2021 YILI YÖNETİLEN TESPİT VE MÜDAHALE HİZMETLERİ (MDR) RAPORU

İÇİNDEKİLER

1) ÇALIŞMA KAPSAMI

Yönetilen Tespit ve Müdahale Hizmetleri (MDR), siber saldırıları mümkün olan en hızlı şekilde tespit etmek ve saldırıya hemen müdahale etmek için yürütülen çalışmalardır.

MDR hizmeti kapsamında kurum içine konumlandırılan, uç noktada görünürlüğü arttıran teknolojiler yardımıyla oluşabilecek bir siber olayın bütün detayları elde edilebilmekte ve oluşacak hasar en aza indirilebilmektedir.

Bu araçlar MDR ekibi tarafından tespit edilen saldırıların;

- Yüksek oranda doğruluk payına sahip olmasına,
- İlgili siber olay öncesi ve sonrasında nelerin meydana geldiğinin detaylı şekilde görülebilmesine,
- Siber saldırıdan hemen sonra bu saldırıyı hızlıca önlemek için yapılacakların planlanmasına

olanak sağlamaktadır. Bu sayede hem bilinen hem de bilinmeyen siber saldırılara karşı kurumlar direnç kazanmaktadır.

MDR Analistleri gerçek zamanlı siber olay tespiti yapabilir ve tespit edilen bu siber saldırılar ile ilgili çok hızlı aksiyon alabilir.

Hızlı doğrulama ve aksiyon alma yetenekleri, gelişmiş siber saldırıların müdahalesinde çok ciddi önem taşımaktadır.

MDR takımları tarafından kullanılan teknolojilerin sunmuş olduğu detaylı kayıtlar ve işletilen süreçler sayesinde bir siber saldırının kök nedeninin tespiti çok hızlı şekilde yapılabilmektedir. Bu durum, mevcut saldırının hızla engellenmesinde ve benzerlerinin gerçekleşmemesi için alınması gereken aksiyonların belirlenmesinde kilit rol oynamaktadır.

ADEO MDR SERVİSİ

2021 YILINDA NELER YAPTIK?

3) 2021 İSTATİSTİKLERİ

En Yoğun Gün:**17 Aralık**
Bu Gün İncelenen Alarm Sayısı:

485

Olay Müdahalesi Gerekmeden Çözülen Alarm Yüzdesi

%99

ALARM

Siber saldırıları tespit edebilmek için kullanılan güvenlik araçlarına düşen uyarı mesajlarına denir. Bu alarmlar kritiklik seviyelerine göre gruplandırılırlar.

En Çok Hedef Alınan Sektörler ve Bu Sektörlerdeki Taplam Vakalar

Üretim
9 Vaka

Haberleşme
5 Vaka

VAKA (INCIDENT)

Tespit edilen gerçek bir alarmın analiz edilmesi sonucunda derinlemesine analiz ve olay müdahalesi süreçlerinin işletilmesini gerektiren saldırgan aktiviteleridir. Çoğunlukla kısa süre içerisinde birden fazla makinede yayılım ve kalıcılık gösteren aktivitelerdir.

En Yoğun Geçen Hafta:**13-19 Aralık**
Bu Hafta Gerçekleşen Vaka Sayısı:

5

2021 İSTATİSTİKLERİ

Ocak 2021'de **600** adet olan Tespit Kuralı sayısı yıl sonunda **2.000**'e çıkartıldı.

Ocak 2021'de **5.000** adet olan IOC sayısı yıl sonunda **20.000**'e çıkartıldı.

Toplam Geliştirilen Kural Sayısı

2000+

ADEO MDR Tehdit Avcıları tarafından yeni çıkan zafiyetler **7x24x365 gün** takip edilir ve ilgili kurallar yazılır.

ADEO İstihbarat Servisi gerçek olaylardan ve güncel saldırılardan sürekli olarak beslenmektedir.

İçeriden ve Dışarıdan Sağlanan Tehdit İstihbaratı ile Taranan IOC Sayısı

20K+

En Çok Kullanılan İlk Erişim Tekniği Dışarıya Açık Zafiyetler

%41

Saldırgan, çeşitli zafiyetlerden yararlanarak sisteme **ilk erişimi** sağlayıp hedeflere ulaşarak diğer taktik ve teknikleri **kullanmaya başlar.**

4) MDR EKİBİNİN GÜNLÜK RUTİNİ

İncelenen alarmların **%96**'sı **ADEO MDR** ekipleri tarafından müşterilere bildirmeden analiz edilerek, kullanılan ürünün olgunluğuna göre gerekli **müdahale prosedürleri** uygulanır. Bu sayede, müşterilerimiz güvenli bir şekilde günlük iş akışlarına odaklanabilmektedirler. Yapılan analizler ve alınan aksiyonlar raporlanarak belirli periyotlarda müşterilere iletilir.

ADEO MDR ekibi tarafından günlük olarak ortalama **20** kadar yeni **tespit kuralı** yazılmakla birlikte yanlış pozitif (**false positive**) olarak değerlendirilen kurallar özelinde ise **sıkılaştırma/iyileştirme** çalışmaları yapılır.

Alarmların **%4**'ü **teyit edilir** ve **onay alındıktan** sonra gerekli aksiyonlar uygulanır.

Tespit edilen **IP ve Domain**, **istihbarat servisleri** tarafında kontrol edilir ve ağ içerisinde iletişimde olduğu makinalar incelenerek **IP bloklama** işlemi yapılır.

Zararlı yazılım tespit edilmesi sonucunda aktiviteler **tehdit avcılığı** yaklaşımıyla incelenerek, zararlı yazılım yayılan makineler **izole edilir** ve **gerekli aksiyonlar** alınır.

5) Yönetilen Tespit ve Müdahale Vaka Yönetim Aşamaları

VAKA (INCIDENT)

Tespit edilen gerçek bir alarmın analiz edilmesi sonucunda derinlemesine analiz ve olay müdahalesi süreçlerinin işletilmesini gerektiren saldırgan aktiviteleridir. Saldırganların sıfırıncı gün (Zero-day) zafiyetlerini sömürmeleri ya da çalışanlara ait parola/kullanıcı adı bilgilerini ele geçirmeleri gibi bazı ilk erişim teknikleri sonucunda, olay müdahale prosedürleri işletilmesi gerekmektedir. 2021 yılında olay müdahalesi gerektiren ilk erişim tekniklerinin dağılımı 20. sayfada belirtilmiştir.

Vaka (Incident) Yönetim Aşamaları

ADEO MDR ekibi tarafından **güvenliği ihlal edilmiş** makinelerin **araştırılması** ve **tespit edilmesi** ile ilgili çalışmalar yürütülmektedir.

MDR tespit aşaması şüpheli aktivitenin sistemler üzerinde görülüp tanımlanmasını içerir. **EDR, NDR, SOAR** vb. güvenlik ürünlerinden ve MDR Analistleri'nin yetkinliklerinden faydalanılarak olası **acil ve kritik** anomali hareketlerin medyan tespit süresi (Dwell Time) ~**4 dakika**'dır. Mandiant firması tarafından 2021'de yayınlanan rapora göre global vakalardaki ortalama tespit süresi 24 gün olarak belirlenmiştir[1].

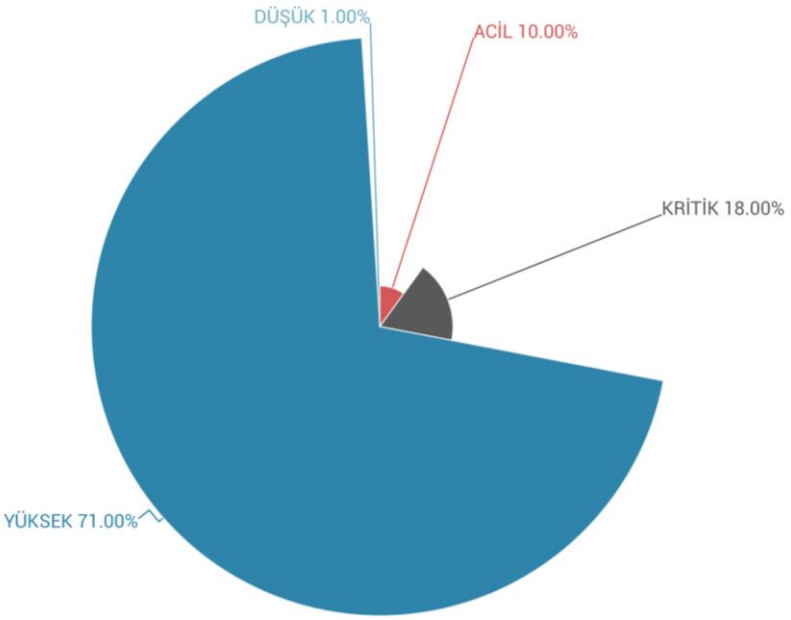
Çeşitli güvenlik ürünleri vasıtasıyla tespit edilen şüpheli aktiviteler **7x24x365 gün ADEO MDR Analistleri** tarafından detaylı olarak incelenir.

