PERKANECİLİK İLE İLGİLİ ESET SEKTÖR RAPORU:

Veri ve ödemelere karşı gelişen tehditler

İÇİNDEKİLER

1

PERAKENDECİLİK İLE VERİ VE ÖDEMELERE KARŞI GELİŞEN TEHDİTLER

Brent McCarty
ESET Kuzey Amerika Başkanı

Teknolojinin benimsenmesinin ve tehditlerin baskısı altında dönüşen perakendecilik

2020 baharının başlarında, dünya genelinde alıcılar ve satıcılar, on yıldır yükselişte olan perakende sektörünün aniden ortaya çıkan bilinmez bir olayla karşılaşmasına tanıklık etti: SARS-CoV-2 veya COVID-19. Evlerdeki, iş yerlerindeki, sokaklardaki ve mağazalardaki alışkanlıkları değiştiren İspanyol gribinden bu yana perakende pazarları ve tüketici alışkanlıkları bir virüsten bu denli etkilenmemişti.

Ancak günümüzde bu virüs, sanal pazar yerlerini etkilemenin yanı sıra dijitalleşmenin dönüştürücü döneminin ortasında olmamıza rağmen çevrim içi ortamı ve çevrim içi davranışlarımızı da değiştirdi. Bazı sorular akla geliyor: Perakende sektöründeki bu kesintiler, mevcut dijitalleşme seviyesi açısından ne anlama geliyor? Dijitalleşmenin etkileri sağlam temellere mi dayanıyor? Perakendeciler, BT altyapısının ve e-ticaretin sunduğu fırsatlar ve riskler arasında nasıl bir denge kurmalıdır? Ve siber güvenlik, perakende sektöründeki değişimi anlamamıza veya fikirlerimizi değiştirmemize yardımcı olur mu?

Müşterilerin, satıcıların, pazarlamacıların, tedarikçilerin ve perakende sektörünün bir kesiti olarak ödeme işlemcilerinin ilgili çevrim içi davranışlarını değerlendirerek bu yeni dinamikteki tehditleri daha iyi anlayabiliriz. Başka bir deyişle, perakende sektörünün hayatta kalma ve gelişme arayışı göz önüne alındığında, hangi siber güvenlik riskleri artış gösterdi ve hangileri perakendecilere yeni fırsatlar sundu? Bu raporun amacı, siber suçluların kendilerini yeni perakende ortamında daha iyi konumlandırmak için nasıl geliştirdiğini göstermektir.

Ofisteki dönüşüm...

2021 yılında birçok yerde pandeminin en kötü ticari etkilerinde somut bir rahatlama görüldü: Birçok dükkan, restoran ve otel yeniden açıldı. Ancak iş yerlerine dönen, dışarıda yemek yiyen, birebir eğitim alan ve fiziksel alışveriş yapan kişilerin sayısı aynı oranda olmadı.

Bunu büyük ölçüde toplu yaşamın riskleriyle ilgili bilgilenmemizi sağlayan toplum sağlığı yetkilileri ve tıp araştırmacılarına borçluyuz. Ancak değişen diğer bir konu ise 2020 yılında denenen ve başarılı olan dijital çözümlerin popüler hale gelmesidir. Bu dijital çözümler, bir çok şirketin ve perakende hizmetin yeniden şekillenmesine ve yeni bir kılığa bürünmesine olanak tanıdı. İster kurumsal bir şirket çalışanı olalım ister bir girişimci, "birçoğumuz" arka alanda bunun kanıtlarını görüyoruz. İşin büyük bir kısmı *Microsoft Teams* ve *Zoom görüşmelerine* taşındı ve Kaseya gibi verimlilik ve iş birliği araçları her yerde kullanılır oldu. Ancak işletmelerle ilgili bu teknolojiler, beraberinde kendi risklerini de getirdi.

Önde gelen kurumsal platformlar arasında yer alan e-posta hizmeti Microsoft Exchange ve BT yönetimi için Kaseya VSA *2021 yılının başlarında hedef alındı* ve bu saldırıların sonuçları dünya genelinde hala hIISediliyor. Bu kesintiler, kurumsal perakendeciler dahil çeşitli alanlardaki birçok şirketin sürekliliğini etkiledi. ESET ve daha yaygın güvenlik sektörü fidye yazılım, verilerin dışarı sızdırılması ve diğer kesintiler gibi sonraki etkilerini belgelendirdi.

Bu geniş çaplı saldırıların etkileriyle ilgili daha ayrıntılı bilgi almak için kaynaklara *buradan* göz atabilir, fidye yazılımları ile bilgileri *burada* bulabilir veya tehdit ortamıyla ilgili anketimizi incelemek için *buradan Tehdit Raporu T2*'ye erişebilirsiniz.

... ve daha fazlası

Perakendecilerin idari ofislerini etkileyen değişen tehdit ortamının yanı sıra sorunlar mağazaları da etkiliyor. Çevrim içi perakende, doğrudan satış, nakliye ve gıda dağıtımındaki büyük artışla birlikte, benzersiz zorluklar perakende sektörünün pazarlama, satış ve ödemeler ile birlikte mağaza BT ortamı ve bununla ilgili araçlar, uygulamalar ve süreçler yoluyla risklere maruz kalmasına neden oluyor. 2021'deki siber güvenlik ortamının müşteri veritabanlarının, satış noktası (POS) cihazlarının, pazarlama otomasyon araçlarının, web arama optimizasyon araçlarının yanı sıra kredi ve banka kartı dolandırıcılığına ve veri hırsızlığına en açık uçlar olan ödeme işlem platformları ve hizmetleri açısından büyük şirketlerden küçük girişimlere kadar önemli etkileri olmuştur. Risklerle ilgili bir örnek vermek gerekirse, önde gelen İsveç süpermarketler zinciri Coop dahil birçok perakendeci 2021 Ocak ayında *Kaseya tedarik zinciri saldırısına* uğradı.

Yeni teknoloji, güvenlik konusunda değişmeyen odak

Büyük ve küçük perakendeciler yeni teknolojiyi benimserken veya sürekli olgunlaşan iş platformlarında daha fazla yer almaya başlarken, riskler giderek artıyor. Bu rapor kötü amaçlı kişilerin neden olabileceği yazılım ve BT altyapısı risklerine büyük ölçüde yer veriyor. Ancak ele alınması gereken diğer bir hassas konu ise süreçlerin, teknoloji kullanımının ve platform yönetiminin barındırdığı risklerle ilgilidir.

