kaspersky geleceği yakalayın

Şirketler karmaşık siber saldırılara karşı nasıl korunmalıdır

Bir gece yarısı bir çeşit gelişmiş siber tehdidin alt yapınızda saklanıyor olabileceği, sadece fikri mülkiyetinizi çalmak ya da işletmenizi fidye için ele geçirmek için doğru anı beklediğinden endişe ederek uykunuz kaçtı mı?

Eğer öyleyse, iyi bir nedeniniz var demektir. Adından da anlaşılacağı gibi, gelişmiş kalıcı tehditler (APT'ler) sistemlerinize erişim sağlamak için sofistike bilgisayar korsanlığı teknikleri kullanır. Savunmanızı kırdıklarında, daha üst düzey erişim ayrıcalıkları elde ederek ve potansiyel olarak yıkıcı sonuçlarla verilerinizi toplayarak ve dışarı sızdırarak aylarca veya hatta yıllarca gizli kalabilirler.

Kimler risk altında?

Beklendiği üzere, ana hedeflerinin genellikle devlet sektörleri veya yatırımlarının karşılığını verecek hassas veya özel verilere sahip büyük şirketleri hedef alarak APT veya hedefli bir saldırı düzenlemek için önemli miktarda beceri, çaba ve kaynak gerekir.

Ancak buna rağmen APT'ler, orta ölçekli işletmelerin bile potansiyel olarak risk altında olduğu, her yerdeki işletmelerin radarında olması gereken bir saldırı yöntemidir.

Örneğin, APT saldırganları artan bir şekilde kendi nihai hedeflerinin tedarik zincirini oluşturan daha küçük şirketleri hedef almaktadır. Çünkü bu tür şirketler genel olarak daha az korunurlar, birlikte çalıştıkları daha büyük kuruluşlara erişim sağlamak için basamak görevi görebilirler.

Sonuç olarak, ister büyük bir kuruluşunuz olsun isterse daha büyük bir kuruluşu hedef almak için potansiyel olarak kullanılabilecek daha küçük bir işletmeniz olsun, karşılaşabileceğiniz tehditlerin **doğasını** anlamanız önemlidir. Buna APT'ler ve diğer hedefli saldırılar ve bunlara karşı savunmak için gereken yetenekler de dahildir.

Hedef alınan tüm sektörler

Son iki yıl boyunca, insan kaynaklı hedefli saldırılar tüm sektörlerde gözlemlendi. 2024 yılında, BT ve kamu sektörleri sırasıyla %14,7 ve %13,8 ile başı çekmektedir.

Kaynak: Kaspersky Managed Detection and Response 2024 Analist raporu

4.88 milyon dolar

2024 yılında bir veri ihlalinin küresel ortalama maliyeti 2023 yılına kıyasla %10'luk bir artış ve şimdiye kadarki en yüksek toplama ulaşmıştır. Orta Doğu bölgesinde bu gösterge önemli ölçüde daha yüksek olup 8,75 milyon dolara ulaşmaktadır.

Kaynak: IBM 2024 Bir Veri İhlalinin Maliyeti Raporu

258 gün

Bir ihlali tespit etme ve kontrol altına alma süresi. Bu uzun toparlanma dönemi sadece mali kayıpları arttırmakla kalmaz, aynı zamanda kuruluşları daha fazla saldırıya karşı savunmasız bırakır.

Kaynak: IBM 2024 Bir Veri İhlalinin Maliyeti Raporu

APT'ler nasıl çalışır?

Bir APT'nin tüm olayı bilgisayar korsanlarının genellikle beş aşamalı bir süreç ile eriştikleri BT ve/veya OT (operasyonel teknoloji) hedefine sürekli ve kalıcı bir erişim edinmektir.

Şekil 1: Gelişen bir APT'nin aşamaları

1. aşama

Erişim edinme

Bir levye ile bir hırsızın kapıyı açmaya zorlaması gibi, siber suçlular genellikle hedef ağ içerisinde zararlı yazılım yerleştirmek için bir virüslü dosya, istenmeyen veya kimlik avı e-postası veya uygulama zayıf noktaları gibi bir 'dijital levye' kullanarak ilk girişi edinirler.

2. aşama

Bir dayanak noktası oluşturma

Bunu yaptıktan sonra, sistemlerde fark edilmeden dolaşmak için kullanabilecekleri arka kapılar ve tüneller oluşturmalarını sağlayan zararlı yazılımlar yerleştirirler.

