Başlangıcı WannaCry ile benzerlik göstermiştir; salgın hiçbir yerden fark edilmemiş ve hızla yayılmıştır. Ancak WannaCry'dan farklı olarak bu kötü amaçlı yazılım, spam e-postaları yoluyla yayılmış, bilgisayarı hemen yeniden başlattıktan sonra ekranda şöyle bir mesaj göstermiştir:



Şekil 15: Petya saldırganlarının yolladığı ekran mesajı örneği

Bu ekran kullanıcılar tarafından ilk bakışta sistem hatası gibi görünse de, aslında Petya yazılımı, sistemin arka planında sessizce dosya şifrelemesi gerçekleştirmiş. Kullanıcı sistemi yeniden başlatmaya çalışırsa veya dosya şifreleme işlemi gerçekleştirilirse, ekranda yanıp sönen kırmızı bir iskelet belirmiş ve "Herhangi bir tuşa basın" ifadesi görünmüştür. Tuşa bastıktan sonra, fidye notu ile yeni bir pencere açılmıştır:

Şekil 16: Petya saldırganlarının fidye notunun ardından ekrana gelen görüntü

Saldırının failleriyle ilişkili e-posta alanlarından biri süreç içinde iptal edilmiş, böylelikle mağdur bir bilgisayara eşleşen şifre çözücüyü almaya yardımcı olacak belirli bir kod atanmadığından veri kurtarma imkansız hale gelmiştir. Başta Ukrayna olmak üzere Rusya, İngiltere, Fransa, Danimarka, İran, Brezilya, Meksika gibi ülkelerde etkili olmuştur. Saldırıyı ayrıca İspanya, Hollanda ve Hindistan da onaylamıştır. Ukrayna, saldırıdan en fazla ülke olmuştur. Ülkenin çeşitli kamu kurumlarını da saran Petya zararlı yazılımı; ayrıca Kiev Havalimanı, metro sistemleri, enerji santralleri, nükleer santraller gibi geniş bir alana tesir etmiş, sistemleri durma noktasına getirmiş ve çok sayıda aksamaya neden olmuştur. Ukrayna'da hayatı durma noktasına sürükleyen saldırıdan yine Ukraynalı bir yazılım şirketi olan MeDoc sorumlu tutulmuştur. MeDoc bu iddiaları reddetse de, pek çok siber güvenlik uzmanı firmanın ilk kaynak olduğunu ortaya koyan kanıtlara sahip olduğunu iddia etmiştir.

Kamu otoritelerince, etkilenen kurumların müşteri hizmetleri ve bankacılık işlemlerini yürütmekte zorluk çektiği belirtilmiş, ATM'lerin çoğunun servis dışı olduğu ya da ekranlarında Petya'nın fidye yazılım mesajını görüntülendiği gözlemlenmiştir.[54]

Saldırının Ukrayna'nın ulusal tatil gününe denk gelmesi ve ülkenin daha önce de benzer saldırılara maruz kalması da göz önüne alındığında, finansal amaçtan çok, ülkede karışıklık çıkarmaya yönelik politik bir saldırı olduğu anlaşılmaktadır.[55]

E-posta yoluyla gerçekleştirilen bu saldırının sonucunda kamu kurumların çalışanların bile sahte bir e-postayı algılamak, açmamak, sahte bir ofis dokümanı indirmemek açısından yeterince bilinçli olmadıkları, pek çok sistemin fidye yazılımları karşısında yeterince savunmaya sahip olmadığı anlaşılmıştır. Bu tip saldırıların boyutu siber güvenlikle ilgili farkındalık, güvenlik açığı taraması, testi, doğru siber güvenlik uygulamalarının kullanımı ve yedekleme alınması konularında da ne denli yaygın bir yetersizlik olduğunu ortaya koymuştur. Ayrıca dosyaların şifrelenmesinden ziyade sistemi kullanılamaz hale getirmeyi hedefleyen Petya, bu yönüyle paradan çok yıkıcı etkide bulunmayı amaçlamıştır, denebilir.

2.1.3. SamSam

İlk kez Aralık 2015'te görülen ve 2016 itibariyle yaygınlaşmaya başlayan SamSam isimli fidye yazılımı hakkında bugüne dek yapılan en kapsamlı araştırma raporu Küresel siber güvenlik şirketi Sophos' aittir. Nisan 2018'de yayınlanan Sam Sam Ransomware Choses Its Targets Carefully raporuna göre, rastgele saldıran tanınmış fidye yazılımı ailelerinin çoğunun aksine, SamSam,

[54]Lizzie Dearden, The Independent, Ukraine cyber attack, 27 Haziran 2017, https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html
[55]Dick O'Brien, Internet Security Report, Ransomware 2017, sf. 11, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf

hastaneler veya okullar gibi verilerini geri almak için en çok para ödeyebilecekleri öngörülen belirli kuruluşlara karşı kullanılmıştır. [56] Spam kampanyaları yerine, SamSam'ın arkasındaki siber suçlular, mağdurların ağına erişmek veya Uzak Masaüstü Protokolü'nün (RDP) zayıf şifrelerine karşı kaba kuvvet taktikleri kullanmak için güvenlik açıklarından yararlanmışlardır. SamSam'ı diğer fidye yazılımı saldırılarından ayıran özelliklerden başlıcası da bu durum olmuştur. Mağdur seçilen kurumun BT altyapısına en kısa sürede en yüksek düzeyde zararı verecek şekilde kurgulanan süreç, sistemlere sızma konusunda ustalık gösteren bir kişi ya da grubun sızdıkları ağdaki zayıflıkları tespit etmesi ve burada zararlı yazılımı manuel olarak çalıştırmasına dayanmaktadır. Potansiyel hedefler keşfedildikten sonra, saldırganlar PSEXEC ve toplu komut dosyaları gibi araçları kullanarak SamSam zararlı yazılımını seçilen sistemlere manuel olarak dağıtmışlardır.

Saldırının ilk kurbanı Atlanta olmuştur. Saldırı, şehrin 13 yerel yönetim biriminin beşinde, ciddi dijital kesintilere yol açmıştır. Saldırının mahkeme sistemini sekteye uğratmak, konut sakinlerinin su faturalarını ödemelerini engellemek, kanalizasyon altyapısı talepleri gibi hayati iletişimleri sınırlamak ve Atlanta Polis Departmanı'nı bilgisayar yerine kağıt – kalemle çalışmaya zorlamak gibi geniş kapsamlı etkileri olmuştur.[57] İstenilen fidye miktarı 50 bin dolar civarında olmakla birlikte, bu saldırıların bertaraf edilmesi için ilk etapta 2.6 milyon doların üzerinde harcama yapıldığı basına yansımıştır. Harcamaların büyük bir kısmı, sistemlerin geri alınmasına yönelik yapılan acil müdahale, adli bilişim, ilave personel alımı ve Microsoft Bulut Altyapı

[56]Dorka Polatay, Peter Mackenzie, Sam Sam Ransomware Choses Its Targets Carefully ,2018, https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-ransomware-chooses-Its-targets-carefully-wpna.pdf

[57]Lily Hay Newman, Wired.com, The Ransomware that hobbled Atlanta will strike again, 30 Mart 2018,https://www.wired.com/story/atlanta-ransomware-samsam-will-strike-again/

Uzmanlığı ile ilgilidir. İlave olarak kriz iletişim merkezi ve acil müdahale danışmanlığı için de ilave 650 bin dolar harcadığı basına yansımıştır.[58]

Yine Sophos'un Samsam:The (Almost) Six Million Dollar Ransomware adlı rapora göre ise, SamSam saldırısı ile toplanan fidye miktarı 2018 yılı itibariyle 6 milyon doların üzerine çıkmıştır. [59] Bu rapordan çarpıcı bazı veriler şöyledir:

- Bilinen mağdurların yüzde 74'ü ABD'de bulunmaktadır. Saldırıdan en fazla etkilenen ülkeler arasında Kanada, İngiltere ve Orta Doğu ülkeleri sıralanmaktadır.

- Bitcoin cinsinden yapılan transferlere göre, SamSam saldırganları bireysel mağdurlardan tek seferde 64 bin dolara kadar fidye koparmayı başarmıştır.

- SamSam saldırısının ortaya çıkışının akabinde yeni versiyonları da geliştirilmiş, her yeni versiyonda daha karmaşık saldırı yöntemleri kullanılmış ve geride iz bırakmamak için operasyonel güvenlik önlemlerinden korunmak üzere daha yetkin önlemler alındığı gözlemlenmiştir.

- SamSam saldırganları yüzde 50 oranında sağlık, eğitim ve hükümet alanındaki orta ila büyük ölçekli kamu sektörü kurumlarını, yüzde 50 oranında özel sektör şirketlerini hedef almışlardır.

- Saldırganların saldırı hazırlığı titizdir. SamSam saldırganları en uygun anı beklemiş; çoğu kullanıcının uykuda olduğu gece yarısında ya da mağdurun yerel saat diliminde sabahın erken saatlerinde şifreleme komutlarını başlatmışlardır.

[58]Lily Hay Newman, Wired.com, Atlanta spent $2,6 million $ to ransomware scare, 23 Nisan 2018, http s://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/

[59]Samsam:The (Almost) Six Million Dollar Ransomware, 2018, https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

SamSam örneğinde, saldırganlar bir sunucuyu başarılı bir şekilde enfekte ettikten sonra, ağ haritalama ve kimlik bilgilerini de çalarak ek mağduriyetler yaratmışlardır. Bu saldırıyı, basit bir hırsızlıktan ziyade profesyonel bir elmas hırsızlığı şeklinde yorumlamak yerinde bir tespit olacaktır. Zira hem saldırı yöntemi, hem de hedeflenen kritik kuruluşlar bu tespitimizin temel dayanaklarıdır.

2.2. Fidye Yazılımlarının Ekonomisi

Ünlü ekonomist Prof.Dr. Kerem Alkin'e göre, küresel suç örgütleri genel olarak siber saldırılar yoluyla uyuşturucu madde ticaretinden daha fazla gelir elde etmektedirler. [60]

Fidye yazılımlarını devasa ölçüde yaygın kılan unsur da hiç şüphe yok ki saldırganlar açısından önemli bir gelir kaynağı olmasıdır. Diğer birçok siber saldırı biçiminden farklı olarak fidye yazılımları, son derece hızlı ve kolay uygulanabilmekte ve yine son derece hızlı ve kolay şekilde gelir getirebilmektedir.

CyberSecurity Ventures'in 2018 CyberCrime Report. [61] başlığı ile 6 Şubat 2019'da yayınladığı verilere göre:

- Fidye yazılımlarının yol açtığı hasarın maliyetinin 2021'de 2015'e kıyasla 57 kat daha fazla olması beklenmektedir. Bu veri, fidye yazılımlarının en hızlı büyüyen siber suç türü olduğunu göstermektedir. ABD Adalet Bakanlığı, fidye yazılımını siber suç için yeni bir iş modeli ve küresel bir fenomen olarak tanımlamıştır.

[60] Prof.Dr. Kerem Alkin, 6 trilyon dolarlık siber hırsızlığa hazır mıyız?, 6 Mayıs 2018, https://www.sabah.com.tr/yazarlar/kerem-alkin/2018/05/06/6-trilyon-lik-siber-hirsizliga-hazir-miyiz

[61] Steve Morgan, Cybercrime Damages $6 Trillion By 2021, 2019, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

- Küresel fidye yazılımı hasar maliyetleri 2015'te 325 milyon dolar iken, 2017'de 5 milyar dolar olarak tespit edilmiştir. Bu rakamın 2019'da 11.5 milyar dolara, 2021'de 20 milyar dolara ulaşacağı öngörülmektedir. 2015'ten 2021'e artış oranı 57 mislidir.

