

SİBER FİDYE 2020 RAPORU

YA PARANIZ
YA DATANIZ

FİDYE YAZILIM SALDIRILARINDA STRATEJİK DÖNÜŞÜM VE YENİ TRENDLER



INTEGRA
SIGORTA BROKERİ



BGA
SECURITY

Yönetici Özeti

Fidye yazılım saldırılardan kaynaklanan yıllık maliyetlerin 2021 yılına kadar 20 milyar doları aşacığı tahmin ediliyor.

Tüm dünyayı etkisi altına alan Covid-19 salgınıyla birlikte çeşitli kişisel ve kurumsal bilgisayarları hedef alan fidye yazılım saldırılarında önemli ölçüde artış oldu. Ticari ve finansal işlemlerin giderek artan bir şekilde dijital taşınması ve bilgisayar sistemlerinde daha fazla verinin paylaşılması saldırıcılar için birçok yeni hedefin ortaya çıkmasına neden oldu. Tehdit aktörlerinin operasyonlarına hedef olabilecek dijital verinin sadece miktarının artmadığı, aynı zamanda çeşitliliğinin de genişlediği görülmektedir.

Fidye yazılımları kullanan tehdit aktörleri geçtiğimiz beş yıl içerisinde şifreleme tekniklerinden, yazılımları geliştirirken kullandıkları programlama diline kadar birçok operasyonel değişime gittiler. Fakat bugün yaşanan değişimin merkezinde aktörlerin saldırılarını nasıl gerçekleştirdiklerinden



daha çok saldırı sonrasında veriyi hedefteki kurum için nasıl daha zararlı bir hale getirilebileceği sorusu bulunuyor.

Saldırganların artık hedef aldıkları sistemlerde sadece dosyaları şifreleme ile yetinmedikleri, elde ettikleri verileri hedef kurumun itibarına zarar verecek şekilde kamuoyu ile paylaşmakla tehdit ettikleri örneklerin sayısındaki artış dikkat çekiyor.

Cybersecurity Ventures raporuna göre, fidye yazılım saldırılardan kaynaklanan yıllık maliyetlerin 2021 yılına kadar 20 milyar doları aşacığı tahmin ediliyor. Birçok şirket hedef olamayacak kadar küçük olduğu yanlışına kapılırken, fidye yazılımının bulaşma olasılığılarındaki algılar, fidye yazılımı önleme ve tespit prosedürlerini etkiliyor. Raporumuz sektör ayırmaksızın hedeflerine zarar vererek maddi kazanç elde etmeye çalışan siber saldırıcıların en sık kullandığı silah olan fidye yazılımlar hakkında kapsamlı bilgi sunma amacını taşımaktadır.

Bu rapor, fidye yazılımlarının tüm sektörlerde yarattığı yıkıcı etkinin değerlendirilmesi amacıyla BGA Security ve Integra Broker tarafından, SOCRadar verilerinden beslenerek hazırlanmıştır.

İndeks

- 1** Giriş
- 2** Fidye Yazılım ve Gelişimi
- 3** Fidyecilik Saldırı Vektörleri
- 3.1** Oltalama Saldırıları
- 3.2** RDP
- 3.3** Güvenlik Açıklıkları
- 3.4** Fidye Yazılım Saldırılarına Sebep Olabilecek Diğer Vektörler
- 4** Fidye Yazılım Saldırısı Trendleri-2020
- 4.1** Fidye Saldırısı Nedenli Kesinti Maliyeti
- 4.2** En Tehlikeli 3 Fidye Yazılımı
- 4.3** En Büyük 3 Fidye Yazılımı Saldırısı
- 4.4** Fidye Yazılım Saldırılarında Hedef Alınan Endüstriler
- 4.5** Fidye Yazılım Saldırırganlarının Hedef Aldığı Ülkeler
- 4.6** Fidye Yazılımların Hedef Aldığı İşletim Sistemleri
- 4.7** Türkiye Fidye Yazılımı Trendleri
- 5** Fidye Yazılım Saldırılarından Korunmak İçin 8 Adım
- 6** Fidye Yazılım Saldırılarında Siber Sigortanın Önemi
- 7** Öneriler
- 8** Fidye Yazılım Saldırısı Başınıza Geldiğinde Ne Yapmalısınız

Fidye yazılımı, kurbanın dosyalarını şifreleyen kötü amaçlı bir yazılım türüdür. Saldırgan, ödeme yapıldıktan sonra verilerine tekrar erişebilmesi için kurbandan fidye talep eder.

Kullanıcılara şifre çözme anahtarını almak için nasıl ücret ödeyeceklerine dair talimatlar verilir. Talep edilen fidye ücretleri genellikle Bitcoin olmak üzere kripto para cinsinden istenir. Fidyenin miktarı birkaç yüz dolardan binlerce dolara kadar değişebilir. Fidye yazılım saldırılarının kurum ve kişilere:

- Hassas veya özel bilgilerin geçici veya kalıcı kaybı,
- Düzenli operasyonların aksaması,
- Sistemleri ve dosyaları geri yüklemek için maruz kalınan mali kayıplar,
- İtibar kaybı gibi birçok olumsuz etkisi vardır.



Fidye yazılım saldırılara başvuran siber tehdit aktörleri arasında siber suç çeteleri ve ulus-devlet destekli hacker grupları bulunmakla beraber pandemi ile birlikte bazı organize suç gruplarının da siber kabiliyetleri bünyesine ekleyerek fidye yazılım saldırılara bir kazanç kapısı olarak başvurdukları gözlemlenmiştir.

Başta Kuzey Kore olmak üzere İran ve Rusya gibi bölgesel ve uluslararası kurumların yaptırımlarına uğrayan devletlerin sıcak nakit akışını sağlamak için kripto para elde etmek amacıyla fidye yazılım saldırılara başvurulduğu bilinmektedir. Bazı ulus devlet destekli fidye yazılım grupları aşağıda sıralanmıştır:

 Bear / Rusya	 Crane / Güney Kore	 Lynx / Gürcistan
 Buffalo / Vietnam	 Kitten / İran	 Panda / Çin
 Chollima / Kuzey Kore	 Leopard / Pakistan	 Tiger / Hindistan



Kaynak: CrowdStrike

2. Fidye Yazılımı ve Gelişimi

Kolluk kuvvetleri başta olmak üzere birçok kurum, fidye yazılım saldırısına uğrayan hedeflerin saldırınlara fidye ödememesi konusunda tavsiye verse de ABD'deki eyalet yönetimleri de dahil olmak üzere birçok kurum saldırınlara fidye vermeyi tercih ediyor. Unutulmaması gereken bir nokta şu ki,