Müdahe aşaması, analiz sonucunda zararlı olarak tespit edilen aktivitelerin **durdurulması, engellenmesi ve aktivitenin kurum içerisinde yayılmaması** için alınan aksiyonlardır. **2021** yılı içerisinde ADEO MDR ekibinin **acil ve kritik** vakalara medyan **müdahale süresi** **1 saat 37 dakika** olarak ölçülmüştür. IBM tarafından 2021 yılında yayınlanan rapora göre bu süre global vakalarda ortalama 287 gün olarak belirlenmiştir[2].

İyileştirme aşaması, tehdit oluşturan durumların **ortadan kaldırılması, iyileştirilmesi ve tekrarlanmamasına** yönelik önlemleri kapsamaktadır.

[1] M-Trends 2021, Mandiant
[2] Cost of Data Breach 2021, IBM

6) YILLIK ALARM SAYILARI VE SEVİYELERİ



ADEO'nun **kural geliştirme ve iyileştirme** çalışmaları sürekli olarak devam etmektedir.

Bu çalışmalar kapsamında **2022 yılı hedefi, kritik** ve **yüksek** seviyeli alarm sayılarının **düşürülmesi** ve **gerçek pozitif** alarm sayılarının **arttırılmasıdır**.

TESPİT VE MÜDAHALE SÜRESİ

MEDYAN (MEAN) TESPİT SÜRESİ

4dk 8s

MEDYAN (MEAN) MÜDAHALE SÜRESİ

1s 37dk 8s

2021 yılında oluşan tüm alarmların **medyan tespit süresi 1 saat 15 dakika**, **medyan müdahale süresi 4 saat 39 dakika** olurken; sadece acil ve kritik seviyedeki alarmların medyan tespit süresi **4 dakika**, medyan müdahale süresi ise **1 saat 37 dakika** olarak ölçümlenmiştir.

7) ALARMLARIN SEKTÖRLERE GÖRE DAĞILIMI

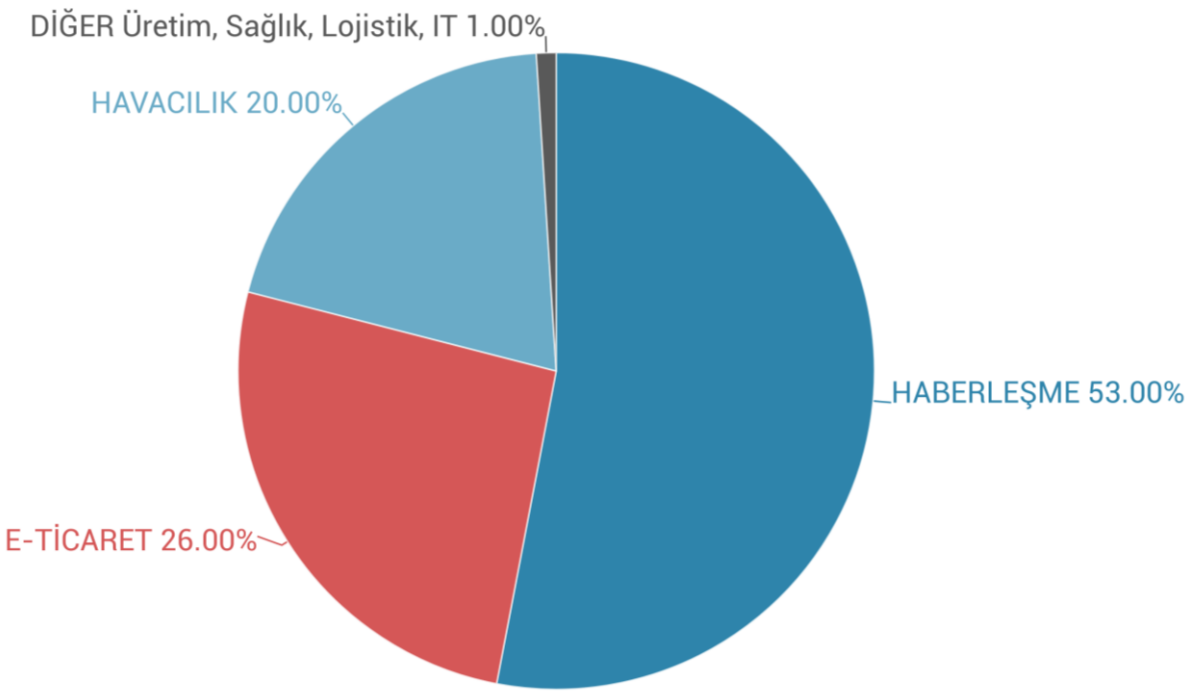
EN ÇOK ALARM GÖZLENEN SEKTÖRLER

HAVACILIK

Sektörün stratejik önemi çok büyüktür ve bu sebeple siber saldırı gruplarının hedefindedir.

HABERLEŞME

Çalışanların çoğunlukla sahada bulunduğu, dağıtık yapıda bir sektördür.
Saldırılara bu dağıtık yapı sebebiyle maruz kalınmıştır.



8) EN ÇOK VAKANIN GERÇEKLEŞTİĞİ SEKTÖRLER

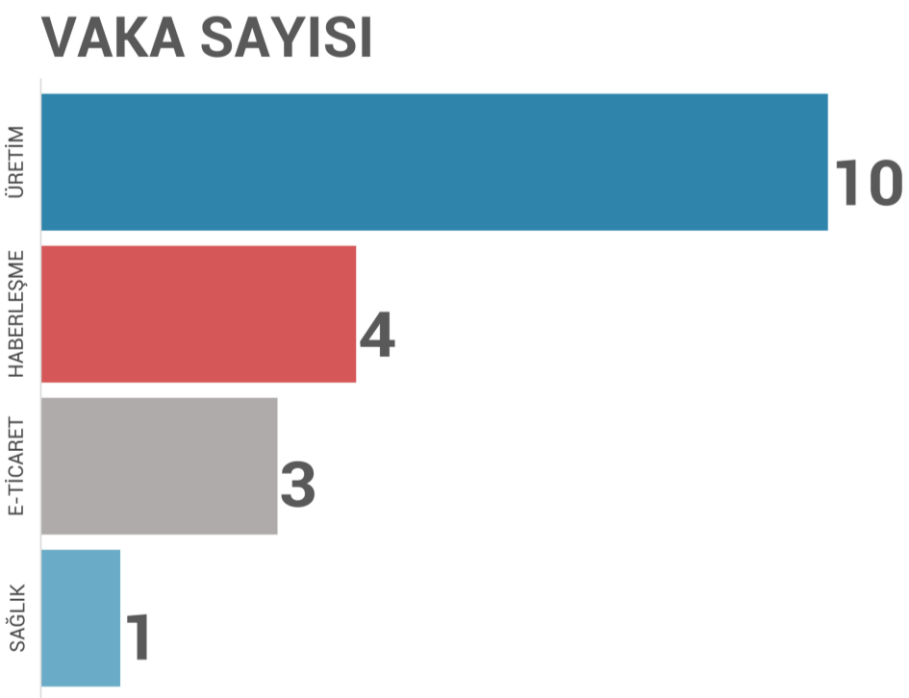
- **Ransomware** grupları özellikle **Üretim** sektörünü hedef alıyor.

Neden Üretim Sektörü

- **Sektör dağıtık** bir yapıda ve **yönetim merkezden değil,** bölgedeki ekipler tarafından yapılıyor. Yerel ekip kontrolünde olmasından kaynaklı **farkındalık düşük** oluyor.

- Bu düşük farkındalık sonucunda **görünürlük az** oluyor ve **geç tespit** ediliyor.

- **OT ortamlarında görünürlük** düzeyinin çok düşük olması sebebiyle güvenlik standartlarının karşılanmadığı ve OT saldırılarına karşı **farkındalıkların** ya da önlemlerin **çok zayıf** olduğu görülmüştür.



9) 2021 YILINDA YAŞANAN ÖNEMLİ GÜVENLİK ZAFİYETLERİ & ADEO MDR SERVİSİ KURAL ÇALIŞMALARI

2021 yılında yayınlanan önemli Top 20+ güvenlik açığı hakkında **ADEO MDR** olarak **yazdığımız kurallar** ve **eklediğimiz IOC'lerin sayısı** aşağıdaki tabloda gösterilmiştir. Buradan da görüleceği üzere siber olayların sayısı her geçen gün artmaktadır.

Meydana gelen siber atakların detayına indiğimizde, bu atakların tespit edilme oranı önceki saldırıların tespit edilme oranına göre düşüktür. Ürünlerin kendi tespit yeteneklerine ek olarak, yeni çıkan saldırıların tespiti için **proaktif güvenlik çözümlerine ihtiyaç** bulunmaktadır.

Bu noktada siber tehdit istahbaratı kaynaklarından yapılan düzenli araştırmalar sonucu elde edilen **tehdit göstergelerinin bloklanması** ve bu kaynaklardan elde edilen **saldırıların analiz edilip**, ilgili saldırıların **tespitine dair kuralların geliştirilmesi** ve yazılan kuralların **laboratuvar ortamlarımızda test edilip**, **ADEO kural veri tabanına eklenerek müşterilerimizin sistemleri üzerinde yaygınlaştırılması** sağlanmaktadır.