FBI'ın son olarak 22 Nisan 2019'da yayınladığı "The Internet Crime Report"a (İnternet Suç Raporu) göre, 2018 yılında FBI'a bildirilen fidye yazılımı olaylarında bin 493 mağdur toplam 3 milyon 621 bin dolarlık kayba uğramıştır. Elbette bu istatistik yalnızca FBI'a bildirilen kısmı temsil etmektedir; gerçekte rakamların çok daha yüksek olduğu bilinmelidir. Üstelik kaybedilen para miktarı, sorunu çözmek için yapılan yatırımları da kapsamamaktadır.[62]

2017 yılında yayımlanan E-Dolandırıcılık ve İstihbarat Raporu'na (Phishing Trends And Intelligence Report) göre, 2016 yılında tüm e-dolandırıcılık (phishing) saldırılarının yüzde 91'inden fazlasının finansal kurumlar, bulut depolama / dosya barındırma hizmetleri, web posta / çevrimiçi hizmetler, ödeme hizmetleri ve e-ticaret şirketlerini hedef aldığı görülmektedir.[63]

Fidye yazılım saldırılarında, talep edilen fidye miktarının ağırlıklı (yüzde 47) olarak 501 -2.000 USD[64] arasında değiştiği ve 2017 yılında 183,6 milyon fidye yazılım saldırısı olduğu dikkate alındığında (2016 yılı için 638 milyon olduğu belirtilmiştir.[65]), milyonlarca dolarlık bir fidye ekonomisi olduğu yadsınamaz bir gerçektir.

Fidye ödeme davranışı ile ilgili olarak IBM'in, ABD'deki farklı sektörlerden 600 şirket yöneticisi ve bini aşkın tüketici ile yaptığı fidye yazılımı ve veri yönetimi uygulamaları ve algıları hakkındaki çalışma da bu alanda harcanan paralarla ilgili

[62] FBI, The Internet Crime Report, Nisan 2019, sf: 11
[63]Phish Labs, Threat Intellgience Report, Kasım 2018, sf. 15, https://pages.phishlabs.com/rs/130-BFB-942/images/2017%20PhishLabs%20Phishing%20and%20Threat%20Intelligence%20Report.pdf
[64] Statista.com, Statistics report, 2017, https://www.statista.com/statistics/701003/average-amount-of-ransom-requested-to-msp-clients/
[65] 2018 Sonicwall Siber Tehdit Raporu, sf. 5, http://www.m2s.com.tr/bulten/2018_Sonicwall_siber_tehdit_raporu-TR.pdf

çarpıcı rakamlar ortaya koymuştur: Örneklemde, yöneticilerin neredeyse yüzde 50'si şirketlerine fidye saldırısı yapıldığını bildirmiştir. Bu yöneticilerin çoğunluğu (yüzde 70) olayın çözümlenmesi için fidye ödemesi yaptıklarını açıklaşmışlardır. Bunların yüzde 50'sinin 10 bin dolardan fazla, yüzde 20'sinin ise 40 bin dolardan fazla fidye ödemesi yaptığı tespit edilmiştir. Aynı çalışma, henüz saldırıya uğramamış kişilere bakıldığında, bunlar arasından şirket yöneticilerinin yüzde 25'inin kaybettiği veri türüne bağlı olarak 20 bin ila 50 bin dolar arasında bir fidye ödemeye razı olacağını ortaya koymuştur. [66]

Fidye yazılımları pazarı doğal olarak siber güvenlik pazarını da büyütmektedir. Dünya çapında zararlı yazılımları önleme çözümlerinin yanı sıra DDoS etkisini azaltma (çevrimiçi erişimi engellemeye yönelik saldırılar), güvenlik duvarı, anti-virüs, olağan üstü durum kurtarma gibi çözümler de dahil olmak üzere siber güvenlik pazarının 2018 itibariyle 152 milyar dolarlık bir pazar teşkil ettiği Markets And Markets isimli küresel pazar araştırma kuruluşu tarafından tahmin edilmektedir. Öte yandan aynı kuruluş tarafından bu rakamın 2023 yılında yüzde 10,2'lik artışla 248 milyar dolarlık büyüklüğe erişeceği öngörülmektedir.

Fidye yazılımları ekonomisinin önemli bir boyutu da fidye yazılımları pazarıdır. Merkezi Massachusetts'te bulunan çok uluslu bir siber güvenlik şirketi olan Carbon Black'in 2018'de yayınladığı bir araştırmaya göre, fidye yazılımı saldırılarının dünya çapında işletmelere maliyetini 2017 yılı itibariyle 1 milyar doların üzerinde tahmin etmektedir. Rapordan bazı çarpıcı satır başları şöyle özetlenebilir:[67]

- Dünya çapında 6 bin 300'den fazla mecrada 45 bini aşkın fidye yazılımı satılmaktadır.

[66] IBM Study: Businesses More likely to Pay Ransomware than Consumers, Aralık 2016
[67] The Ransomware Economy, Carbon Black, 2017

- 2016 – 2017 yılları arasında karanlık ağdaki fidye yazılımı satışlarında yüzde 2 bin 502'lik bir artış olmuştur. Bu artış pazarın 249 bin dolardan 6 milyon 237 bin dolara erişmesinin sonucudur.

- Ortalama olarak fidye yazılımı satıcıları, sadece bu yazılımlarını satarak yılda 100 bin doların üzerinde gelir elde etmektedirler.

Fidye yazılımları pazar ekonomisi içerisinde eğitim harcamalarının da payı bulunmaktadır. Siber güvenlik pazarına ilişkin araştırma ve raporlar sunan, Kaliforniya, New York ve İsrail'de ofisleri bulunan CyberSecurity Ventures'in 6 Şubat 2019'da yayınladığı verilere göre; siber güvenlik endüstrisinde en hızlı büyüyen kategorilerden biri olan çalışanlar için güvenlik bilinci eğitimi konusunda küresel harcamaların, 2014 yılında yaklaşık 1 milyar dolar iken; 2027 yılına kadar 10 milyar dolara ulaşacağı tahmin edilmektedir.

2.3. İş Modeli Olarak Fidye Yazılımları

Bu boyutta bir ekonomi söz konusu olduğunda, iş modelinin ne şekilde işlediği / maliyeti / fiyatlandırması ve karlılığı öne çıkmaktadır.

Fidye yazılımı iş modeli olarak kabul edilirse;[68]

2.3.1. Maliyeti

Kurulum maliyeti / ilk maliyet: Söz konusu kripto fidye yazılım olduğu göz önüne alındığında, ilk maliyetin büyük bir kısmı tekniktir. Karanlık webde 0.5 dolardan 3.000 dolara kadar araçlar satılmaktadır.

[68]Dr. Holger Nitsch Bavarian University of Policing, Internet Forensic Platform For Tracking The Money Flow Of Financiallymotivated Malware,
https://www.cepol.europa.eu/sites/default/files/S18%20Nitsch%20RAMSES_CEPOL_1.pdf

Fidye yazılımların teknik maliyeti, seçilen stratejiye bağlıdır. Fidye yazılım gelişimi beceri ve zaman açısından masraflıdır. [69] Fidye yazılımlarının geliştirilmesinde yer alan bireyler, sahip oldukları teknik yeteneklerle en azından kısa vadede başka yerlerde daha fazla kar elde edebilmektedir. Fidye yazılım satın almak daha az maliyetlidir ve bu nedenle potansiyel saldırganlar için daha caziptir.[70]

Yaygınlaştırma maliyeti: Fidye yazılımlarının dağıtımı için donanım sahibi olma, çalıştırma ve geliştirme maliyetini temsil eder. Ayrıca, Zeus veya Gameover gibi botnet'lere yük atma maliyetini de temsil edebilir. Bu, operatörlerin fidye yazılımı uygulamalarını yaymaya devam etmek istemeleri durumunda ortaya çıkan bir maliyettir. [71]

Müşteri hizmetleri maliyeti: Fidye yazılımı her ne kadar işlem bazlı bir sistem olsa da iki tarafın karşılıklı anlaşmasına bağlıdır. Bir taraf baskı altında olsa bile, diğeri istekli mağdurun fidye ödemesi için her fırsatın verilmesini sağlamalıdır. [72]

Uygun profesyonel web varlığı ve iletişim kanallarının geliştirilmesi ve bunların işletilmesi için gerekli uzmanlığın geliştirilmesini içerebilir. Çağrı masalarının (veya eşdeğerlerinin) barındırılması ve yönetilmesi gibi bakım maliyetleri de dikkate alınır.

Fidye yazılımının puanlaması 4 başlık dikkate alınarak yapılırsa;

[69] Darren Hurley-Smith, Findings on economic modelling of malware as business model, https://ramses2020.eu/wp-content/uploads/sites/3/2016/09/D4.1-Findings-on-economic-modelling-of-malware-as-a-business-model.pdf
[70]Darren Hurley-Smith, Findings on economic modelling of malware as business model, https://ramses2020.eu/wp-content/uploads/sites/3/2016/09/D4.1-Findings-on-economic-modelling-of-malware-as-a-business-model.pdf
[71] Darren Hurley-Smith, Findings on economic modelling of malware as business model, https://ramses2020.eu/wp-content/uploads/sites/3/2016/09/D4.1-Findings-on-economic-modelling-of-malware-as-a-business-model.pdf
[72] Darren Hurley-Smith, Findings on economic modelling of malware as business model, https://ramses2020.eu/wp-content/uploads/sites/3/2016/09/D4.1-Findings-on-economic-modelling-of-malware-as-a-business-model.pdf

- **Profesyonellik:** Suç eylemi olsa da profesyonellik alacaklıya bütünlük sağlar. Ayrıntılı ve bilgilendirici fidye yazılımlarının, kopyalanan ya da bilgisiz ara yüzlerden daha iyi bir müşteri desteği düzeyi sağladığı görülmüştür.

- **Öğreticilik/eğiticilik:** Nasıl ve ne kadar ödeyeceğini bilen mağdur genelde daha işbirliği içinde hareket eder.
- **Dil desteği:** Genelde İngilizce bilgilendirme yapılmaktadır.

- **Ücretsiz deneme şifre çözümü:** yapılan araştırmada sadece bir fidye yazılımında ücretsiz deneme şifre çözümü verilse de, mağduru ödemeye yöneltmekte olumlu bir katkısı olacaktır.

Para aklama maliyeti: Fidyeden değer yaratmak için, kanun uygulayıcı kurumlar tarafından belirlenen nihai kimlik ve tutuklama masraflarından kaçınırken biri geliri aklamak zorundadır. Bunun yapmanın en yaygın yolu kriptolu para yani Bitcoindir. Bitcoin kullanılarak yapılan maliyetler arasında, Bitcoin'leri cüzdanlar arasında taşımak için talep edilen yüzde 2.5'lik işlem ücreti bulunmaktadır.

RaaS'ın (Ransomware as a Service) yükselişi, kendi fidye yazılımlarını işletmek yerine yazılımlarını satmaya istekli olanlara teknik ve geliştirme yükünün boşaltılmasının da giderek yaygınlaştığını göstermektedir. Pek çok siber güvenlik uzmanı, fidye yazılımı saldırganlarının büyük ölçüde deneme yanılma yoluyla, maliyetlerini optimize ettiğine inanmaktadır. Sonuç olarak, fidye yazılımı uygulama ve işletim maliyetinin kar potansiyeline sahip olduğu açıktır. Diyebiliriz ki; fidye yazılımları ile siber suç hayatına giriş maliyeti neredeyse bedavaya yakındır.

2.3.2. Fidye Fiyatının Belirlenmesi

Basit bir şekilde, fidyenin fiyatını mağdurun dosyayı kurtarmak için ödemeye razı olduğu tutar belirlemektedir. Ancak, fiyat ve dolayısıyla kar, şifrelenen dosyaların mağdur için değeri, mağdurun saldırganlara güveni, suçlulara para verme isteği gibi ölçülemeyen durumlara göre değişkenlik gösterecektir.[73] Yapılan bir araştırmada, mağdurların yüzde 52'sinin dosyasını kurtarmak için fidye bedelini ödemeye razı olduğu belirtilmektedir. Yine aynı araştırmada, mağdurların yüzde 12'si fidye miktarının 500 dolar ve üzerinde olması halinde ödeme yapacağını belirtirken, yüzde 59'u fidye miktarının 100 dolar ve altında olması halinde ödeme yapabileceğini belirtmektedir.[74]

Değişkenleri göz ardı edersek, optimum kar "Talebin Fiyat Esnekliği" ile ölçümlemeye çalışılabilir.[75] "Talebin Fiyat Esnekliği" özetle; malın fiyatındaki bir birimlik değişikliğin, talep edilen miktarda ne kadarlık değişime sebep olduğunu açıklar. Çıkan sonuç, birden büyük olması, ürüne olan talebin fiyat değişikliğine hassas olduğunu gösterirken, birden küçük olması ise, fiyat değişimlerine hassas olmadığını göstermektedir.