**fidye ödense dahi şifrelenen verilerin
geri alınması mümkün olmayabilir.**

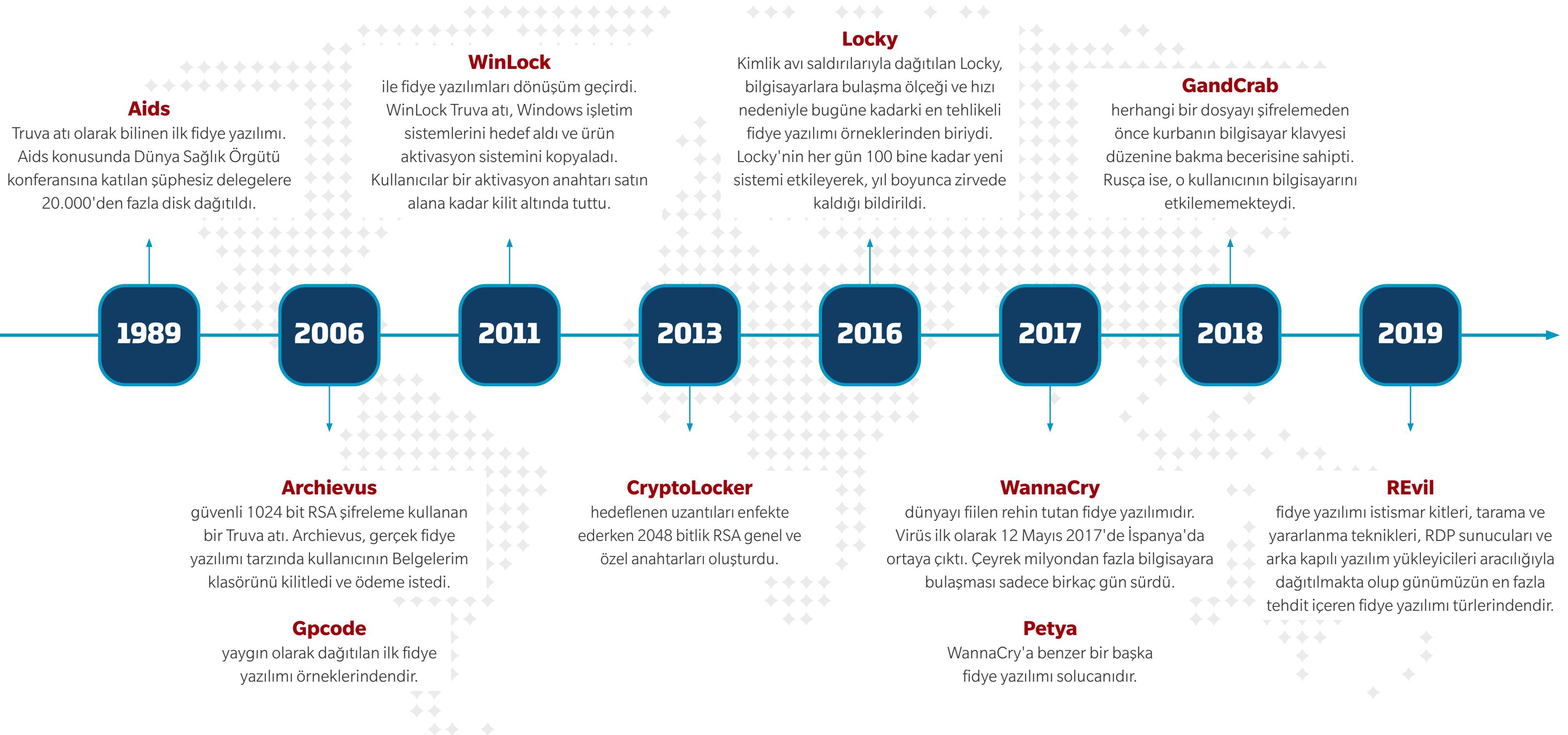
Çünkü siber saldırınların sözlerinde durması için makul bir gerekçe bulunmuyor.

Veriler geri alınsın ya da alınmasın, saldırınlar her zaman güvenliği ihlal edilmiş bir makineden yararlı verileri çıkarmaya çalışırlar. Dahili veya web kaynakları için kullanıcı adları ve parolalar, ödeme bilgileri, kişilerin e-posta adresleri ve daha fazlasını içerebilecek makinedeki tüm hassas veriler ele geçirilebilir.



Fidye yazılımlarında yeni türlerin ortaya çıkışı yavaşladı ancak fidye yazılımı etkisi artan bir saldırı haline geldi. Fidye yazılım saldırının ilk kullanılmaya başlandığı günlerde bilgisayar korsanları çoğunlukla tüketicileri hedef alıyordu. Sonraki süreçte fidye yazılımı çeteleri, işletmeleri hedef alarak çok daha fazla para kazanacaklarını fark etti.

Tehdit aktörleri artık yaklaşımlarında çok daha akıllılar. Kötü amaçlı yazılım, içeri girdikten sonra hacker'ın kurbanları için hangi verilerin en değerli olduğu, ne kadar isteyebilecekleri ve onlara neyi şifreleyebilecekleri konusunda tam bir analiz yapıyorlar.

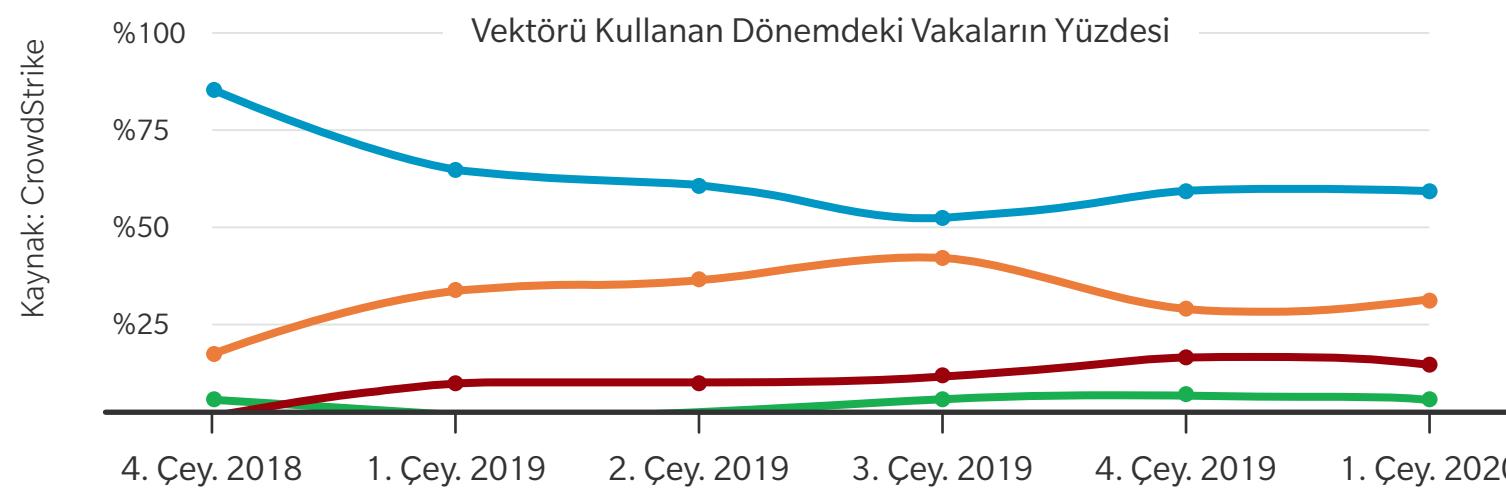


3. Fidyeçilik Saldırı Vektörleri

Fidye yazılımı on yıllarda şirketleri tehdit ettiğinden, beklenmedik bir tehdit olarak değerlendirilmiyor.