Veri koruma düzenlemelerine daha sonra değineceğiz ancak güvenlik yazılımları, veritabanlarını ve veritabanlarına erişimi koruma konusunda büyük bir rol oynasa da en iyi uygulamaları kullanmanın ve doğru yapılandırmaların çok önemli olduğunu da vurgulamalıyız. Bu, özellikle perakende sektöründeki *birçok soruna neden olabilecek BT yöneticileri* başta olmak üzere hoşnutsuz *çalışanlar* konusunu ele almak açısından önemlidir. Daha somut olmak gerekirse, büyük şirketler pazarlama kampanyalarında ve satış takibinde kullanılan büyük veri tabanlarını yönetmek üzere HubSpot, Adobe Campaign veya Eloqua gibi ürünlerden yararlanır. Ancak başlı başına karmaşık olan bu araçlar, fırsatları güvence altına almanın yanı sıra riskleri de arttırır. Güvenlik yazılımlarının dağıtımına gösterilen özenin yanı sıra Oracle'ın *Eloqua yöneticileri* için yayınladığı yapılandırma literatüründe değindiği üzere, sistem derinlemesine bir bakış ile güçlendirilmelidir.

Çalışanlar, kullanılan ve ihmal edilen yazılımlar gibi içeriden ve dışarıdan kaynaklanan risklerin çok daha fazla olduğu 2022 yılında, siber güvenlik, fırsatları güvence sağlamak için gereklidir. Yeni yıl, Kara Cuma veya Noel gibi kampanya zamanlarını bir düşünün. Bugünlerde dönüşen perakende ortamından teknoloji ile daha fazla yararlanmaya çalışan, hem fiziksel hem de çevrim içi mağazalar olduğunu görüyoruz. Bu durum aynı zamanda değer zinciri boyunca daha fazla oyuncunun, yukarıda bahsedilen "genel" dijital iş çözümlerine ve perakende tabanlı şirketleri müşterilerine bağlayan ve mal ve hizmet alışverişine imkan tanıyan daha yeni teknoloji katmanlarına yatırım yaptığı anlamına da geliyor.

Siber güvenliğin bu teknolojilerin bazılarındaki etkilerine göz atalım.

2

E-TİCARET SİBER SUÇU: ELE GEÇİRİLECEK KREDİ KARTI HAZİNE SANDIKLARI

Martin Kováč

Küresel Dijital Şirketler Direktörü

Ödemeleri çevrim içi almak, parayı siber çetelerle ve tehlikelerle dolu internetin Vahşi Batısı'ndan geçirmeyi gerektirir.

Paranın olduğu her yerde dolandırıcılık da vardır

Pandemiden önce de ödeme teknolojisindeki inovasyonlar, e-ticarete yönelimi artırmış durumdaydı. Ödeme uygulamalarından dijital cüzdanlara ve web sayfası eklentilerine kadar e-ticaret çağı, siber suç çetelerine para kazanmak için yeni dijital kanallar açtı. Ayrıca e-ticareti destekleyen yeni teknolojilerin yayılması her zaman en güvenli uygulamaların da beraberinde kullanıldığı anlamına gelmiyor. Birçok durumda pandemi kaynaklı kısıtlamalar, bu yayılmaları hızlandırdı.

Aynı zamanda, finansal kazançla motive olan siber suçlular, ganimet elde edebilecekleri bir güvenlik açığı için e-ticaret sistemlerinin her köşesinde avlanıyor. Ödemeleri çevrim içi almak, parayı siber çetelerle ve tehlikelerle dolu internetin Vahşi Batısı'ndan geçirmeyi gerektirir.

Hesap bilgileri, kredi ve banka kartı bilgileri ve müşteri bilgilerinin peşine düşen bu dolandırıcılar özellikle çevrim içi perakendeciler için bir tehdittir. Ancak, satış noktası (POS) yazılımı yoluyla mağazada kartla ödeme kabul eden perakendeciler için de aynı riskler söz konusudur. POS yazılımı genellikle bilgisayarlar üzerinden çalışır ve bu bilgisayarlar güvenli olmayan yapılandırmalarla internete bağlıdır. Dolayısıyla gerçek anlamda faaliyet gösteren şirketleri hedef almak yerine e-ticaret web sayfalarını hedef almaya bir geçiş söz konusu olmasına rağmen POS sistemlerine yönelik tehditler halen vardır ve tüm perakende şirketlerin bunlardan ders çıkarması gerekir. Bu nedenle günümüzdeki e-ticaret sistemlerinin karşılaştığı tehditlere yönelmeden önce POS kötü amaçlı yazılımlarına kısaca bir göz atalım.

Tehdit ortamındaki değişim: POS'tan e-ticaret yazılımına

Kredi kartı pazarının büyümesiyle POS yazılımı, perakende şirketlerde ödemelerin ele alınmasıyla ilgili ön sıralarda yer almaya başladı. Ancak her yeni teknolojide olduğu gibi güvenlik uygulamaları, daha sonra ele alındı. 2013 yılında Target'ın ve 2014 yılında Home Depot'un POS sistemlerine düzenlenen büyük ölçekli *saldırılar* sonrasında sektör, perakendecilerin güvenlik uygulamalarını iyileştirilmesi gerektiğinin farkına vardı ve dolayısıyla POS sistemlerini güvenceye almak için birçok çalışma yapıldı. Ancak 2021 yılına gelindiğinde İsveç'teki Coop süpermarketi Kaseya fidye yazılım saldırısı sonrasında *500 mağazasını kapattı*. Bu saldırıda tedarik zincirinde üst sırada yer alan bir hizmet sağlayıcının sistemi ele geçirildi ve Coop'un bazı POS sistemlerinin işlevleri kesintiye uğradı. Tedarik zincirindeki tüm yazılımın yanı sıra ödeme yazılımını güvende tutmak kaçınılmaz bir ihtiyaçtır.

Target ve Home Depot örneklerinde olduğu gibi POS sistemlerine yönelik kötü amaçlı yazılımın dağıtımı, üçüncü tarafların perakende ağlarına sağladığı erişimin ihlal edilmesiyle gerçekleşti. Bu ihlaller, çalınan bilgilerin işe yaramamasını sağlayan *çok faktörlü kimlik doğrulama* gibi sağlam kimlik doğrulama uygulamalarına duyulan ihtiyacı ortaya koydu. Ayrıca bu ihlaller, ağ segmentasyonunun, saldırganın daha az hassas bir alandan POS sisteminin bulunduğu yer gibi daha değerli bilgilere sahip bir alana yönelmesini durdurabileceğini de gösterdi.

