GÜNCEL SİBER GÜVENLİK TEHDİTLERİ: FİDYE YAZILIMLAR

Soner ÇELİK*

Barış ÇELİKTAŞ**

Özet

Son yıllarda bilgi teknolojilerinin gelişmesi ve yaygınlaşmasıyla birlikte bilişim sistemlerini tehdit eden zararlı yazılımların çeşitlenerek etkilerinin arttığı düşünülmektedir. Günümüzde fidye yazılımları siber ortamlarda saldırganlar tarafından etkili bir siber saldırı aracı olarak kullanılmaktadır. Fidye yazılımları 2000'li yılların ortalarından günümüze kadar etkisini arttırarak devam eden güçlü bir saldırı yöntemi olarak saldırganlar tarafından kullanılmaktadır. Buradan hareketle son birkaç yılda artış gösteren fidye yazılım saldırıları, geniş güvenlik bütçelerine sahip çok uluslu büyük firmalardan devlet kuruluşlarına, küçük işletmelerden bireylere kadar birçok kesimi etkilemektedir. Fidye yazılımlarının önümüzdeki dönemde tehdit düzeyini ve etkisini arttırarak daha kolay erişim ve daha fazla finansal kazanç sağlama motivasyonlarıyla sayılarının artması beklenmektedir. Fidye yazılımlarındaki şifreleme düzeyi, ticari güvenlik ürünlerinde görülen şifreleme seviyesine hızlı bir şekilde yaklaşmaktadır.

Bu çalışmada, kişileri, kurum ve kuruluşları üst düzeyde tehdit eden fidye yazılımları ele alınmıştır. Fidye saldırılarında kullanılan yöntemler araştırılmış, farklı fidye saldırı tipleri incelenmiş ve bilişim sistemlerine verdiği zararları azaltmayı sağlayacak etkili bir mücadele için çözüm önerileri sunularak fidye yazılımlarına karşı farkındalık oluşturulması amaçlanmıştır.

Anahtar Kelimeler: Siber Tehditler, Siber Güvenlik, Fidye Yazılım, Güvenlik Farkındalığı

Contemporary Cyber threats: Ransomware

Abstract

* Doktora Öğrencisi, Süleyman Demirel Üniversitesi, İİBF-Uluslararası İlişkiler Bölümü, E-posta: sonercelik85@gmail.com

** Doktora Öğrencisi, İstanbul Teknik Üniversitesi, E-posta: celiktas16@itu.edu.tr

In recent years, the development of information technology and information systems with widespread threats, which experienced an increase and diversify the effects of malware is known from cyber-attacks. Nowadays, ransomware is used by cyber attackers as an effective tool for attacking cyberspace. Ransomware has been used by attackers as a powerful attack method that continues to increase from the year 2000 to the day. From here, ransomware attacks that have increased in the last few years have affected many sectors, from large multinational companies with large security budgets, to government agencies, small businesses to individuals. It is expected that the ransomware will increase the threat level and influence in the coming period and increase the numbers with easier access and motivation to provide more financial gain. The level of encryption in ransomware is rapidly approaching the level of encryption seen in commercial security products.

In this study, ransomware which threatens people, institutions and organizations at high level is discussed. It was aimed to raise awareness of ransomware by presenting solution proposals for an effective struggle to investigate the methods used to attack, investigate the different types with the changes they have undergone, and reduce the damage to the information systems.
Keywords: Cyber Threats, Cybersecurity, Ransomware, Security Awareness

GİRİŞ

Günümüz dünyası için fidye kavramı yeni bir olgu değildir. İnsanlık tarihi boyunca fidye, eski Roma'dan korsanlığa ve günümüz rehine alma olaylarına kadar saldırganların kullandığı yaygın bir taktik olmuştur. Bugün ise saldırganlar bu taktiği siber dünyada uygulamaya başlamıştır. Saldırganlar, sistemleri güvence altına almak amacıyla keşfedilen şifreleme teknolojilerini kullanarak kendileri için kazanç sağlamak için son derece etkili ve kolay bir şekilde fidye yazılım saldırılarını kullanabilmektedir.

Bu tehlikeli yazılımlar reklamlar, bilgilendirme mailleri ve sosyal mühendislik saldırıları gibi çeşitli yöntemlerle kullanıcıların bilgisayarlarına kolayca bulaşabilmektedir. Fidye yazılımlar, bulaştığı sistemlerdeki dosyaları çözülmesi zor olan şifreleme algoritmaları ile şifreleyerek özel anahtarlar üretmekte ve bu anahtarlar özel bir sunucuda ayrı olarak tutulmaktadır. (Luo, X. , Liao, Q., 2007, s. 197).

Ayrıca şifreleme işleminin yanı sıra, fidye yazılımın yerleştiği bilgisayarın kayıt defterine girilen kod ile bilgisayar her açıldığında zararlı yazılımın çalışması sağlanmaktadır. Netice olarak kullanıcı, saldırganın istemiş olduğu ücreti ödeme yapmadığı durumda sahip olduğu sistemdeki elektronik verileri kaybetmesi veya erişememesi ile tehdit edilmektedir. Mağdur, talep edilen ücreti saldırganın belirlediği sınırlı bir süre içinde ödeme yapması için uyarı ekranı ile Bitcoin, MoneyPack, Ucash ve Kashu gibi günümüz sanal para ödeme sistemlerine yönlendirilmektedir. Saldırganlar ayrıca ek bir tedbir olarak veriyi kurtarma girişimlerini engellemek için mağdurun kendisinin denediği her hatalı şifre anahtarı girişinde verilen bu süreyi azaltılmaktadır. Ödeme yapılıp teyit alındığında saldırganlar dosyaların şifresini açacak anahtarı iletmekte; aksi durumda elektronik veriler erişilemez olmakta veya kaybedilmektedir. (Uitsec Teknoloji, 2014, s. 3).

Fidye yazılımlar 2010 yılı itibarı ile siber dünyada saldırganlar için ciddi bir gelir kaynağı haline gelmiş ve zararlı fidye yazılım türevlerinin gün geçtikçe artmasına neden olmuştur. Birçok anti-virüs firması tarafından yayınlanan raporlarda, fidye yazılımlarının geçmiş yıllara göre 2017 sonunda 3 kattan fazla bir artış göstermektedir. Son dönemlerde gerçekleşen saldırılardaki saldırı vektörleri ve motivasyonları dikkate alındığında, fidye yazılım saldırılarında kullanılan teknolojiler ve araçlar çok gelişmiş, saldırı şiddeti ve hacmi artmış, saldırı hedeflerinde stratejik öneme sahip kamu kurum ve kuruluşları, çeşitli altyapılar, hastaneler, üniversiteler ve büyük ölçekli firmalar bulunmaktadır. (J.Crowe, 2017, s. 2).

2017 yılında Barkly firması tarafından yayınlanan istatistiklere göre, şirketler ortalama 40 saniye de bir fidye yazılım saldırısına uğramakta ve her 10 zararlı

yazılımdan 6 adedi fidye zararlısı olarak karşımıza çıkmaktadır. Ayrıca hedeflenen şirketlerin %71'ine fidye zararlısı bulaştırılmıştır. İstenen fidye tutarı yaklaşık olarak 1,077 dolara yükselmiştir. Saldırganlar tarafından talep edilen ödemeyi yapan 5 şirketten 1'sine dosyalarına erişim hakkı verilmemiştir. Bu şirketlerin %72'si sahip olduğu verilere ortalama 2 gün ve üzeri süreyle erişim sağlayamamıştır. Netice olarak küresel anlamda fidye yazılımların tahmini zararı **5 milyar dolar** olacağı tahmin edilmektedir. (Barkly, 2018, s. 4).

Kişilere ve kurumlara farkında olmadan büyük zararlar veren ve yakın tarihlerde gerçekleşen fidye yazılım saldırıları incelendiğinde, netice olarak bu saldırılara karşı yeterli önlemlerin alınmadığı ortaya çıkmaktadır. Bu makalede fidye yazılımlara karşı kesin bir korunma sağlanamasa da bu tür yazılımlara karşı daha etkili bir mücadele için yapılması gerekenler açıklanmaya çalışılmıştır. Yapılan incelemede, fidye yazılımların başlangıcından itibaren günümüze dek geçirdiği evrim ve gelecekte nasıl bir hal alacağı değerlendirilerek alınabilecek muhtemel tedbirler önerilmiştir.