Büyük ve küçük kuruluşlar dosya şifreleyen kötü amaçlı yazılımlar tarafından tuzağa düşürülmeye devam ediyor. Yıllar boyunca fidye yazılımı tarafından saldırıya maruz kalmış şirketler incelediğinde, e-posta, kimlik avı saldırıları ve uzak masaüstü protokolü en önemli 3 sebep olarak karşımıza çıkıyor.

■ Uzak Masaüstü Protokolü ■ E-posta Oltalama ■ Güvenlik Açıkları ■ Diğer



3.1 Oltalama Saldırıları

E-posta kimlik avı, fidye yazılımı kampanyaları için hala en önemli saldırı vektörü olma konumunu koruyor. Bunun arkasındaki sebep, kimlik avı e-postalarının gönderilmesinin kolay olması ve saldırganlar için daha hızlı bir yatırım getirisi sağlamasıdır. Sosyal mühendislik planlarının bir parçası olarak kimlik avı, kötü niyetli tehdit aktörünün eylemlerini kurbanları fark etmeden gerçekleştirmesini kolaylaştırır.

3.2 RDP

RDP, bilgi teknolojileri yöneticilerinin sistemlere uzaktan erişim sağlamasına olanak tanıyan yasal bir araçtır. Ancak RDP'nin uç noktalarına erişebilen herhangi bir suçu, bir kurumsal ağda yer edinmek için bağlı sistemleri kullanabilir ve ayrıcalıklarını artırarak birçok başka bağlı sisteme erişmeye çalışabilir. Pandemi süreciyle birlikte evden çalışmaya geçiş, RDP kullanımını %41 oranında artırdı. Tehdit aktörlerinin RDP'ye yönelmesi de yükselişe geçmiş oldu.

3.3 Güvenlik Açıklıkları

Yazılımlardaki güvenlik açıklarının yaması bulunmasına rağmen kapatılmaması fidye yazılım saldırganları için büyük bir fırsat oluşturmaktadır. Büyük fidye yazılım saldırılarının birçoğu bilinen açıklıklardan faydalananlarak gerçekleştirilir.

3.4 Fidye Yazılım Saldırılarına Sebep Olabilecek Diğer Vektörler

- Şahsa ait olmayan veya tanınmayan USB bellek, CD vb. kötüçül medya cihaz kullanımı
- Güvenliği ihlal edilmiş web siteleri
- Enfekte edilmiş dosya indirmeleri
- Zararlı mobil uygulamalar
- Mesajlaşma uygulamaları üzerinden gelen beklenmeyen dosyaların açılması (WhatsApp, Facebook Messenger, vb.)
- Zayıf parola kullanımı
- Zayıf güvenlik politikaları

4. Fidye Yazılımı Saldırı Trendleri - 2020

Pandemi döneminde bir kurbanın ödediği ortalama fidye %60 artış gösterdi.

Siber saldırırganlara karşı verilen mücadelede kritik noktalardan biri de tehdit aktörlerinin operasyonlarını nasıl güncellediklerini ve yöneldikleri değişimleri anlamaktır. 2019 yılın verilerine göre;

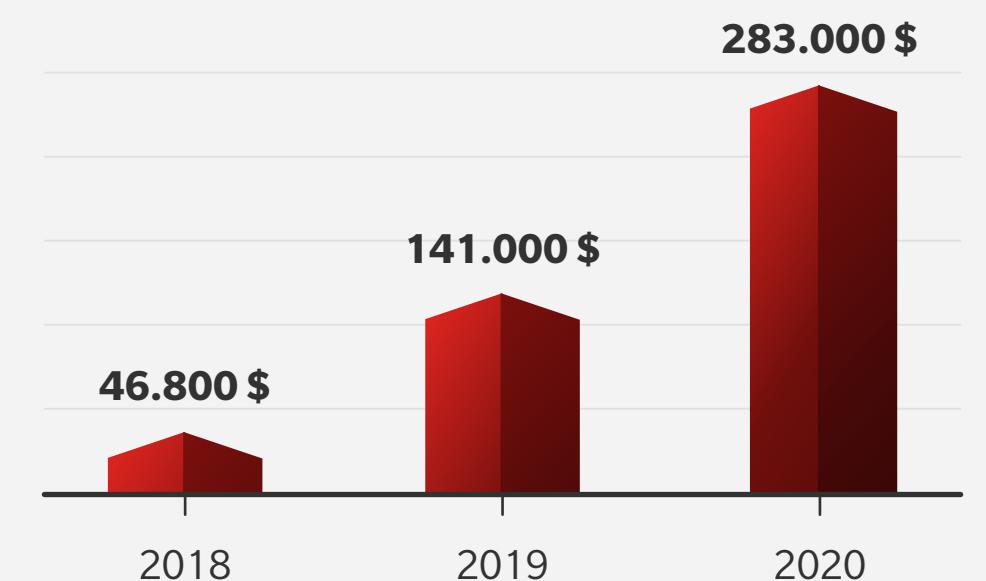
- Kuruluşların **%51**'i fidye yazılım saldırısına uğradı.
- Fidye yazılım saldırılарının **%73**'ü verilerin şifrelenmesi ile sonuçlandı.
- Fidye yazılım kurbanlarının **%26**'sı verilerini siber suçlulara ödeme yaparak geri aldı.
- Fidye ödeyen ancak verilerini geri alamayan kurumların oranı **%1** olarak tespit edildi.
- Kurumların **%56**'sı yedekleme sistemleri sayesinde verilerine erişti.

2020 yılı fidye yazılım saldırıları için bir dönüm noktası oldu. Covid-19 salgını nedeniyle insanların evlerine kapanması, çevrimiçi yapılan işlemlerde büyük bir artıa neden oldu. 2020 yılının birinci ve ikinci çeyreği karşılaştırıldığında, bir kurbanın ödediği ortalama fidye **111.605 dolardan** %60 artarak **178.254 dolara** yükseldi.

4.1 Fidye Saldırısı Nedenli Kesinti Maliyeti

Bilgisayar korsanlarının fidye yazılım kaynaklı siber saldırıları, fidye ödemesi gibi maliyeti yüksek hasarlara neden oluyor. Birçok şirket, bir fidye yazılımı saldırısının sonucu olarak veri kaybının yanı sıra operasyonel aksaklılıklar / kesintiler yaşıyor. Kesinti süreleri, yol açtığı maliyetin yanı sıra müşteri tarafından ciddi bir güven kaybına yol açıyor.