Tehdit algılama ve istihbarat analistlerimiz **yeni çıkan güvenlik açıkları** hakkında **düzenli olarak araştırmalar** yapmaktadırlar. Zafiyetlerin teknik olarak incelenip labaratuvar ortamlarından test edildikten sonra **tespit edilen IOC'ler** ve gözlemlenen farklı paternler özelinde **atak yüzeyinin görünürlüğünü artırmak** için **birden fazla kural setleri** geliştirilmektedir.

9) 2021 YILINDA YAŞANAN ÖNEMLİ GÜVENLİK ZAFİYETLERİ & ADEO MDR SERVİSİ KURAL ÇALIŞMALARI

GÜVENLİK AÇIĞI	YAZILAN CUSTOM KURAL SAYISI	ÜRÜNLERE EKLENEN IOC SAYISI
Apache Log4j Zero-Day Vulnerability	16	3000+
LockBit Ransomware	13	122
Possible InstallerFileTakeOver LPE | Zero-Day Vulnerability	13	4
PetitPotam - NTLM Relay Attack	13	5
Emotet Botnet | TrickBot Malware	12	300
Microsoft Exchange ProxyShell Attack	11	39
LockFile Ransomware & ProxyShel	10	13
Web Shell Attack	10	48
Microsoft MSHTML Remote Code Execution Vulnerability	10	235
PrintNightmare aka SeriousSAM Vulnerability	9	24
macOS Finder RCE Zero-Day	9	4
Coronavirus Phishing & Malware	7	233
Windows Print Spooler Remote Code Execution Vulnerability	7	340
FiveHands Ransomware	6	50
Angry Conti Ransomware	5	30
Cobalt Strike Defender's	5	120
Revil Kaseya Ransomware Attack	5	1282
Razer MauseCVE-2021-30494	5	5
DarkSide Ransomware	4	28
BazarLoader Malware	3	50
Ryuk Ransomware	3	545

10) 2021 YILINDA YAŞANAN ÖNEMLİ GÜVENLİK ZAFİYETLERİ & İLK GÖRÜLME ZAMANLARI

İlgili güvenlik zafiyetleri ve saldırıları hakkında geliştirilen kurallar ve MDR güvenlik analistleri yetkinlikleri ile düzenli periyotlarla müşterilerimizin sistemleri üzerinde **tehdit avcılığı** gerçekleştirilmektedir. Potansiyel siber saldırıların gerçekleşmesi öncesinde ilgili zafiyetin veya saldırı göstergelerinin tespiti yapılmaktadır. Yapılan tespit sonrasında, gereken önlem ve aksiyonlar alınarak, konu özelinde kuruma bilgilendirmeler yapılır. Saldırı ile ilgili kurallar müşteri sistemlerine eklenerek, **MDR güvenlik analistleri** tarafından **7x24x365** gün boyunca **izlenmektedir**. Düzenli olarak MDR raporlarıyla müşterilerimize tespit edilen bulguların detayları paylaşılmaktadır.

Güvenlik analistleri tarafından izlenmekte olan müşteri sistemlerine kurallar eklendikten belli bir süre sonra ilgili zafiyetin istismar edilmesine dair alarmlar analistler tarafından tespit edilmektedir. Yapılan incelemeler doğrultusunda, siber atakların istismarı, geliştirilen kurallar ve IOC'ler aracılığı ile engellendikten sonra analistler tarafından zafiyete sebebiyet veren **kök neden** (root cause) **araştırılmaktadır**.

Analizler sonrasında elde edilen **bulgu ve IOC** verileri ile **ADEO tehdit istihbarat kaynağı** güncellenmektedir. Saldırılara ait elde edilmiş istihbarat veri setleri düzenli olarak müşterilerimizin sistemlerine eklenmektedir. Böylelikle eklenen IOC ve istihbarat verileri ile tüm müşteri sistemleri üzerinde ilgili güvenlik açığının istismar edilmesinin önüne geçilmektedir.

Aşağıda yer alan tabloda **minimum 1 gün, maximum 1 hafta** içerisinde ilgili güvenlik açığının mevcut müşteri sistemleri üzerinde istismar edilmeye çalışıldığına dair **istatistik veriler görülmektedir**.

GÜVENLİK AÇIĞI	Güvenlik Açığının Kurumlarda Ortalama İlk Görüntülenme Zamanı
Apache Log4j Zero-Day Vulnerability	2 GÜN
Possible InstallerFileTakeOver LPE | Zero-Day Vulnerability	3 GÜN
PetitPotam - NTLM Relay Attack	2 GÜN
Emotet Botnet | TrickBot Malware	4 GÜN
Microsoft MSHTML Remote Code Execution Vulnerability	3 GÜN
PrintNightmare aka SeriousSAM vulnerability	1 HAFTA
Coronavirus Phishing & Malware	1 GÜN
Razer MauseCVE-2021-30494	1 HAFTA
macOS Finder RCE Zero-Day	2 GÜN

2021 YILINDA YAŞANAN ÖNEMLİ GÜVENLİK ZAFİYETLERİ & GÖRÜLME ZAMANLARI

Apache Log4j Zero-Day Vulnerability

2 GÜN

Possible Installer File Take Over LPE | Zero-Day Vulnerability

3 GÜN

PetitPotam - NTLM Relay Attack

2 GÜN

Emotet Botnet TrickBot Malware

4 GÜN

Emotet

Microsoft MSHTML Remote Code Execution Vulnerability

3 GÜN

Microsoft MSHTML

PrintNightmare aka SeriousSAM Vulnerability

1 HAFTA

Coronavirus Phishing & Malware

1 GÜN

Razer Mause CVE-2021-30494

1 HAFTA

macOS Finder RCE Zero-Day

2 GÜN

11) YILIN EN SICAK GÜNDEMİ LOG4J

ADEO MDR SERVİSİ

LOG4J

Global trendlerin kontrolü ve **tehdit istihbaratlarının** takip edilmesiyle, **güncel zafiyetlere yönelik kurallar hızlıca** eklenmektedir.

En Yoğun Geçen Hafta: **13-19 Aralık**
Bu Hafta Gerçekleşen **Vaka Sayısı: 5**

En Yoğun Gün: **17 Aralık**
Bu Gün İncelenen **Alarm Sayısı: 485**

LOG4J

YILIN EN SICAK GÜNDEMİ #1 LOG4J

ADEO MDR SERVİSİ

1

13-19 Aralık haftası neden bu kadar yoğunduk?

Log4j'nin çıktığı haftaydı ve bu zafiyetin atak yüzeyinin çok geniş olması sebebiyle, tüm müşterilerin varlık envanterleri baz alınarak **tehdit avcılığı** çalışmaları yapılıp, müşterilerimize özel raporlar hazırlandı.

Bu hafta toplam **5 vaka** görüldü, bu 5 vaka yıllık vaka sayısının yaklaşık **%25'ine** karşılık gelmektedir.

2

Log4j zafiyeti için ne tür araştırmalar yapıldı?

Log4j'nin tespit edilebilmesi için globalde yayınlanan raporlar ve tehdit istihbaratı platformlarından **~3000 IOC** toplanıp, analiz edildikten sonra müşterilerimizin ürünlerine eklendi.

3

Özel oluşturduğumuz tespit kurallarını ne kadar süre ile güncelledik?

MDR servisi olarak Log4j zafiyetini kendi laboratuvar ortamlarımızda canlandırıp, ilgili zafiyetin tespit edilebilmesi için farklı paternler kullandık. Toplam **16 tespit kuralı** yazılarak tüm müşterilerimize **5 saat** içerisinde aktarılmıştır.

4

Log4j zafiyetinin kurumlarda görülme zamanı ve alınan aksiyonlar?

Log4j ile ilgili oluşturduğumuz özel kural setlerini ve tehdit istihbaratı platformlarından topladığımız IOC'leri müşterilerimize ekledikten **2 gün sonra,** ilgili zafiyet hakkında gerçek pozitif alarmlar alındı ve MDR Analistleri müdahale işlemlerinde bulunarak **zafiyetin sömürülmesini engelledi.**

12) YILIN EN SICAK GÜNDEMİ #2 LockBit Ransomware

ADEO MDR SERVİSİ

1

LOCKBIT ?

LockBit fidye yazılımı, kullanıcıların bilgisayar sistemlerine erişimini engellemek ve onları fidye ödemek zorunda bırakmak amacıyla tasarlanan bir kötü amaçlı yazılımdır. LockBit kullanımıyla gerçekleştirilen saldırılar **Eylül 2019'da o günkü adıyla ".abcd virus" ile başladı.** Yazılım, bugüne kadar **ABD, Çin, Hindistan, Endonezya ve Ukrayna**'daki kuruluşları hedef aldı. Ayrıca Avrupa genelinde birçok ülkede (Fransa, Birleşik Krallık, Almanya) saldırılar görüldü.