Coop örneğinde ise meydana gelen, Coop'un POS sistemlerinin bağlı olduğu bir hizmet sağlayıcı tarafından kullanılan ve güvenlik açığına sahip bir BT yönetim aracı olan Kaseya VSA'nın suistimal edilmesiyle ortaya çıkan bir ödeme hizmeti kesintisiydi. Tüm BT hizmetlerinin gözlemlenmesinin ve yönetiminin şirket içinde yapılması haricinde bu gibi kesintileri önlemek için yapılabilecek bir şey yoktur. Diğer durumlarda, çok hızlı yama uygulamalarına sahip olmak (ancak yama hala geliştirilmekte olduğu için Kaseya VSA durumunda bu yardımcı olmazdı) ve bir saldırının en erken belirtilerini algılayabilen *ESET Enterprise Inspector* gibi bir uç nokta algılama ve tepki çözümüne sahip olmak çok önemlidir.

Günümüzde, POS sistem güvenliği tarihindeki bilinen bu saldırıların yanı sıra birçok farklı tehdit bulunmaktadır. Örneğin 2020 yılında ESET araştırmacıları dünya genelinde yüz binlerce barda, restoranda, otelde ve konaklama tesisinde kullanılan belli bir Oracle POS yönetim yazılımı ürününü yürüten cihazlarda saklanan hassas bilgilere erişim sağlayabilen ModPipe adlı arka kapıyı keşfetmiştir. *ESET Endpoint Security* gibi en iyi güvenlik uygulamaları, çok katmanlı uç nokta korumaya sahiptir. *ModPipe* gibi kötü amaçlı yazılımları algılayabilir ve tüm cihazların her zaman güncel işletim sistemine ve yazılıma sahip olmasını sağlar.

Bazı perakende işletmelerinin 2021'de hala desteklenmeyen işletim sistemleri kullanması şaşırtıcı olabilir; örneğin, Birleşik Krallık'ta 2014 yılında kullanım ömrünün sonuna ulaşan Windows XP kullanan ve üzerinde POS yazılımı çalıştıran *önde gelen bir golf kulübü gibi*.

POS cihazlarındaki tüm finansal ve hassas veriler göz önünde bulundurulduğunda, bu cihazların hedef alınması durumunda *GDRP uyarınca büyük sorunlar* dahil olmak üzere oldukça tehlikeli sonuçlar doğurabilir.

Yönetmelik açısından baktığımızda 17 Nisan'da Otomatik Benzin Pompaları için *EMV sorumluluk değişikliğinin* yürürlüğe girmesiyle 2021 yılında ABD'deki benzin perakendecileri üzerinde daha fazla baskı oluşmuştur. 2015'ten beri yürürlükte olan bu yönetmelik ile kredi kartı dolandırıcılığıyla ilgili sorumluluğu American Express, Discover, Mastercard ve Visa gibi büyük kredi kartı şirketleri yerine EMV çip kullanmak veya PIN girmek yerine *manyetik şeridi* kaydırarak kart ödemesi kabul etmeye devam eden perakendeciler üstleniyor.

Düzenleme, EMV çip kullanımının sunduğu artan güvenliği yansıtmak için yarar sağlarken, Apple Pay ve Google Pay gibi teknolojiler, ödeme güvenliğindeki inovasyonlarla ilerleme kaydetmiş durumda. Bu hizmetleri kullanırken tüccarlar gerçek kredi kartı numaralarına gerek duymuyor; onun yerine her ödemede oluşturulan sanal hesap numaraları kullanılıyor. Bu sayede Apple Pay ve Google Pay, EMV çipe ve PIN'e sahip gerçek bir kredi kartından *bile daha güvenli seçeneklerdir*.

Bir e-ticaret şantajı

E-ticarete geri dönecek olursak, 2018'de *Ticketmaster UK* ve *British Airways* web sitelerinden yüz binlerce ödeme kartı kaydının kopyalandığını duyduğumuzda, Target ve Home Depot ihlallerine benzer, sektörü harekete geçiren bir deneyimle karşılaşıyoruz. Bu web siteleri, usta bir şekilde ödeme kartı çalmaya yönelik birçok kötü amaçlı yazılımın tuzağına düşenler arasında ilk sıralarda yer alıyordu.

Kart hırsızlarının ortak bir yöntemi, web sitesi müşterileri satın aldıkları ürünler için ödeme yaparken müşterilerin ödeme verilerini çalabilen komut dosyalarını yasal web sitelerine enjekte etmektir. 2020 yılında Keeper olarak bilinen bir siber suç grubu, dünya çapında 55 ülkede *570'ten fazla şirketin* web sitesine sızmıştır. 2020 yılındaki bir diğer saldırıda ise, Magecart çeteleri kötü amaçlı bir kopyalama yazılımı ile popüler bir e-ticaret platformu olan Magento'yu kullanan *2.800'den fazla çevrim içi mağazayı* mağdur etti.

Pandeminin bir sonucu olarak birçok şirketin e-ticarete geçmeye ihtiyaç duyduğunu ve tüketicilerin çevrim içi alışverişlerindeki artışı göz önünde bulundurduğumuzda, çevrim içi gelir de doğal olarak artış göstermekte. Çevrim içi mağaza oluşturmak için kullanılan başka bir popüler platform Shopify, 2020'nin ikinci çeyreğinde *gelirini neredeyse ikiye katladı*. Deloitte'un *analizine* göre, bu artışın nedenlerinden biri de pandemide çevrim içi satın almanın sunduğu kolaylıklar için müşterilerin daha fazla ödemeye istekli olmasıdır. Bu nedenle, e-ticaret yeteneklerini geliştirebilen şirketler, pazarda rekabet avantajını elinde bulundurarak stratejik olarak üst sıralara ilerleyebilir. Kazanç nedir? Bu kadar yüksek potansiyelde para akışı, finansal olarak motive olan suçlular için de güçlü bir mıknatıs görevi görür.

IIStealer: E-ticaret işlem verilerini yakalama

Son birkaç yılda e-ticaret web siteleri yoluyla kredi ve banka kartı verilerini ele geçirmek üzere birçok hile ve araç tespit edildi. Kart çalmak üzere kullanılan kötü amaçlı yazılımlar, *CSS dosyalarında*, *sosyal medya paylaşım simgelerinde* ve *site ikonu meta verilerinde* bile bulunuyor. Ancak kötü amaçlı aktörlerin yaratıcı yöntemlerine rağmen, birçok satıcı ve şirket bu tehditlerin öneminin farkında değil. Kredi kartı sahipleri olarak kredi kartı faturalarında yetki dışı işlemler görene veya BT yöneticileri olarak şirket sunucularında güvenlik anormallikleri keşfedene kadar birçok çevrim içi kredi kartı hırsızlığı hiç fark edilmeyebiliyor. Bu durum, e-ticaret sunucularına sızarak kredi kartı bilgilerini çalan ve en sinsi kötü amaçlı yazılım örneklerinden biri olan *IIStealer* için de geçerlidir.