Bunu fidye yazılımlarına uyarlarsak; fidye bedelinin 300 dolar olarak belirlenmesi durumunda, mağdurlardan yüzde 40'ının bu bedeli ödediğini / ödemeye razı olduğunu, bedelin 350 dolara çıkarılması durumunda ise mağdurların yüzde 30'unun bu bedeli ödemeye razı olduğunun kabul edilmesi durumunda, talebin fiyat esnekliğinin yüksek olduğu ifade edilebilir. [76]

Fiyat farklılaştırmasının da karı artırabileceği öne sürülebilir. Fiyat farklılaştırması üç ana başlıkta genelleştirilebilir:

[73] Julio Hernandez - Castro1, Edward Cartwright ve Anna Stepanova, Economic Analysis of Ransomware, Economic Analysis of Ransomware, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2937641
[74]Carbon Black Reports, The Ransomware Economy, Ekim 2017, https://www.carbonblack.com/wp-content/uploads/2017/10/Carbon-Black-Ransomware-Economy-Report-101117.pdf
[75]Julio Hernandez - Castro1, Edward Cartwright ve Anna Stepanova, Economic Analysis of Ransomware, Economic Analysis of Ransomware, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2937641
[76]Julio Hernandez - Castro1, Edward Cartwright ve Anna Stepanova, Economic Analysis of Ransomware, Economic Analysis, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2937641

- Kişiye özel fiyatlama yapılması,
- Mağdurlara bir fiyat menüsü /paket fiyat verilmesi (Word dosyalar için ayrı fiyat / resim dosyaları için ayrı fiyat uygulanması),

- Mağdurları kategorize ederek, kategoriye göre fiyatlama yapılması.

Mağdurlarından 300 - 600 dolar arasında ödeme talep eden WannaCry sonrasında, ilgili Bitcoin cüzdanlarında 140 bin doların üzerinde para biriktiği ve Ağustos 2017 başlarında bu bedelin cüzdandan çekildiği tespit edilmiştir.[77] Yayınlanan bir akademik çalışmaya göre bazı fidye yazılımı saldırılarında pazarlık oranları şöyle gerçekleşmiştir:[78]

FAMILY	STARTING DEMAND	LOWEST DEMAND	%DISCOUNT
CERBER	530	530	0%
CRYPTOMIX	1900	635	67%
JIGSAW	150	125	17%
SHADE	400	280	30%
			AVERAGE: 29%

[77] WannaCry ransomware bitcoins move from online wallets, BBC.com, 3 Ağustos 2017, http://www.bbc.com/news/technology-40811972

[78] Economic Analysis of Ransomware; Julio Hernandez-Castro1, Edward Cartwright2, Anna Stepanova2; 1School of Computing, Cornwallis South, University of Kent, UK, 2School of Economics, Keynes College, University of Kent, UK, Mart 2017 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2937641

Şekil 17: Bazı fidye yazılımı saldırılarında pazarlık oranları

3. FİDYE YAZILIMLARININ GELECEĞİ

Özellikle son beş yılda fidye yazılım saldırılarının artan ölçeği ve karmaşıklığı, çoğu siber güvenlik uzmanını daha küresel arenada büyük saldırıların ve veri ihlallerinin yaşanacağı konusunda endişelendirmektedir. Siber suçluların fidye yazılımlardan elde ettikleri gelirdeki artış da göz önüne alındığında, gelecekte çok daha fazla fidye yazılımı saldırısının gerçekleşmesini beklemek hayalcilik ya da felaket tellallığı olmayacaktır. Bu saldırganların bugüne değin sergiledikleri inovatif yaklaşımlar, tablonun ürkütücülüğünü artırmaktadır.

Fidye yazılımları sadece toplumsal sorunlara yol açmayıp, hepimizin geleceğini de ipotek altına almaktadır. Önümüzdeki dönemde, özellikle sosyal hayatımızın İnternet'e bağlı nesnelerle (buzdolapları, televizyonlar, araçlar v.b.) daha da dijitalleştiği zamanlarda bu yazılımların etkisi çok daha büyük olacaktır. Artık tüm kişisel ve kurumsal verilerimiz bilgisayarlarda yedeksiz bir şekilde depolanmaktadır. Dolayısıyla fidye yazılımı saldırganlarınca ele geçirilme ve şifrelenme riski taşımaktadır. Bu sebeple diyebiliriz ki, konu sosyal hayatımızı da etkilemektedir ve ilerde daha da etkileyecektir.

Belki de fidye yazılımlarının geleceğinde değişmeyecek tek unsur siber güvenlik zincirindeki en zayıf halkayı; yani insanları kullanmaları olacaktır. Örneğin, NotPetya saldırısının yayılmasına izin veren yazılım güvenlik açığı, WannaCry saldırısının bir ay önce dayandığı güvenlik açığıyla aynıydı. Microsoft, WannaCry'nin başlatılmasından birkaç ay önce bu güvenlik açığını düzeltmişti. Dünyanın en büyük ransomware saldırılarının ikisinin, kullanıcılar yazılımlarını zamanında güncellemiş olmaları durumunda önemli ölçüde hafifletilebilirdi.

3.1. Teknolojik Açıdan

Fidye yazılımıyla ilgili en büyük endişelerden biri, bilgisayarlar ve akıllı telefonlar dışındaki dijital cihazları hedeflemeye başlama potansiyelidir. Nesnelerin İnterneti (IoT) kullanımı arttıkça, günlük hayatımızda kullandığımız pek çok cihaz dijital hale getirilmekte ve İnternet'e bağlanmaktadır. Dünya çapında bilinen en büyük telekom sektörü sivil toplum kuruluşu olan ve özellikle mobil telekomünikasyon alanında her yıl sektörün en büyük kongresini düzenleyen GSMA'nın (GSM Association) 2018 yılında yayınladığı tahminlerine göre, 2025 yılında 25 milyardan fazla IoT cihazı kullanımda olacaktır.[79] Bu tahminle örtüşen bir başka tahminin kaynağı da Gartner olmuştur; küresel araştırma, denetim ve danışmanlık kuruluşu Gartner'ın 2017'de sunduğu tahminlerine göre 2020 yılına gelindiği toplamda 20 milyarı aşkın cihaz İnternet'e bağlanacaktır.[80] Ve tahmin etmesi hiç de güç olmayacaktır ki; bu cihazların tamamı saldırıya konu olabilecek risk potansiyeli taşımaktadır…

Bu, araç sahiplerinin araçlarına erişmelerini engellemek için fidye yazılımını kullanmayı seçebilecek ya da fidye ödemedikçe evindeki merkezi ısıtma sistemini kilitleyebilecek siber suçlular için devasa yeni bir pazar yaratmaktadır. Bu şekilde, fidye yazılımlarının günlük yaşamlarımızı doğrudan etkileme kabiliyeti artacaktır.

Yeni kötü amaçlı yazılımların sistemdeki varlığını ve konumunu tespit etmek daha zordur. Hackerlar, geleneksel anti-malware yazılımlarının güncellenebileceğinden daha hızlı davranmakta ve bu yönde yaklaşımlarını değiştirmektedirler. Kötü amaçlı yazılımların altı yeni biçimi, etkinleştirilmeden ve yeniden düzenlenmeden önce haftalar veya aylar boyunca hareketsiz kalabilir ve bu da bunları tanımlamayı daha da zorlaştırır.

---

79 GSMA Intelligence, IoT at Mobile World Congress, Shanghai Haziran 2018

80 Leading the IoT, Gartner, 2017, https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

Bu alandaki en son trend "dosyasız kötü amaçlı yazılım" saldırıları olmuştur. "Dosyasız kötü amaçlı yazılım", Fin7 isimli hacker grubunun restoranlar, finans kuruluşları ve devlet kurumlarına yönelik son saldırılarının bir parçası olarak tespit edilmiştir. Temel amaç finansal bilgileri çalmaktır. Dosyasız kötü amaçlı yazılım saldırılarının, geleneksel dosya tabanlı anti-malware çözümleri tarafından tespit edilmesi son derece güçtür. Saldırılar doğrudan sistem belleğine enjekte edilebilir.[81]

Blockchain'in temel bir teknoloji olacağını öngören uluslararası araştırma kuruluşu Forrester'a göre, bu teknoloji ikili itibar kontrolleri ile kötü amaçlı yazılım ve fidye koruması sağlayacaktır.[82] Burada anahtar Bitcoindir. Günümüzde birçok fidye yazılım operatörleri fidyeyi Bitcoin olarak talep etmektedir. Ve Bitcoin'in anonim yapısı sebebiyle, işlemler güvenlik ekiplerinin ve kolluk kuvvetlerinin yetki alanı dışındadır. Ancak madalyonun öbür yüzünde, Bitcoin işlemleri / dönüşümleri Blockchain yapısı altında merkezi olmayan bir kayıtta işlenir. Korsanlar, fidye olarak alınan Bitcoinler'i kullanabilmek için bunları üçüncü tarafın adresine, muhtemelen hizmet sağlayıcıların sabit döviz bozdurma işlemini gerçekleştirdikleri bir Bitcoin siciline veya cüzdanına aktarmalıdır. Bu tedarikçiler, fidye yazılımı kampanyalarıyla ilişkili Bitcoin adreslerini belirleyebilir ve siber güvenlik uzmanlarını hızlı bir şekilde haberdar edebilir.[83]

Ayrıca şu gibi etmenler de Blockhain'i saldırganlar açısından kullanışlı kılmaktadır:

- Blockchain'de veri saklama problemi bulunmamaktadır.

Siber suçlarda, suçluyu bulmak için, servis proseslerini servis sağlayıcıdan başka bir servis sağlayıcıya kayıtların izini sürerek (kimi zaman farklı ülkelerde de

[81] For Security & riSk ProFeSSionalS august 22, 2017 | updated: | updated: august 29, 2017
Forrester Data: Endpoint Security Software Forecast, 2016 To 2021 (Global)
82 Forrrester_Predictions2018_Cybersecurity
83 Archana Chimankar, Is Blockchain the key to stopping ransomware attacks?, 13 Temmuz 2017, https://securityintelligence.com/is-blockchain-the-key-to-stopping-ransomware-attacks/

olabilir) gerçek suçluyu bulacak dataya aylar ve hatta yıllar içerisinde zor ulaşılmaktadır. Ancak, Blockchain'de böyle bir sorun söz konusu değildir.

- Blockchain "üçüncü taraf doktrini" meselelerini ileri süremez.

Üçüncü taraf doktrini, kolluk kuvvetlerinin bir arama emri yerine bir mahkeme celbi ile banka, İSS veya cep telefonu kayıtları almasını mümkün kılan esastır. Blockchain, tasarımı gereği halka açık ve erişilebilir olduğundan böyle bir sıkıntı bulunmamaktadır.

- Blockchain sınırsızdır.