FİDYE YAZILIM (RANSOMWARE)

Fidye yazılım, siber suçlular tarafından mobil telefonlar, bilgisayarlar ve diğer bağlantılı cihazlar üzerindeki elektronik verileri fidye için elinde tutup, bu dosyalara yeniden erişim için para talep ettikleri her türlü zararlı yazılımlardır. Basitçe ifade etmek gerekirse, fidye yazılım, bilgisayar sistemlerine veya dosyalara erişimi kısıtlayan ve veri sahibine geri yüklenen erişim karşılığında fidye ödemekle yükümlü kılan zararlı yazılımlardır. Yakın geçmişte yaygın olarak kullanılan fidye yazılım örnekleri arasında CryptoLocker ve WannaCry yer almaktadır. (https://renew.stratus.com.tr/cryptolocker/index.html, 2018).

Bu saldırılardan WannaCry incelendiğinde günümüzde gerek devletlerin gerekse de bireyler ve özel şirketlerin siber uzay kaynaklı tehditler ile doğrudan karşı karşıya kalabildikleri açıkça görülmektedir. Eşi görülmemiş

büyüklükte bir fidye yazılımı saldırısı olan "WannaCry", tüm dünyadaki organizasyonları ve bireysel kullanıcıları etkileyebilmeyi başarmıştır (Darıcılı, Siber Uzay ve Siber Güvenlik Nedir?, 2017, s. 233).

Fidye yazılımlar (ransomware), isminden de anlaşılacağı gibi, bulaştırıldıkları sistemlerde kullanıcıya bir ekran uyarısı görüntüleyerek, kullanıcı dosyalarını şifrelediklerini ve kısıtladıkları sistem erişiminin yeniden açılması için fidye ödenmesi gerektiğini belirtmektedirler. Bir zamana kadar fidye yazılımlara yapılan ödeme, geleneksel para birimlerinin doğal olarak izlenebilir nitelikte olması nedeniyle fidye yazılımların oluşturulmasında sorumlu kişi veya gruplar için önemli bir problem olmuştur. Fakat Bitcoin vb. ödeme sistemlerinin ortaya çıkışı ile ödeme talebinin bu sistemler üzerinden gerçekleşmesiyle siber savunma ekipleri ve kolluk kuvvetleri tarafından saldırganların tespiti zorlaşmıştır.

Ayrıca fidye yazılımlarının dünya genelinde yılın en önemli siber tehdidi olmaya devam ettiği; özellikle finans, sağlık ve telekomünikasyon kurumlarına yönelik fidye yazılım saldırılarının artış gösterdiğini tespit edilmiştir. Bu durumu daha da vahim hale getiren hususun, bazı fidye yazılımlarının kaynak kodunun temel yazılım bilgisi ile ele geçirilebilir olması ve Bitcoin kullanımının yardımı ile organize saldırıların kolaylaştırılması olarak gösterilmektedir. Bu konuda dikkat çekici bir nokta da fidye yazılımlarıyla ilgili Amerikan Federal Araştırma Bürosu (FBI) tarafından yapılan çarpıcı tespitlerdir. FBI'a göre Amerika Birleşik Devletleri (ABD) şirketleri geçen yıl içerisinde 25 milyon dolar fidye ödemiş durumdadır ve 2016 sonunda bu rakamın 200 milyon dolardan fazla olmasını bekleyen FBI, fidye yazılımlarıyla baş etmek için herkese 'İnternette güvenliğe dikkat' çağrısı yapmaktadır. (Hallam-Baker, 2016, s. 2).

Günümüzde fidye yazılımlar iki tür olarak karşımıza çıkmaktadır. Birincisi **(locker-ransomware)** kilitleyicilerdir. Bu tip fidye yazılımlar genellikle bilgisayarın veya aygıtın kilitlenmesi ve daha sonra kullanıcının ona erişimi sağlamak için bir ücret ödemesini istemektedir. Kilitlenen bilgisayarlar

kısmen, yalnızca kullanıcının fidye yazılımı ile etkileşime girmesine ve fidye ödemelerine izin vereceği şekilde açık bırakmaktadır. (Fasheem, 2017, s. 52).

İkinci tür ise, kurbanın kişisel dosyalarını şifreleyerek dosyalara erişilmesini engelleyen (**crypto-ransomware)** şifreleyicilerdir. Bu tür fidye yazılımlar, bilgisayarda depolanan değerli verileri bulmak ve şifrelemek için tasarlanmıştır. Mağdur şifre çözme anahtarı almadıkça şifrelenen verilere ulaşamamaktadır. Her iki durumda da mağdur fidye ücreti ödemeye zorlanmaktadır. Dolayısıyla saldırıya uğramış elektronik verilere fidye ödenene veya şifre çözme anahtarı sağlanıncaya kadar erişilememektedir. (Fasheem, 2017, s. 52).

Bunlara ilave olarak bu zamana kadar Windows tabanlı sistemlere yönelik çıkan fidye yazılımları çoğunlukla son kullanıcıları hedef almıştır. Fakat günümüzde fidye yazılımları artık son kullanıcıları hedef almaktan çok kurum ve kuruluşları da hedef almaya başlamıştır. Çünkü kurum ve kuruluşların kaybedecekleri veriler veya kilitlenecek sistemleri, son kullanıcılara göre daha kritik olduğu için saldırıya uğrayan kurum ve kuruluşun imajı ve itibarı zedelenecek; netice olarak toplum önünde güvenilirliği kaybolacaktır. Bu nedenle kurumların istenen fidyeyi ödemesi son kullanıcılara göre daha muhtemel olmaktadır. Bunun ilk örneği olarak, 2015 yılında ortaya çıkan ve web sunucularını hedef alan ilk linux ransomware yazılımı (Trojan.Ransom. Linux.Cryptor) görülebilir. Bu zararlı yazılım sonucunda 2000 adet web sayfası zarar görmüştür. (Kaspersky Security Bulletin, 2015, s. 4) Siber saldırganların başarılı bir fidye yazılımı saldırısı gerçekleştirmek için uyguladıkları genel yöntemler asgari olarak aşağıda belirtilen aşamaları içermektedir;

1. **Bir sistemin veya cihazın kontrolünün ele geçirilmesi:** Bu adım saldırganlar tarafından tek bir bilgisayar, cep telefonu veya yazılımı çalıştırabilen başka bir sistemin kontrol altına alınması şeklinde olabilmektedir. Çoğu fidye yazılımı saldırısı, kullanıcıları web tarayıcısında bir ek açma veya kötü amaçlı bir bağlantı izlemesi için kandırmak için sosyal mühendisliği kullanan saldırı vektörü ile başlamaktadır. Netice olarak

saldırganın ilk amacı bir sisteme kötü amaçlı yazılım yükleyip kullanıcıyı kontrol altına almaktır.

2. **Kullanıcının sistemdeki elektronik verilerine erişmesini önlenmesi:** Saldırganın bu adımdaki işlemi şifreleme, kilitleme ekranları veya basit korkutucu taktikler yoluyla olabilmektedir.

3. **Veri sahibine fidye için ödenmesi gereken miktarı ve ödeme metodunun bildirilmesi:** Bu aşama kısmen belli olabiliyor olsa da saldırganların ve kurbanların çoğu zaman farklı diller konuştukları, dünyanın farklı yerlerinde yaşadıkları ve çok farklı teknik yeteneklere sahip oldukları unutulmamalıdır. Ayrıca farklı ödeme yöntemleri geliştirilmiş olup kullanıcının bu ödeme metotları hakkında bilgi sahibi olmadığı düşünülerek ayrıntılı açıklama yapılmalıdır.

4. **Veri sahibi tarafından yapılan ödemenin kabul edilmesi ve teyidi:** Saldırganlar, kullanıcının veriyi kurtarma girişimlerini engellemek için belirli bir ödeme süresi vermekte ve bu süre mağdurun veriyi kurtarmak için denediği her hatalı şifre girişinde azaltılmaktadır. Ödeme yapılıp teyit alındığında program, dosyaların şifresini açmakta; aksi durumda elektronik veriler erişilemez olmakta ve kaybedilmektedir.

5. **Ödeme alındığında veri sahibine tam erişim verilmesi:** Saldır ödemeleri kabul ederek ve cihazlara erişimi iade etmeyerek kısa sürede başarabilir, ancak zamanla bu da planın etkililiğini yok edecektir. Değerli eşyalarının iade edileceğine inanmadıklarında fidye ödemezsiniz.

Saldırganlar yukarıda belirtilen aşamalardan herhangi birinde başarısız olması halinde fidye yazılımı saldırısı nihai amacına ulaşamamaktadır. Fidye yazılımlar kavramı onlarca yıldır var olmakla birlikte, güvenilir şifreleme ve şifre çözme gibi aşamalar içeren saldırı adımlarını tamamlayabilmek için geniş bir ölçekte gerekli olan teknoloji ve teknikler sadece birkaç yıl öncesine kadar mevcut olmamıştır. Ancak günümüze baktığımızda, 2017 yılında en önemli güvenlik tehditlerinden biri fidye yazılım saldırı türüdür. Yukarıda saldırı aşamaları anlatılan bu tehdit türünün geçmişten günümüze geçirdiği evrimsel değişimi incelemenin alınacak önlemler ve öneriler açısından faydalı olacağı değerlendirilmektedir. (Trendlabs, 2018, s. 2).