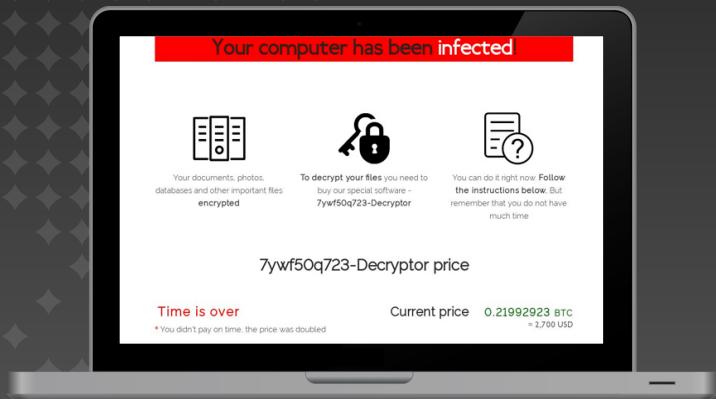
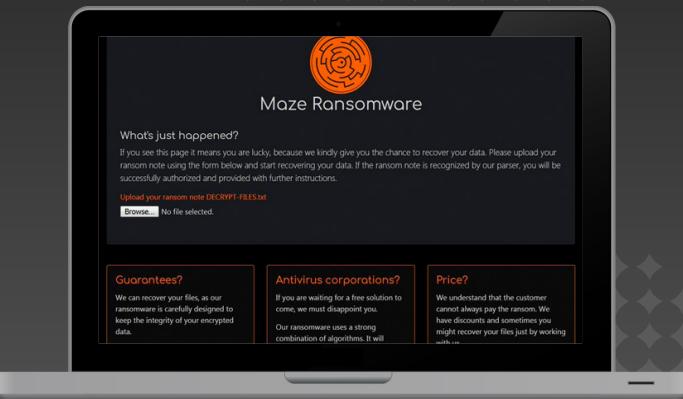
Fidye yazılımının neden olduğu kesinti sürelerinin ortalama maliyetinin 2018'de 46.800 iken 2019'da 141.000 dolara, 2020'de ise 283.800 dolara yükseldiği hesaplandı.



Kaynak: CrowdStrike

4.2

En Tehlikeli 3 Fidye Yazılımı



Maze

2020 fidye yazılım saldırıları listesinde yer alan, yıkıcı etkisi yüksek kötü amaçlı yazılımlardan biridir. Maze fidye yazılımı, hassas verileri herkese açık olarak yayınladığı yeni saldırı yaklaşımı ile ünlenmiştir. Maze fidye yazılımı, tüm dosyaları şifreler ve dosyaların kurtarılması için fidye talebinde bulunur. Mağdurun talep ettiği fidyeyi ödememesi halinde elindeki verileri yayılmamakla tehdit eder.



REvil

REvil, tüm dosyaları şifreleyen ve sisteme sizliğinde kurbandan para talep eden bir dosya şifreleme yazılımıdır. Fidye talebinde suçlular kurbanları Bitcoin üzerinden ödeme yapmaya zorlar. Kurban belirli bir süre içinde fidyeyi ödemezse, fidye oranı iki katına çıkar. Büyük bir hukuk şirketi olan Grubman Shire Meiselas & Sacks vakasındaki veri sızıntısı, bir REvil Ransomware saldırısıydı. Saldırganlar, şirketin ünlü müşterilerine ait verileri ele geçirip bunları Darknet'te paylaştılar.

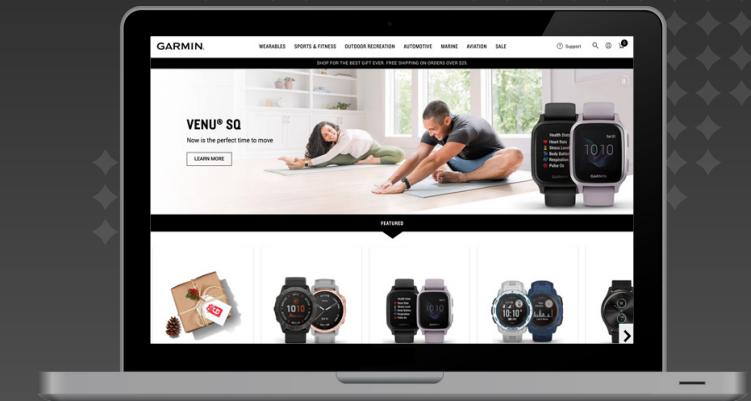
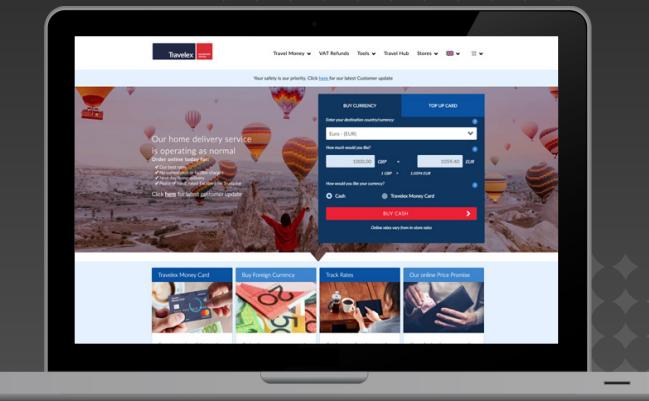


Sodinokibi

Sodin olarak da bilinen Sodinokibi fidye yazılımı, REvil fidye yazılımının farklı bir versiyonunu kullanır. Oracle Weblogic sunucularında sıfırıncı gün güvenlik açığını istismar ederek Eylül 2019'da yayıldı.

4.3

En Büyük 3 Fidye Yazılımı Saldırısı



Çevrimiçi ortamda kullanıcılarına döviz alım-satım hizmeti veren Travelex, 2020 başında fidye yazılımı saldırısına uğradı. Saldırı, şirket kullanıcılarının internet sitesinde ve mobil uygulamada işlem gerçekleştirmesini engelledi. Saldırganların, web sitesini yaklaşık 20 gün sonra kullanıma açabilen şirketten 4,6 milyon Sterlin ödeme talep ettiği ve müşterilerin kişisel verilerini halka açıklamakla tehdit ettiği ortaya çıktı. Travelex'in sistemlerini geri yüklemek için bilgisayar korsanlarına 2,3 milyon Dolar tutarında kripto parayı fidye olarak ödediği kayıtlara geçti.



Fitness teknolojileri geliştiren Garmin şirketi, ürettiği giyilebilir cihazların, uygulamaların, internet sitesinin ve müşteri destek işlevlerinin beş gün süreyle çevrim dışı kalmasına neden olan bir siber saldırıya uğradı. Basına yansyan haberlere göre Garmin, bir üçüncü taraf aracılığıyla saldırganlara yüklü miktarda fidyeyi ödemeyi kabul etti.