ESET araştırmacıları tarafından keşfedilen IIStealer, ürünler için ödemek yapmak üzere HTTP POST talepleri için web sitesinin ziyaretçi trafiğini izler. Kötü amaçlı yazılım, bu taleplerden elde ettiği bilgileri (kredi kartı bilgileri gibi) daha sonra ihlal edilen sunucudan almak üzere bir günlük dosyasına kaydeder. Aynı zamanda, web sitesi, alışveriş yapanlardan beklendiği üzere ürünler için ödeme yapması için HTTP yanıtları oluşturmaya devam eder.

Kaydedilen verileri almak için kötü amaçlı yazılım operatörleri, ihlal edilen sunucuya ustaca gizlenmiş bir HTTP talep gönderir; bu talep IIStealer'dan toplanan verileri bu talebe yanıt olarak HTTP yanıtında gömülü şekilde iletmesini ister. HTTP kullanarak IIStealer, web sitesi ziyaretçileri tarafından paylaşılan kredi kartı bilgilerini ele geçirirken, BT yöneticilerinin bir şeylerin ters gittiğini anlaması neredeyse imkansızdır. Çalınan verilerin yasal web sitesi trafiği içerisinde gizlenmesine yönelik bu hile yaygın değildir. Başka kötü amaçlı yazılımlar tarafından kullanılan bir diğer hile ise *dışarı sızdırılacak verilerin JPG dosyalarında gizlenmesidir*. Bu hilede yalnızca web sitesinden resimler indiriliyormuş gibi bir izlenim uyandırılır.

HTTPS kullanan web sitelerinde tarayıcının adres çubuğunda yer alan *kilit* işaretini hatırlıyor musunuz? Bu işaret, web sitesinin trafiğini SSL/TLS şifreleme ile korumak içindir. Ancak bu, IIStealer'a karşı koruma sağlamaz, çünkü IIStealer sunucudan bilgi almadan önce taleplerin sunucu tarafından deşifre edilmesini bekler.

Müşteriler açısından baktığımızda, alışveriş yaptıkları e-ticaret web sitesinin IIStealer gibi sunucu tarafında yer alan bir kötü amaçlı yazılımdan etkilenip etkilenmediğinin bilmenin bir yolu yoktur. Ödeme verilerini ele alma konusunda güvenilirliği olmayan bir web sitesi yerine güvenilir üçüncü taraf ödeme noktası kullanmak daha iyi bir seçenektir.

Şirket açısından baktığımızda ise ziyaretçilerin ödeme bilgilerini korumak bir öncelik olmalıdır. E-ticaret web sitelerine ödeme noktası entegre ederek bunu yapabilirler. Diğer birçok *seçeneğin* yanı sıra PayPal, Apple Pay, Google Pay, Amazon Pay ve Alipay gibi seçenekler de vardır.

Güvenlik açıkları ve kimlik avı hırsızlıkları

Ancak bu ödeme hizmetlerinden birini kullanmak, hırsızlık tehdidi alan değiştirdiği için hırsızlık tehdidini tamamen ortadan kaldırmaz. Siber suçlular, bazı ödeme hizmetlerinin sahip olduğu itibarın farkındadır; bu durum en popüler markaların genellikle kötü niyetli kampanyalar için bir kılıf olarak kötüye kullanılması anlamına gelir. Bu nedenle, tüccarlar ve müşteriler paralarını korumak üzere birçok *dolandırıcılık* ve *kimliğe bürünme* taktiğinin farkında olmalıdır.

Alıcılar ve satıcılar için yaygın bir tehdit, *en çok taklit edilen markalardan biri olan* PayPal kılığına girerek kimlik avı hırsızlığıdır. Kimlik avı hırsızlığı, popüler bir ödeme hizmeti gibi bir e-posta veya *SMS metin mesajı* göndererek "hesabınızda alışılmadık bir etkinlik" olduğunun iddia edilmesiyle başlar. En iyi yöntem bu bağlantılardan hiçbirine tıklamamaktır ve mesajın doğruluğunu onaylamak üzere doğrudan hizmet sağlayıcı ile iletişime geçmektir.

Ayrıca tüccarlar da seçtikleri e-ticaret eklentisini etkileyebilecek birçok güvenlik açığı bulunduğunun farkında olmalıdır. 2020 yılında saldırganlar *WooCommerce'teki güvenlik açıklarını* (popüler bir WordPress eklentisi ve web siteleri için e-ticaret motoru) suistimal etti. Bu sayede diğer WordPress hedeflerini tarama olanağına sahip oldular ve web sitesinin veri tabanına bağlanarak toplam sipariş ve ödeme sayısı gibi WooCommerce ile ilgili verileri sorgulamak için bu veri tabanından yararlandılar.

Sunucu güvenliğiyle ilgili ipuçları

E-ticaretin günümüzde karşılaştığı tehditleri göz önünde bulundurarak, e-ticaret sunucunuzu korumaya yardımcı olmak üzere aşağıda bazı ipuçlarına yer veriyoruz:

- Sunucunun yönetimi için *sağlam ve eşsiz parolalara sahip*, bu amaca yönelik hesaplar kullanın.
- Daha fazla koruma için tüm yönetimsel ve ayrıcalıklı hesaplarda *çok faktörlü kimlik doğrulama* kullanılmasını sağlayın.
- İşletim sisteminizi ve uygulamalarınızı düzenli olarak güncelleyin ve sunucu ihlali riskini azaltmak amacıyla hangi hizmetlerin internete açık olduğu konusunda dikkatli olun.
- Hırsızlar için kullanışsız hale gelmesini sağlamak üzere sakladığınız müşteri verilerini *şifreleme* ile koruyun.
- Sunucunuzda *ESET Server Security* gibi bir güvenlik çözümünün yanı sıra İnternet uygulamaları için güvenlik duvarı kullanmayı düşünün.

3

IISTEALER: ÇEVRİM İÇİ SATICILAR VE ALICILAR ARASINDAKİ GÜVEN İLİŞKİSİNİN TEHLİKEYE GİRMESİ

Zuzana Hromcová
Kötü Amaçlı Yazılım Araştırmacısı

Ne yazık ki internet kullanıcılarının şüpheli web sitelerinden uzak durma ve web sitelerinin SSL/TLS şifreleme ile korunduğunu doğrulaması gibi doğru davranışları, IIStealer'dan kaçınmak için yeterli değildir.