Siber suçlarda suç başka bir ülke sınırları içerisinde işlendiğinde veri ve kayıtlara ulaşmak sıkıntı yaratırken, blockchainde bu sıkıntı bulunmamaktadır.[84]

Fidye yazılımlarının geleceğini şekillendirecek en önemli konulardan bir diğeri de yapay zeka ve makine öğrenmesi konuları olabilir. Yapay zekayı fidye yazılımı saldırılarını önleme amacıyla kullanmak üzere çeşitli şirketler çözüm denemelerinde bulunmuşlardır. Bunlardan biri Yeni Zelandalı siber güvenlik kuruluşu Emsisoft olmuştur. Emsisoft'un baş teknoloji sorumlusu Fabian Wosar, Haziran 2017'de basına verdiği demeçlerde ekranda ilerleme çubuğu göstermeden şifrelemeye başlayan bir programın, şüpheli etkinlik yaptığı için yapay zeka tarafından engellenebileceğini öne sürmüştür.[85] Ancak bu mümkün olsa bile pratikte ancak bazı dosyalar zararlı yazılım tarafından kilitlendikten sonra devreye geçebilecek bir sistemdir. Wosar'ın farklı bir çözüm yaklaşımı, zararlı yazılımları çalışmaya başlamadan önce tanıyabilecek, onları gözlemlenebilir karakteristiklerini kullanarak tanımak olmuştur. Bu yaklaşıma göre, yapay zeka çözümü, bilgisayara giriş yapmak isteyen zararlı bir yazılımı, örneğin yüz tanımak

[84] Jason Weinstein, How can law enforcement leverage the blockchain in investigations, 12 Mayıs 2015, https://coincenter.org/entry/how-can-law-enforcement-leverage-the-blockchain-in-investigations

[85] Associated Press, The battle of the machines: Experts say the war on ransomware could see good AI taking on bad, 28 Haziran 2017, https://www.dailymail.co.uk/sciencetech/article-4648256/How-artificial-intelligence-taking-ransomware.html

için PDF simgesini kullanan bir program olduğunda bu şekilde tanıyacaktır. Bunun için zararlı yazılımların yapay zeka içinde profillenmesi gerekmektedir. Ancak burada da zararlı yazılımların tek ya da sayılı birkaç karakteristikten oluşmaması gerçeği devreye girmiştir. Yüzlerce binlerce özelliği bulunan programları zararlı / zararlı değil diye tanımlamak olası görünmemektedir.

Bu aşamada devreye "makine öğrenmesi" girmektedir. Makine öğrenmesi, yapay zeka içinde, bilgisayar modelleri ve istatistik modellerini oluşturmak için istatistik prensiplerinden yararlanan bir çalışma alanı olarak tanımlanmaktadır. Yapay zekanın bir türü olan makine öğrenmesi, iyi ve kötü yazılım örneklerini inceleyerek zararlı yazılımların hangi faktör kombinasyonlarında olduğunu belirleyebilmektedir.[86] Bu yönde pazara sunulan CrowdStrike, SentinelOne ve Cylance gibi çözümlerin fiyatları ise henüz erişilebilir karşılanmamaktadır.[87]

Singapur merkezli çok uluslu siber güvenlik şirketi Acronis'in siber güvenlik uzmanları konuyu şöyle açıklamaktadır:[88]

"Makine öğrenmesinin gizli silahı tahmin gücüdür. Bu güç, öğrenebileceği daha fazla ve daha ayrıntılı veri noktalarına erişimle süper güce dönüşür. Aynı partnerle tekrar tekrar satranç oynamak, aynı oyunu yüzlerce oyuncu ile tekrar tekrar oynamak gibi düşünün. Zamanla rakiplerinizin eğilimlerini öğrenir ve bir sonraki hareketini önceden tahmin edebilirsiniz. Diğer rakiplerden öğrenilen dersleri çizerek, kendi stratejinizi buna göre ayarlayabilmeniz için daha fazla seçeneğiniz vardır. Makine öğrenmesi için yığın iz analizi sürecin temelidir. Bu alanda yenilikçiler çözümler geliştirmeye devam etmekteyiz."

3.2. Etki Alanı Açısından

[86] Introduction to Machine Learning, Alex Smola ve S.V.N. Vishwanathan, Purdue Üniversitesi, 2018
[87] Yapay zeka fidye yazılımlarıyla nasıl mücadele ediyor?, 20 Ağustos 2017, http://www.hurriyet.com.tr/teknoloji/yapay-zeka-fidye-yazilimlariyla-nasil-mucadele-ediyor-40556040
[88] How machine learning can be used to prevent ransomware, Acronis, https://www.acronis.com/en-us/articles/machine-learning-prevent-ransomware/

Fidye yazılımlarının beklenen etkileri bilimkurgu filmlerini aratmayacak cinstendir.

ABD Ulusal İstihbarat Dairesi'nin 2017 yılında yaptığı araştırmada;

- Fidye yazılımı araçlarının çoğalması nedeniyle saldırıların sayısı artacağı,
- Nesnelerin İnterneti (IoT) cihazlarının hedeflenmesini de içerecek şekilde genişleyeceği,

- Sosyal mühendisliğin bir bilgisayar sistemine erişilmesinin en kolay yollarından biri olmaya devam edeceği,

- Bu bilgileri toplamak için teknolojiyi ve insan manipülasyon yöntemlerini içeren çeşitli tekniklerin kullanılmaya devam edileceği belirtilmiştir.[89]

Aynı çalışmada, gelecek iki yılda, politik ya da ideolojik amaca yönelik fidye yazılımı saldırılarının artacağı öngörülmekle birlikte, esas olarak finansal amaca yönelik saldırı olmaya devam edeceği öngörülmektedir.

Ayrıca, IDC'nin Dünya Sağlık Tahminleri Raporu'nda, 2018 yılına gelindiğinde, sağlık sektöründe görülen fidye yazılım saldırılarının sayısının iki katına çıktığını belirtmiştir[90]. Bu, hackerların, sağlık hizmeti sağlayıcılarına ve sektördeki diğer kişilere, hassas hastalara ve diğer değerli verilere erişimle daha fazla odaklanmasının bir sonucu olarak ortaya çıkmaktadır.

Yukarıda belirtilenlere ilave olarak; fidye yazılımlarının PoS /ATM gibi ödeme sistemlerini kapatmak için de kullanılabileceği öngörülmektedir.

89 The Future of Ransomware and Social Engineering, 24 Ağustos 2017, sf. 17-19 https://www.dni.gov/files/PE/Documents/6---2017-AEP_The-Future-of-Ransomware-and-Social-Engineering.pdf

90 Elizabeth Snell, IDC Predicts Healthcare Ransomware Attacks to Double by 2018, 2018, https://healthitsecurity.com/news/idc-predicts-healthcare-ransomware-attacks-to-double-by-2018

3.3. Korunma yöntemleri açısından

Anti-virüs yazılımları, güvenlik duvarları, güvenli e-posta ve web ağ geçitleri ve izinsiz giriş önleme sistemleri gibi geleneksel güvenlik çözümleri, bilinen tehditleri algılamak ve engellemek için statik analiz ve imzalara güvenmektedir. Ancak bu çözümlerin, bir siber saldırgan tarafından rahatlıkla bypass edilebildiği görülmektedir.

Bunları engellemek için;

- Fidye yazılımı aktivitesini gösterebilen davranışları tespit etmek için e-posta, IPS, ağ ve uç noktaları izleyen güvenlik kurulmalı / mevcut güvenlik yöntemleri bu doğrultuda sıkılaştırılmalıdır.

- Tüm bunlar uygun tercihen saha dışında düzenli olarak yedeklenmelidir.

- E-posta güvenliği için temel spam ve anti-virüs filtreleri eklenmelidir.

- Son nokta güvenliği için, tehditleri tespit etmede yardımcı olabilecek etkili bir uç nokta görünürlüğü sağlanmalı; böylelikle siber güvenlik uzmanlarının bir tehdidi algılaması ve harekete geçmesi için gerekli zemin oluşturulmalıdır.

- Çalışanlar fidye yazılımı saldırılarına ilişkin güncel taktikler ve korunma yöntemleri hakkında eğitilmelidir.[91]

- VPN kullanımı tercih edilmelidir. VPN kullanmak fidye yazılı saldırılarına karşı koruyamaz, ancak sistemin güvenlik seviyesini artırarak daha güvenli hale getirir. VPN kullanıldığında, IP adresi gizlenir ve İnternet'e anonim olarak erişilebilir. Bu, kötücül yazılım yaratıcılarının bilgisayarı hedeflemesini zorlaştırır

[91] Fireeye Report and Analysis: Defenses Against Ransomware: Effective Solutions To Protect Your Critical Data, 2017, https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/sb-ransomware.pdf

ve genel olarak daha savunmasız kullanıcılar aramaya yönlendirir. Bir VPN kullanarak çevrimiçi şekilde veri paylaşıldığında veya veriye erişildiğinde, bu veriler şifrelenir ve kötücül yazılım üreticilerine karşı büyük ölçüde erişilemez kılar. Ayrıca güvenilir VPN servisleri şüpheli URL'leri kara listeye alır. Kaydolunan VPN sağlayıcısının saygın bir servis olduğundan ve çevrimiçi güvenlik alanında gerekli uzmanlığa sahip olduğundan emin olunmalıdır.

4. ALINABİLECEK ÖNLEMLER

Şimdiye kadar fidye yazılımlarını çok yönlü olarak masaya yatırdık. Bu bölümde taradığımız kaynaklar ve edindiğimiz bilgiler doğrultusunda teknolojik, hukuki, sosyolojik ve ekonomik açıdan alınabilecek önlemlere değineceğiz. Şüphe yoktur ki fidye yazılımı saldırıları ile mücadele alanında teknoloji kadar hukuksal düzenlemeler, sosyolojik yaklaşımlar ve ekonomik önlemlerle birlikte netice elde edilmesi mümkün olabilecektir.

4.1. Teknolojik Açıdan

Fidye yazılımları sinsidir. En sık e-posta yoluyla yayılsalar da, mağdurlarının bilgisayarlarına girmek için türlü arka kapılardan dolaştıkları ya da güvenlik açıklarından yararlandıklarını artık bilmekteyiz. Bu durum karşısında alınabilecek teknolojik önlemleri şöyle sıralamamız mümkündür:

- **ÖNCESİ: Proaktif olmak.** Fidye yazılımlarından korunmanın en geçerli yolu, her şeyden önce saldırıları önlemek adına proaktif olmaktan geçmektedir.

  - **Eğitim şart.** Bireysel ya da profesyonel tüm bilgisayar kullanıcıları, kimlik avı saldırısının belirtilerini tanımalı; çalıştırılabilir dosyaları veya bilinmeyen bağlantıları tıklamama konusunda bilinçli olmalıdır. Şirketlerde verilen siber güvenlik bilinçlendirme eğitimleri, çalışanların fidye yazılımı saldırılarının şirketin bilgisayar sistemine ulaşmasını engellemedeki rollerini göstermek ve

onları bu yönde bilinçlendirmek adına son derece büyük öneme sahiptir. Bu eğitimlerde, güvenilir bir kaynaktan geldiğinden emin olmak için bağlantıları ve ekleri incelemenin önemi vurgulanmalıdır. Uzaktan çalışan çalışanlara halka açık kablosuz ağ (Wi-Fi) kullanmamaları gerektiği bildirilmelidir. Bir saldırı gerçekleşene kadar beklemek, çok geç cevap vermek anlamına geleceğinden; bu konuda herhangi bir endişeye düşen çalışanın başvurabileceği bir birim de kendilerine gösterilmelidir.

- **Siber güvenlik çözümleri kullanmak.** Fidye yazılımlara karşı korumak için anti-virüs ve anti-casus çözümleri yeterli olmamakta, anti-fidye çözümlerinin de kullanılması gerekmektedir. Özetle güvenlik sistemi; virüsten koruma, kötü amaçlı yazılım önleyici ve kötü amaçlı yazılım korumasından oluşmalıdır. Virüs tanımlarının düzenli olarak güncellenmesi de çok önemlidir.

- **Sistemin günlük olarak yedeğini almak.** Bilgisayar sistemlerinin günlük olarak ayrı bir fiziki ortamda ve bulut ortamında yedeklenmesi, kaybedilecek ve üzerine pazarlığa girişilecek veri miktarını önemli derecede azaltacaktır. Yedeklemek, bir saldırı durumunda eski sistemin silinmesini ve yedek dosyalar ile onarılmasını da kolaylaştıracaktır. Özellikle bulut tabanlı yedekleme platformları ek bir koruma katmanı da sağlamaktadır. Birden fazla yedekleme yapmak da riskin en aza indirgenmesi adına önemli bir yaklaşım olacaktır.

- **Ağ erişimini sınırlandırmak.** Bir saldırganın erişebileceği verileri sınırlandırmak için, dinamik kontrol erişimiyle tüm ağ güvenliğinin tek bir saldırıda riske girmemesi sağlanabilir. Bunun için bilgisayar ağı, her biri farklı kimlik bilgileri gerektiren farklı bölgelere ayrılmalıdır.