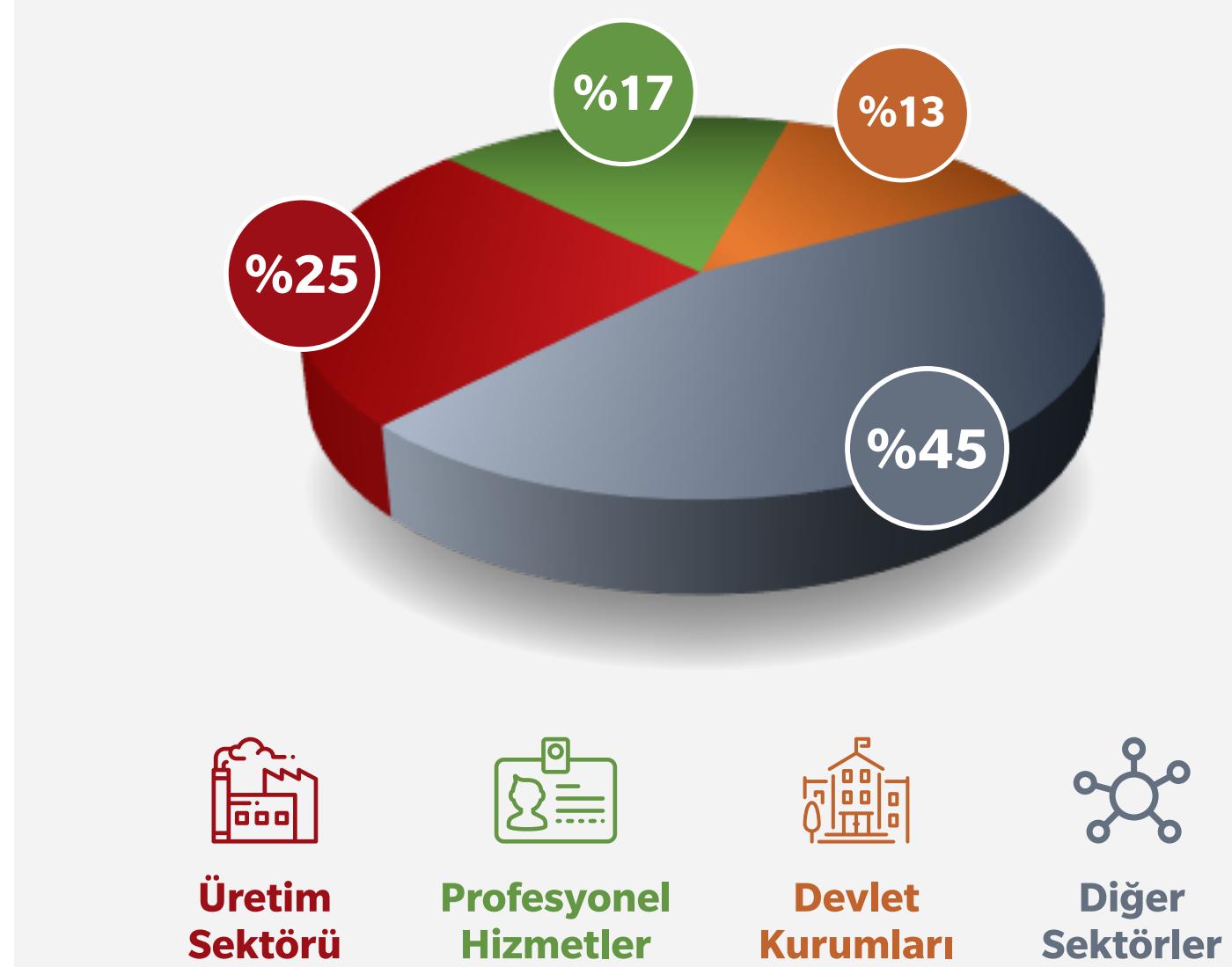
Şirketlere güvenlik ve temizlik gibi alanlarda hizmet sağlayıcı olarak dünya çapında faaliyet gösteren ISS World, 2020 Şubat ayında bir fidye yazılım saldırısına uğradı. Şirket, olayın başında bunun bir zararlı yazılım saldırısı olduğunu açıklayarak geçiştirmeye çalıştı. Ancak şirkete ait 43 bin kurumsal e-posta hesabına erişimin engellendiği haberi medyada hızla yayıldı. Şirketin zarar gören dijital varlıklarını yeniden inşa edebilmesi için 22,5 milyon ile 45 milyon Dolar arasında bir maliyete katlandığı bilinmektedir.

4.4 Fidye Yazılım Saldırılarında Hedef Alınan Endüstriler

Araştırmalar fidye yazılım saldırının hedefleri konusunda sektörel bir seçiciliğe sahip olmadığını gösterse de en fazla zararı oluşturabilecekleri ve fidye ödemek zorunda kalacak olan sektörlerin yöneldiklerini işaret ediyor. Bu sektörlerin başında üretim sektörü geliyor. 2020 yılının istatistiklerine göre, fidye yazılım saldırının yaklaşık dörtte biri üretim sektörünü hedef alıyor.

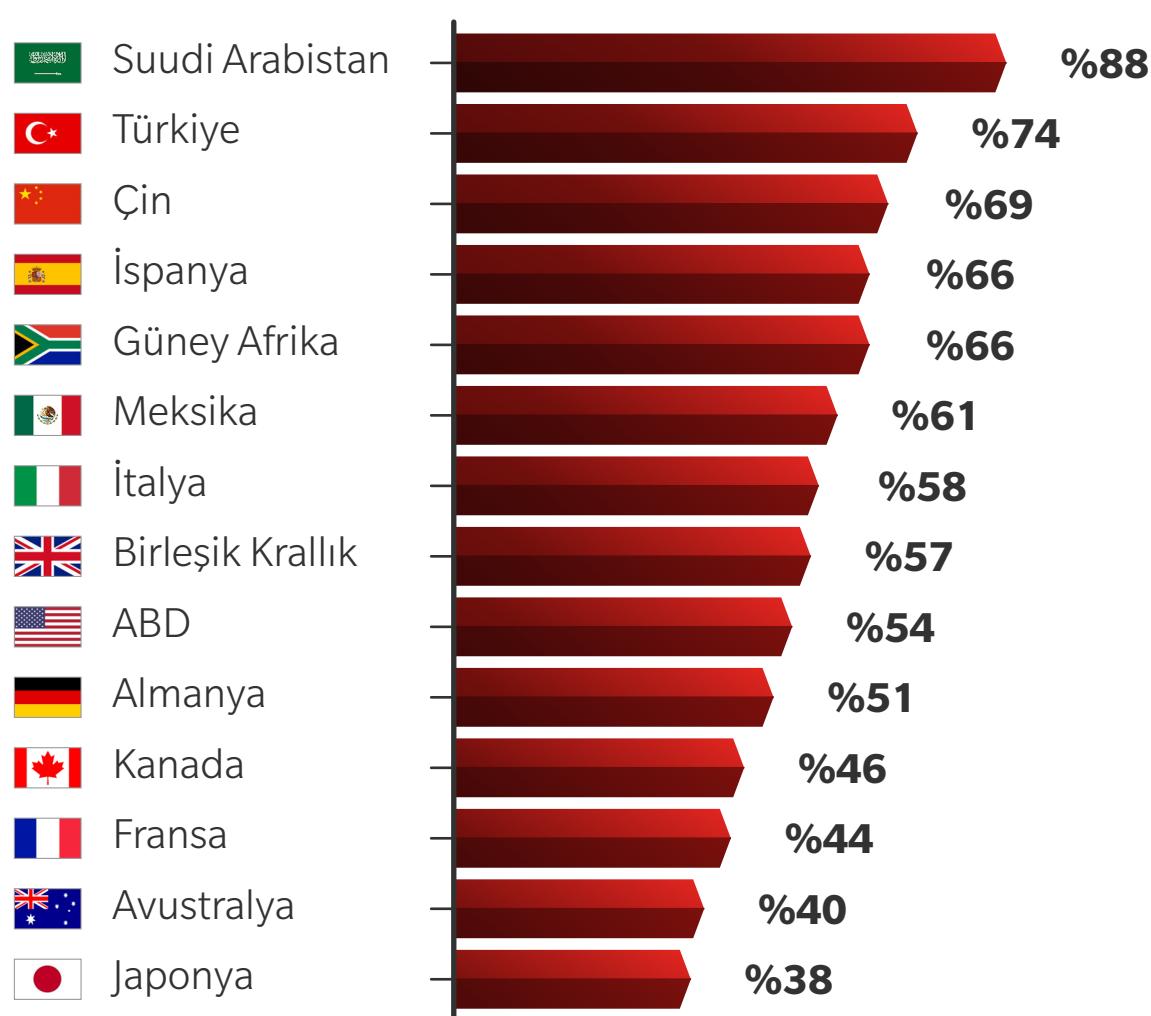
Yandaki grafikte yer alan üç sektörde yapılan saldırılar, fidye yazılımı tehdit aktörlerinin, üretim ağları gibi kesinti sürelerine karşı düşük toleranslı kurbanlara öncelik verdiğiğini gösteriyor. Yüksek çalışma sürelerine ihtiyaç duyan kuruluşlar, üretimin durması nedeniyle her gün milyonlarca dolar kaybetme riski taşıyorlar. Bu nedenle, verilere yeniden erişim elde etmek ve operasyonların devamını sağlamak için fidye ödemeyi kabul edebiliyorlar.