2

Lockbit, 2.0 ile Tekrar Sahada

Temmuz 2021'de LockBit 2.0, Active Directory grup ilkelerini kötüye kullanarak Windows etki alanlarında cihazların otomatik olarak şifrelenmesini sağlayan bir güncelleme yayınladı. FBI açıklamasına göre, **Ağustos 2021'de** ise LockBit 2.0, potansiyel kurban ağlarına **ilk erişim kurmaları için** kurum çalışanları ile anlaşarak, yapılan saldırının başarılı olması halinde **elde edilen gelirin bir kısmını gruba destek olan kişiler ile paylaşacağı** vaadinde bulundu.

3

Lockbit 2.0'ın 2021 Faaliyetleri

Haziran: En hızlı ve en verimli şifreleme özelliğine sahip veri sızdırmayı otomatikleştiren kötü amaçlı yazılım StealBit'in oluşturulması ve kullanılması gözlemlendi.

Ağustos: En hızlı ve en verimli şifreleme özelliğine sahip veri sızdırmayı otomatikleştiren kötü amaçlı yazılım StealBit'in oluşturulması ve kullanılması gözlemlendi.

Ekim: Linux ve VMware ESXI hypervisor yönetici platformlarını hedefleyen LockBit sürümü piyasaya sürüldü.

4

Özel oluşturduğumuz algılama kurallarını ne kadar süre ile güncelledik?

MDR servisi olarak Lockbit 2.0 zafiyetini kendi laboratuvar ortamlarımızda canlandırıp, ilgili zafiyetin tespit edilebilmesi için farklı paternler kullandık. Toplam **13 tespit kuralı ve 122 IOC** tüm müşterilerimize **6 saat** içerisinde aktarılmıştır.

LOCKBIT 2.0

13) YILIN EN SICAK GÜNDEMİ #3 PrintNightmare

ADEO MDR SERVİSİ

1 PrintNightmare Zafiyeti Nedir?

29 Haziran 2021'de Sangfor Technologies'deki güvenlik araştırmacıları tarafından, halka açık GitHub deposunda **PrintNightmare** kod adıyla bir Windows sıfırıncı gün (**ZeroDay**) güvenlik açığı yanlışlıkla açıklandı. Print Nightmare, Microsoft Windows işletim sistemini etkileyen kritik bir güvenlik açığıdır.

2 PrintNightmare zafiyetinin etkileri nedir?

Güvenlik açığı, yazdırma biriktirici hizmetinde (print spooler service) oluşur ve SYSTEM düzeyinde ayrıcalıklarda, kötü amaçlı kod yürütmek için, uzaktan kimlik doğrulamalı bir girişe izin verir. Bu zafiyet, tam kullanıcı haklarına sahip sistemlerde **yeni kullanıcılar oluşturulmasına, kötü amaçlı yazılım yüklenmesine ve verilerin değiştirilmesine veya silinmesine olanak tanır.**

3 Özel oluşturduğumuz algılama kurallarını ne kadar süre ile güncelledik?

MDR servisi olarak PrintNightmare zafiyetini kendi laboratuvar ortamlarımızda canlandırıp, ilgili zafiyetin tespit edilebilmesi için farklı paternler kullandık. Toplam geliştirilen **9 tespit kuralı** ve çeşitli global CTI kaynaklarından toplanan **364 zararlı IOC** tüm müşterilerimize **4 saat** içerisinde aktarılmıştır.

4 PrintNightmare zafiyeti görülme zamanı ve alınan aksiyonlar?

PrintNightmare ile ilgili oluşturduğumuz özel kural setlerini ve tehdit istihbaratı platformlarından topladığımız IOC'leri müşterilerimize ekledikten **1 hafta sonra** ilgili zafiyet hakkında **gerçek pozitif** alarmlar aldık ve MDR Analistleri müdahale işlemlerinde bulunarak **zafiyetin sömürülmesi engelledi.**

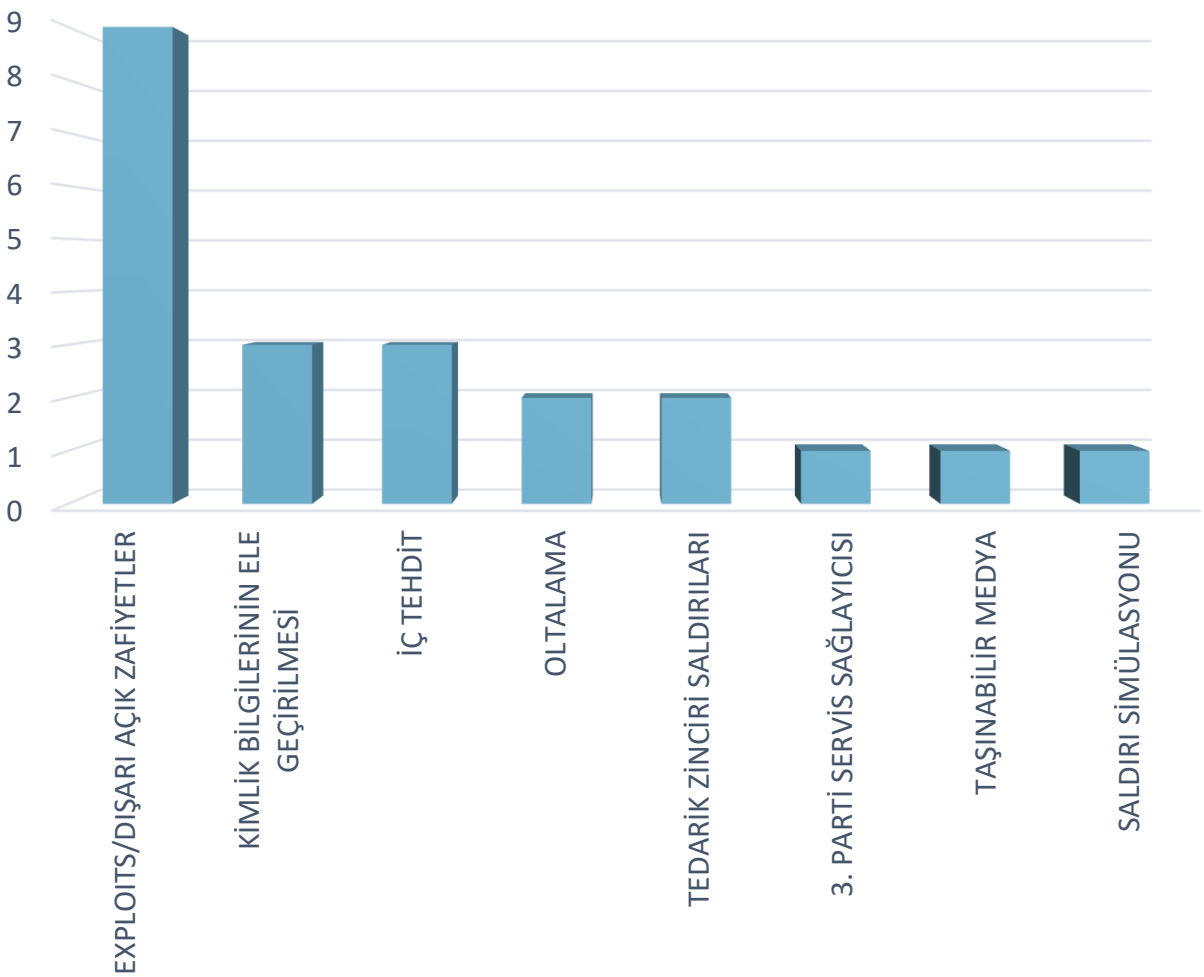
14) EN ÇOK KULLANILAN İLK ERİŞİM (INITIAL ACCESS) TEKNİKLERİ

Bir saldırganın ortamda yer edinebilmesi ilk erişim (**initial access**) ile başlar.

Güvenliği ihlal edilmiş hesapların kimlik bilgileri, çeşitli tekniklerle ele geçirilerek ağ içindeki sistemlerde farklı kaynaklara uygulanan erişim denetimlerini atlamak için kullanılabilir.

Saldırgan ilk erişimin ardından hedeflere ulaşmak için diğer taktik ve tekniklere geçiş yapabilir. Dolayısıyla ilk erişimin engellenmesi sistemin güvenliği açısından önem arz etmektedir.

Aşağıdaki grafikte yer alan Saldırı Simülasyonu başlığı Kırmızı/Mor Takım (Red/Purple Team) aktivitesini ifade etmektedir. Dolayısıyla gerçek bir ilk erişim taktiği içermemektedir.