3. aşama

Erişimi derinleştirme

Bilgisayar korsanları sisteme girdikten sonra sistem üzerinde daha fazla kontrol sahibi olmalarını ve hatta daha üs seviye erişim sahibi olmalarını sağlayan yönetici haklarına erişmek için parola kırmak gibi teknikler kullanırlar.

4. aşama

Yanlamasına hareket etme

Sistemin derinliklerine girdiklerinde ve ağ yöneticisiyle aynı haklara sahip olduklarında istedikleri gibi hareket edebilirler. Bu onların birden fazla sunucuya ve ağın diğer güvenli bölümlerine erişmelerini sağlar.

5. aşama

Bak, öğren ve devam et

Sisteminize daha derin bir erişim edinerek, siber suçlular sistemin nasıl çalıştığını ve güvenlik açıklarını tam olarak anlar ve bu sayede diledikleri zaman istedikleri bilgileri toplayabilirler. Aynı zamanda muhtemelen bu sürecin süresiz bir şekilde devam etmesini sağlamak veya hedeflerine ulaştıklarında ayrılmak üzere girişimde bulunabilirler.

Bir APT saldırısının kurbanı olmanın potansiyel sonuçları nelerdir?

Hedefli bir saldırıya maruz kalan herhangi bir kuruluşun medyada yer alan haberlerini okuduğunuzda, etkilerinin hem ciddi hem de uzun süreli olabileceği açıkça görülecektir. Hemen görülen etkiler genellikle veri kaybı ve iş kesintisinden kaynaklanan mali zararı içerirken, daha uzun vadeli etkiler kuruluşun itibarına, müşteri güvenine ve potansiyel yasal işlemlere zarar vermeyi içerebilir.

Ardından elbette tamamlanması genellikle aylar veya hatta bazen yıllar alan kuruluşun BT alt yapısına verilen zararın giderilmesi sorunu ortaya çıkar. Ve iş yaptığınız sektöre bağlı olarak, ayrıca sektöre özel sonuçlar da olabilir.

Şekil 2: APT'lerin iş güvenliği üzerindeki etkisini anlamak

Finans

- Kritik hizmetlerde kesinti
- Yetkisiz işlemler
- Nakit çıkışı saldırıları
- Kimlik hırsızlığının yasal sonuçları

Kamu

- Siber casusluğun potansiyel etkileri
- Kritik altyapının zarar görmesi
- E-devlet hizmetlerinde kesinti
- Vatandaşların kişisel verilerinin ifşa edilmesi

E-ticaret

- Kimlik hırsızlığı yoluyla hesap ele geçirmenin yasal sonuçları
- Hileli işlemler
- BT hizmetlerinin reddi, gelir kayıpları
- GDPR, PCI DSS vb. kapsamında olası cezalar

Nakliye

- Operasyonel kesintiler ve kapanmalar
- Tedarik zincirinde gecikmeler ve artan maliyetler
- Yaşam tehdidi
- Kritik altyapının zarar görmesi

Gıda

- Stok sıkıntısı ve üretim kesintileri
- Gıda kalitesinin risk altına girmesi
- Kimyasallar, toksinler vb. ile potansiyel kirlenme
- Manuel işlemlere gerileme gerekliliği

Sağlık

- Kritik hizmetlerde kesinti
- Hastaların kişisel verilerinin ifşa edilmesi
- Kamu güvenini zedeleme
- Potansiyel yaşam tehdidi

BT ve Telekomünikasyon

- Müşteri kaybı
- Satış kaybı
- Planlanmamış ağ kesintileri
- Sabit ve mobil hizmet kesintisi

Üretim

- Çevresel felaketler
- Operasyonel kesinti
- Planlanmamış duruş sürelerinde artışlar
- Basamaklı arızalar veya sistem genelinde kesintiler

>2

her gün olan yüksek şiddette olaylar.

%43

Kaspersky tarafından 2024 yılında tespit edilen yüksek şiddetli olayların yukarıda belirtilen oranı insan kaynaklı hedefli saldırılardır (APT'ler).

Kaynak: Kaspersky Managed Detection and Response 2024 Analist raporu

Bu siber savunmanız için ne anlama geliyor?