Bu sektörlerde ek olarak, akademik kurumlara yapılan fidye yazılımı saldırılarında da artış gözlemlenmektedir. Covid-19 nedeniyle okullar ve üniversitelerin faaliyetlerini çevrimiçi alana taşımları saldırıcıların bu kurumları hedef almasına yol açmıştır.



4.5 Hedef Ülkeler

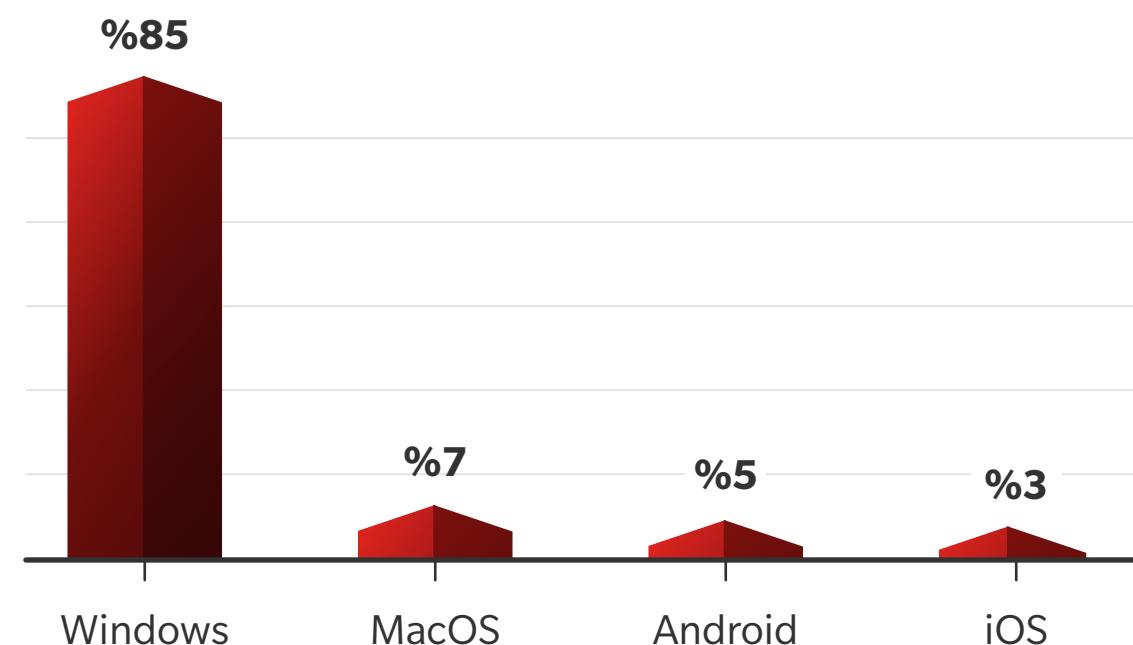
2019 yılı içerisinde güvenilirliklerini, itibarlarını ve dolayısıyla işletmesini riske atan fidye yazılımı saldırısı raporlayan şirketler arasında ilk 3 sırada Suudi Arabistan, Türkiye ve Çin yer almaktadır.



Kaynak: Safetydetectives

4.6 Hedef Sistemler

Windows işletim sistemine sahip bilgisayarlar, daha ekonomik olmaları nedeniyle tüketiciler tarafından daha fazla tercih edilir. Windows tabanlı bilgisayar kullanıcılarının çoğu sistem güncellemelerini yüklemeye ihmalkâr davranır ya da güvenlik açıklarını kapatın yamaları yüklemeyi önemsemeyezler. Böylelikle siber saldırganların harekete geçmesi için uygun şartlar kullanıcılar tarafından oluşturulmuş olur.



Kaynak: Safetydetectives

4.7 Türkiye Fidye Yazılımı Trendleri

2020'nin ilk 5 ayında tespit edilen fidye yazılım saldırısının %26'sından fazlası Türkiye'de gerçekleşti.

Küresel olarak pandemide olduğumuz bu dönemde siber suçlular da dünyanın farklı bölgelerindeki kullanıcıların sistemlerine saldırımıaya devam ediyor. Trend Micro, düzenli olarak küresel siber saldırıları incelediği raporunun 2020 yarıyıl değerlendirmesinde hazırlan ayına kadar tespit edilen fidye yazılım saldırısının yüzde 26'sından fazlasının Türkiye'de gerçekleştiği bilgisini paylaştı.

Buna göre fidye yazılım saldırılarında Türkiye, araştırmadaki diğer ülkeler arasında ilk sırada yer aldı. Türkiye'deki fidye yazılım saldırısının, ilk 5'te yer alan Hindistan, Birleşik Arap Emirlikleri (BAE) ve ABD'nin toplamından daha fazla sayıda olduğu tespit edildi.

SOCRadar analistlerinin yapmış olduğu çalışmaya göre;

Son 3 yılda yaklaşık 280 firmaya fidye yazılım saldırısı gerçekleştirilmiş ve 2020 yılında Kişisel Verileri Koruma Kurumu'nun sitesinde yayınlanan bildirilerimlerin %45'inin fidye yazılım kaynaklı olduğu tespit edilmiştir.

Fidye yazılım saldırısının pandemi sürecindeki başlıca sebebi RDP servislerinden kaynaklanmaktadır. SOCRadar araştırması Türkiye'de RDP servisi açık olan 29,574 sistem tespit etmiştir.

2020'de fidye yazılımı saldırılarında çok sayıda saldırganın kuruluşlara ilk girişi sağlamak için kullandığı iki zayıf dikkat çekmektedir:

CVE-2019-19781: Türkiye'de 33 sistemde tespit edilmiştir.

CVE-2019-11510: Türkiye'de 2 sistemde tespit edilmiştir.

Türkiye'de şirketlere yönelik gerçekleşen fidye yazılım saldırılarında talep edilen en yüksek rakam 24.600.000 TL, en düşük rakam ise 1300 Dolar olarak kaydedilmiştir.

5. Fidye Yazılım Saldırılarından Korunmak İçin 8 Adım

Fidye yazılımı saldırılarının sonuçlarıyla başa çıkmak oldukça zorlu bir süreçtir. Şifreli verileri kurtarmak için tek seçenek talep edilen fidyeyi ödemek gibi görünse de etkilenen verilerin ödeme karşılığında geri alınacağına dair herhangi bir garanti söz konusu değildir.