FİDYE YAZILIM SALDIRILARI GEÇMİŞTE NASILDI?

1989: AIDS Truva Atı

Bugün yeni yeni tanımaya başladığımız bu bilgi güvenliği tehdidinin ortaya çıkışı, yani **ilk yaygın olarak bilinen fidye yazılım saldırısı** olayı yaklaşık 30 yıl önce gerçekleşmişti. 1989'da Harvard akademisyeni Joseph L Popp, Dünya Sağlık Örgütü'nün AIDS konulu konferansına katılıyordu. Konferansa hazırlanırken, delegelere göndermek için "AIDS Hakkında Bilgilendirme" başlıklı 20.000 disk hazırlamıştı.

Fidye yazılım saldırısı kapsamında Dr. Popp tarafından kullanılan taktikler, o gün koşullarında oldukça karmaşık gözükmekteydi ama en önemlisi, siber suçluların bugünün kripto fidyeciliğine dönüşmesi için öğrenecekleri ve tanımlayacakları çeşitli tasarım kusurları içermekteydi. Popp'un ilk sosyal mühendislik saldırısı zekiceydi, popüler ilgi çekici bir kültürel konuyu saldırı aracı olarak kullanmıştı. Bununla birlikte, AIDS, arka planda, AUTOEXEC.BAT başlatma komutunu kötü niyetli talimatlarla değiştiriyordu. Kurbanın ana bilgisayarının önyüklemesi ile fidye bildirimi kullanıcının ekranına sunularak tüm dosya dizinleri ve dosya adları, özel bir şifreleme algoritmasıyla şifrelenmişti. Ekranda, Panama'daki bir posta ofisine 189 dolar gönderdikten sonra sisteminin normal haline geri döneceğini bildiren bir mesaj gösterilmişti.

Dr. Popp'un yaratıcılığı zamanının ötesindeydi ve başka birisinin fidye yazılım fikrini benimsemesine ve internet çağında kullanmasına kadar 16 yıl geçti. Dr. Popp gerçekleştirdiği bu olay sebebiyle tutuklandı ancak zihinsel sağlığının kötü olması nedeniyle yargılaması yapılamamıştır. Ayrıca o tarihlerde bu tür olaylarla ilgili yeterli yasal düzenlemeler yapılmamıştı. Ancak Dr. Popp gerçekleştirmiş olduğu fidye yazılımdan kazandığı geliri AIDS araştırmalara destek olarak vermeye söz vermişti. (https://www.techrepublic.com/blog/it-security/ransomware-extortion-via-the-internet/, 2018).

2005-2008: GPCoder

Yeni fidye yazılımı örnekleri ortaya çıktığında, Dr. Joseph L Popp çoktan unutulmuştu ve bilgi dünyası internete dönüştürülmüştü. Tüm avantajlarıyla **internet ortamı**, her türden kötücül yazılımın siber saldırganlar tarafından daha kolay dağıtılmasını sağlamış ve devam eden yıllarda saldırganların Dr. Popp tarafından kullanılanlardan çok daha güçlü şifreleme yöntemleri geliştirmelerine izin vermiştir.

Çevrimiçi dağıtılan fidye yazılım ürününün ilk örneklerinden biri de GPCoder Truva Atıydı. İlk kez 2005 yılında tespit edilen GPCoder, Windows sistemlerine bulaştı ve çeşitli uzantılara sahip dosyaları hedef aldı. Bulduktan sonra, dosyaları şifrelenmiş biçimde kopyalıyordu ve orijinallerini sistemden siliyordu. Yeni şifreli dosyalar okunamıyordu ve güçlü RSA-1024 şifreleme yönteminin kullanılması, dosyaların kilidini açmak için yapılan girişimlerin başarılı olamayacağı konusunda garanti veriyordu. Kullanıcıların ana ekranında, fidyenin nasıl ödeneceği ve etkilenen dosyaların kilidinin nasıl açılacağına dair ayrıntıları içeren bir .txt dosyasına kullanıcıları yönlendiren bir ileti görüntüleniyordu. 2008 yılının ortalarıyla beraber, Gpcode, TROJ.RANSOM.A, Archiveus, Krotten, Cryzip ve MayArchive gibi Truva atları, daha karmaşık RSA şifreleme şemalarını daha da artan anahtar uzunlukları ile beraber kullanmaya başlamıştır. (http://www.securityfocus.com/news/11523, 2018).

2009-2011: Nakit ödeme-Vundo

Değişimin ilk belirtileri 2009 yılında ortaya çıkmaya başladı. Bu tarihte bilinen bir 'korku'(scareware) zararlısı olan Vundo taktik değiştirdi ve fidye yazılımı olarak işlev görmeye başladı. Daha önce, Vundo bilgisayar sistemlerine bulaşıyor ve daha sonra kendi güvenlik alarmını çalıştırarak kullanıcıları sahte bir şekilde düzeltmeye yöneltiyordu. Bununla birlikte, 2009 yılında analistler, Vundo'nun kurbanların bilgisayarlarındaki dosyaları şifrelemeye başladığını ve bunları çözmek için gerçek bir anahtar sattığını fark etti. Bu, **saldırganların fidye yazılımlarından para kazanabileceklerini hissettikleri ilk olaydı**. Anonim çevrimiçi ödeme platformlarının yaygınlaşması sayesinde, kitlesel boyutta fidye alımı da

kolaylaşıyordu. Ek olarak, fidye yazılımının kendisi de giderek daha karmaşık bir hal almaktaydı. (Symantec Labs, 2009, s. 4).

2011 yılına gelindiğinde, yılın ilk çeyreğinde, 60,000 yeni fidye yazılım saldırısı tespit edildi. 2012 yılının ilk çeyreğine kadar, bu sayı 200.000'e yükseldi. Symantec'in araştırmacıları 2012 yılının sonunda, fidye yazılım karaborsasının **5 milyon dolar** değerinde olduğunu ve bunun gelecekte artacağını tahmin ediyordu. (https://www.cnet.com/news/ransomware-a-growing-menace-says-symantec/, 2018).

2011: Truva Atı WinLock

2011'de yeni bir fidye yazılım formatı ortaya çıktı. **WinLock Truva Atı, 'Kilitleyici' fidye yazılım türünde bilinen ilk yaygın zararlı** olarak düşünülmektedir. Kurbanın cihazındaki dosyaları şifrelemek yerine kilitleyici fidye yazılım türü, cihaza girişi imkânsız hale getirerek kullanıcının erişimini kısıtlamaktaydı. (Security Response, 2017, s. 4).

WinLock Truva Atı, eski taktiklerinde olduğu gibi orijinal ürünleri taklit eden bir fidye yazılım trendi başlattı. Windows sistemlerini etkilemek için Windows Ürün Etkinleştirme sistemini kopyaladı ve bir etkinleştirme anahtarı satın alana kadar kullanıcıları kilitledi. Saldırıya biraz masumiyet eklemek için, sahte etkinleştirme ekranında görüntülenen mesaj, aslında kurbanlara Windows hesaplarının dolandırıcılık yüzünden yeniden etkinleştirilmesi gerektiğini söyledi. Ayrıca kullanıcıların makinelerinin kilitlerini açabilmeleri sağlayacak bir kodu vermek için kullanıcılardan bir SMS (yaklaşık 10 dolar civarında tutan) göndermelerini istiyordu. Bu dolandırıcılık faaliyeti, Rusya ve çevre ülkelerdeki pek çok kullanıcıyı etkilemiştir. Raporlara göre grup bu saldırılardan toplamda **16 milyon dolardan** fazla para kazanmıştır. (https://www.pcworld.com/article/204577/article.html, 2018).

2012: Reveton ve 'Polis' Fidye Yazılımı

Yazılım ürünlerini taklit ederek sahte lisans ücretleri ile kurbanları kandırmak konusundaki değişim, sözde "polis" fidye yazılımlarının ortaya çıkması ile

başladı. 2012'de **Reveton** olarak bilinen büyük bir fidye yazılımı yayılmaya başladı. Dosya bir kolluk kuvveti ajansından bilgisayarın lisanssız yazılım veya çocuk pornosu gibi illegal aktiviteler için kullanıldığını iddia eden bir uyarı göstermekteydi. Bu davranışından ötürü, genelde **"Polis Truva atı"** olarak da anılmaktadır. (http://www.thejournal.ie/gardai-garda-police-trojan-scam-virus-logo-locking-488837-Jun2012/, 2018).