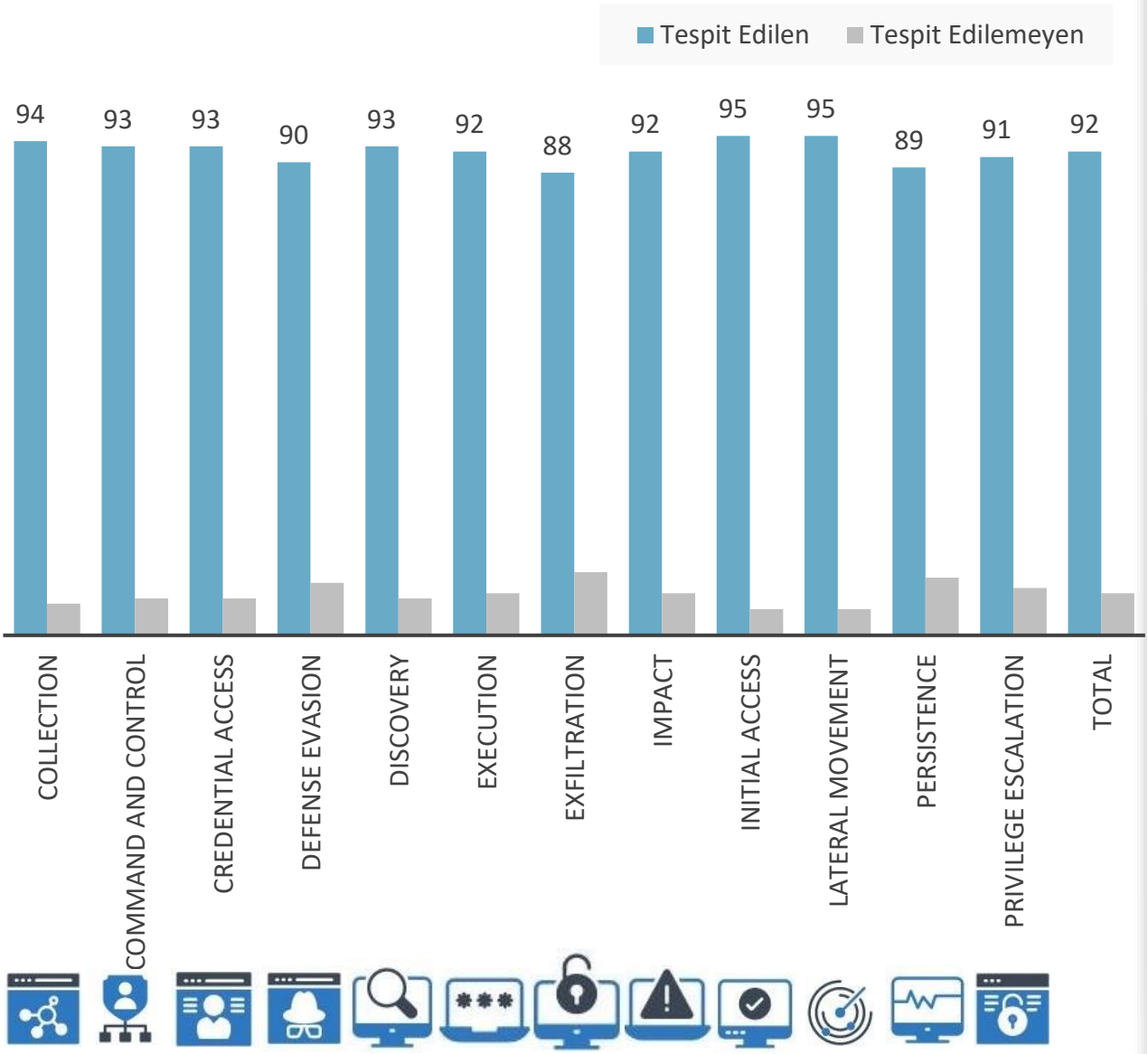
ADEO MDR SERVİSİ

TAKTİKLER, TEKNİKLER &TESPİT KURALLARIMIZ

16) SALDIRI TESPİT KURALLARIMIZ

ADEO MDR Servisi olarak MITRE ATT&CK® Framework'de bulunan tüm taktileri geliştirmiş olduğumuz özel algılama kuralları, tehdit istihbaratı platformlarından topladığımız IoC'ler ve güçlü lider ürün portföyümüz aracılığı ile tespit edebilmekteyiz.

MDR Servisi, gerçekleştirdiği güvenlik testlerinin sonucu olarak, EDR aracılığı ile **~1000 teknikten %96.6'sının tespit edilebildiği** raporlanmıştır. Tespit edilmeyen ~100 teknikten ise sadece **30 tanesinin EDR ile tespit edilebilir** olduğu gözlemlenmiştir.



17) TAKTİKLER

1) VERİ TOPLAMA (COLLECTION)

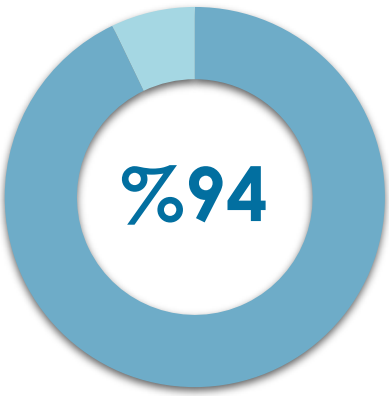
Saldırgan, amacına uygun verileri toplamaya çalışır.

Bu taktik, saldırganın amacına hizmet eden verileri toplamak için kullandığı tekniklerden oluşur.

Genellikle hedef alınan kaynaklar arasında çeşitli sürücü tipleri, tarayıcılar, ses ve video dosyaları ve e-postalar bulunur.

Ekran görüntüsü alma, klavye girişi takip etme yaygın yöntemler arasındadır.

Veri Toplama (Collection) taktiği kullanılarak yapılan saldırıların **%94'ü ADEO MDR Servisi'miz** tarafından tespit edilebilmektedir.



Bu ve benzeri saldırıların tespiti için **EDR teknolojisine ek olarak,** veri kaybı önleme sistemlerinin uygulanması önerilir. Saldırı riski, etkisi ve derecesinin azaltılması gibi kontrolleri planlamak ve politikaların sürekliliğinin sağlanması gibi çalışmalar için ek veri sızıntısı engelleme sistemi olan **DLP** teknolojisi kullanılması tavsiye edilir.

Sıkıştırılmış veya şifrelenmiş dosyaların sızdırılma teşebbüslerini engellemek ve kullanıcı davranış analizlerini **(UBA)** yapabilmek için **XDR, NDR, Firewall ,DLP** vb. teknolojilerin kullanılması tavsiye edilir.

Kullanıcı farkındalığının artırılması için düzenli periyotlarda **farkındalık eğitimleri**nin organize edilmesi önem arz etmektedir.

Kullanılan sistem imajlarının ve **yazılımlarının güncel tutulması** tavsiye edilir.

Exchange ortamında, yöneticilerin kötü amaçlı olabilecek otomatik iletme, indirme ve açma gibi etkinliklerini engellemek için **Exchange** kurallarının sıkılaştırılması gerekmektedir.
Dışarıdan erişime açık e-posta sunucuları için **çok faktörlü kimlik doğrulamasının (MFA)** kullanılması saldırıları büyük oranda azaltacaktır.

TAKTİKLER

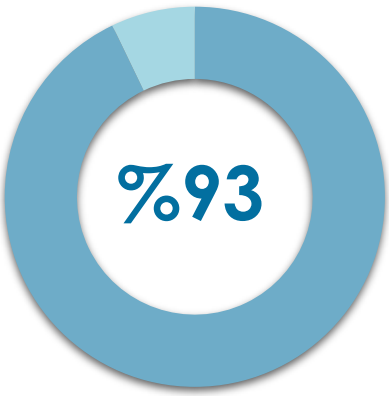
2) KOMUTA VE KONTROL (COMMAND AND CONTROL)

Saldırgan kontrolü ele geçirmek için güvenliği ihlal edilmiş sistemlerle iletişim kurmayı dener. Bunu yaparken tespit edilmekten kaçınmak için genellikle normal, beklenen trafiği taklit etmeye çalışır.

Komuta ve Kontrol (**C&C**), saldırganların kendi kontrolleri altındaki sistemlerle bir hedef network aracılığı ile iletişim kurduğu tekniklerden oluşur.

Saldırganın komuta ve kontrol taktiğini oluşturmasının, saldırı altındaki network'un yapısına ve savunmasına bağlı olarak çeşitlilik gösteren birçok yolu vardır.

Komuta ve Kontrol (Command and Control) taktiği kullanılarak yapılan saldırıların **%93'ü ADEO MDR Servisi'miz** tarafından tespit edilebilmektedir.



Bilinen **kötü veya şüpheli etki alanlarına (Domain)** giden/gelen **web trafiğinin izlenmesi** gerekmektedir.

DNS isteklerinin; bilinmeyen, güvenilmeyen veya bilinen kötü etki alanlarına ve kaynaklara **firewall üzerinden filtrelenmesi** tavsiye edilir.

Bu ve benzeri saldırıların tespiti için EDR'a **ek Firewall, NDR, IDS/IPS;** kullanıcı davranışı analizleri için **UBA** tabanlı ürünlerin kullanılmalısı tavsiye edilir.

Network'te oluşan **trafiğin izlenmesi** ve içeriden dışarıya giden ve dışarıdan gelen IP'lerin **istihbarat servisleriyle sürekli olarak kontrol edilmesi** gerekmektedir.