Bu nedenle devam eden bir fidye yazılım saldırısını tespit etmiş olmak yeterli değildir. İlk etapta fidye yazılımının bulaşmasını önlemeye odaklanmak gereklidir. Bunu aşağıdaki güvenlik önlemlerini takip ederek gerçekleştirebilrsiniz.



1. Dijital varlık envanterinizi çıkartın

Bir fidye yazılımı bulaşmasına karşı korunmak için öncelikle ağınzıaa hangi donanım ve yazılım varlıklarının bağlı olduğunu bilmeniz gereklidir. Farklı departmanların personelleri tarafından dağıtılan ve kullanılan varlıkları da tespit etmek için pasif keşif ile kapsamlı bir varlık envanteri oluşturmalısınız.



2. "Dosya Uzantılarını Göster" özelliğini kullanın

"Dosya Uzantılarını Göster", potansiyel olarak zararlı dosyalardan uzak durabilmeniz için hangi tür dosyaların açılmakta olduğunu kolayca belirlemenize olanak tanıyan yerel bir Windows işlevidir. Bu işlev, dolandırıcıların bir dosyanın iki veya daha fazla uzantıya sahip gibi göründüğü kafa karıştırıcı bir teknik kullanmaya çalıştığı durumlarda yararlıdır.



3. Yazılımınızı yamalayın ve güncel tutun

Bir yama olmadığında, kötü niyetli kişiler işletim sisteminizdeki, tarayıcınızdaki, antivirüs aracınızdaki veya diğer yazılım programlarınızdaki bir güvenlik açığından rahatlıkla yararlanabilir.



4. E-posta kullanıcılarının kimliğini doğrulayın

Kötü niyetli kişilerin e-posta sahtekârlığı tekniklerini kullanmasını önlemek için SPF, DMARC ve DKIM gibi teknolojileri de kullanmalısınız.



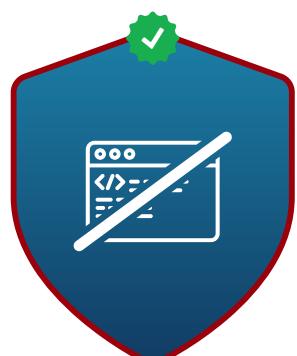
5. Uzak hizmetleri devre dışı bırakın

Uzak Masaüstü Protokolü, saldırı yüzeyini genişletmek ve ağınızda bir yer edinmek için tehdit aktörleri tarafından kullanılabilir. Bu tehdidi engellemek için uzak hizmetleri devre dışı bırakmalısınız.



6. Bilinen kötü niyetli Tor IP adreslerini engelleyin

Tor (The Onion Router) ağ geçitleri, fidye yazılımı tehditlerinin C&C sunucuları ile iletişim kurması için birincil araçlardandır. Bu nedenle, kritik kötü amaçlı işlemlerin geçmesini engellemeye yardımcı olabileceğinden bilinen kötü amaçlı Tor IP adreslerini engelleyebilirsiniz.



7. Windows Script Host'u devre dışı bırakın

Bazı tehdit aktörleri, virüs bulaşmış bir bilgisayarda fidye yazılımı çalıştırmak için VBS dosyalarını (VBScript) kullanır. Zararlı yazılımın bu dosya türünü kullanmasını engellemek için Windows komut dosyası ana bilgisayarını devre dışı bırakmalısınız.



8. Windows PowerShell'i devre dışı bırakın

PowerShell, Windows bilgisayarlara özgü bir görev otomasyon çerçevesidir. Tehdit aktörleri genellikle PowerShell'i bellekten fidye yazılımı çalıştırmak için kullanır ve geleneksel antivirüs çözümleriyle tespit edilmekten kaçmaya yardımcı olur. PowerShell'i iş istasyonlarında devre dışı bırakmak oldukça faydalı olacaktır.

6. Fidye Yazılım Saldırılarında Sigortanın Önemi

Uzman bir brokerlik şirketinden alınan hizmet ile riskin sigortaya transfer edilmesi, kurumları siber saldırırlara karşı daha korunaklı hale getiriyor.

Kurumları maddi ve itibar kayıpları ile karşı karşıya bırakılan zararlı fidye yazılımlarından doğan zararlar ciddi boyutlara ulaşabilmektedir. Bu riskin sigortaya transferinde kullanılan önemli araçlardan biri de siber risk sigortasıdır. Türkiye'de fidye yazılım saldırılarında talep edilen tutarlar 10.000 ila 25 milyon TL arasında değişkenlik göstermekle beraber, fidye bedellerinin ciddi artış göstermesi dikkat çekmektedir.

Siber sigorta hasar taleplerinin büyük çoğunluğunu fidye yazılımı kaynaklı saldırılar oluşturur; bu oran 2020 yılının ilk yarısında %41 seviyesine ulaşmıştır. Sophos'un yaptığı bir araştırmaya katılan şirketlerin %84'ünün siber sigortası bulunmasına rağmen sadece %64'ünün poliçesi fidye yazılım saldırılarından doğan zararları karşılayacak şekilde düzenlenmiştir. Bu sebeple siber sigorta teminatı alırken poliçe içeriklerinin kapsayıcılığına dikkat etmek önem arz etmektedir.



Siber sigorta ile yalnızca fidye yazılımlarına ilişkin ödemeleri değil, aşağıdaki kalemleri de teminat altına almak mümkündür:

✓ **Siber olay müdahale masrafları**

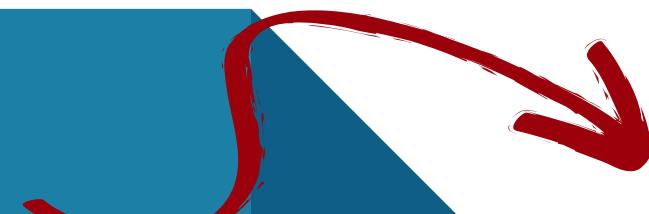
✓ İş durması kaynaklı oluşabilecek kar kaybı

✓ KVKK ve muadili kanunlar kapsamında gizlilik ihlali iddiası ile şirkete kesilebilecek idari para cezaları ve süreçte oluşan savunma masrafları

✓ Verisi ifşa olan bireylerin tazminat talepleri ve savunma masrafları

✓ Veri kaybına ilişkin giderler

✓ Sigortalı şirketin ağ güvenliği sorumluluğu kapsamında 3. taraflarca açılabilecek tazminat davaları ve savunma masrafları



Herhangi bir hasar veya hasara yol açması muhtemel olay / iddia durumunda ilk devreye girecek teminat kalemi **siber olay müdahale masrafları** olacaktır. Müdahale masrafları genel olarak aşağıdaki kalemlerden oluşur:

✓ **Profesyonel bir kurumdan alınacak adli bilişim hizmetleri**

* Sigorta şirketinin anlaşmalı kurumları veya sigortalının tercihleri doğrultusunda poliçeye dahil edilen diğer kurumlar

✓ **Gizlilik mevzuatı uyarınca veri sahiplerine bildirim masrafları**

* KVKK mevzuatına atıf yapılan bildirim masrafları

* Gerekli durumlarda ilave çağrı merkezi hizmetlerine ilişkin maliyetler de dahil

✓ **Hukuki danışmanlık ücretleri**

* Gizlilik mevzuatının ihlali ile ilintili

✓ **Halka ilişkiler ve kriz yönetimi danışmanlık ücretleri**

* İtibar kaybını önlemeye yönelik

✓ **Kişisel veri ihlaline maruz kalan kişiler için ilave hizmetler:**

* Kredi izleme, kimlik hırsızlığı hizmeti masrafları vb.