Bu raporda değinilen eşsiz tehditlerden biri IIStealer'dır. Martin Kováč bu kötü amaçlı yazılımın zararlarının altını çizmiştir, ancak bir sunucunun ihlal edilmesiyle verilere anında ve dünya genelinde erişim sağlanabilmesine de değinilmesi gerektiğine inanıyoruz. IIStealer, Microsoft'un web sunucusu yazılımı olan İnternet Bilgi Hizmetleri'nin (IIS) kötü amaçlı bir uzantısıdır. Dolayısıyla IIS kullanan bir sunucudan geçen ve IIStealer bulaşan tüm ağ iletişimi saldırganlara açıktır. Bu iletişime parolalar, kullanıcı adları, e-ticaret işlemlerinde kullanılan ödeme bilgileri de dahildir.

Ne yazık ki internet kullanıcılarının şüpheli web sitelerinden uzak durma ve web sitelerinin SSL/TLS şifreleme ile korunduğunu doğrulaması gibi doğru davranışları, IIStealer'dan kaçınmak için yeterli değildir. E-ticaret sitesi güvenilir ve iletişim kanalı güvenli olsa bile web sitesi ziyaretçileri açısından bakıldığında, ziyaret ettikleri web sitesinin bulunduğu sunucuların güvenlik durumunu bilmeleri gibi bir durum söz konusu olamaz. Ancak verilerin işlendiği ve ziyaretçilerden habersiz çalındığı yer bu sunucudardır. Bu noktada "IIStealer tehdidi ne kadar gerçektir?" sorusu akla geliyor.

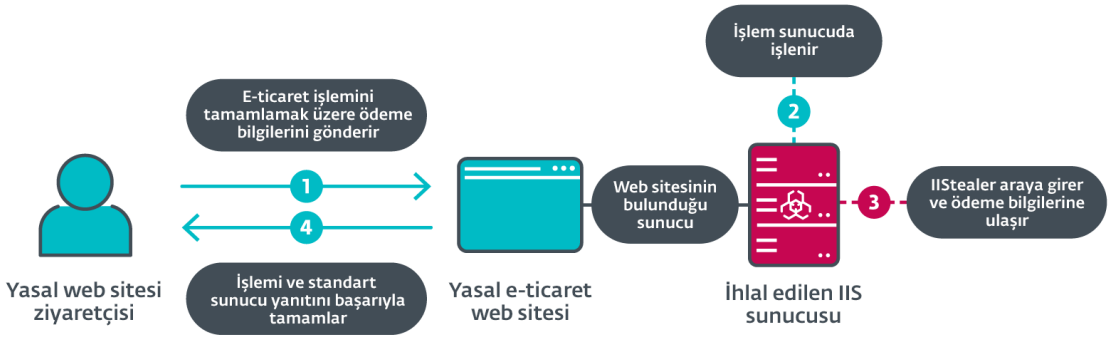
IIStealer'ın gerçek dünya kullanımı

ESET telemetrisi IIStealer'ın ABD'de 2020 Eylül ile 2021 Ocak arasında aktif olduğunu ve e-ticaret web sitelerini hedef aldığını ortaya çıkardı. Analiz ettiğimiz IIStealer örneklerinde, gömülü koda sahip ödeme sayfası URI'larını aradığını gördük. Bu durum bu kötü amaçlı yazılımın belli e-ticaret web siteleri için özel olarak tasarlandığı anlamına geliyor. IIStealer diğer ülkelerdeki e-ticaret web sitelerini de hedef alabilir, ancak böyle bir durumu gözlemlemedik. ESET telemetrisi yoluyla IIS sunucularında sınırlı görünürlüğe sahip olduğunu tespit ettik.

Bu kısıtlama, büyük ölçüde şirketlerin sunucularını güvenlik yazılımı ile korumamalarının sonucu olarak yaygındır.

Aşağıdaki şekilde gösterildiği üzere, ödeme sayfalarını talep eden web sitesi ziyaretçi trafiği IIStealer tarafından engellenir ve kaydedilir. Daha sonra saldırgan, e-ticaret web sitesine özel bir istek göndererek sunucu ile iletişime geçer. IIStealer bu talebi alır ve müşterinin ödeme bilgilerini ekleyerek sunucu yanıtını değiştirir.

IIStealer: veri müdahalesi



MStealer: veri müdahalesi

Önlemek için ipuçları

IIStealer tehdidi, satıcı (sunucu) ve alıcı (web sitesi ziyaretçisi) arasında kurulması gereken güven ilişkisini tehlikeye atar. Ancak IIS sunucusu yöneticileri, kendilerini eğiterek ve en iyi güvenlik uygulamalarından yararlanarak bunu önleyebilir. Bu nedenle IIS sunucusu yöneticilerine şunları yapmaları önerilir:

- Yalnızca güvenilir kaynaklardan ana IIS modülleri kurun.
- Düzenli olarak şunları kontrol edin:
  - `%windir%\system32\inetsrv\config\ApplicationHost.config` dosyası,
  - `%windir%\system32\inetsrv\` dosyası ve
  - `%windir%\SysWOW64\inetsrv\` dosyası

  Bu sayede kurulan tüm ana IIS modüllerin yasal olduğunu doğrulayabilirsiniz. Başka bir deyişle, güvenilir bir sağlayıcıdan olduklarını veya amaçları doğrultusunda kurulduklarını doğrulayabilirsiniz.
- Sızıntının gerçekleşmesi durumunda tüm tarafları bilgilendirin, bu sayede hızlı bir şekilde tepki verebilirler.
- IIS kötü amaçlı yazılım ile ilgili *Ana IIS Kötü Amaçlı Yazılım'ın Anatomisi* adlı teknik raporu okuyun.

IIS tehditlerinin ele alınmasıyla ilgili tüm sorumluluk IIS sunucusu yöneticilerinin omuzlarında olsa da web geliştiriciler de aşağıdaki ipuçlarından yararlanarak zararı azaltabilir:

- SSL/TLS üzerinden bile olsa, sunucuya parola göndermeyin.
- Bunun yerine kullanıcıların kimliğini doğrulamak üzere *Güvenli Uzak Parola (SRP)* gibi bir protokol kullanın. Bu protokol, şifrelenmemiş bir parolanın sunucu dışına aktarılması ihtiyacını ortadan kaldırır. Ayrıca, IIStealer yeniden kimlik doğrulamak için veri kullanabileceğinden sunucu tarafında hesaba dayalı adreslemeye güvenmeye de gerek olmaz.
- Ödeme işlemlerini ele almak için güvenilir üçüncü taraf sağlayıcıların ödeme noktası hizmetlerini kullanın. Bu sayede hassas ödeme bilgilerinin sunucunuzda işlenmesini önleyebilirsiniz.

Son olarak web sitesi ziyaretçileri olarak aşağıdaki ipuçları ödeme kartı bilgilerinizin çalınması durumunda karşılayacağınız etkileri azaltmaya yardımcı olabilir:

- Küçük ve sıra dışı ödemelere karşı *kredi kartı ekstrenizi gözden geçirin*: Genellikle küçük miktarlar kartların geçerli olup olmadığını test etmek için denenir.
- Sıra dışı bir şey fark etmeniz durumunda, derhal bankanızı bilgilendirin.