Sisteme yüklenebilen uygulamaların onay mekanizmasından geçmesi ve izin verilen uygulamalar listesinde **(White List)** olması zorunlu kılınmalıdır. Bilgisayar sisteminiz herhangi bir uygulamanın çalıştırılmasına veya yüklenmesine izin vermemelidir. Bilinmeyen kaynaklardan uygulamaların **yüklenmesini engelleyerek**, C2 kanalları oluşturmak için kullanılan **kötü amaçlı yazılımların sisteminize yüklenmesini önleyebilirsiniz.**

TAKTİKLER

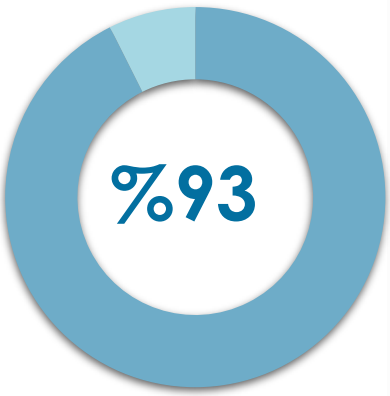
3) KİMLİK BİLGİLERİ ERİŞİMİ (CREDENTIAL ACCESS)

Saldırgan bu taktik ile hesap adlarını ve parolalarını çalmayı dener.

Kimlik bilgilerini almak için kullanılan yaygın teknikler arasında keylogging ve kimlik bilgisi dökümü (**Credential Dumping**) bulunur.

Meşru kimlik bilgilerinin kullanılması, saldırganların sisteme erişmesini sağlayabilir, tespit edilmelerini zorlaştırabilir ve hedeflerine kolay ulaşmalarına yardımcı olacak daha fazla hesap oluşturmalarına olanak sağlar.

Kimlik Bilgileri Erişimi (Credential Access) taktiği kullanılarak yapılan saldırıların **%93'ü ADEO MDR Servisi'miz** tarafından tespit edilebilmektedir.



WAF, kuruluşlar tarafından web sistemlerini sıfırıncı gün istismarlarına, uzaktan komut çalıştırmaya, diğer bilinen ve bilinmeyen tehdit ve güvenlik açıklarına karşı koruma sağlayan yaygın **bir güvenlik kontrolü** olup, **kurum içinde konumlandırılması** önem arz etmektedir .

Parolaların farklı platformlarda kullanılmaması, parolanın **en fazla 1 veya 3 aylık periyotlarda değiştirilmesi** ve özel karakter barındırmasına dikkat edilmesi gerekmektedir. **Gereksiz/fazla yetkilendirmeden kaçınılması**, personel işten çıktıktan sonra mevcut hesaplarının kapatılması önem arz etmektedir. **Dosya paylaşımları** yalnızca gerekli kullanıcılara erişimi olan **belirli dizinler ile sınırlandırılmalıdır.**

Kritik kaynaklara erişim izinlerine sahip kullanıcıların hesaplarının güvenli bir şekilde yönetilmesi için **Ayrıcalıklı Erişim Yönetimi – Privileged Access Management (PAM)** ürünlerinin kurum içinde konumlandırılması tavsiye edilir.

Başta VPN ve E-posta erişimleri olmak üzere, mümkün olan bütün girişlerde **MFA aktif edilmesi** önem arz etmektedir.

VLAN kullanılarak departmanların birbirinden izole edilmesi ile olası tehlikelerin en aza indirilmesi konusu önem arz etmektedir. Başta Domain Controller sunucuları olmak üzere **Kimlik bilgilerinin barındırıldığı** uygulamaların **güvenlik güncellemelerinin** düzenli periyotlarda yapılması tavsiye edilir.

TAKTİKLER

4) SAVUNMAYI ATLATMA (DEFENSE EVASION)

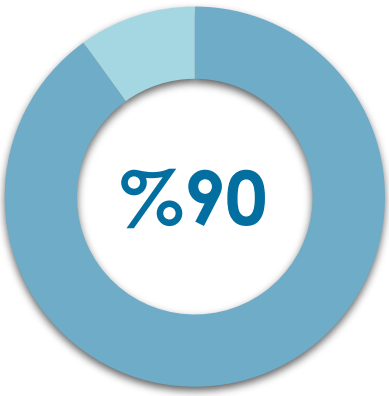
Saldırgan tespit edilmekten kaçınmaya çalışır.

Savunmayı Atlatma, saldırganların yarattıkları tehlike boyunca tespit edilmekten kaçınmak için kullandıkları tekniklerden oluşur.

Savunmayı Atlatma için kullanılan teknikler arasında güvenlik yazılımının kaldırılması/devre dışı bırakılması veya veri ve komut dosyalarının gizlenmesi/şifrelenmesi yer alır.

Saldırganlar ayrıca kötü amaçlı yazılımlarını gizlemek ve maskelemek için güvenilir süreçleri kötüye kullanır.

Savunmayı Atlatma (Defense Evasion) taktiği kullanılarak yapılan saldırıların **%90'ı ADEO MDR Servisi'miz** tarafından tespit edilebilmektedir.



PowerShell ve **Command Prompt** komut satırı uygulamaları aracılığı ile yapılan aktivitelerin analiz edilebilmesi için ilgili uygulamaların **Log**larının merkezi bir noktada **kaydedilmesi/arşivlenmesi** önerilir.
Hizmet engelleme saldırılarından (**DoS / DDoS**) korunmak ve atak türlerini minimize etmek için **Load Balance** (Yük Dengeleme), **DDoS Protection**, ürünlerinin kurum içinde konumlandırılması tavsiye edilir.

Kullanıcı **ayrıcalıklarının sınırlandırılması** önerilir.
Yalnızca yetkili kullanıcılar hizmet değişiklikleri yapabilecek şekilde sınırlanmalıdır.
Dosya indirme dizinleri ve geçici dosya (Temporary Files) dizinleri gibi kullanıcı dizinlerinden **yürütmenin engellenmesi** önerilir.

Saldırganlar, kötü amaçlı kodu gizlemek için derlenmiş **HTML dosyalarını (.chm)** kötüye kullanabilir. CHM dosyaları genellikle Microsoft HTML yardım sisteminin bir parçası olarak dağıtılır. CHM dosyaları **VBA, JScript, Java ve ActiveX** gibi gibi çeşitli içeriklerin sıkıştırılmış derlemeleridir. **Application whitelist yazılımları** ile bu tarz yaygın kullanılmayan **script uzantılarının** çalıştırılması **engellenebilir** ya da **tespit** edilebilir.

Kurum içinde **ihtiyaç duyulmayan uygulamaların** güvenlik açığı verebilecek özelliklerinin **devre dışı bırakılması/kaldırılması** önerilir.
E-posta yolu ile yapılan **oltalama saldırılarılarının** önlenmesi için **Sandbox** türevi teknolojilerin ve **Email Security Gateway** ürünlerinin konumlandırılması, kullanılan **uygulama envanterlerinin** düzenli periyotlarda **güvenlik güncelleştirmelerinin yapılması** önem arz etmektedir.

TAKTİKLER

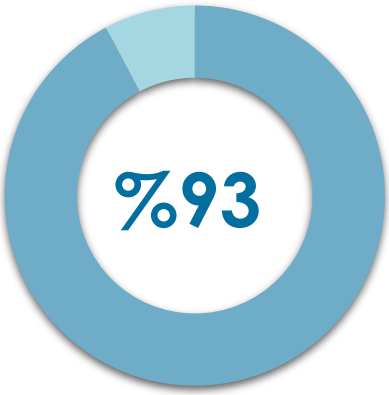
5) KEŞİF (DISCOVERY)

Saldırgan hedefini tanımaya, keşfetmeye çalışır.

Keşif, saldırganın sistem ve dahili network hakkında bilgi edinmek için kullanabileceği tekniklerden oluşur. Bu teknikler, saldırganın nasıl hareket edeceğine karar vermeden önce çevreyi gözlemlemesine ve planına yön vermesine yardımcı olur.

Bu teknikler saldırgana ayrıca neyi kontrol edebileceği ve giriş noktalarının çevresinde neler olabileceği konusunda fikir verir, fayda sağlar.

Keşif (Discovery) taktiği kullanılarak yapılan saldırıların **%93'ü ADEO MDR Servisi'miz** tarafından tespit edilebilmektedir.



Kurumlarda var olan ortam (**Active Directory, Firewall, Network Segmentasyon** ve varsa diğer güvenlik cihazlarının yardımı ile) ihtiyaca uygun şekilde sıkılaştırılarak, **atak yüzeyi daraltılmalıdır**. Ortamlar üzerinde çalışan **Audit** ve **Log seviyelerinin** sıkılaştırılması ve olgunlaştırılması tavsiye edilir.

Keşif ve olası sömürü riskini önlemek için varlık envanterlerinin belirli periyotlarda incelenmesi, **gereksiz bağlantı noktalarının, hizmetlerin ve servislerin kapalı** olduğundan emin olunması gerekmektedir.

Uzaktan hizmet taramalarını algılamak ve önlemek için **IPS/IDS teknolojilerinin** kullanılması tavsiye edilir.

Birçok önemli bilgi, Windows Yönetim Araçları ve PowerShell gibi Windows sistem yönetim araçları aracılığıyla da edinilebilir. Sistem ve ağ bilgilerini toplamak için gerçekleştirilebilecek bu tarz eylemleri tespit edebilmek için **Windows event logları** yapılandırılmalı ve merkezi olarak toplanlanmalıdır.