APT'lerin ve diğer hedefli saldırıların bir büyük tehlikesi de şudur ki, keşfedildiklerinde ve hemen ortaya çıkan tehditler geride kalmış gibi göründüklerinde bile, bilgisayar korsanları istedikleri zaman geri dönmelerini sağlayan birden fazla arka kapı bırakabilirler.

Bir başka problem de şudur ki, antivirüs ve güvenlik duvarı gibi birçok geleneksel siber savunmanın bu tür saldırılara karşı koruma sağlayamamasıdır.

Bir APT veya bir hedefli saldırı başlatmaya dahil olan adımların yukarıda belirtilen kısa özetinden şu anlaşılır ki, bu tür tehditlere karşı savunma yapma uç noktalar, ağlar, bulut, e-posta, internet erişimi ve dahasını koruma kabiliyeti olan çözümleri de dahil eden çok seviyeli bir yaklaşım olması gereklidir.

Bu sadece sofistike saldırı riskinin önlenmesine ve azaltılmasına yardımcı olmakla kalmayacak, aynı zamanda bu tür olayların meydana gelmesi halinde ortaya çıkacak aksaklık ve maliyetlerin de en aza indirilmesine yardımcı olacaktır.

Peki bu ne tür çözümler içeriyor ve bunları nasıl kullanmalısınız?

Şirketler karmaşık siber saldırılara karşı nasıl korunmalıdır

Bir uç koruma platformu (EPP) kendi başına hedefli saldırılara karşı koruma sağlamaz, yeni, devam eden veya geçmişte olan saldırıların analizinde kullanılacak olan verilerin hayati bir veri kaynağını temin edecektir. Sonuç olarak, aşağıdakileri de içeren bir çözüm paketinin parçası olarak kullanılmalıdır:

- Uç nokta koruması ve yanıtı (EDR) - Cihaz seviyesinde uç nokta koruması ve görünürlüğü sağlar ve çalışma istasyonları ve sunucular v.b. üzerindeki tehditleri tanımlar ve bunlara yanıt verir.
- Ağ tespiti ve yanıtlama (NDR) - Ağ trafiğini izler ve analiz eder, anormallikleri tespit eder ve ağ düzeyinde potansiyel tehditlere yanıt verir.
- Genişletilmiş tespit ve yanıt (XDR) - Görünürlüğü geliştirmek ve tehdit yanıtını otomatikleştirmek için EDR, NDR ve diğer güvenlik katmanlarını birleştirir.

Şekil 3: EDR, NDR, XDR: Nasıl çalışırlar?

NDR

Özellikle şifreli trafik içerisindeki zararlı faaliyeti, ağ içerisindeki yanal hareketi ve aykırı davranış ve benzerlerini tanımlayarak ağ trafiğinin analiz edilmesi ile tehditleri tespit eder.

Öne çıkan NDR özellikleri

- **Derin paket incelemesi:** Şifreli trafikte olanlar dahil olmak üzere tehditleri tespit etmek ve bunlara yanıt vermek için paket katmanı verilerini analiz eder. Örneğin, tehlike belirtilerini tanımlamak için TLS parmak izi kullanır.
- **Anormallik tespiti:** Alt yapı için potansiyel tehditleri belirtebilecek olan ağ trafiği içerisindeki anormallikleri tanımlar.
- **Tehdit yanıtı:** Manuel yanıtı geliştirir veya şüpheli cihazları izole etme veya IP adreslerini bloke etme gibi otomatik yanıtları tetikler.

EDR

Masa üstü, diz üstü, sunucu ve sanal makineler gibi uç noktaları hedef alan siber tehditleri tespit eder, soruşturur ve bunlara yanıt verir.

Öne çıkan EDR özellikleri

- **Sürekli izleme:** Potansiyel tehditlerde gerçek zamanlı bir görünürlük sağlayarak kesinti olmaksızın uç nokta faaliyetini izler.
- **Adli veri:** Bir saldırının nasıl başladığı, nasıl yayıldığı ve hangi sistemlerin etkilendiğini izleyerek uç nokta olaylarının detaylı bir analizini sağlar.
- **Otomatik yanıt:** Virüslü sistemlerin otomatin izolasyonu ve zararlı yazılım dosyalarının karantinaya alınması gibi özellikler içerir.