IIS kötü amaçlı yazılımla ilgili dijital ses dosyası

IIS kötü amaçlı yazılımı hakkında daha fazla bilgi edinmek için, *Spotify*, *Google Podcasts*, *Apple Podcasts* ve *PodBean* gibi popüler dijital ses dosyası uygulamalarının herhangi birinden ESET Research dijital ses dosyalarına abone olabilirsiniz.

4

DÜZENLEYİCİ RADAR: VERİ KORUMA VE ÖDEME KARTI STANDARTLARI

Tony Anscombe
Kıdemli Güvenlik Misyoneri

Ödeme sistemlerini de kapsayan perakende sektörünün BT altyapısının güvenliğini sağlamak, karmaşık birçok teknik zorluk barındırır. Bazıları teknolojiyle ilgili doğrudan risklerdir. Gömülü olan ve uygulama katmanındaki yazılım buna örnektir. Bazıları ise ikinci sırada olmasına rağmen yine de önemli olan ve sektör standartlarının, yönetmelik zorunluluklarının teknik uygulamaları ile ilgili risklerdir.

2004 yılında verileri korumak ve dolandırıcılık riskini azaltmak amacıyla ödeme kartı sektörü, Ödeme Kartları Sektörü Veri Güvenliği Standartları (PCI DSS) olarak bilinen bir standartlar seti oluşturdu. Başlıca kredi kartı sağlayıcıları; işlemin kredi kartı ödeme sistemi yoluyla alındığı kredi kartı veya banka kartı ile ödemeleri kabul eden tüccarların bu standartlara uymasını gerekli tutar. Ayrıca tüccarların kart sahibinin verilerini saklarken, işlerken ve aktarırken minimum seviyede güvenliği yerine getirmesi de gereklidir.

PCI DSS dünya genelinde benimsendi ve 2006'dan bu yana Ödeme Kartı Sektör Güvenlik Standartları Konseyi tarafından yürütülüyor.

15 yıl sonra, PCI DSS ve Avrupa Birliği Genel Veri Koruma Yönetmeliği (GDPR) gibi gizlilik yönetmeliklerinin ödeme kartı verileri anlamında birçok benzerlik gösterdiğini görüyoruz. Hatta bazı gizlilik yönetmelikleri PCI DSS'i içerdiğini görüyoruz.

Örneğin GDPR, ödeme kartı verilerini kapsayan belli gereklilikler bulunduruyor. Bu sayede PCI DSS, yalnızca bir sektör standardı olmaktan çıkıp zorunlu bir yönetmeliğe dönüşüyor. Bununla birlikte, bazı bölgelerde PCI DSS'in cezalar ve düzenleyicilerin gözetimi ile birlikte etkin bir şekilde uygulanan bir mevzuat olmasına rağmen, diğer bölgelerde kendi standartlarını düzenlemek sektörün sorumluluğundadır. Bu durumda Visa ve Mastercard gibi ödeme işleme santralleri, uyumsuzluk nedeniyle potansiyel olarak para cezası uygulayabilir. Bu, bazı bölgelerde daha karmaşık hale gelebilir. Örneğin, PCI DSS'nin federal yasa tarafından zorunlu tutulmadığı ABD'de bazı eyaletlerde PCI DSS veya denk hükümler yürürlüktedir. Bu yönetmelik gerekliliklerıyle ilgili şüpheniz olması durumunda, profesyonel yasal tavsiye almanız önerilir.

PCI DSS, aşağıda yer alan altı kontrol amacı doğrultusunda siber güvenlikle ilgili rehberlik sunar:

1. Güvenli bir ağ ve sistem oluşturulması
2. Kart sahibinin verilerinin korunması
3. Güvenlik açığı yönetimi programının kullanılması
4. Güçlü erişim kontrol önlemlerinin uygulanması
5. Ağların düzenli olarak izlenmesi ve test edilmesi
6. Bir bilgi güvenliği politikasının uygulanması

*PCI Güvenlik Standartlarının tam metnine *buradan* ulaşabilirsiniz.

Kaliforniya Müşteri Gizliliği Kanunu (CCPA) gibi benzer gizlilik yönetmelikleriyle karşılaştırıldığında, PCI DSS "mantıklı siber güvenlik" gereksinimiyle ilgili oldukça belirgin bir rehberlik sunar.

*Güncellenmiş *PCI DSS (4.0), Mart 2022'de itibariyle yürürlükte olacaktır*

İşlemlerin veya verilerin fidye için yönlendirilmesi - belki de her ikisinin de!

Kişisel verilerin güvenlik riskleri, özellikle bu veriler şirketler ve kuruluşlar tarafından büyük ölçekte işlendiğinde ve/veya saklandığında, pandemiden çok önce bile perakende sektörünü hedef alan kötü amaçlı etkinliklerin artmasına neden oldu. Son zamanlarda, bu durum bir şirketin sistemlerine ve verilerine erişimini engelleyen kötü amaçlı yazılımın etkinleştirilmesinden önce verilerin saldırgan tarafından dışa aktarıldığı fidye yazılım saldırılarının çalışma biçimindeki değişiklikle daha da arttı.

Fidye yazılımla ilgili daha fazla bilgi edinmek istiyor musunuz?

2021 teknik raporumuzda göz atın

9 Ocak 2020 tarihinde Dünya Sağlık Örgütü resmi olarak COVID-19'la ilgili açıklama yaptığında kişisel veriler ve gizlilik daha fazla önem kazandı. Daha sonrasında dünyanın büyük bir kısmı hayatımıza hükmeden uzaktan çalışma, evden eğitim ve çevrim içi perakende satışlar ile dijital altyapıya dayalı hale geldi. Pandemi devam ettikçe teknoloji; aşının piyasaya sürülmesi, testlerin kaydedilmesiyle ve yönetilmesiyle ilgili stratejilerin başlatılması, virüs bulaş oranlarının izlenmesi ve son zamanlarda da aşı karnelerinin düzenlenmesi konularında oldukça önemli bir yerdedir. Bu durum, dünya genelinde hükümetler ve şirketler açısından verilerin bulundurulması ve gizliliğiyle ilgili sorunlar oluşturuyor.

Veri ve gelir elde etmek isteyen siber suçlular hazırda bekliyor ve *COVID-19 kısıtlamalarının azaltılması çalışmalarından* yarar sağlamak üzere yeni yaklaşımlar geliştiriyor ve perakende sektöründen de daha fazla gelir elde etmek istiyor.