Başlangıçta Avrupa'da yayılmış olan Reveton, ABD'de de görünmeye başlayacak kadar yaygınlaştı ve kurbanlara FBI tarafından gözetim altında tutulduklarını ve cihazlarının kilidini açmak için 200 $ ceza ödemelerine karar verildiğini söyledi. Uyarı, sistemlerinin kilidini çözebilmek için, Ukash veya Paysafecard gibi anonim nakit hizmetleri kullanarak bir ücret ödemeleri gerektiğini söylemekteydi. Bilgisayarın bir kolluk kuvveti tarafından takip edildiği hissini oluşturmak için, ekranda bilgisayarın IP adresini ve kurbanın takip edildiği hissini vermek için kurbanın webcaminden bir kamera görüntüsü göstermekteydi. (https://www.techworld.com/news/security/ransom-trojans-spreading-beyond-russian-heartland-3343528/, 2018).

2013: CryptoLocker

2013 yılının ikinci yarısında, siber güvenlik mücadelesine yeni bir yaklaşım getiren şifreleme fidye yazılımının farklı türü ortaya çıktı. Şifreleme fidye yazılımlar, 2013 sonlarına doğru fidyeyi Bitcoin platformunu kullanarak toplayan CryptoLocker'ın yaygınlaşması ile tekrar yaygın hale gelmiştir. 2048-bit RSA anahtar çifti üreten ve bunu bir komuta-kontrol sunucusuna gönderen ve dosyaları belirli dosya uzantılarından oluşan bir beyaz liste kullanarak şifreleyen ve "**CryptoLocker**" olarak bilinen bir truva atı ile Eylül 2013'de tekrar ortaya çıkmıştır. (https://www.theguardian.com/money/2013/oct/19/cryptolocker-attacks-computer-ransomeware, 2018).

CryptoLocker, 2 Haziran 2014'de US Adalet Bakanlığı tarafından resmen ilan edildiği üzere, Gameover ZeuS botnetinin ele geçirilmesi ile durdurulmuştu. Adalet Bakanlığı, botnetin yöneticisi olduğu gerekçesi ile Rus

hacker Evgeniy Bogachev hakkında iddianame düzenlenmişti. Cryptolocker 234.000'den fazla bilgisayara bulaşmıştı ve bunların yaklaşık yarısı ABD'de bulunmaktaydı. Bir tahmin, Cryptolocker'ın ortaya çıkmasından bu yana ilk iki ayda fidye ödemelerinin **27 milyon dolardan** fazla yapıldığını göstermekteydi. (https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware, 2018).

Cryptowall

Windows işletim sistemini hedef alan bir başka büyük fidye virüsü olan CryptoWall, ilk olarak 2014'de görülmüştür. CryptoLocker, Gameover Zeus botneti ele geçirildiğinde 2014'te büyük oranda durduruldu, ancak o zamana kadar onun yerini almak için hazır olan birçok taklitçi oluşmuştu. Bunlardan biri olan CryptoWall, Tor ağı ekranının arkasında üretilen ve kimlik avı dolandırıcılıkları yoluyla dağıtılan aynı RSA genel-özel anahtar şifrelemesini çalıştıran en dikkat çekici yazılımdı. Bir CryptoWall türü, birkaç büyük web sitesini hedef alan ve 2014 Eylül sonlarında Zedo reklam ağında yapılan bir kötücül reklam kampanyası parçası olarak dağıtılmıştır; reklamlar dosyayı indirmek için tarayıcı eklenti istismarlarını kullanan sahte web sitelerine yönlendirme yapmaktadır. Dosyaları şifrelerken, kötü amaçlı yazılım gölge kopya servisi bilgilerini de silmekte bunun yanında parolaları ve Bitcoin cüzdanlarını çalan bir casus yazılım yüklemekteydi. (http://blog.trendmicro.com/trendlabs-security-intelligence/cryptowall-3-0-ransomware-partners-with-fareit-spyware/, 2018).

CryptoWall ayrıca Bitcoin'in fidye saldırılarında oynadığı rolün arttığını da doğruladı. 2014 yılına kadar, kripto para birimi tercih edilen ödeme yöntemiydi. Ön ödemeli elektronik krediler anonimdi ancak aklama yapmadan nakit çıkışı yapmak zordu; oysa Bitcoin ticaret yapmak ve doğrudan işlem yapmak için normal para birimi gibi çevrimiçi olarak kullanılabilirdi. 2015'e gelindiğinde, **CryptoWall'un tek başına 325 milyon dolar** kazandığı tahmin ediliyordu. (https://terramedusa.com/dosyalari-sifreleyip-bitcoin-isteyen-zararli-yazilim-325-milyon-dolar-kazandirdi/, 2018).

2016: Locky ve KeRanger

Agresif kimlik avı tabanlı dağıtımıyla **Locky**, dağıtım hızı ve ölçeği açısından kendisini takip eden WannaCry gibilerine bir emsal oluşturdu. Doruk noktasına geldiğinde, günde 100.000 yeni sisteme bulaştığı bildirilmişti, gün geçtikçe daha fazla suçluyu dağıtımına teşvik etmek için ilk kez Android araç kitleri tarafından kullanılan franchise sistemini kullandı. Aynı zamanda, sağlık hizmeti sağlayıcılarını hedef alarak WannaCry saldırısının habercisi oldu; yazılımın yaratıcıları, önemli kamu servislerinin, sistemlerini yeniden çalışır hale geitrmek için fidyeleri çok daha hızlı ödediklerini anlamıştı. (Palmer, 2017, s. 2).

2016, ayrıca Mac sistemlerini etkileyen ilk fidye yazılımların ortaya çıktığı yıldı. **KeRanger,** Time Machine yedeklemelerini ve diğer Mac dosyalarını şifrelediği için özellikle yıkıcı bir yazılımdı. Time Machine, Mac'lerde bir sorun oluştuğunda önceki sürümlere geri dönme yeteneği sağlıyordu. KeRanger'dan kısa bir süre sonra birden fazla işletim sistemine bulaşabilen ilk fidye yazılımı ortaya çıktı. JavaScript'te programlanan Ransom32, teoride Windows, Mac veya Linux'ta çalışan tüm cihazları etkileyebilirdi. (Wikipedia, 2016).

2017: WannaCry ve Diğerleri

2016 yılındaki fidye yazılım saldırılarının ölçeği ve karmaşıklığı göz önüne alındığında çoğu siber güvenlik uzmanı, en büyük fidye yazılım saldırılarının ve veri ihlallerinin yer alacağı gerçek bir küresel olay gerçekleşeceğine kısa bir zaman kaldığına inanıyordu. WannaCry bu endişelerin yersiz olmadığını doğrulamıştır.

12 Mayıs 2017'de, dünya tarafından tanınacak olan bir fidye yazılım olan WannaCry'ın ilk kurbanları İspanya'da ortaya çıkmıştır. Fidye zararlısı kısa bir süre için farklı ülkelerde farklı şehirlerde yüzlerce bilgisayara ulaşmıştır. Aradan zaman geçtikçe etki alanı genişlemiş ve **WannaCry kendisini bu tarihe kadarki en büyük fidye saldırısı** olarak kaydettirmiştir.

WannaCry fidye zararlısını bu kadar etkili kılan ve insanları şok eden şey bu kadar nasıl hızlı yayılabildiğidir. Herhangi bri botnet ya da indirmenin yapılacağı bir web sitesi bulunmamaktaydı. Bunun yerine, WannaCry zararlısı bilgisayarların bilinen güvenlik açıklarını hedef alan yeni yöntemine imza atmıştır. Bir ağdaki bir bilgisayara bulaştıktan sonra, aynı güvenlik zafiyetine sahip olan bilgisayarları hızlı bir şekilde bulup kendini otomatik olarak enfekte etmekteydi. WannaCry'ın aynı zamanda çok fazla popüler olması ve gündemde kalmasının basit ama temel nedeni de bu olmuştur. Dahası "WannaCry" fidye yazılımı küresel ölçekte en çok sağlık, üretim, enerji (petrol ve gaz), teknoloji, gıda ve içecek, eğitim, kamu, medya ve iletişim sektörlerinde olumuz etkisini hissettirerek, büyük çapta maddi zarara neden olabilmiştir (Darıcılı, Siber Uzay ve Siber Güvenlik Nedir?, 2017, s. 233).