Varlık envanterinde olan uygulamaların **güvenlik güncelleştirmeleri** düzenli periyotlarda kontrol edilmelidir.

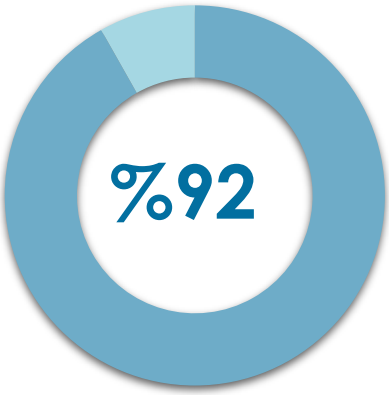
Kullanıcı hesap yönetimi sağlanmalı, **minimum ayrıcalık ilkesi** uygulanmalıdır.

6) YÜRÜTME (EXECUTION)

Yürütme, yerel veya uzak bir sistemde saldırganın kontrolündeki kodun çalıştırılmasını sağlayan tekniklerden oluşur.

Kötü amaçlı kod çalıştıran teknikler, bir network'u keşfetmek veya veri çalmak gibi daha geniş hedeflere ulaşmak için genellikle diğer tüm taktiklerdeki tekniklerle eşleştirilir. Örneğin bir saldırgan, uzaktan sistem keşfi yapan bir Powershell betiğini çalıştırmak için bir uzaktan erişim aracı kullanabilir.

Yürütme (Execution) taktiği kullanılarak yapılan saldırıların **%92'si ADEO MDR Servisi'miz** tarafından tespit edilebilmektedir.



Kullanıcı, kötü amaçlı bir dosyayı veya bağlantıyı açarak kötü amaçlı kod yürütmek için sosyal mühendislik saldırısına maruz kalabilir. Bu tür saldırıları önlemek için son kullanıcı tarafındaki e-posta ya da internet tarayıcı **uygulamalarının denetiminin ve güncellemesinin düzenli periyotlarda yapılması gerekmektedir.**

Saldırganların **RCE zafiyetinden yararlanmalarını** engellemek ya da tespit etmek için **NGFW** veya **NDR** ürünleri ile ağ trafiği üzerindeki görünürlük artırılmalıdır.

Kurumlarda var olan ortam **(Active Directory, Firewall, Network Segmentasyon ve varsa diğer güvenlik cihazlarının yardımıyla)** ihtiyaca uygun şekilde sıkılaştırılarak, **atak yüzeyi daraltılmalıdır**. Ortamlar üzerinde çalışan **Audit** ve **Log seviyelerinin** sıkılaştırılması, olgunlaştırılması ve **SIEM** teknolojilerinin kullanılması tavsiye edilir.

Dışarıya açık sunucularda bulunabilecek bir **RCE zafiyeti** saldırganın kolaylıkla kurum ağına girmesini sağlayacaktır. **Zero Trust** güvenlik stratejisi ile dışarıya açık sunuculardan içeriye ya da diğer sunuculara **yapılan erişimler, ağ erişim kontrolü (NAC) araçları** ile **sınırlandırılmalı** ve **takip edilmelidir.**

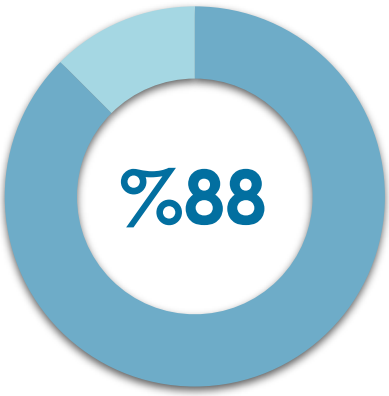
TAKTİKLER

7) VERİ KAÇIRMA (EXFILTRATION)

Veri Kaçırma, saldırganların ağınızdan veri çalmak için kullandığı tekniklerden oluşur. Saldırganlar verileri topladıklarında tespit edilmekten kaçınmak için onları sıkıştırma ve şifrelemeyi içerebilecek biçimde paketler.

Hedef bir ağdan veri elde etme teknikleri, tipik olarak, verinin kendi komuta ve kontrol kanalı veya alternatif bir kanal üzerinden aktarılmasını içerir. Ayrıca aktarıma boyut sınırları da koyulabilinmektedir.

Veri Kaçırma (Exfiltration) taktiği kullanılarak yapılan saldırıların **%88'i ADEO MDR Servisi'miz** tarafından tespit edilebilmektedir.



Verilerin ağdan ayrılabilmesi için tasarlanmış bir çıkış noktasından geçmesi gerektiğinden, tipik olarak C2 algılaması için yararlı olan imza tabanlı virüsten koruma özelliklerine sahip, **yeni nesil bir güvenlik duvarı (NGFW)** veya trafik protokollerini görebilen ağa izinsiz giriş önleme sistemi **(IPS) sızıntıyı tespit etmeye ve önlemeye yardımcı olabilir**.

DLP, kullanıcı tarafından hassas verilere yetkisiz olarak erişimi ve bu verilerin kullanımını izler. Verilerin dışarı çıkmasını önlediği için kullanılması tavsiye edilir.

Saldırganlar, **USB üzerinden** zararlı kodu çalıştırarak, ağ üzerinden yayılırlar. Bazı durumlarda bir kullanıcı tarafından tanıtılan bir **USB aygıtı aracılığıyla veri kaçırma gerçekleşebilir**. USB aygıtı, son veri kaçırma noktası olarak veya başka şekilde bağlantısız sistemler arasında geçiş yapmak için kullanılabilir. Bunun önüne geçebilmek için **farkındalığın düşük olduğu yerlerde usb portlarının devre dışı bırakılması önerilir.**

Saldırgan, verileri tek parça göndermek yerine **dosyaları parçalayarak gönderebilir.** Bu şekilde minimum yükleme boyutunu aşmadan verinin iletimini sağlar. Saldırıyı önlemek için **network trafiğinin sürekli olarak izlenmesi** önerilir.

TAKTİKLER

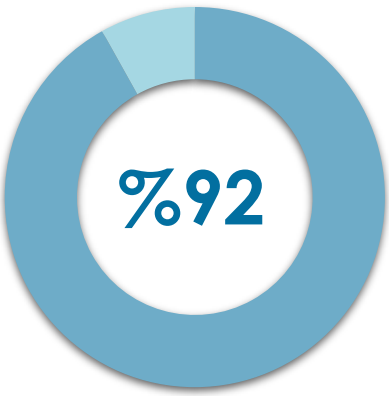
8) ETKİ (IMPACT)

Saldırgan, sistemlerinizi ve verilerinizi manipüle etmeyi, kesmeyi veya yok etmeyi dener.

Etki, saldırganların iş ve operasyonel süreçleri manipüle ederek kullanılabilirliği bozmak ve bütünlüğü tehlikeye atmak için kullandığı tekniklerden oluşur.

Etki için kullanılan teknikler verileri yok etme veya bozmayı içerebilir. Bazı durumlarda iş süreçleri iyi görünebilir, sorunsuz durur ancak saldırganın hedeflerine fayda sağlayacak şekilde değiştirilmiş olabilir.

Bu teknikler saldırganlar tarafından nihai hedeflerine ulaşmak veya bir gizlilik ihlalini örtmek için kullanılabilir.



Etki (Impact) taktiği kullanılarak yapılan saldırıların **%92'si ADEO MDR Servisi'miz** tarafından tespit edilebilmektedir.

Fidye yazılımı, sistem ve ağ kaynaklarına **erişimi kesmek** için hedef sistemlerdeki veya bir ağda bulunan çok sayıda sistemdeki verileri şifreleyebilir. Saldırıları önlemek için **felaket senaryoları hazırlanarak yedekler alınması** ve bu yedeklerin saldırganlar tarafından erişilmez hale getirilmesi önerilmektedir.

DDoS saldırısında; saldırıya uğrayan kaynağın, birden çok makineden gelen isteğe maruz kalmasıyla kapasiteyi aşarak yanıt vermemesi ile hizmet engelleme saldırısı başarıyla sonuçlanır. **DDOS önlemek için** trafiği filtreleyerek **İçerik Dağıtım Ağları (CDN)** veya **DoS** azaltma konusunda uzmanlaşmış sağlayıcılar tarafından sağlanan **DDoS önleme hizmeti alınması** önerilmektedir.

Veri Manipülasyonu: Saldırganlar, farklı sonuçlar ile faaliyetlerini gizleyerek verileri ekleyebilir, silebilir. Bu şekilde rakibinin verilerini manipüle ederek bir iş sürecini, organizasyonel anlayışı veya karar vermeyi etkilemeye çalışabilir. Oluşabilecek maddi kayıpları önlemek için **veriyi şifreleme, saklama yöntemi** ve **DLP** çözümlerinin kullanılması önerilir.

Man in the middle saldırısı ağda iki bağlantı arasındaki iletişimin dinlenmesi ile çeşitli verilerin ele geçirilmesi veya iletişimi dinleyip, yanıltıcı bir iletişim oluşturarak verinin manipüle edilmesi şeklinde gerçekleşen bir saldırı yöntemidir. **Mitm** saldırı türlerini önlemek için **SSH, IPSec** protokollerinin, **HTTPS** destekli sitelerin kullanılması, public ortamlarda paylaşılan şifresiz **WIFI** ağlarına bağlanılmamasına dikkat edilmesi önemlidir.