- **Erken tehdit tespit sistemleri kullanmak.** Potansiyel saldırıların belirlenmesine yardımcı olacak fidye yazılımı koruma yazılımları da kullanılabilir. Erken birleşik tehdit yönetimi programları, izinsiz girişler yapıldığı anda tespit edebilmekte ve önleyebilmektedir. Bu çözümler, şüpheli bilgisayarı

ağdan çıkarmayı, bir güvenlik taraması başlatmayı ve BT departmanını bilgilendirmeyi de kapsayabilmektedir.

- **Filtreleme yöntemleri kullanmak.** Bilgisayarlara ve ağlara yetkisiz erişimi engelleyen geleneksel bir güvenlik duvarı tek başına yeterli gelmeyebilir. Dolayısıyla özellikle kötü amaçlı yazılımların bulaşabileceği sitelere odaklanan ve web içeriğini bu yönde filtreleyen bir program da kullanılmalıdır. Ayrıca, istenmeyen eklerin e-posta kutusunda görünmesini engellemek için e-posta güvenlik uygulamaları ve spam filtreleri kullanılmalıdır.

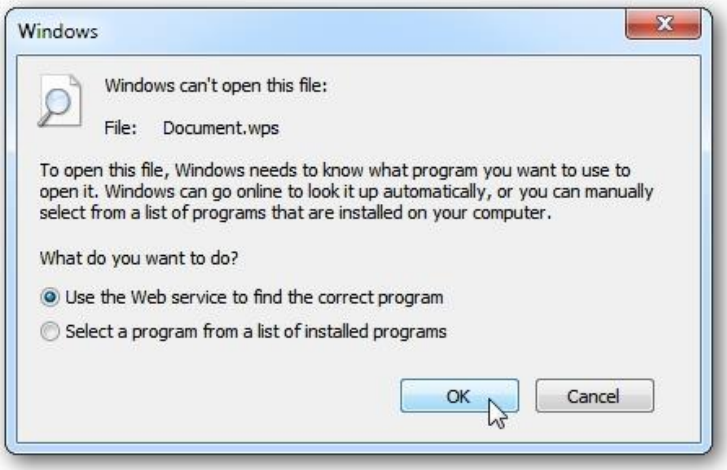
- **Güncelleme yapmak.** Kullanılan sistemlere gelen tüm yazılım güncellemeleri veya yamaları indirilip yüklenmelidir. Bu güncellemeler bilgisayarların ya da mobil cihazların çalışma verimini iyileştirmekle kalmaz, güvenlikteki hassas noktaları da onarırlar. Böylelikle yazılım açıklarından yararlanmak isteyebilecek saldırganları uzak tutmaya büyük ölçüde yardımcı olurlar. Güncellemeleri yapmamak ise, veri ve sistemleri hedef haline getirmektedir. Örneğin, tarihin en büyük fidye yazılımı saldırılarından biri olan WannaCry, Windows'un eski sürümlerindeki bir güvenlik açığından yararlanmıştır. WannaCry İnternet üzerinden yayılmış, bilgisayarlara bir yama yapmadan ve kullanıcı etkileşimi olmadan bulaşmıştır. WannaCry tarafından saldırıya uğrayan bireysel ve kurumsal kullanıcıların bilgisayar işletim sistemleri güncel tutulmuş olsaydı, WannaCry bu denli büyük bir yayılıma erişemeyecekti; ancak son derece pahalı bir dersle sonuçlanmıştır.

- **Geri yükleme ve kurtarma noktaları oluşturmak.** Windows işletim sistemlerinde “Sistem Geri Yükleme” bölümü bulunmaktadır. Bu menüden “sistem koruması” açılabilmekte ve düzenli geri yükleme noktaları oluşturulabilmektedir. Bilgisayarın saldırganlar tarafından kilitlenmesi durumunda, sistemin kurtarılabilmesi için bir geri yükleme noktası kullanılabilmektedir.

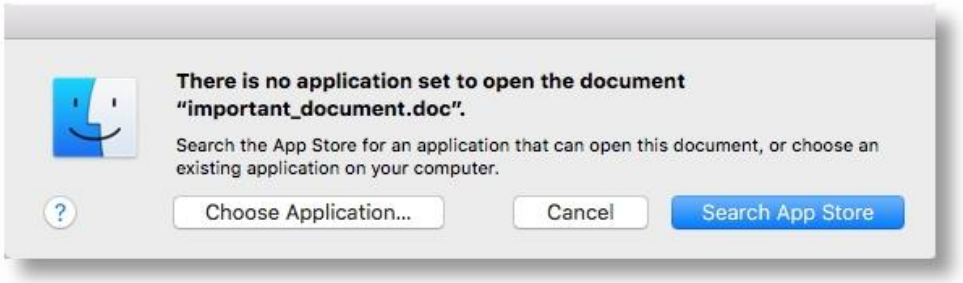
o **Güçlü şifreler kullanmak.** “abc123”, “123456” gibi zayıf şifreler yerine ardışık sayı, doğum tarihi, şirket ismi gibi içermeyen güçlü şifreler kullanılmalıdır.

o **Bilinen kötü amaçlı yazılım adreslerini e-posta sunucusuna tanımlamak.** E-posta sunucuları bilgisayarda çalıştırılması mümkün olmayan eklere sahip e-postaları, bilinen spam göndericileri ve kötü amaçlı yazılım adreslerini reddedecek şekilde ayarlanmalıdır.

o **Bilinmeyen dosya türlerini açmamak.** Bazı dosyalar hakkında bilgisayar sistemleri “Bilinmeyen dosya türü” uyarısı vermektedir. Bu dosyalar açılmamalı; illa açılması gerekiyorsa öncelikle bir siber güvenlik uzmanına danışılmalıdır.



Şekil 18: Bilinmeyen dosya türü açılmaya çalışıldığında Windows’ta açılan pencere



Şekil 19: Bilinmeyen dosya türü açılmaya çalışıldığında Machintosh’ta açılan pencere

o **Java ve Flash eklentileri engellemek.** Fidye yazılımı saldırganlarının bilgisayarları etkilemek için kullandığı pek çok web eklentisi türü arasında en yaygın iki tanesi “Java” ve “Flash”tır. Aynı zamanda pek çok sitede standart olarak bulunan bu programlar, kolayca saldırı yapılabilen alanlardır. Uzmanlar, virüslerden etkilenmemelerini sağlamak için bunları düzenli olarak güncellemeyi önermektedir. Bununla birlikte bazı şirketler daha ileriye giderek şirketlerinde bu programların kullanımını tamamen yasaklamışlardır.

o **Kablosuz ağ şifrelerini düzenli olarak değiştirmek.**

o **Acil durum eylem planı yapmak.** Elbette saldırıya uğramayı beklemeden önce yapılması gereken en önemli eylemlerden biri de “acil durum eylem planı” hazırlamaktır. Böyle bir durumda kimin kimi ne zaman ve nasıl haberdar edeceği, sırasıyla izlenecek adımlar ve resmi mercilerle kimin hangi şekilde irtibata geçeceği gibi konular bu plan dahilinde açıklığa kavuşturulmalıdır. Ayrıca şunlar da plana dahil edilmelidir:

- İşlemlerin devam etmesi için kiralanması ya da satın alınması gereken ekipmanlar.
- Mevcut donanımların günlerce kullanılamayacağı durumlarda işlerin nasıl yürütüleceğine ilişkin talimatlar.
- Yedeklerin nerede bulunduğu ve nasıl alınacağına ilişkin talimatlar.

- Çözüm sağlayıcıların iletişim bilgileri.

o **Sistemin bütününü güvenli hale getirmek.** Özellikle çok şubeli / lokasyonlu / bayili şirket yapılarında, herhangi bir noktanın güvenlik zafiyetinin tüm sisteme mal olacağı gerçeği gözden kaçırılmayarak sistemin bütününü güvenli hale getirecek yaklaşımlar benimsenmelidir.

- **SONRASI: Fidye yazılımı ile mücadele etmek.** Tüm bu önlemlere rağmen fidye yazılımı saldırısına uğranılması durumunda da atılacak adımlar özenle seçilmelidir.

o **Fidye yazılımını karantinaya almak ve silmek.** Fidye yazılımı saldırısını önlemek adına başarısız olunduğunda, kullanıcıyı şifreli veya kilitli bir bilgisayar veya dosyalar ile bir fidye notu bekleyecektir. Kötü amaçlı yazılım ve anti-virüs denetleyicisinin sık sık güncellenmesi durumunda, bu güvenlik yazılımları da fidye yazılımını tespit edebilir ve uyarı verebilir. Bu durumda fidye yazılımını karantinaya almak ve silmek mümkün olabilir.

o **Cihazı izole etmek.** Fidye yazılımı saldırıya uğrayan bilgisayar ya da mobil cihazı varsa bağlı bulunduğu ağdan derhal izole etmek, saldırganların ağa daha fazla erişimini engellemek ve hasarı en aza indirgemek adına önem taşımaktadır.

o **Sistemi yeniden oluşturmak.** Saldırı sisteme değil, dosyalara yönelik yapılmışsa, bu aşamada, sistem yeniden oluşturulmalı ve yedekler indirilmelidir. Böylelikle birçok kaynağı kurtarmak mümkün olabilecektir.
Önemli veriler, bir bulut sunucusunda yedeklenmişse, geri yükleme için güvenli bir İnternet ağı kullanılması gerekmektedir.

4.2. Hukuksal Açıdan

Fidye yazılımı saldırılarının "İnternet devriminin şafağında" ortaya çıktığını göz önüne aldığımızda, aradan geçen yıllara rağmen konunun hukuki boyutu hala tartışmaya açık durumda ve fidye yazılımı mağdurlarının haklarını hukuki platformda nasıl arayabileceklerine ilişkin net ve basit bir cevap bulunmamaktadır. [92] Dolayısıyla hukuksal açıdan alınabilecek önlemlerin başında öncelikle mağdurların haklarını aramalarını kolaylaştıracak bir takım adımlar atılması gerekliliği gelmektedir.

Fidye yazılımı saldırılarına ilişkin literatür eksikliği de göze çarpmaktadır. Spesifik olarak fidye yazılımlarını hukuksal açıdan ele alan akademik çalışmaların da zenginleşmesine ihtiyaç olduğu tespit edilmiştir.

Bilgi ve iletişim teknolojilerinin kötüye kullanımını önlemenin yolu kesinlikle toplumda bu teknolojilerin kullanımını sınırlamak, engellemek olmamalıdır. Teknolojik anlamda alınan önlemlerin ya da tepki toplayan yasakların tek başına çözüm getirmediği / getirmeyeceği apaçık ortadadır. Hukuka aykırı fiilleri suç olarak tanımlayan ve bu suçlara en ağır cezaları karşılık getiren bir takım hukuki düzenlemeler, bu alandaki kötü niyetli girişimlere karşı etkili bir caydırıcı güç olacaktır.

Konuyu farklı yönleriyle maddeler halinde şöyle ele alabiliriz:

- **Sözleşmeler uyarında bilgilendirme zorunluluğu.** Dünyanın teknoloji borsası olarak kabul gören, merkezi New York'ta bulunan Nasdaq Borsası, şirketlerin öncelikle fidye yazılımı saldırısı yoluyla verilerini tehlikeye atabilecek tüm durumlardan kaçınmalarını önermektedir. Böyle bir durumla karşılaşan şirketlerin öncelikle yetkili kamu otoritelerine başvurmalarının altını önemle çizmekte; ardından sırasıyla hissedarlarını, etkilenebilecek üçüncü kişi ve kuruluşları, sigorta şirketlerini, müşteri ve tüketicilerini ve çalışanlarını haberdar etmesini tavsiye etmektedir. Aslında tavsiye niteliğindeki bu beklenti, şirketlerin

[92] Robert E. Litan, *Law and Policy in the Age of the Internet,* sf. 1045; basım yılı 2001

açıklama yükümlülükleri veya hissedar sözleşmeleri uyarınca da zorunlu bir durum halini alabilmektedir.[93]

Burada kritik konu, bir fidye yazılımı saldırısına uğrayan şirketin bunu ifşa etmesi durumunda itibarının zarar görebileceği ve aynı zamanda gelecekteki yeni saldırıları üzerine çekebileceğidir. Çünkü bu şirketin zayıf bir siber güvenlik sistemine sahip olduğu düşünülebilecektir. Bu nedenle, yasal olarak zorunlu olmayan mağdurlar, bu durumu ifşa etmeye isteksiz kalabilmektedir. Bu durum da mağdur açısından sanıldığı gibi avantajlı olmayabilir; zira iletişimi yapılmayan, üstü örtülmeye çalışılan konuların da bir gün açığa çıkma ve açığa çıktığında iletişimi yapılan konulara oranla çok daha büyük olumsuz etki / infial yaratma olasılığı bulunmaktadır. Dolayısıyla fidye yazılımı saldırısına uğrayan bir kurumun tüm paydaşlarını konudan haberdar etmesinin zorunlu hale getirilmesi de hukuksal açıdan alınabilecek etkili bir önlem olacaktır.