Sigorta satın alan kurumların poliçe içeriğini aşağıdaki konular açısından test etmesi önem arz eder:

1. İş durmasına bağlı kâr kaybı teminatını tetikleyen hallerin asgaride aşağıdakileri içerecek şekilde yapılandırılması:

- Kötü niyetli bilgisayar eylemi (Hizmet engelleme saldırısı / Kötü amaçlı yazılım / Bilgisayar korsanlığı vb. dahil),
- Yetkisiz erişim ve kullanım,
- İnsan hatası,
- Ağ güvenliği ihlali,
- Programlama hatası,
- Bilgisayar sistemlerinin yukarıda sayılan hallerden korunmak üzere makul ve gerekli olarak kapatılması,
- Sigortalı tarafından kontrol edilen elektrik sistemindeki güç kesintisi, dalgalanma veya azalma

2. Muafiyet tutarı ve iş durması bekleme süresi

3. Poliçede istisna edilen haller

4. Teminat "geriye yürürlük tarihi"

5. Teminat geçerlilik sahası (ABD/Kanada dahil/harici olma durumu)

6. Poliçede yer alan önemli tanımların kapsamı (bilgisayar sistemleri, kötü niyetli bilgisayar eylemi vb.) ve sigortalının faaliyet konusuna uygun şekilde uyarlanması

7. Anlaşmalı danışman kurum paneli ve hasar bildirim yükümlülükleri

8. Elektronik suç unsurlarına ilişkin genişletmeler

Siber sigorta policesinin gerek içerik gerekse teminat limiti bakımından yeterliliği ve kurumunuza uygunluğu dikkatlice test edilmelidir. Sigorta konusunda uzman brokerlik şirketlerinden alacağınız hizmet ile doğru bir satın alma yapabilir, riskin önemli bir kısmını sigortaya transfer ederek kurumunuzu daha korunabilir hale getirebilirsiniz.

7. Öneriler



Her an saldırıyla
uğrayabileceğinizi
varsayıın



Fidye yazılımından
korunmak için ilgili
teknolojilere yatırım
yapın



Siber sigorta
yaptırın ve fidye
yazılımı saldırılarını
kapsadığından
emin olun



Kullanıcılarınızı
eğitin



Siber tehdit
istihbarat
çözümlerini
kullanın

8. Fidye Yazılım Saldırısına Başınıza Geldiğinde Ne Yapmalısınız?

Fidye yazılım saldırısına uğradığınızda cihazınızdaki dijital dosyalar saldırırganlar tarafından şifrelenir. Şifreyi almak için fidye ödemenizi isteyen saldırınlara ödeme yapmanız halinde bile dosyalarınızı geri alacağınızı dair bir garanti söz konusu değildir.

Saldırıya uğradığınızda ne yapmanız gerekiğine dair somut önerilerin bulunduğu Europol ve bazı siber güvenlik şirketleri tarafından hazırlanan **No More Ransom** sitesi size yardımcı olacaktır.



<https://www.nomoreransom.org/tu/index.html>



Kaynakça

The State of Ransomware 2020 | Sophos

<https://www.sophos.com/en-us/mediabinary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf>

The State of Ransomware in 2020 | Blackfog

<https://www.blackfog.com/the-state-of-ransomware-in-2020/>

Global Surges in Ransomware Attacks | Check Point

<https://blog.checkpoint.com/2020/10/06/study-global-rise-in-ransomware-attacks/>

ENISA Threat Landscape 2020 | Ransomware

<https://www.enisa.europa.eu/publications/ransomware>

Quarterly Ransomware Report | Coveware

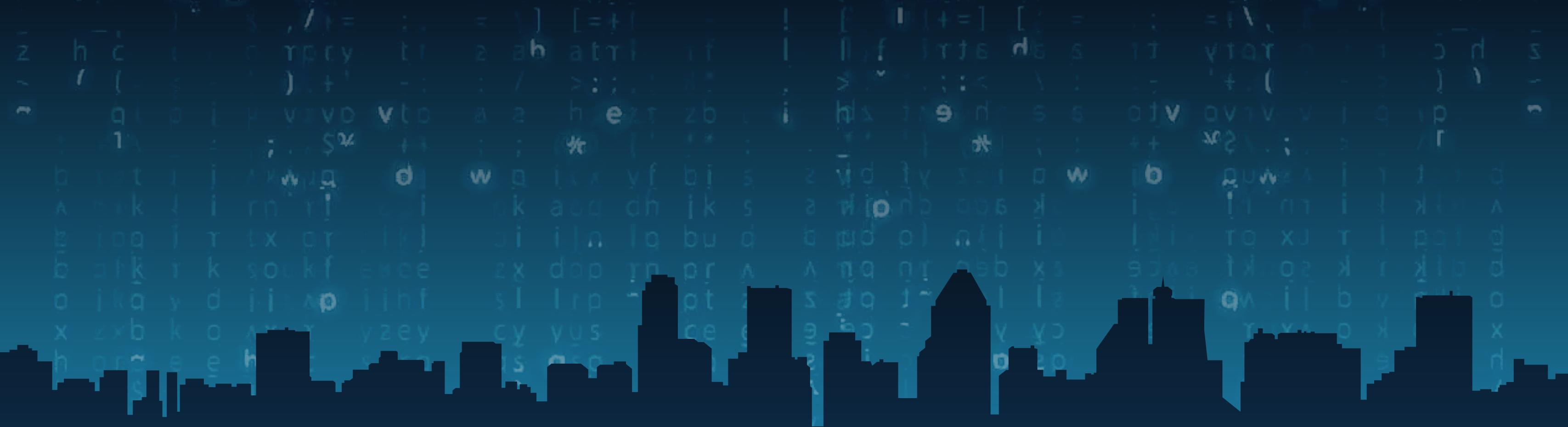
<https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report>

2020 Global Threat Report | CrowdStrike

<https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report>

Ransomware Facts, Trends & Statistics for 2020 | SafetyDetectives

<https://www.safetydetectives.com/blog/ransomware-statistics/>



INTEGRA
SIGORTA BROKERİ

İNTEGRA SIGORTA VE REASÜRANS BROKERLİĞİ A.Ş.

Cengiz Topel Cad. Le Meridien Plaza, No:39 K:3 Etiler
Beşiktaş 34377 İstanbul

Telefon : +90 (212) 708 67 00
Faks : +90 (850) 219 99 37

info@integrabroker.com
www.integrabroker.com



BGA
SECURITY

BGA BİLGİ GÜVENLİĞİ A.Ş.

İçerenköy Mah. Topçu İbrahim Sok. AND Plaza No:8 -10D
Ataşehir-İstanbul

Telefon : +90 (216) 474 00 38
Faks : +90 (216) 474 93 86

bilgi@bga.com.tr
www.bga.com.tr