Bunun yanında birçok güvenlik uzmanını şok eden asıl olay, WannaCry'ın Windows'ta kullandığı güvenlik zafiyetinin yıllar önce ABD Ulusal Güvenlik Ajansı (NSA) tarafından tespit edilmiş olduğu gerçeğiydi. Fakat tüm dünyayı böyle bir zararlı hakkında uyarmak yerine, NSA sessiz kalmış ve bu zafiyeti bir siber silah olarak kullanmak için kendi istismar kodunu geliştirmeyi tercih etmiştir. Saldırı, Europol tarafından eşi benzeri görülmemiş şekilde tarif edilmiştir. (http://www.bbc.com/news/world-europe-39907965, 2018).

WannaCry'ın hemen arkasından gerçekleşen başka bir uluslararası fidye yazılım saldırısı, dünyanın dört bir köşesinde binlerce bilgisayarı hedef almıştır. **Petya** olarak bilinen bu saldırıda en dikkat çekici olan şey, WannaCry tarafından kullanılan aynı Windows güvenlik zafiyetinin kullanması ve NSA'nın planladığı ve geliştirdiği bir yazılımın ne kadar güçlü olabileceğini göstermiştir. Ayrıca, WannaCry saldırısının ardından çeşitli ortamlardan duyurulan ve yaygın olarak kullanılmaya başlanan bir yamaya rağmen kullanıcıların sürekli olarak güvenlik güncelleştirmeleri etkinleştirmelerinin ne kadar zor olduğunu göstermiştir.

FİDYE YAZILIMLARA KARŞI ETKİLİ MÜCADELE

Pratikte bilinen anti virüs yazılımları ve sandbox çözümleri yeni nesil zararlılara karşı büyük oranda başarısız olmaktadır. Bu durumun en büyük nedeni ise dijital imzalarını sürekli değiştirme yeteneğine sahip yeni nesil zararlıların artık imza tabanlı ve statik analizler ile tanınamamasıdır. Fidye yazılım geliştiricisi kötü niyetli saldırganlar, geliştirdikleri yöntemler ile sezgisel ve davranış tabanlı otomatik analiz mekanizmalarını kolaylıkla atlatabilmektedir. Bazı durumlarda ise bu teknolojilerin yeni zararlıları keşfetmede geç kalabildikleri görülmektedir. Önceki bölümlerde anlatıldığı gibi fidye yazılım saldırılarının mevcut durumuna nasıl dönüştüğünü anlamak, siber suçluların neden bazı taktik veya yöntemler kullanıp kullanamayacağını ve onlara karşı nasıl savunacağımızı daha iyi anlamamızı sağlamaktadır.

1. Yedekleme ve Veri Kurtarma

Fidye yazılım saldırılarına karşı en iyi savunmalardan biri yedekleme ve veri kurtarma işlemlerinizdir. Şifrelenmiş dosyalarınızı yedeklerinizden kurtarabiliyorsanız, organizasyonunuz üzerinde çok az veya hiç etkileri olmayan başarılı bir fidye saldırısını zararsız bir şekilde atlatmışsınız demektir. Yedeklemeler zararlı yazılımın erişemeyeceği bir yerde tutulmalıdır. Saldırganların, değerli dosyaların şifrelenmesi çabalarının bir parçası olarak yedeklemeleri hedefledikleri bilinmektedir. Ancak bir eksilik olarak dosyaların **yedekten kurtarma sürecinin test edilmesi**, yedekleme kadar önemli bir faaliyet olarak karşımıza çıkmaktadır. Kurtarma işleminizi hiç test etmediyseniz, yedeklemelerinizin düşündüğünüz kadar güvenli olmadığını fark edebilirsiniz.

Yedeği alınacak kritik sistemlerin **yedekleme politika ve prosedürlerini** (back-up policy) yazılı olarak hazırlanmalıdır. Sistemin kullanım dışı kalması durumunda, sistem herhangi bir veri kaybına uğramadan yeniden başlatılabilmesi sağlanmalıdır. Ayrıca yedekleme işleminin düzenli olarak yapılabilmesi ve takvimlenmesini sağlayan mekanizmalar ile yedekleme işlemlerinin sonlanma durumunu ve hatalarını raporlayabileceğine bir yönetim sistemine sahip olunmalıdır.

2. Ağ Yapısı ve Yönetilmesi

Fidye yazılım saldırına karşı yeterli ağ tasarım gereksinimlerinin sağlandığından emin olmak için, **ağ yapılarının izlenmesi ve doğru şekilde yönetilmesi** gerekmektedir. Güncel ağ topolojisi bir an önce çıkarmalı ve bu iş periyodik olarak takip edilmelidir. Ağ yönetimi genel olarak aşağıdaki fonksiyonları içermelidir:

- Ağdaki yapılandırma değişikliklerinin takibi ve yönetilmesi,
- Ağ paylaşım izinlerinin tek merkezden takibi ve yönetilmesi,
- Ağ hatalarının tanımlanabilmesi,
- Performans seviyelerinin takibi,
- Ağdaki uç noktalarının güvenli erişimin sağlandığından emin olması için düzenli olarak izleme yapılması ve raporlanması.

Genel bir ağ yönetim mimarisi aşağıdaki bileşenlerden oluşmalıdır:

- Ağ Yönetim Sistemi (NMS: Network Management Sistem): CiscoWorks, SolarWinds, HPE NNMi, gibi ürünleri kullanarak ağ sistemi bileşenlerinin izlenmesi ve yönetilmesi,
- Ağ Yönetim Protokolü: Ağ cihazları ve Ağ Yönetim Sistemleri arasında bilgi değişiminin yapılabilmesi için protokol desteğinin sağlanması. (Örneğin SNMPv3 gibi),
- Yönetilen Cihazlar: Yönlendirici (Router) veya Anahtar (Switch) gibi ağ cihazlarının, NMS tarafından yönetilmesi.
- Yönetim Ajanları: Yönetilen cihazlardan ağ yönetim bilgilerini toplayan ve kayıt altına alan yazılımlar.

Günümüz BT dünyasının siber güvenlik gereksinimleri olan Güvenlik Duvarları, IDS, IPS, WAF gibi çözümlerin ağ yapısına entegrasyonu gerekmektedir. Bunun yanında yukarda belirtilen güvenlik gereksinimlerini karşılamak için ağ trafiği izolasyonunun sağlanması gerekmektedir. (Örneğin, MPLS / VRF'ler (sanal özel ağ yönlendiricileri / ileticiler) ile genel yönlendirme kapsüllemesi [GRE] gibi tünel oluşturma). Bu sayede güvenlik, performans ve yönetilebilirlik değerleri en yüksek seviyede tutulabilmektedir.

3. Güvenlik Farkındalığı Eğitimi

İyi yetiştirilmiş ve bilinçlendirilmiş **insan kaynağı,** herhangi bir kurum veya kuruluşa ait sistemlerin güvenlik temelini oluşturmaktadır. Kurum ve kuruluşlar, siber güvenlik planlarını gerçekleştirmek için gerekli uzmanlığı sağlamalı ve fidye yazılım saldırılarına karşı ilk savunma hattının insan olduğu unutulmamalıdır. Dünyaca ünlü bilişim firmalarının son yıllarda yaşadığı bilgi güvenliği ihlal olayları detaylıca incelendiğinde, sorunun ana kaynağının çalışanların bilgi güvenliği farkındalıklarının eksikliği olduğu ortaya çıkmaktadır. Çalışanların farkındalık seviyelerinin arttırılmasında en önemli maddelerden biri, düzenli olarak eğitim verilmesi ve eğitimler sonrası farkındalık senaryolarını içeren saldırı simülasyonlarının gerçekleştirilmesidir. Güncel saldırı yöntemleri ve bunlara karşı alınabilecek önlemlerin senaryolar eşliğinde eğitim yapılması ve sonrası gerçekleştirilecek **farkındalık seviyesi ölçüm/değerlendirme sınavı** ile katılımcıların farkındalık seviyesindeki artışı da somut olarak görülebilmektedir.

4. Yama yönetimi ve güncelleme süreçlerinin gözden geçirilmesi

Fidye yazılım geliştiricileri sıklıkla bilinen açıklara sahip güncel olmayan yazılımlardan faydalanıp kullanıcıların sistemlerine sessizce sızarak virüsleri bulaştırabilmektedir. Eğer yazılımlarınızı sıklıkla güncelliyorsanız fidye yazılımlarının bulaşmasına karşı daha korumalı olduğunuz söylenebilir. Bazı yazılım üreticileri güncellemelerini düzenli olarak (Microsoft ve Adobe her ayın 2. salı günü) yayınlamaktadır, ancak bazı acil durumlarda bu standart zamanlar dışında da güncelleme yayınlanmaktadır. Kurum ve kuruluşa özgü yama yönetimi takibi yapılması bu tür zararlılarla mücadele anlamında önem arz etmektedir.