Diğer kaynaklar

XDR

Birden fazla seviyeden verileri (ağ, e-posta, bulut, uç nokta, vb.) bir merkezi sisteme entegre ederek EDR ve NDR'nin kabiliyetlerini genişletir. Bu yaklaşım, saldırı yüzeyinde görünürlüğü artırır ve tehdit tespitinin doğruluğunu geliştirir.

Öne çıkan XDR özellikleri

- **Çapraz vektör korelasyonu:** Uç noktaları, ağ trafiğini, bulut ortamlarını vb. kapsayan içgörüler sağlayarak verileri çeşitli güvenlik katmanlarında toplar.
- **Birleştirilmiş tehdit tespiti:** Birden fazla kaynaktan verileri eşleştirerek, XDR tüm saldırı yüzeyinde birleştirilmiş bir tespit ve yanıt sağlar.
- **Tehdit istihbaratı (TI) ile entegrasyon:** TI beslemelerinden gelen gerçek zamanlı verilerle tespit ve olay analizi yeteneklerini zenginleştirir.

2024 yılında, yüksek şiddetli olayları soruşturma ve raporlama için ortalama süre %48 arttı, bu da 2023 yılına kıyasla saldırıların ortalama karmaşıklığında bir artış olduğunu gösterir. Bu durum, tetiklenen tespit kurallarının ve IoA'ların büyük çoğunluğunun önceki yıllarda olduğu gibi işletim sistemi (OS) günlükleri yerine özel XDR araçları tarafından gerçekleştirilmiş olmasıyla desteklenmektedir.

Source: Kaspersky Managed Detection and Response 2024 Analist raporu

Peki hangi çözüm(ler)i seçmelisiniz?

Doğru çözüm(ler)in seçilmesi kuruluşunuzun özel ihtiyaçlarına, altyapısına ve tehdit ortamına bağlıdır:

- Artık geleneksel uç nokta koruma araçları etkili değilse ve uç noktaları hedef alan siber tehditlere (zararlı yazılım, fidye yazılımı, kimlik avı ve dahası gibi) karşı daha gelişmiş bir korumaya ihtiyacınız varsa EDR'yi seçin.
- Eğer ağ tabanlı tehditler birincil endişeniz ise ve ağ trafiği anormalliklerini analiz etmek ve bunlara yanıt vermek için gelişmiş kabiliyetlere ihtiyacınız varsa NDR'yi seçin.
- Eğer birden fazla vektör üzerinden kapsamlı bir koruma ve tüm BT alt yapınızda tehditleri ilişkilendirmek istiyorsanız XDR'yi seçin.
- Daha da iyisi, çok kapsamlı kaçamak ve gelişmiş siber tehditlere karşı kapsamlı bir savunma sağlamak istiyorsanız EDR, NDR ve XDR'yi tek bir güvenlik ekosisteminde birleştirin.

Şekil 4: EDR, NDR, XDR – sizin için en iyisi hangisi?

Siber güvenlik çözümü	Hangi kuruluş için en iyisi?
EDR	• Uç nokta korumasına öncelik veren ve uç nokta etkinliği hakkında gerçek zamanlı içgörülere ihtiyaç duyan kuruluşlar. • Uç nokta temelli tehditleri gerçek zamanlı olarak tespit etmek ve bunlara yanıt vermek için EDR kabiliyetinden büyük ölçüde faydalanacak olan sağlık tedarikçileri veya finansal kurumlar gibi birçok dağıtılmış uç noktası olan kuruluşlar.
NDR	• Ağ tabanlı tehditleri tespit etmek için gelişmiş kabiliyetlere ihtiyaç duyan ve ağ trafiğine büyük ölçüde bağlı olan kuruluşlar. • Veri merkezleri, hizmet tedarikçileri veya devlet kurumları gibi yüksek seviye düzenlemeye tabi olan veya tahsis edilmiş olan bir BT güvenlik ekibi olan şirketler ağ tabanlı tehditleri tespit etmek ve bunlara yanıt vermek için NDR kabiliyetinden faydalanabilirler.
XDR	• Tüm BT alt yapılarında kapsamlı tehdit tespiti ve yanıtı kabiliyetleri olan birleştirilmiş bir güvenlik platformu ihtiyacı olan kuruluşlar. • Güvenlik için kapsamlı bir yaklaşıma ihtiyaç duyan karmaşık BT ortamları olan büyük kuruluşlar. Örneğin, veri merkezleri ve bulut ortamları tesisleri olan çok uluslu kurumlar, olay yanıtını merkezileştirerek operasyonel karmaşıklığı azaltırken tüm platformlarda birleştirilmiş tehdit tespiti sağlamak için XDR kabiliyetinden faydalanabilir.