Öte yandan siber suçlularla mücadelede arkasına kamusal ve yasal gücü almayan bir şirket, bunun tam tersini yapan bir şirkete oranla muhakkak ki daha zayıf bir mücadele sergileyecektir. Bu doğrultuda şirketlerin bu durumu önce yetkili resmi otoritelere, ardından da tüm paydaşlarına açıklamasının hukuki açıdan bir gereklilik haline getirilmesi önem taşımaktadır. Örneğin 25 Mayıs 2018 tarihinde yürürlüğe giren EU General Data Protection Regulation (GDPR; AB Genel Veri Koruma Tüzüğü) uyarınca, herhangi bir şirketin bir saldırıya uğraması durumunda, kişisel verilere erişildiğinde ve veri ihlalinden haberdar olunduktan sonra, gecikmeden (en geç 72 saat içinde) resmi denetim otoritesine ve etkilenen taraflara bildirimde bulunması gerekmektedir. Ayrıca fidye yazılım saldırısının, önemli bir istisna yaratabilecek tüketicilerin "hak ve özgürlükleri için bir riskle sonuçlanabileceği" anlamına geldiği de belirtilmelidir.[94] AB'nin bu yönergesi henüz bir zorunluluk olarak kabul görmese de, AB Veri Koruma Yönetmeliği'ni ihlal etmenin 10 milyon Avro'ya kadar para cezasına veya küresel grup cirosunun

[93] Nasdaq Borsası, Ransomware Payment: Legality, Logistics, and Proof of Life Part Three: Notification, Remediation, and Insurance, John Reed Stark, 2017
[94] EU GDPR, Sıkça sorulan sorular, https://eugdpr.org/the-regulation/gdpr-faqs/

yüzde 2'sine kadar para cezasına tabi olduğu da göz ardı edilmemelidir. Konunun hukuki bir zorunluluk tanımlanması anlamlı bir önlem niteliği teşkil edecektir.

- **Güvenlik güçlerinin rolü.** Dünya çapında yaşanan en büyük fidye yazılımı saldırılarına baktığımızda genel olarak güvenlik güçleri tarafından açıkça sonuçlandırılmış bir örneğe rastlayamadık. Bunun birkaç nedeni olabilir. Birincisi güvenlik güçleri kendilerine ulaşan çok sayıdaki başvuruyu sonuçlandıracak yeteri miktarda insan kaynağına sahip değildir. İkincisi fidye yazılımı saldırganlarının çoğu uluslararası arenada gerçekleşmekte; dolayısıyla suçlular farklı ülkelerde bulunmaktadır. Bu durumda kovuşturma süreci zorlaşmaktadır. Üçüncüsü ise siber saldırılarla mücadele konusunda özel eğitimli, casus yazılımların ve kripto para ödemelerinin izini sürebilecek yetkin personel açığı bulunmaktadır. Tüm bunlar ancak kamu otoritelerinin konuya daha fazla eğilmesi ile çözüme kavuşturulabilecektir. Atılması gereken adımlar sırasıyla; siber suçlarla mücadele polis ekiplerinin sayıca artırılması, uluslararası suç durumlarında ortaklaşa çalışmayı teşvik eden protokoller oluşturularak imzalanması, kripto para ödemelerinin izini sürebilecek özel eğitimli personel açığının kapatılması şeklinde özetlenebilir.

- **Türk Ceza Kanunu'nda siber suçların yeri.** Türkiye'de bilişim alanında gerçekleştirilen yasal düzenlemeler, genel olarak AB direktifleri ile uyumlu olacak şekilde hazırlanmıştır.[95] 5237 sayılı Türk Ceza Kanunu'nun (TCK) 10. bölümünde bilişim alanında işlenen suçlar ve cezaları tanımlanmıştır. Bu maddelerden konumuzla ilgili olan bazı satırlar şöyledir:

  - **Bilişim sistemine girme**: Madde 243 - (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir. (2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi

[95] Türkiye'de Bilişim Hukuku, Bilgi Teknolojileri ve İletişim Kurumu (BTK), 29 Kasım 2016, http://internet.btk.gov.tr/turkiye-de-bilisim-hukuku-detay-70.html

hâlinde, 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.

- **Sistemi engelleme, bozma, verileri yok etme veya değiştirme**: Madde 244 - (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 fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır. (4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.[96]

Bu doğrultuda saldırıya uğrayan bir kişi ya da kurumun ilgili kanıtları hukukun gerektirdiği kurallar çerçevesinde toplaması ve saklaması, ilgili soruşturma sürecinin daha sağlıklı ve hızlı ilerlemesine katkı sağlayacaktır. Ayrıca cezai yaptırımların artırılması, adli para cezası yerine hapis cezasına ağırlık verilmesi suçluları caydırıcı önemli bir etken olacaktır.

Sonuç olarak hukuk yavaş değişen, başta teknoloji olmak üzere toplumda meydana gelen değişim ve yenilikleri geriden takip eden bir bilim dalıdır. Bu durum olağandır; zira hukuk kuralları toplumsal gereksinim ve beklentilere göre şekillenir. Ancak teknoloji ve buna bağlı riskler o kadar hızlı gelişmektedir ki, bilişim hukukunun yavaş hareket etme, geriden takip etme gibi bir lüksü olmamalıdır. Bilişim sistemlerinin yapısı ne kadar dinamik ise, hukuk sistemlerinin yapısı da bir o kadar hantal kalmamalıdır; sürekli değişim ve gelişim içinde olunmalıdır. Öte yandan günümüz bilgi toplumunda gereksinim duyulan

[96] Türk Ceza Kanunu, http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf

hukuksal kuralları tek bir çatı altında toplamak mümkün değildir; fidye yazılımlarının özel bir yeri ve niş tanımları olmasına ihtiyaç vardır. Hızla ilerleyen teknoloji sürecinde ortaya çıkan tehdit unsurları ne yazık ki tam anlamıyla netlikle tanımlanmamıştır. Bununla birlikte bu suçların Türk Ceza Kanunu'ndaki en belirgin karşılığı 243 ve 244 numaralı maddelerde yer almaktadır. Neticede burada sözü edilen "bir bilişim sistemine hukuki olmayan yollarla girme" suçun ilk aşamasına işaret etmektedir. Fidye yazılımı saldırganları sisteme girmekle kalmamakta, mağdurların girişini engellemekte, sistemin işlerliği ya da verileri bozmakta, silmekte ya da değiştirebilmektedir ki bu durumu karşılayan madde de 244 olarak görülmektedir. Mevcut duruma göre en geçerli TCK maddeleri bu şekilde olmakla birlikte net bir şekilde fidye yazılımları için ayrı bir hüküm getirilmemesi bir eksiklik olarak karşımıza çıkmaktadır. Bu hukuki boşluk bir çerçeve kanun ile ayrıca tanımlanmalıdır; böylelikle bu tip saldırıların ayrıntıları ve oldukça geniş etki alanları daha net ifade edileceği gibi yükümlülükler ve yaptırımlar da özelleştirilmiş olacaktır.

4.3. Sosyolojik Açıdan

Siber saldırganların en önemli motivasyonlarının para kazanmak olduğunu pek çok örnekte gördük. Peki konunun sosyolojik derinliğine indiğimizde hala tek motivasyon unsuru para mıdır? Bu bölümde bunu tartışacağız.

Öncelikle şunu belirtmek gerekmektedir ki, fidye yazılımlarını sosyolojik açıdan ele alan özel bir akademik çalışmaya rastlanmamıştır. Bu alanda önemli bir eksiklik olduğu tespit edilmiştir.

Fidye yazılımı saldırılarını artıran motivasyonlar arasında birkaç etkeni sıralayabiliriz. Örneğin "yeraltı iş"lere meraklılık, yeni fidye yazılımı araçlarını deneme isteği, sanal bir kimlikle ünlü olma arzusu, siyasi ve ideolojik tepkileri ortaya koyma hedefi, aktivistlik, büyük şirketleri zor durumda bırakabilecek güçte olma isteği / tatmini… Bu profildeki kişileri haberlerde ve çevremizde de sıklıkla

gözlemleyebilmekteyiz. Dolayısıyla saldırganlar açısından – belki en önemli değil ama - kesin olarak tek motivasyon unsurunun para olduğunu söyleyemeyiz.

Fidye yazılımı saldırılarının artışını önlemek için şüphesiz sosyolojik etkenlerle başa çıkmak da büyük önem taşımaktadır.

Konuyla ilgili olarak ABD Ulusal İstihbarat Ofisi'nin 24 Ağustos 2017'de yayınladığı "The Future of Ransomware and Social Engineering" (Fidye Yazılımlarının ve Sosyal Mühendisliğin Geleceği) başlıklı rapordan bazı çarpıcı satır başlıkları şunları göstermektedir:[97]

- Önümüzdeki iki yıl boyunca, fidye yazılımı temelde finansal olarak motive olmuş bir faaliyet olmaya devam edecek, ancak politik ya da ideolojik olarak motive edilmiş fidye saldırıları da artacaktır. Siber aktörler taciz aracı olarak fidye yazılımı kullanmaya devam ettikçe hedef tahtasına oturtulan mağdurların sayısı da o kadar artacaktır.

- Fidye yazılımları ile ilgili kamu kamuoyu bilincinin ve savunma teknolojilerinin gelişmesi, geleneksel fidye yazılımı saldırılarının başarısını azaltacağından, saldırganların fidye yazılımı tekniklerini başka yöntemlerle birleştirmeye başlamaları beklenmektedir.
- Sosyal mühendislik, potansiyel belirleme, değerlendirme, uzlaşma ve yönetme konusunda önemli bir araç olmaya devam edecektir.

- Fidye yazılımı saldırganları açısından yükselen bir başka motivasyon kaynağı da aktivizmdir. Aktivistler, şirketlere ve hükümetlere tepki olarak fidye yazılımı kullanabilirler.

[97] The Future of Ransomware and Social Engineering, 24 Ağustos 2017, sf. 22 - 25, https://www.dni.gov/files/PE/Documents/6---2017-AEP_The-Future-of-Ransomware-and-Social-Engineering.pdf

- "Canı sıkılmış ama meraklı gençler" olarak adlandırılan bluğ çağındaki çocuklar bunu sırf eğlence olsun diye yapabilirler. Ancak bu gruptaki saldırganlar, gelişmiş savunmaları olan bir sisteme girmeye çok fazla zaman harcamazlar.