5. Anti-spam / malware korumasının özelleştirilmesi

Düzenli olarak güncellenen, ileri düzey özelleştirilmiş anti spam koruması fidye yazılım saldırılarına karşı etkili bir önlem olmaktadır. Yeterli kurum veya kuruluşa özgü ayarları yapılmış spam önleme servisleri, e-posta sunucusu yazılımlarımı ile eş zamanlı çalışmasıyla çok daha güvenli ve yüksek oranlarda verimlilikle hizmet vermeleri sağlanabilir.

6. Ağınızın korunması için yeni nesil güvenlik sistemlerinin kullanılması

Güvenlik duvarınız, imza tabanlı algılama yaklaşımlarını da içermelidir ancak sürekli olarak güncellenen bir tehdit özet akışına dayalı bilinen tehditleri de engellemelidir. Sandboxing (kum havuzu analizi), sürekli olarak görünen yeni bir fidye yazılımın saptanması için alternatif bir yöntem olarak **Olay yanıtı planlaması.**

"Biz fidyeyi ödeyelim ama bize şifre çözme anahtarı vermezlerse **?**" Birçok kuruluş güvenlik olaylarına nasıl yanıt vereceğini ancak bir saldırıya uğradıktan sonra öğrenmektedir. Maliyetini ve zararını azaltmak için bir saldırı gerçekleşmeden önce **olay yanıtı planınızın** olması önemlidir. Etkili bir olay yanıt planı, üç temel özelliğe bağlıdır: tehditlere karşı koruma, tehditleri algılama ve yanıtlama. Koruma; olayları önlemek, algılama; tehditleri erken belirlemek ve yanıt; saldırganı uzaklaştırıp sistemleri geri yükleyerek bir ihlalin etkilerini azaltmak içindir.

Muhtemelen kurum ve kuruluşunuzda bir ihlal olayına yönelik genel tepki planınız vardır ancak, fidye yazılım saldırıları diğer zararlı yazılım olaylarından çok farklı ve özel bir iyileştirme süreci gerektirdiğinden bu saldırı türüne özgü bir yanıt planı geliştirmeniz önerilmektedir. Olay gerçekleşmeden önce bir ekibin toplanması kuruluşunuz için çok önemlidir ve olayların nasıl ele alındığını olumlu yönde etkilemektedir. Kaynakları izlemek için doğru araçlara sahip olunması bu ekibin bir güvenlik olayını düzeltmek üzere doğru adımları uygulamasına yardımcı olabilmektedir. Olay yanıt planında bu tür senaryoları ne kadar ayrıntılı düşünüp planlarsanız, yanıtlama sürenizde o kadar kısa olacaktır.

7. Tehdidi Anlama

Günümüz fidye yazılım saldırılarından korunmak için ekonomik sınırlar dâhilinde güvenliği sağlamak için uygulama bazında tedarik ve operasyonların zaman ve maliyetini azaltacak risk odaklı bir yaklaşım izlenmelidir. Bu riske dayalı yaklaşım, belirli uygulamalar bağlamında

belirlenmiş riskleri ele alarak gelecekte yapılacak güvenlik yatırımlarını kolaylaştıracağı düşünülmektedir.

Doğru bir güvenlik risk analizi yapmak için güvenlik ekipleri, yönetilen varlıklara yönelik fidye yazılımları tehdit ailesini tam olarak bilmelidir. Potansiyel tehditlere karşı güvenlik risklerini belirlemek, bu riskleri değerlendirmek ve her bir riske nasıl cevap verileceğine karar vermek maksadıyla kurum ve kuruluşlar için **tehdit modelleme metodolojisi** gereklidir. Tehdit modelleme fidye yazılımlarla mücadele için temeldir ve organizasyonların doğru kontrolleri belirlemesini ve bütçe içinde etkili karşı tedbir oluşturmasını sağlar.

8. Hasarın Kontrol Edilmesi

Gerçekleşen fidye yazılım saldırısına yönelik olarak potansiyel delil ve bilgi toplanması olay sonrası inceleme ve tehdidin tekrar ortaya çıkmaması için önem arz etmektedir. Yinelemeyi önlemek için ele alınması gereken zayıf noktaları ve sistem zayıflıklarını belirlemek için zararlı yazılımın kaynağı analiz edilmelidir. Ancak önce düşünülmesi gereken başka şeyler vardır. Örneğin, saldırıya uğrayan sisteminizde nelerin eksik olduğunu biliyor musun? Saldırgan fidye yazılım ile dosyalarınızı şifrelediğini iddia ediyor, ancak önemli bir şeyi kaybettiniz mi?

Bu kapsamda olay müdahale ekipleriniz mevcutsa, en son yedekleri veya hizmetin sürekliliğini ve güvenliğin ihlal öncesi durumuna dönüş için alternatif çözümleri belirlemek size hasarın etkisini azaltacaktır. Olay müdahale ekibinin saldırıyı tüm yönleri ile analiz etmek için adli verileri kullanması gerekmektedir. Bir fidye yazılım saldırısı durumunda olay müdahale ekiplerinin tüm bilgileri aklında tutması, elle bir rapor oluşturması zaman almaktadır. Son yıllarda kuruluşları etkinleştirmek için otomatik çözümler kullanılabilir hale gelmiştir. Otomatik adli analiz araçlarının uygulanması saldırıyı kapsamlı olarak anlamak açısından olay müdahale ekibinin yeteneğini büyük ölçüde arttırmakta ve iyileştirme için yol gösterici olmaktadır. Bu araçlar olay analizi için önemli ölçüde zaman azaltmakta ve bilgi güvenliği personelinin saldırıları anlayarak daha etkili ve verimli şekilde yanıt verebilmelerini sağlamaktadır.

Hatırlanması gereken önemli nokta, yanıtınızı planlamaya başlamadan önce bir yanıtın gerçekten gerekli olduğundan emin olmanızdır. Modern fidye yazılımı, en değerli dosyaları ve güçlü şifreleme standartlarını öncelik sırasına koymak için uygulama beyaz listelerini kullandığından, kaba kuvvetle erişmenizi önlemek için durumunuzun idealden daha az olduğunu bulacaksınız ancak kontrol etmeniz zarar vermez. Ekran kilitleyen fidye yazılımını ve kripto fidye yazılımının bazı türevlerini algılayabilen, ücretsiz şifre çözme araçları, farklı güvenlik üreticilerinden kolayca temin edilebilir. Bunlar, şifre çözme anahtarlarına ödeme yapmamak için kullanılabilir. Farklı durumlarda, söz konusu fidye yazılımın kum havuzu (sandbox) analizi, kötü amaçlı yazılım davranışını belirlemenize yardımcı olabilir. Bu ayrıca fidye yazılımın yeteneklerini, rutinlerini ve kullanılan taktiklerini tespit etmeyi artırabilir ve gelecekteki olayları önleme yollarını belirlemek için kullanılabilir.

9. Operasyonel Temizleme

Fidye yazılımından kurtulma işlemi iki adımdan oluşmaktadır: Zararlı yazılımın bulaştığı **sistemin temizlenmesi ve şifrelenen dosyaların şifresiz hale geri getirilmesi**.

a. Fidye yazılımın birçok çeşidi, şu anda çoğu güncel anti virüs yazılımı tarafından tespit edilip temizlenebilmektedir. Dolayısı ile öncelikle zararlı yazılımın bulaştığı bilgisayar, zararlı yazılım tespit edilip temizlenene kadar, farklı anti virüsler ile taratılmalıdır.

b.

b. Ancak, fidye yazılımların birçok türevi olduğu ve sürekli olarak şekil değiştirdiği göz önüne alındığında, tespit edilememe ihtimali de oldukça yüksektir. Dolayısı ile tam olarak temizlik için, bulaştığı bilgisayara format atılarak, tekrar işletim sistemi kurulması gerekmektedir.

c. Üst maddede açıklandığı gibi zararlı yazılımı temizlemek, şifrelediği dosyaların şifresini çözmemekte, sadece fidye yazılımın daha fazla dosyanızı şifrelemesini engellemektedir.CryptoLocker vb. fidye yazılımlar, şifrelemede RSA-4096 / AES-256 benzeri çok güçlü şifreleme algoritmaları kullanmaktadır. Dünyada şifre kırma yöntemlerinde gelinen son durumda,

belirtilen algoritmanın kaba kuvvet (brute force) yöntemiyle kırılabilmesi için milyonlarca yıldan çok daha fazla süre gerektiğinden, söz konusu algoritmalar kırılamaz kabul edilmektedir

e. Fidye yazılımların birçok türevi olması, ayrıca saldırganların her bir bilgisayar için farklı anahtarlara sahip virüsler üretmesi nedeniyle, zararlının şifrelediği dosyaların çözülmesi için bir çözücü yazılım üretilmesi de mümkün olamamaktadır. Dolayısı ile şifrenin çözülmesi günümüz şartlarında şifre anahtarını bilmeden mümkün değildir (CryptoLocker vb. fidye saldırılara karşı çözüm geliştirdiğini ifade eden internetteki birçok hilekâra karşı dikkatli olunmalıdır).