Kaspersky Anti Targeted Attack

Kaspersky nasıl yardımcı olabilir?

Kaspersky Anti Targeted Attack (KATA) karmaşık siber tehditlere karşı kapsamlı anti-APT koruması sunar. Kuruluşlara şu konularda yardımcı olur:

- Hedefli saldırıları hızla tespit eder, analiz eder ve bunlara yanıt verir.
- Ağlar, e-postalar, web ve uç noktalar dahil olmak üzere tüm önemli saldırı giriş noktalarında sağlam bir güvenlik sağlar.
- Kritik varlıkları korur.
- Endüstri yönetmeliklerine uygunluğu sağlar.

Yukarıdakiler, Kaspersky Anti Targeted Attack'in üç katmanında mevcut olan güçlü NDR ve EDR teknolojilerinden yararlanılarak mümkün kılınmıştır.

Bu üç KATA katmanı, temel ve gelişmiş NDR'den yerel XDR'ye kadar değişen gelişmiş kalıcı tehditlere (APT) karşı koruma sağlar.

- KATA: Bir ana NDR çözümü sunar ve siber tehditleri tespit etmek ve bunlara yanıt vermek için temel özellikler sunar.
- KATA NDR Enhanced: Gelişmiş NDR yetenekleri sunarak KATA katmanının temel özellikleri üzerine inşa edilmiştir.
- KATA Ultra: Yerel XDR işlevselliği sunmak için NDR ve EDR kabiliyetlerini birleştirir. Ağlar, web, e-posta, uç noktalar, sunucular ve sanal makineler dahil olmak üzere birden fazla tehdit giriş noktasını güvence altına alır.

Şekil 5: Kaspersky Anti Targeted Attack. Esnek bir seçim.

Karşılaştırma kriterleri	KATA	KATA NDR Enhanced	KATA Ultra
Açıklama	Temel NDR	Gelişmiş NDR	NDR+EDR (Yerel XDR)
Gerekli NDR işlevi	•	•	•
Gelişmiş Sandboxing	•	•	•
Kaspersky Threat Intelligence ve MITRE ATT&CK zenginleştirmesi	•	•	•
İyileştirilmiş NDR işlevi		•	•
Uzman EDR işlevselliği			•
Yerel XDR özellikleri			•

Temel veya gelişmiş NDR işlevselliği arasından seçim yapın veya hepsi bir arada bir platform olarak, en sofistike siber tehditlere karşı sizi koruyarak yerel XDR senaryoları için birleştirilmiş NDR ve EDR çözümüne dahil olun. KATA Ultra katmanında, tüm BT altyapınız boyunca tam teşekküllü, hepsi bir arada APT koruması ve görünürlüğü elde edersiniz.

Kaspersky Anti Targeted Attack neden tercih edilmeli

BT altyapınız genelinde tam görünürlük

Kör noktaları ortadan kaldırmak ve tamamı tek bir birleştirilmiş platform içerisinde olmak üzere ağ, web, uç noktalar ve e-posta dahil olmak üzere tüm potansiyel tehdit giriş noktalarını kontrol etmek için benzersiz teknolojilerden oluşan eksiksiz bir yığın sağlar.

Küresel tehdit istihbaratı ile zenginleştirilmiş koruma

Kaspersky Private Security Network (KPSN / KSN) küresel itibar veritabanına ve Kaspersky Threat Intelligence'a doğrudan erişim ve MITRE ATT&CK ile eşleştirme yoluyla tehdit analizini ve müdahalesini zenginleştirir.

Bağımsız olarak test edilmiş ve kanıtlanmış teknolojiler

Lider analitik kurumlar tarafından tanınan ve tüm dünyadan ana müşterilerin güvendiği hızlı olay yanıtı, gelişmiş ML kaynaklı tehdit tespiti, derinlemesi soruşturmalar için yenilikçi teknolojiler kullanır.

Kaspersky Anti Targeted Attack

Daha fazla bilgi

Kaspersky Anti Targeted Attack video sunumu

Şimdi izleyin

Gelişmiş tehdit tahminleri

Şimdi okuyun

www.kaspersky.com.tr