Bu konudaki başyapıtlardan biri olarak kabul edilen "Hacking the Human" kitabının yazarı Ian Mann, şöyle demektedir: "Bilgi güvenliği insanla ilgilidir. Fakat daha ziyade teknik önlemlere odaklanılarak korunmaya çalışılmaktadır." Mann, sosyal mühendisliği şöyle tanımlar: "Sosyal mühendislik, bilgisayar sisteminiz üzerinde kontrol sahibi olmak için sizi manipüle etme, etkileme ya da aldatma sanatıdır." Mann'a göre: "Çoğu kurum neredeyse tamamen teknik güvenliğe odaklanır. Saldırganlar bunu bilir ve genellikle gizli bilgilere erişmek için insanların duygularına hitap etmekten geçen en kestirme yolu kullanırlar. Donanım ve yazılım 'çözümlerini' satmaya odaklanarak genişleyen bir endüstri ile bu güvenlik sürecinin anlaşılması zordur. Bilgi güvenliğinde insani unsurlar yöneticiler tarafından ihmal edilmekte; saldırganlar tarafından ise sömürülmektedir." Yazar, bu doğrultuda çözümü temel olarak farkındalık yaratma ve eğitimde görmektedir. Ona göre ayrıca teknolojik açıdan alınan güvenlik önlemleri, eğer insani açıdan güvenlik risklerine karşı gelen önlemlerle tamamlanmazsa eksik ve yetersiz kalacaktır. Sosyal mühendislik tehdidi ile bağlantılı risk seviyesini her kurum kendi bağlamında değerlendirmelidir.[98]

Sonuç olarak 2013 yılında yayımlanan Uluslararası Güvenlik ve Terörizm Dergisi'nin 4. sayısında Polis Akademisi'nden Yrd. Doç. Dr. Hakan Hekim ve Doç. Dr. Oğuzhan Başıbüyük'ün kaleme aldığı "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları" başlıklı makalede de belirtildiği gibi:

"İnsan unsuru, güvenlikle alakalı pek çok alanda olduğu gibi siber güvenlikte de en önemli etken olarak karşımıza çıkmaktadır. Bir sistemde ne kadar güvenlik tedbiri alınmış olursa olsun, dikkatsiz bir kullanıcının sebep olacağı açıklara mağlup olma riski her zaman vardır. Sosyal mühendislik gibi insan temelli

[98] Ian Mann, Hacking the Human, 2008

saldırıların riskini azaltmak için çalışanların siber güvenliğe ilişkin konularda eğitilmeleri ve bilinçlendirilmeleri gerekmektedir."[99]

Fidye yazılımı saldırganlarının kullandığı sosyal mühendislik yöntemleri karşısında aynı kanaldan alınacak önlemler, en az teknoloji ve hukuk kadar insani yönüyle de konunun ele alınması ve bu doğrultuda uzmanların bir araya gelerek ortaya çıkaracağı tedbir paketleri faydalı olacaktır.

4.4. Ekonomik Açıdan

- **Fidye yazılımı saldırılarını da kapsayan siber güvenlik sigortaları.** Diğer tüm kurumsal riskler gibi, fidye yazılım saldırılarının da finansal, operasyonel ve hatta itibar risklerinin kapsamlı bir siber sigorta poliçesiyle ele alınabileceği apaçık ortadadır. Financial Times'ta yer alan bir habere göre, dünya çapında 60'tan fazla sigorta şirketi, çoğu fidye yazılımı saldırılarına yönelik özel hükümler içeren siber sigorta paketleri sunmaktadır ve 2016 yılı itibariyle özellikle fidye yazılımı saldırılarını kapsayan sigorta paketlerine yönelik talep genel siber sigorta taleplerinin yüzde 25'ine erişmiştir.[100] Siber güvenlik sigortalarının sağlam bir hukuki zemine oturtulması gündemdedir. Böylelikle fidye yazılımı saldırılarını kapsayan siber sigortaların şimdi olduğu gibi çok seçenekli paketler yerine, bir kuruluşun iş kesintisinin yanı sıra gizlilik ihlallerine bağlı üçüncü taraf yükümlülüklerini de kapsayan paketler yaygınlaştırılmalıdır. Ayrıca sigorta şirketleri tarafından şirketin zararının karşılanması için, mağdur konumundaki şirketin olayı fark ettiği anda resmi otoriteleri bildirmesi koşulu aranmalıdır.

- **Bitcoin ödemelerine ilişkin yasal düzenlemeler.** Henüz ülkemizde resmi karşılığı bulunmayan Bitcoin ödemelerine ilişkin yasal düzenlemeler bir an önce hayata geçirilmelidir. Yapılan ödemelerin ne amaçla yapıldığının bildirilmesi sağlanmalıdır. Örneğin ABD'de Hazine Sekreteri, ABD Başsavcısı ve / veya

[99] Yrd. Doç. Dr. Hakan Hekim ve Doç. Dr. Oğuzhan Başıbüyük, Polis Akademisi, Uluslararası Güvenlik ve Terörizm Dergisi, sayı 4., yıl 2013; http://www.acarindex.com/dosyalar/makale/acarindex-1423936102.pdf
[100] Financial Times, https://www.ft.com/content/1c17ee26-448a-11e7-8519-9f94ee97d996

ABD Dışişleri Bakanı Bitcoin mali zincirindeki herhangi bir katılımcının varlıklarını bloke edebilir. Böyle dramatik bir yasal müdahale, ödemeleri almak için Bitcoin'e bağımlı olan fidye yazılımı saldırganlarını caydırabilir.[101]

- **Lisanslı yazılım kullanmak.** İlk başta lisanslı yazılım yerine kaçak yazılım kullanmak ekonomik açıdan daha avantajlı gibi görünmekteyse de, siber saldırganlar tarafından çok daha kolay bir hedef haline dönüşebileceği riski nedeniyle aslında çok daha pahalı sonuçlara yol açabileceği unutulmamalıdır.

- **Fidyeyi ödemek ya da ödememek.** Symantec İnternet Güvenliği Tehdit Raporu'na (Internet Security Threat Report) göre, fidyeyi ödeyenlerin sadece yüzde 47'si dosyalarını geri alabilmektedir.[102] Uzmanların önerisi de fidyenin ödenmemesi gerektiği yönündedir. Bunun dayanağı, suçluların özgüvenini yükselteceği ve zarar veren çabalarına devam etmelerini teşvik edeceği, cesaretlendireceği gerçeğine dayanmaktadır. Öte yandan ayrıca fidyenin ödenmesi durumunda saldırganların şifreyi vereceklerinin de bir garantisi bulunmamaktadır. Şifreyi verseler bile verilerin kopyalanmayacağı ve usulsüz biçimde kullanılmayacağının da bir garantisi bulunmamaktadır. Pek çok siber güvenlik uzmanı, verilerini kaybeden kullanıcıların fidye ödeyerek ayrıca paralarını da kaybedeceklerini savunmaktadır.

FBI Siber Bölüm Başkan Yardımcısı James Trainor'ın bu konudaki açıklamaları şöyledir: "Talep edilen fidyeyi ödemek, bir kullanıcıya verilerini geri alacağını garanti etmez; zira mağdurların fidyeyi ödedikten sonra hiçbir zaman şifre çözme anahtarı almadığı durumlar gördük. Bir fidye ödemek, mevcut siber suçluları sadece daha fazla örgütlenmeye motive etmekle kalmaz, aynı zamanda diğer suçluların bu tür yasadışı faaliyetlere katılmaları için bir teşvik sunar. Ve son olarak, bir fidye ödeyerek, bir kuruluş istemeden yanlışlıkla suçlularla ilgili diğer

[101] Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, Beyaz Saray dokümanları, Federal Register / Vol. 80, No. 63, 1 Nisan 2015, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf

[102] Symantec, Internet Security Threat Report, Haziran 2017, sf. 61, https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf

yasadışı faaliyetlere fon sağlıyor olabilir. ” FBI’a göre, fidye yazılımı mağduru olduğunu düşünen herkes yerel FBI bölge ofisine başvurmalıdır.[103]

- **Siber güvenlik çözümleri kullanımı ve geliştirilmesinin teşvik edilmesi.** Ekonomik açıdan üstesinden gelinmesi oldukça zor vahim sonuçlara yol açabilen fidye yazılımı saldırıları ile ekonomik yönden mücadele etmenin en etkili yollarından biri de bu alanda kullanılan siber güvenlik çözümlerinin daha yaygın kullanımının geliştirilmesidir. Bir diğeri ise şüphesiz bu çözümlerin üretilmesini teşvik edecek kredi ve hibe fonları yaratılarak her geçen gün değişen teknolojilere paralel yenilikçi çözüm geliştiricilerinin artırılmasıdır.

- **Vergi avantajı.** Pek çok kurumun siber güvenlik yatırımlarını yeterli vizyonu olsa bile yeterli bütçesi olmadığı için hayata geçiremediği şüphe götürmez bir gerçek. Dolayısıyla siber güvenlik çözümlerinin maliyetini azaltmak için alınabilecek etkili önlemlerden biri de vergiden muaf tutulmaları olabilir.

[103]FBI, Incidents of Ransomware on the Rise, https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise

SONUÇ

Bu çalışmada günümüzde siber saldırılar arasında en yaygın yöntemlerin başında gelen fidye yazılımı saldırılarının tarihi, işleyiş sistematiği, handikaplar ve alınabilecek önlemler ortaya konmuştur.

Pek çok kaynaktan elde ettiğimiz rakamsal veriler ve ortaya koyduğumuz örnekler, tüm siber saldırılar arasında öne çıkan fidye yazılımı saldırılarına karşı da hem bireylere, hem şirketlere, hem de devletlere önlem alınması ve çözüm geliştirilmesi adına sorumluluklar yüklemektedir. Bugün ister bireysel, ister kurumsal, ister kamusal kullanıma mahsus olsun, bilgisayar, akıllı telefon ve yanı sıra İnternet'e bağlanabilen tüm cihazların anti-fidye koruması altına alınması, bunun bireysel kullanımdaki cep telefonları hatta akıllı TV'lere kadar yaygınlaştırılması paranoyakça bir davranış olmayacaktır. Nasıl ki evlerimizin kapısını kilitlemekte, dükkanlarımıza kepenk taktırmakta, sitelerimize güvenlik kameraları yerleştirmekte, fabrikalarımızda gece bekçileri görevlendirmekte isek, aynı şekilde dijital dünyada da gereken tüm önlemlerin alınması; bunlar içinde yükseliş trendinde bulunduğu aşikar olan fidye yazılımı saldırıları için özel tedbirlerin hayata geçirilmesi gerekmektedir.

Tüm bunlar ancak toplumun her kesiminde yaygın bir farkındalık sağlanması suretiyle mümkün olabilecektir. Farkındalığın temeli eğitim sistemine dayanmaktadır. 2000 yılı ve sonrasında doğan ve "teknolojinin içine doğan nesil" olarak tabir edilen gençlerden başlanmak üzere, gerek konunun ders müfredatlarına girmesi, gerek kamu otoriteleri eliyle bilinçlendirme kampanyaları başlatılması, gerekse özel şirketlerin çalışan ve iş ortaklarına yönelik eğitim programları düzenlemeleri büyük önem taşımaktadır. Zira fidye yazılımı saldırganları özellikle bireylerin yeterince bilinçli olmadan sergiledikleri yanlış dijital davranışlardan faydalanan yöntemler izlemekte; sosyal mühendislik teknikleri kullanmaktadırlar. Bu saldırıları tertipleyen toplum mühendisleri, yerlerinde saymamakta, yeni taktikler ve teknolojilerle sürekli güncel

kalmaktadırlar. Öyleyse tüm İnternet kullanıcıları da en az onlar kadar yeni taktik ve teknolojiler konusunda bilinçli olmak zorundadır. Unutmamak gerekir ki İnternet fırsatlarla olduğu kadar tuzaklarla da dolu bir platformdur ve gerekli bilinçlendirme tam anlamıyla yapılmadığından kullanıcıları bekleyen senaryo elbette bu tuzaklara yakalanmak olacaktır.

Eğitim, bilgisayar kullanıcılarını ne yalnızca, ne de tam anlamıyla garantili bir şekilde saldırılardan korunmaya yetmeyecektir. Ne yazık ki kullanıcıları fidye yazılımı saldırılarına karşı korumanın yüzde 100 etkinliğe sahip sihirli bir yolu yoktur. Eğitimin önemli bir boyutu da tüm önlemlere karşın fidye yazılımı saldırısına uğramış kişi ve kuruluşların sonraki süreçlerde doğru adımlar izlemelerine ve böylelikle zararın etkilerini azaltabilmelerine de katkı sağlayacaktır şüphesiz… Siber güvensizliğin getirebileceği maliyetin, bu alana yapılacak yatırımın maliyetinden çok daha fazla olabileceği aşikardır.

Teknolojik açıdan fidye yazılımları da dahil olmak üzere siber saldırılarla mücadelede bugünün ve geleceğin en geçerli yolunun "makine öğrenmesi" olacağı öngörülmektedir. Makine öğrenmesini öne çıkaran etmen tahmin gücüdür. Bu güç, savunmanın yanında saldırı amacıyla da gündeme gelebilir ve saldırılar bambaşka boyutlara evrilebilir. Dolayısıyla teknolojik açıdan makine öğrenmesi konusuna önem verilmesi bir zorunluluk olarak karşımıza çıkmaktadır.