COVID-19'dan yararlanmak isteyen kötü amaçlı kampanyalar ile perakende sektörünü hedef alan kötü amaçlı taktikler arasında belirgin benzerlikler bulunuyor. Kimlik avı hırsızlığı kampanyaları, SIM takası dolandırıcılıkları, fidye yazılım saldırıları ve ortadaki adam saldırıları (kredi kartı/işlem verilerini çalmak için) gibi teknikleri kullanmak üzere beceri setine sahip suç aktörleri bu durumun büyük ölçüde nedenidir. COVID-19 ile ilgili olarak *2020 yılı Aralık ayında birkaç dolandırıcılık* görüldü. Bu dolandırıcılıklarda sosyal medya üzerinden maskeler, testler ve "tedaviler" satışa sunuldu ve kullanıcıları korkutarak sosyal mühendislikten yararlanıp, kişisel bilgiler satın alındı ve paylaşıldı. 2021 yazında, kişisel verilere erişim sağlamak için *sahte aşı karnesi uygulamaları oluşturma* noktasına bile gelindi. İşin önemli yanı ise *COVID-19 ile ilgili fırsatları hedefleyenlerin sahip olduğu beceri setleri müşterileri ve şirketleri hedef almak için de kullanılabilir*, özellikle de çeşitli perakende süreçlerinde olanları.

Her bir veri, perakendecilerin dijital pazarlamaları açısından çok önemlidir ve satış çabaları da bir risk kaynağıdır. Nasıl? Tüm bu dijital etkinliklerin; ortaklar, tedarikçiler, personel ve işlemlerin dijitalleştirilmesi ile gelişmiş dijital ürünler yoluyla e-ticaret satıcılarını ve gerçek mekanda faaliyet gösteren perakendecileri etkileyen yönetmelik ve uyumluluk risklerini genişletmesi yoluyla.

COVID-19'un perakendeciliğin dijitalleşmesiyle ilgili ortaya çıkardıkları

GDPR ve ABD'deki CCPA gibi gizlilik odaklı yönetmelikler dünya genelindeki şirketlerin temel seviyede veri koruması sunmasını ve müşterilerin bunu talep etmesini zorunlu kılarken, COVID-19 dolayısıyla perakendeciler e-ticaret dünyasına hazırlıksız bir şekilde girdi.

Pandemi dolayısıyla dijital etkinliklerin inanılmaz derece artmasıyla perakende sektörü dahil olmak üzere, süreç olgunlaşma evresini atlamak zorunda kaldı. Bunun yerine, çevre dostu iş yaklaşımlarına geçiş, veri koruma yönetmeliklerine uygunluğun çok ötesine geçti ve çok sayıda şirket perakendecilerin dijital fırsat arayışına yoğunlaşan tehdit ortamıyla tanıştı.

Yeni (sizin için) teknoloji, riskleri ve kötü uygulamaları beraberinde getirir

E-ticareti desteklemek üzere kullanılan birçok araç, dijital tehditler için en az üç ilgi çekici hedef sunar. Bu hedeflerden ilki, satış ve pazarlama platformlarından ve veri tabanlarından sorumlu çalışanların yetersiz veya kötü amaçlı uygulamalarıdır. İkincisi, günümüz BT ağırlıklı perakende ortamını destekleyen ağdaki, uç noktadaki, satış noktası cihazlarındaki yazılımların kötü yapılandırılması ve bu yazılımlardaki güvenlik açıklarıdır.

Son olarak ise, işlemlerin sayısındaki artıştır. Örneğin 2022 yılında *perakende satışların dünya genelinde ortalama 26,7 trilyon Amerikan dolarına ulaşacağını* düşünüyoruz. *Yalnızca ABD'deki perakende satışların*, 2022'de 5,23 trilyon Amerikan dolarına ulaşacağı ön görülüyor. Bu yüklü miktarlar kötü amaçlı kişilerin ilgisini çekiyor. Bunun bir sonucu olarak IBM'in *X-Force Tehdit İstihbaratı Endeksi*'ne göre 2020 yılında perakende sektörünün en çok hedef alınan beş sektör arasında yer alması sürpriz değildir.

Karmaşık yönetmelikler ve standartların gerekliliklerinin yanı sıra müşteri verilerine yönelik artan tehditleri ve riskleri göz önünde bulundurduğumuzda, şirketlerin ister ödeme kartı işlemi olsun ister saklanan müşteri verileri olsun tüm tüketici verilerinin güvenliğini ciddiye alması çok önemlidir. Aksi takdirde tüketicilerin güveni azalır ve düzenleyicilerle karşı karşıya kalırsınız.

ABD gizlilik düzenlemeleri ve değişen siber güvenlik yasaları

2018 yılında AB'nin GDPR yönetmeliğini yürürlüğe koymasının ardından, ABD'de de veri gizliliği düzenlemelerinin uygulanması devlet seviyesinde hız kazandı. Kaliforniya'daki düzenleyiciler 2018 yılında *Kaliforniya Tüketici Gizliliği Yasası*'nı (CCPA) yürürlüğe koydu ve bu yasa 2020 yılından bu yana uygulanıyor. 2020 yılının sonlarında Kaliforniya'da Proposition 24 yürürlüğe girdi; *Kaliforniya Gizlilik Hakları Yasası* (CPRA) anlamına gelen bu yasa 2023 yılında uygulanmaya başlayacaktır. CPRA, bazı açılardan GDPR'ye göre eksik yönlere sahip olsa da birçok açıdan GDPR'den daha iyi olan CCPA'ya önemli eklemeler yapar.

Bu ekler şunları içerir:

- GDPR'de vurgulanan yalnızca bireysel verilere ek olarak hane halkı verileri kavramı;
- Kaliforniya'da ikamet edenlere, geçici nedenlerden ötürü eyalet dışındayken bile koruma sağlama;
- Kişisel verilerin üçüncü taraflara satılmasından cayma hakkı. Şirketler, web sitelerinin ana sayfalarında "Kişisel Bilgilerimi Satma veya Paylaşma" bağlantısı içermelidir.

Veri sahibinin pazarlama amaçları doğrultusunda kullanıma izin vermeme ve ek olarak verinin işlenmesiyle ilgili etkinliklere rıza vermeme hakkı gibi konularla ilgili benzer korumalar GDPR'de yer alır ancak bu kadar net değildir.