f. Halihazırda genel şifre çözme amaçlı geliştirilen yazılımlar, maalesef fidye yazılımlar için kullanılamamaktadır çünkü fidye yazılım ailesinin 20'den fazla bilinen türevi vardır ve sürekli değişiklik arz edebilmektedir.

g. Denenmesi gereken ilk işlem, zararlı yazılım dosyaları şifrelemeyi müteakip orijinal halini hızlı silmiş olabileceği umularak, fidye yazılımın bulaştığı sürücülerde veri kurtarma (File recovery) yazılımları ile silinmiş olan orijinal dosyaları geri getirmeye çalışmaktır. Geri getirme ortamı olarak harici USB disk/bellekler tercih edilmelidir.

h. Yapılabilecek diğer işlem ise, dosyaların virüs tarafından şifrelenmeden önce alınmış bir yedeği varsa, o yedeğin kullanılmasıdır. Bu kapsamda, genel tedbirler olarak;

(1) Kritik dosyalarınızın belirli aralıklarla yedeğini tek yazımlık CD/DVD'lere almanız tavsiye edilmektedir (Tek yazımlık DVD'lerde bulunan dosyaların, DVD'nin yapısından dolayı fidye yazılımlar tarafından şifrelenmesi teknik olarak mümkün değildir).

(2) Bilgisayarlardaki işletim sistemlerinde, dosyaların değişmesi (silinmesi, içeriğinin değişmesi vb.) durumunda otomatik olarak bir önceki versiyonunun arşivlenmesini sağlayan imkânlar bulunmaktadır. Bu işlevleri açık olan bilgisayara fidye yazılımlar bulaşsa bile, şifrelenmeden önceki versiyonlara geri dönülmek suretiyle zararının telafi edilmesi sağlanabilir. Ancak; fidye yazılımların bazı gelişmiş türlerinde, oturumu açan kullanıcının yetkisi var ise, zararlı yazılım, işletim sisteminin tuttuğu eski dosya

versiyonlarını da silmektedir. Bu durumda bu işlevler maalesef işe yaramayacaktır.

10. En Kötü Senaryo Durumu

Fidye yazılım tarafından şifrelenen dosyalara ait anahtarı almak için bir fidye ödemek, bir kurum veya kuruluşun son başvurması gereken çözüm olmalıdır. Şüphesiz ki saldırganlara yapılan ödemeler, suç örgütlerine fon sağlanmasına yardımcı olmaktadır. Bu hususu da unutmamak gerekir. Şifreli verilerinizden yedekleriniz yoksa bile, ödeme yapmadan önce aşağıdaki seçeneklerinizi göz önünde bulundurun:

• Şifrelenen verileri yeniden yaratabilir misiniz?

• Dosyaların yeni bir sürümüyle güncellenebilecek eski bir sürümünü bulunmakta mıdır?

•Zararlı yazılımın erişemediği, verilerinizi barındıran ve etkilenmeyen başka bir sisteminiz mevcut mudur?

Kısacası, ayrıntılı bir mücadele yöntemi ve bu durumun tekrar oluşmasını önlemek için siber güvenliğinize yönelik tedbirlerinizi geliştirmeniz gerekmektedir. Son olarak normale dönüşün gerçekleşmesi için çok katmanlı güvenlik anlayışını içeren bir yaklaşımınız olmalıdır. Güncellenmiş varyantlar ve fidye yazılım aileler ile hemen hemen her gün yenisi yayınlanan zararlı yazılımların hızlı gelişimi, siber suçluların bunu kârlı bir saldırı biçimi olarak gördüğünü göstermektedir.

Fidye yazılım saldırıları ile mücadelede güvenlik için çok katmanlı bir yaklaşım, olası tüm giriş noktalarının fidye yazılımından korunmasını sağlamada hayati öneme sahip olmaktadır. Bu tehdit türünün getirdiği riskleri en az düzeye indirmek için çok katmanlı, adım adım bir yaklaşımdan yararlanılması kurum ve kuruluşlar için fayda sağlayacağı düşünülmektedir. Kurum ve kuruluşun mevcut yapısında gerçekleştirilecek analiz çalışmaları göz önünde bulundurularak kendine özgü bir güvenlik anlayışı oluşturulması gerekmektedir.

Çok katmanlı bu yaklaşımda aşağıdaki katmanlar ve katmanlarda kullanılması önerilen uygulamalar genel hatlarıyla şunlardır;

- **E-posta ve Web Koruması**: Fidye yazılımlar, kullanıcılarınıza, e-postalara ve web ağ geçitlerine erişmeden engellenmelidir. E-posta ağ geçidinde fidye yazılımı tespiti daha derin bir e-posta inceleme seviyesi ile daha iyi hale getirilmelidir. Koruma sisteminiz e-posta ağ geçidinizle birlikte çalışarak, fidye yazılımlarının sisteminize taşınması için sıklıkla kullanılan oltalama e-postalarını ve zararlı e-posta eklerini engellenmelidir. E-postalar dışında, kullanıcılarınız kasıtlı olarak zararlı olacak şekilde tasarlanmış ya da ele geçirilmiş web sitelerine tıklayarak da fidye yazılımlarından etkilenebilir. Sıfırıncı gün açıklarını ve tarayıcı açıklarını tarayarak vir URL'nin fidye yazılımı için bilinen bir iletim aracı olup olmadığını belirlemek için gerçek zamanlı web analizi yapılmalıdır.
- **Uç Nokta Koruması:** Fidye yazılımlar, verilerinizi kurtarmak için sizleri ödeme yapmaya zorlamadan önce uç noktada yakalanmalıdır. Son kullanıcıya ulaşan fidye yazılımın dosyalarını sadece çalışma zamanından önce değil, çalışma sırasında da analiz eden yüksek yoğunluklu makine öğrenimi bir tedbir olarak uygulanmalıdır. Uygulama kontrolü ile uygulama beyaz listeleri oluşturmalıdır. Bu kontrol ile sadece bilinen iyi uygulamaların yürütülmesine izin verilerek fidye yazılımları gibi bilinmeyen uygulamaların da yürütülmesi engellenmelidir. Birden fazla dosyanın hızlı bir şekilde şifrelenmesi gibi fidye yazılımlarıyla ilişkili şüpheli davranışlar için davranış izleme ile şifreleme süreci otomatik olarak durdurularak fidye yazılımın sistemdeki verilerde daha fazla zarara yol açmadan kontrol altına alınması sağlanabilir.

- **Ağ Koruması:** Ağınızdaki fidye yazılımlar tespit edilip engellenmelidir. E-posta ve web yaygın fidye yazılımı giriş noktalarıdır ancak diğer ağ protokolleri ve saldırı yöntemleri de kurum ve kuruluşları fidye yazılım saldırılarına maruz bırakabilir. Fidye yazılımların, tüm siber saldırı aşamaları boyunca model ve davranış tabanlı analiz yapılarak komuta-kontrol sunucu trafiğinin tespit edilip engellenmesi gerekmektedir.

- **<u>Sunucu Koruması</u>:** Fidye yazılımların, en değerli veri dosyalarınızın bulunduğu sunucularınıza sızması engellenmelidir. Fidye yazılımları giderek daha fazla sunucuyu hedef almaktadır. Örneğin SAMSAM (SAMAS olarak da bilinen) gibi yüksek profilli örneklerde saldırganlar fidye yazılımını sızdırmak için bilinen yazılım açıklarını kullanmaktadır. Sunucular ve uygulamalar için bir koruma oluşturup, bir yama veya onarım uygulanana kadar bilinen yazılım zayıflıklarından yararlanılmasını önlenmelidir.

SONUÇ

Geçtiğimiz son birkaç yılda artış göstererek yaşanan fidye yazılım saldırıları, geniş güvenlik bütçelerine sahip çok uluslu büyük firmalarından devlet kuruluşlarına kadar çoğu kurum veya kuruluşun; kullanıcılarını, sistemlerini ve süreçlerini en son tehditlerden ve akıllı siber saldırganlardan tamamen koruyamadıklarını göstermektedir. Saldırganlar hedef olarak güvenlikte en zayıf halka olan kullanıcılara yöneltmekte ve bu sayede istedikleri verilere ulaşabilmektedirler. Çoğu vakada karşımıza çıkan saldırıların temel zafiyetler; çalınmış yetkiler, güvenlik yamaları yüklenmemiş bir sistem veya dikkatsiz bir kullanıcı olmaktadır. WannaCry örneğinde de açıkça görüldüğü üzere, devletlerin güvenliklerini sağlama noktasında, geleneksel güvenlik anlayışına göre şekillenmiş tüm kurum ve stratejilerini, etkili bir siber saldırı ve siber savunma kapasitesi oluşturmak adına yeniden organize etmesi de gerekmektedir (Darıcılı, Siber Uzay ve Siber Güvenlik Nedir?, 2017, s. 234).