Fidye yazılımları günümüzde hem bağımsız "hacker grup"ları tarafından, hem de saldırı izlerini sürmek ve dikkat çeken hedefli saldırılarda dikkati dağıtmak için devlet destekli "yasal hacker grup"ları tarafından kullanılmaktadır. Bu çok geniş bir evrendir ve en ufak bir aralık pencere bulan siber suçlular her tipten kullanıcıya büyük zarara uğratabilecek potansiyele sahiptir. Literatürde belirtilen çalışmalar da buna işaret etmektedir. Ancak durumun vahameti ne yazık ki özellikle bireysel ölçekte yeterince bilinmemektedir. Bu bağlamda fidye yazılımları alanında oluşan tüm tehditlere karşı devlet, şirket ve bireylerin birlikte hareket ederek, hatta devletler bazında iş birlikleri kurularak tüm dünyada bilinç

seviyesinin artırılması gerekmektedir. Nitekim bu çalışmanın sonuçlandırıldığı son günlerde bile aynı anda pek çok ülkeyi etkisi altına alan fidye yazılımı saldırısı haberleri yayınlanmaktaydı. Örneğin, basına da yansıyan bir habere göre: "Sophos güvenlik araştırmacıları, daha önce nispeten alt sıralarda yer alan bir tehdit olan MegaCortex fidye yazılımının 1 Mayıs 2019'dan itibaren başta Amerika Birleşik Devletleri, Kanada, Arjantin, İtalya, Hollanda, Fransa, İrlanda, Hong Kong, Endonezya ve Avustralya olmak üzere dünyanın pek çok yerinde aynı anda görülmeye başladığını tespit etti." [104]

Nitekim bazı saldırıların devlet eliyle yürütüldüğü düşünülmektedir. Önümüzdeki yıllarda fiziksel saldırılar kadar etkin bir yıkıcı silah olarak fidye yazılımı saldırılarının kullanılabileceği, hatta fiziksel saldırıların yerini alabileceği öngörülmektedir. Dolayısıyla ülkeler açısından bakıldığında, fidye yazılımı saldırıları ulusal güvenlik unsurları ve stratejileri kapsamında ele alınması gereken ciddi bir konudur. Bu alanda kullanılan güvenlik çözümlerinde dışa bağımlılık, teknoloji üretmeyen ülkeleri ciddi bir tehlikeye sürüklemektedir. Siber güvenlik başta olmak üzere yazılım ve teknoloji üretimi devlet eliyle teşvik edilmelidir. Bu teşvik vergi muafiyeti, kamu ihalelerinde yerli çözümlerin tercih edilmesi gibi ekonomik alanda ortaya konabileceği gibi, yaratılacak motivasyonla da pekiştirilmelidir. Sosyal hayatın içine siber güvenlikle ilgili düşünce, yenilikçi bakış açısı ve çözüm geliştirme kültürü adapte edilmeli; bu yöndeki çalışmalar ödüllendirilmelidir. Örneğin üniversitelerin yalnızca bilgisayar mühendisliği değil hemen her bölümünden gönüllüler bir araya getirilerek kümelenmeleri ve böylelikle düşünce ve çözüm geliştirmeleri teşvik edilmelidir. Böylesine bir atmosfer yaratılması konunun saldırıdan ziyade çözüm tarafında ağırlık kazanmasına vesile olacaktır. Gençlerin teknolojiye olan meraklarını, bu konuda taşıdıkları heyecanı doğru yönlendirmek, pek çoğunun bir eğlence aracı olarak görebildikleri fidyecilik oyununa değil, etik yollara yönelmelerini sağlamak, geleceğimiz açısından kritik bir konudur

[104]http://www.hurriyet.com.tr/teknoloji/megacortex-adli-yeni-bir-fidye-yazilimi-tehlike-saciyor-41204760,6.5.2019

Teknolojideki sürekli gelişme ile birlikte fidye yazılımı alanında da kullanılan yöntemler o kadar hızlı değişmekte ve birbiri ardına yepyeni tanımlar doğuran saldırılar o kadar hızlı meydana gelmektedir ki, alınan önlemler ve yapılan yasal düzenlemeler yetersiz kalabilmektedir. Bu nedenle ağır işleyen hantal bir bürokratik yapı ile olaylara müdahale edilmesi mümkün görünmemektedir. Fidye yazılımı saldırılarını önleme ve korunma açısından hız, en az eğitim ve teknoloji kadar büyük önem taşımaktadır.

Bu çalışma ile fidye yazılımlarına ilişkin teknolojik, hukuksal, ekonomik ve sosyolojik açıdan geniş bir bakış açısı ortaya konmuş, bu doğrultuda alınabilecek önlemler açıklanmıştır. Bu kapsamda çeşitli ülkelerden uzmanların hazırladığı fidye yazılımı veri ve raporları incelenmiş, bunun sonucunda tehditler, riskler, güvenlik zafiyetleri tanımlanmış ve analiz edilmiş, alınması gereken önlemler ve farkındalık konusunda önerilere yer verilmiştir. Bu çalışmanın fidye yazılımı saldırılarının zararlı etkilerini azaltma ya da engelleme adına faydalı bir içerik sunduğu düşünülmektedir.

KAYNAKÇA

Allan, Gallo	:	Liska, Allan; Gallo, Timothy,Ransomware: Defending Against Digital Extortion (Kindle Locations 154-156)
Allan, Timothy	:	Liska, Allan; Gallo, Timothy. Ransomware: Defending Against Digital Extortion (Kindle Locations 154-156). O'Reilly Media. Kindle Edition.
Becker's Health IT&CIO Report	:	Becker's Health IT&CIO Report, First known ransomware attack in 1989, Mayıs 2016
Beyaz Saray Dokümanları	:	Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, Beyaz Saray dokümanları, Federal Register / Vol. 80, No. 63, 1.4.2015, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf
BTK	:	Türkiye'de Bilişim Hukuku, Bilgi Teknolojileri ve İletişim Kurumu (BTK), 29 Kasım 2016, http://internet.btk.gov.tr/turkiye-de-bilisim-hukuku-detay-70.html
Carbon Black	:	The Ransomware Economy, Carbon Black, 2017
Castro, Cartwright, Stepanova	:	Economic Analysis of Ransomware; Julio Hernandez-Castro, Edward Cartwright, Anna Stepanova ; Economic Analysis of Ransomware ,Mart 2017 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2937641
Chung	:	Marcus Chung CEO at BoldCloud,A New Wave of Ransomware Is Coming This Fall
Cisco Systems	:	Cisco Systems, 2019 Threat Report, Ocak 2019
Deloitte	:	Tehdit İstihbaratı ve Analitiği, Deloitte, Sayfa: 6, 12.8.2016
Doevan	:	Jake Doevan ,Fidye Yazılımı Nasıl Temizlenir?, 2016
Fawkes	:	Guy Fawkes ,VPNmentor.com, 2017
FBI	:	FBI, The Internet Crime Report, Nisan 2019

FBI Releases : FBI Releases the IC3 2017 Internet Crime Report and Calls for Increased Public Awareness, Mayıs 2018

For Security& Risk Proffessionals : For Security & Risk Professinoals, 22 Ağustos 2017

Forrester Data : Jennifer Adams, Chris Sherman, Forrester Data: Endpoint Security Software Forecast, 2016 To 2021

Gartner : Mark Hung,Leading the IoT, Gartner, 2017, https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

GBConcepts Online : GBConcepts Online, 17.9.2009, http://www.gbconcepts.net/blog/tag/troj-ransom-a/#

Gonzalez : Daniel Gonzalez, Thaier Hayajneh, IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), Detection and prevention of crypto-ransomware, 2017

GroupIB : Group IB, Hi-Tech Crime Trends 2018, https://www.group-ib.com/resources/threat-research/2018-report.html

GSMA Intelligence : GSMA Intelligence, IoT at Mobile World Congress, Shanghai Haziran 2018

Hekim, Başıbüyük : Yrd. Doç. Dr. Hakan Hekim ve Doç. Dr. Oğuzhan Başıbüyük, Polis Akademisi, Uluslararası Güvenlik ve Terörizm Dergisi, sayı 4., yıl 2013; http://www.acarindex.com/dosyalar/makale/acarindex-1423936102.pdf

Huang, Aialapoulios, Li, Invernizzi, McRoberts, Bursztein, Levin, Levchenko, Snoeren, McCoy : Danny Yuxing Huang, Maxwell Matthaios Aliapoulios, Vector Guo Li, Luca Invernizzi, Kylie McRoberts, Elie Bursztein, Jonathan Levin,Kirill Levchenko, Alex C. Snoeren, Damon McCoy, Tracking Ransomware End-to-end;

IBM : IBM Study: Businesses More likely to Pay Ransomware than Consumers, Aralık 2016

Indian Journal of Science : Ransomware Digital Extortion: A Rising New Age Threat; Indian Journal of Science and Technology,

and Technology : Vol 9(14), DOI: 10.17485/ijst/2016/v9i14/82936, Nisan 2016
İnanç : Volkan İnanç ,TOR nedir?, Media Click
Journal of Health Care Compliance : Journal of Health Care Compliance, Ekim 2018
Knights : Miya Knights, Rene Millman,IT Pro, 22.8.2007
Los Angeles Times : Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating, Los Angeles Times, 18 Şubat 2016
Mann : Ian Mann ,Hacking the Human, basım yılı 2008
Morgan : Steve Morgan, Cybersecurity Business Report, Kasım 2017
Nazarov, Emelyanova : Denis Nazarov, Olga Emelyanova, SecureList.com, , Blackmailer: The story of Gpcode, 26.6.2006
NTT Security : Dimension Data, NTT Security 2018 Global Threat Intelligence Report, Ocak 2019
Simone : Alina Simone, The Strange History of Ransomware, 26.3.2015,
Smith : George Smith, 12.8.2002, The Original Anti-Piracy Hack
Smola, Vishwanathan : Alex Smola ve S.V.N. Vishwanathan, Introduction to Machine Learning, , 2018
SonicWall : SonicWall Siber Tehdit Raporu 2018, http://www.m2s.com.tr/bulten/2018_Sonicwall_siber_tehdit_raporu-TR.pdf
Stark : Nasdaq Borsası, Ransomware Payment: Legality, Logistics, and Proof of Life Part Three: Notification, Remediation, and Insurance, John Reed Stark, 2017
Symantec : Symantec Internet Security Threat Report, Volume 24, Şubat 2019
Thakkar, : Dhanya Thakkar, Preventing Digital Extortion, Birmingham, Sayfa: 39, Mayıs 2017
The Daily Telegraph : The Daily Telegraph, İngiltere
The Epoch Times : The Epoch Times, New York
The Intependent : The Intependent, İngiltere
The Nation : The Nation, Tayland
TrendMicro : TrendMicro TrendLabs Security Roundups and Predictions Report, Mart

2019

Türk Ceza Kanunu : Türk Ceza Kanunu, http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf

Waddell : Kaveh Waddell,TheAtlantic.com, 10.5.2016

Wilkinson : Bella Wilkinson What is ransomware and how does it affect your business?,

İnternet Kaynakları

https://www.telegraph.co.uk

http://internet.btk.gov.tr

http://money.cnn.com

http://www.bbc.com

http://www.hurriyet.com.tr

http://www.m2s.com.tr

http://www.milliyet.com.tr

http://www2.imm.dtu.dk

https://arxiv.org

https://bitcoin.org

https://coincenter.org

https://eugdpr.org

https://go.kaspersky.com

https://pages.phishlabs.com

https://ramses2020.eu

https://securityintelligence.com

https://www.acronis.com

https://www.cepol.europa.eu

https://www.cnnturk.com

https://www.csoonline.com

https://www.dailymail.co.uk

https://www.dni.gov

https://www.fbi.gov

https://www.fireeye.com

https://www.ft.com

https://www.haberturk.com

https://www.independent.co.uk

https://www.statista.com

https://www.symantec.com

https://www.us-cert.gov
https://www.wired.com