2019 Nisan ayındaki *Tüketici Çevrimiçi Gizlilik Hakları Yasası*'nda (COPRA) yer alan federal tüketici gizlilik düzenlemesine ihtiyaç olduğuyla ilgili yaygın görüş ve Biden yönetiminin federal gizlilik düzenlemesine ihtiyaç olduğuyla ilgili beyanlarından yola çıkarak bu konuda girişimlerin olacağına inanıyoruz. Ayrıca Başkan Yardımcısı Kamala Harris, gizlilik uygulamalarıyla ilgili sağlam bir geçmişe sahiptir. Harris'in Kaliforniya eyaleti Adalet Bakanlığı'nı yürüttüğü sırada *Kaliforniya Çevrimiçi Gizlilik Koruma Yasası* (CalOPPA) değiştirildi ve güçlendirildi. Ayrıca, Obama döneminde kanun tasarısına katkıda bulunan bazı çalışanlar da halen görevdedir.

Pandeminin devam ettiği günümüzde gözler sağlık hizmetleri sağlayıcıların ve temaslı izleme, test ve aşılama sağlayan ajansların üzerindedir.

Şu anda durumun aciliyeti ve tıbbi gereklilikleri dolayısıyla kişisel verilerin toplanmasıyla ilgili bazı süreçler ayrıntılı bir şekilde ele alınamıyor olabilir. Ancak bu durum geçici olacağı ve bu gibi veriler için siber güvenliğin güçlendirilmesinin gerekliliği unutulmamalıdır.

Ayrıca internetin dünya genelinde sınırları ortadan kaldıran bir ortam oluşturduğu ve her şeyin aynı bulutta erişilebilir olduğu aşikardır. Gizlilik düzenlemeleri, sürekli olarak geliştirilmesi gereken bir süreçtir. Bu süreçte yapay zeka, Nesnelerin İnterneti ve teknolojideki diğer gelişmeler gibi yeni teknolojileri de göz önünde bulundurursak düzenlemelerin sürekli olarak gelişen koşullara göre uyarlanması gerekir. Bu durum dünya çapında eyaletler, ülkeler ve kıtalar arasında standardizasyona ve uyuma ihtiyaç olduğunu gösteriyor. Nerede olursa olsun şirketler ve kuruluşlar tüm tüketicilere aynı gizlilik politikası haklarını sunmalıdır.

Gizlilik düzenlemeleri, 2022'de tüm yasa düzenleyiciler ve şirketler için bir öncelik teşkil etmeye devam edecektir. Bu nedenle, okuyucular, fırsatların ve ürünlerin bu raporda bahsedilen teknolojiler sayesinde bizlere sunulduğunu, ayrıca standartlar ve düzenleyici sorumlulukları üzerine süregelen diyaloğun yanı sıra güvenlik uygulamalarına ve yeterli yatırıma daha fazla saygı gösterilmesi gerektiğini unutmamalıdır.

5

SUNUCU GÜVENLİK ÇÖZÜMLERİNE DAHA YAKINDAN BİR BAKIŞ

Bir sunucu güvenlik çözümü, bir kuruluşun ana sunucularını tehditlerden korumak üzere tasarlanır.

Günümüzde şirketler, çalışanlarının şirket ağına dosya kaydetmesine izin veriyor, ancak ağlarını kötü amaçlı dosyalara karşı genellikle yeterince iyi korumuyor. Ağ sürücüsüne kötü amaçlı bir dosya kaydeden tek bir çalışan, kuruluşun dosyalarını erişilemez hale getiren büyük bir soruna neden olabilir.

Ayrıca birçok web sitesi, sunucuyu korumak üzere herhangi bir güvenlik yazılımı bulunmayan sunucularda yer alıyor. Sunucular, ödeme kartı bilgileri ve parolalar gibi hassas verileri barındırdığı veya işlediği için genellikle daha fazla rağbet gören hedeflerdir.

Ne yazık ki perakendeciler başa çıkılması gereken geniş ve gittikçe büyüyen tehdit yüzeylerine sahiptir ve her zaman önlemeye, savunmaya ve onarmaya öncelik vermelidir. Düzenleyici sorumluluklarının artması ve teslimatlar ilgili lojistiğin yanı sıra pazarlama ve çevrim içi alışveriş deneyiminin otomatikleştirilmesine duyulan ihtiyaç bunu gerektirmektedir.

Dolayısıyla, bir saldırı veya veri ihlali meydana geldiğinde, kuruluşlar savunmalarına nasıl sızıldığı veya saldırıdan tamamen habersiz olmaları konusunda şaşkınlık yaşıyor. Saldırı nihayetinde keşfedildikten sonra kuruluşlar, bu saldırının tekrar gerçekleşmesini engellemek üzere çeşitli uygulamalara başvurur.

Bir sunucu güvenliği çözümü kurarak, proaktif bir yaklaşım benimsemek, bu durumu tersine çevirir. *ESET Server Security* tüm genel sunucular, ağ dosya depolama ve çok amaçlı sunucular için gelişmiş bir tehdit koruması sunmak üzere tasarlanmıştır. Sunucuların istikrarını korumasını ve çatışmanın olmamasını sağlar.

Ayrıca iş sürekliliğini kesintiye uğratmamak amacıyla en az seviyede yeniden başlar.

Ayrıca ESET Server Security, ESET'in *bulut kum havuzu* ve *uç nokta algılama ve tepki* teknolojilerini de destekler. Bu sayede şirketler önleme, algılama ve tepki aşamalarına sahip sağlam ve çok katmanlı uç nokta savunmasına sahip olur.

ESET HAKKINDA

ESET® dünya çapında 30 yılı aşkın bir süredir şirketleri, önemli altyapıyı ve dünya genelindeki tüketicileri gittikçe artan karmaşık dijital tehditlerden korumak üzere işletmeler ve tüketicilere yönelik sektör lideri BT güvenliği yazılımları ve hizmetleri geliştiriyor. Uç nokta ve mobil güvenlikten şifreleme, çok faktörlü kimlik doğrulaması ile uç nokta algılama ve yanıt çözümlerine kadar ESET'in yüksek performanslı, kullanımı kolay ürünleri 7/24 rahatsız etmeden koruyup denetler ve önlemlerini gerçek zamanlı olarak günceller. Böylece kullanıcıları güvende tutarken şirketlerin kesintisiz faaliyet göstermesini sağlar. Gelişen tehditlere karşı teknolojinin güvenli bir şekilde kullanılmasını sağlayan bir BT güvenlik şirketine ihtiyaç vardır. Dünya çapındaki ESET AR-GE merkezleri ortak geleceğimizi desteklemek üzere bu amaca ulaşmak için çalışır. Daha fazla bilgi için bizi **www.eset.com.tr** adresinde ziyaret edin veya **LinkedIn**, **Facebook** ve **Twitter**'da takip edin.

Katkıda Bulunan Editörler:

James Shepperd, ESET İçerik Yöneticisi
Rene Holt, ESET PR Yazarı II

Ek Katkı sağlayanlar:

ESET Creative Studio