Siber saldırganlar istediklerini bir kere elde ettikten sonra, kolayca bunu istismar ederek diğer kurum ve kuruluşlara ait değerli verileri de çalabilmektedirler. Bu açıdan siber tehdit istihbaratının elde edilmesinde ve analizinde vazgeçilmez bir unsur olan kurumlar ve kuruluşlar arası **bilgi paylaşımı**, üzerinde durulması gereken bir konu olarak karşımıza çıkmaktadır. Fidye yazılım saldırıları ile mücadele kapsamında kurumlar ve kuruluşlar arası işbirliğine dayanan güvenlik istihbarat teknolojileri kullanılarak siber atakları tespit etme ve kontrol altına alma konusunda daha etkin bir mücadele yapılabileceği değerlendirilmektedir.

CryptoLocker, WannaCry, Petya, ve daha birçok fidye zararlı yazılımı ortaya çıkmaya devam edecektir. Ancak geliştirilen zararlı fidye yazılımlarının saldırı noktaları ve etki hacimleri, saldırılarda kullanılan yöntemlerle doğrudan ilişkilidir. NSA, TAO, CIA gibi birimler tarafından geliştirilmiş ve sızdırılan bu siber silahların sistemlerde ne tür zafiyetleri sömürebileceğini önceden tespit etmek için gönüllü inisiyatiflerin yanında resmi araştırma birimleri oluşturulmasına zemin hazırlanması çok büyük önem arz etmektedir.

Bu gibi gizli servislerin çeşitli işletim sistemleri içerisinden önceden tespit ettikleri zafiyetler aracılığı ile dünya genelindeki tüm ülkelere APT (Advance Persistent Threat) saldırıları gerçekleştirdikleri, bizlerin ise bu zafiyetlerden ancak WannaCry veya Petya gibi dünya genelini etkisi altına alabilecek ve kritik altyapıları zarara uğratacak çapta saldırılar meydana getirdiğinde haberdar olabildiğimiz gerçeğinin altı önemle çizilmelidir. Bu noktada somut adımlar atılarak APT saldırılarının önüne geçilmesi için **milli-yerli ürün ve hizmetler** temelinde acil tedbirler hayata geçirilmelidir. (Sarı, 2017).

Ancak ne tür bir aksiyon alınırsa alınsın hatalardan mutlaka ders çıkarmaya özen gösterilmelidir. Neyin yanlış gittiğini ve gelecekte nasıl engelleneceğini belirlemek için kurum veya kuruluşun işleyişine **özgün bir mücadele yöntemi** belirlenmesi gerekmektedir. Güvenlik açığı ve yama yönetimi, güvenlik farkındalığı eğitimi, sıkı e-posta tarama önlemleri ve kapsamlı bir off-site yedekleme planı gibi mantıklı siber hijyen programların mevcut olduğundan emin olunmalıdır.

Sonuç olarak; çalışmada anlatılmak istenen mücadele yöntemlerinin kullanılması ve fidye yazılım saldırılarına ilişkin bahsedilen temel güvenlik tedbirlerini uygulanmasıyla birçok saldırıdan korunmak ve saldırılardan en az seviyede zarar görecek şekilde hazırlanmak mümkündür. Bu noktada, son kullanıcı güvenlik farkındalığın artırılması ve kurumların siber güvenlik personelinin uzmanlık derecesinin iş bölümü yapılarak üst seviyede tutulmasına yönelik çalışmaların yapılması da oldukça önem arz etmektedir. Çalışmanın sonunda Benjamin Franklin'in bir sözünü hatırlatmakta fayda

görülmektedir: **"İyileşmek için tedavi görmektense, hasta olmamak için tedbir al."**

REFERANSLAR

Darıcılı, A.B. (2017). Siber Uzay ve Siber Güvenlik Nedir? Bursa, Dora Yayınları, s. 233-234.

Fasheem, S. (2017). Detection and Avoidance of Ransomware. *IJEDR, Volume 5, Issue 1*, s. 52.

Gollman, D. (2011). *Computer security*. New York: Wiley.

Hallam-Baker, P. (2016). Ransomware, Everywhere: What's The Science Behind It? s.1.

J.Crowe. (2017). *Must-Know Ransomware Statistics.*

Luo, X. , Liao, Q. (2007). Awareness Education as the Key to Ransomware Prevention. *Information Systems Security*, s.195-202.

Sarı, D. A. (2017). Ransomware ve Son Varyantlar Analizi. *Cezeri Siber Güvenlik Akademisi Yayınları, 1*.

Uitsec Teknoloji. (2014). *Cryptolocker Analiz Raporu.*

Ulaştırma Denizcilik ve Haberleşme Bakanlığı(2017), www.udhb.gov.tr/images/duyurular/74bc0128f065b41.pdf

[Erişim Tarihi: 05.12.2017].

Wikipedia. (2016). https://en.wikipedia.org/wiki/KeRange [Erişim Tarihi: 10.12.2017].

Palmer, D. (2017). https://www.zdnet.com/article/locky-ransomware-why-this-menace-keeps-coming-back/ [Erişim Tarihi: 17.12.2017].

Barkly. (2017). *https://blog.barkly.com/ransomware-statistics-2017* [Erişim Tarihi: 5.10..2017].

Kaspersky Security Bulletin (2015). https://securelist.com/kaspersky-security-bulletin-2015-overall-statistics-for-2015/73038/ [Erişim Tarihi: 15.12.2017].

Microsoft Azure (2017) https://docs.microsoft.com/tr-tr/azure/security-center/security-center-incident-response [Erişim Tarihi: 10.11.2017].

Security Response. (2017). https://medium.com/threat-intel/ransomware-history-3165f10ab5a5 [Erişim Tarihi: 16.12.2017].

Symantec Labs (2009) https://www.symantec.com/security-center/writeup/2009-022723-4223-99 [Erişim Tarihi: 17.12.2017].

Trendlabs, T. M. (2018). https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2017-annual-roundup-the-paradox-of-cyberthreats [Erişim Tarihi: 12.04.2018].

Trend Micro (2015). http://blog.trendmicro.com/trendlabs-security-intelligence/cryptowall-3-0-ransomware-partners-with-fareit-spyware/. [Erişim Tarihi: 17.12.2017].

BBC News(2017). http://www.bbc.com/news/world-europe-39907965 [Erişim Tarihi: 11.12.2017].

Robert L. (2008). http://www.securityfocus.com/news/11523. (2018, 4 20) [Erişim Tarihi: 11.12.2017].

The Journal (2012). http://www.thejournal.ie/gardai-garda-police-trojan-scam-virus-logo-locking-488837-Jun2012/. [Erişim Tarihi: 05.02.2018].

ESET. https://renew.stratus.com.tr/cryptolocker/index.html. [Erişim Tarihi: 17.12.2017].

TerraMedusa Secure (2015)https://terramedusa.com/dosyalari-sifreleyip-bitcoin-isteyen-zararli-yazilim-325-milyon-dolar-kazandirdi/ [Erişim Tarihi: 07.03.2018].

CNeT (2012) https://www.cnet.com/news/ransomware-a-growing-menace-says-symantec/. [Erişim Tarihi: 11.02.2017].

Department of Justice (2017) https://www.justice.gov/archives/opa/documents-and-resources-gameover-zeus-cryptolocker-press-conference ([Erişim Tarihi: 11.12.2017].

PCWorld (2010) https://www.pcworld.com/article/204577/article.html. (2018, 4 22). [Erişim Tarihi: 11.12.2017].

TechRecuplic (2010) https://www.techrepublic.com/blog/it-security/ransomware-extortion-via-the-internet/ [Erişim Tarihi: 11.12.2017].

TechWorld (2012) https://www.techworld.com/news/security/ransom-trojans-spreading-beyond-russian-heartland-3343528/ [Erişim Tarihi: 11.12.2017].

The Guardian (2013) https://www.theguardian.com/money/2013/oct/19/cryptolocker-attacks-computer-ransomeware. ([Erişim Tarihi: 21.01.2018].

FBI News (2016) https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise [Erişim Tarihi: 14.02.2018].