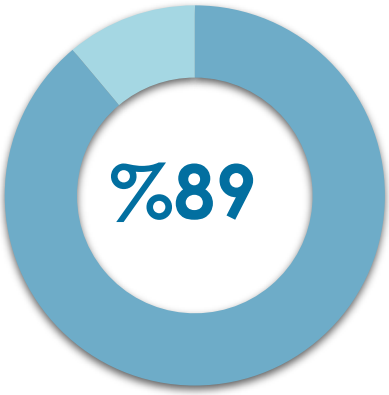
TAKTİKLER

9) KALICILIK (PERSISTENCE)

Kalıcılık, saldırganın sistem erişiminin sürekliliğini sağlamayı hedefleyen tekniklerden oluşur.

Kalıcılık için kullanılan teknikler, meşru kodu değiştirme/ele geçirme veya başlangıç kodu ekleme gibi sistemlerde yerlerini korumalarına izin veren tüm erişim, eylem ve yapılandırma değişikliklerini içerir.

Kalıcılık (Persistence) taktiği kullanılarak yapılan saldırıların **%89'u ADEO MDR Servisi'miz** tarafından tespit edilebilmektedir.



NDR, tüm bağlantı ve protokollerde size şeffaflık sağlar. Bağlantıları, akışları, paketleri ve meta verileri gerçek zamanlı olarak analiz etmek için trafiği derinlemesine tarar ve geriye dönük analiz yapar. **Algılanan bir tehdidin çözüm süresini en aza indirmek** için entegre bir **network algılama ve müdahale** çözümü kullanılması tavsiye edilir.

Önleme: Haftalık olarak ağda olan tüm cihazlar için **zararlı yazılım taraması** yaptırılması önem arz etmektedir. Ayrıca belirli aralıklarla **güvenlik ihlali analiz ve değerlendirme (Compromise Assessment)** çalışması yapılmalıdır.

Saldırganlar çeşitli zafiyetler barındıran varlıklarda **uzaktan komut çalıştırarak**, sistemlerde **sistem kapatma/yeniden başlatma işlemi** yaparak verilerin bozulmasına, e-ticaret ve hastane gibi ortam ve yerlerde maddi zararlara ve can kayıplarına sebebiyet verebilir. Bu ve benzeri atak türlerinin önlenebilmesi için **Extended Detection and Response (XDR), Firewall, Backup (yedekleme)** teknolojilerinin kullanılması tavsiye edilir.

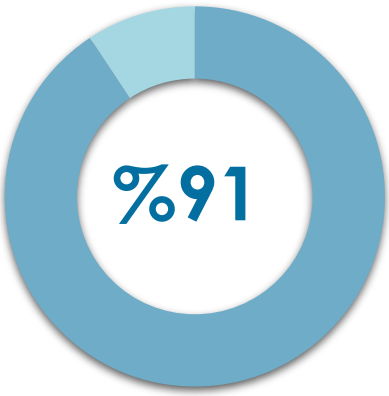
Korsan/Cracklenmiş program, oyun, işletim sistemi gibi yüklemeler sisteminizi ciddi saldırıların hedefi yapabilir. Kurumların fidye, veri ihlali, arka kapı gibi saldırılara maruz bırakılmasına yol açabilir. Bu ve benzeri saldırılar genellikle **kullanıcı farkındalığının az olmasından** kaynaklanır. Bu sebeple çalışanlara düzenli periyotlarda **temel güvenlik eğitimlerinin verilmesi tavsiye edilir.**

TAKTİKLER

10) YETKİ YÜKSELTME (PRIVILEGE ESCALATION)

Yetki Yükseltme, saldırganın bir sistem veya ağ üzerinde daha üst düzey izinler elde etmek için kullandığı tekniklerden oluşur. Saldırganlar genellikle ayrıcalıksız erişime sahip bir ağa girip keşif yapabilir ancak hedeflerini takip edebilmek için artırılmış izinlere ihtiyaç duyar. Yaygın yaklaşımlar, sistem zayıflıklarından, yanlış yapılandırmalardan ve güvenlik açıklarından yararlanmaktır. Yükseltilmiş erişim örnekleri şunları içerir;

- Sistem/ Kök seviyesi (Root Level)
- Domain yöneticisi (Domain Administrator),Yerel yönetici (Local Administrator)
- Yönetici benzeri erişime sahip kullanıcı hesabı (admin-like access),Belirli bir sisteme erişimi olan veya belirli bir işlevi yerine getiren kullanıcı hesapları



Bir saldırganın varlığını sürdürmesine izin veren işletim sistemi özellikleri yükseltilmiş bir bağlamda yürütülebildiğinden, bu teknikler genellikle "**Persistence (Kalıcılık)**" tekniği ile örtüşür.

Yetki Yükseltme (Privilege Escalation) taktiği kullanılarak yapılan saldırıların **%91'i ADEO MDR Servisi'miz** tarafından tespit edilebilmektedir.

Active Directory (AD) veya LDAP gibi dizin sunucularından gelen logların yapılandırılması gerekmektedir. Kullanıcı hak yükseltme veya yeni kullanıcı oluşturma olaylarının takip edilmesi gerekmektedir. Yetkili kullanıcı hesap adlarının, yetkilerinin bir **listesinin oluşturulması** gerekmektedir. **Kimlik tabanlı güvenlik (Identity-based Security)** ürünleri kullanılarak yetki yükseltme saldırıları ya da yetkili kullanıcılara yönelik saldırılar tespit edilebilir.

Ayrıcalıklı erişim haklarının uygun aralıklarla (ayda en az 1 kez) gözden geçirilmesi ve **ayrıcalıklı izinler** atamasının **düzenli olarak gözden geçirilmesi gerekmektedir**. Dosyalara ve veri tabanlarına olan (yerel sistem erişimi dahil) tüm **ayrıcalıklı kullanım erişimlerinin izlenmesi gerekmektedir**. Kritik ayrıcalıklı kullanıcı değişikliklerinin alarm mekanizmalarının Mail-SMS oluşturularak ilgili **BT yöneticileri ile anlık olarak paylaşılması gerekmektedir.**

Kullanıcıların **kötü amaçlı** dosyaların, yürütülmesi için yerleştirilebileceği yerleri azaltmak adına **dizin erişim denetiminin ayarlandığından emin olun.** Tüm yürütülebilir dosyalarda **yazma korumalı** dizinlere yerleştirilmesi tavsiye edilir.

Güvenlik açıklarını saldırganlar bu zafiyetlerden faydalanmadan tespit etmek önem taşımaktadır. **Güvenlik açığı tarama araçları** ile yapılan etkili bir tarama işlemi; sistemdeki **yanlış yapılanmaları, zayıf parolaları ve Web Sunucusu Güvenliği'ndeki zayıflıkları** ortaya çıkarır.
Etkili güvenlik açığı taraması ile kuruluşlar, tehdit vektörlerini uzak tutmak için ek güvenlik katmanlarını **güncelleyebilir, yamalayabilir veya dağıtabilir.**

TAKTİKLER

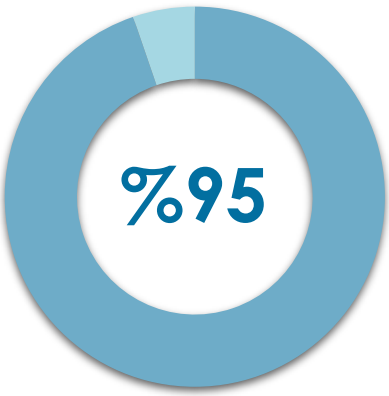
11) İLK ERİŞİM (INITIAL ACCESS)

İlk Erişim, saldırganın hedef ağ içerisinde birincil dayanağını elde etmesine yarayan çeşitli giriş vektörlerinin kullanıldığı tekniklerden oluşur.

Bir erişim elde etmek için kullanılan bu teknikler, hedeflenen kimlik avı ve dışarıya açık web sunucularındaki zayıflıklardan yararlanmayı içerir.

İlk Erişim yoluyla kazanılan erişimler, geçerli hesaplar ve harici uzak hizmetlerin kullanımı gibi sürekli erişime izin verebilir veya değişen parolalar nedeniyle sınırlı kullanım olabilir.

İlk Erişim (Initial Access) taktiği kullanılarak yapılan saldırıların **%95'i ADEO MDR Servisi'miz** tarafından tespit edilebilmektedir.



Kullanıcıların parola belirlerken sosyal ağlarda ve diğer platformlardaki parolalarını kullanmamaları, parolaların değiştirilme aralığının **1 ile 3 ay arasında** olması, özel karekter içermesi ve **minimum 14 karekter** zorunluluğu getirilmesi gerekmektedir.
Hesap yetkilendirme yapılması sırasında gereksiz yetki verilmesinden kaçınılmalıdır. **İşten çıkan personelin hesaplarının kapatılması** önemlidir.

E-posta içindeki **URL incelemesi** (kısaltılmış bağlantıların genişletilmesi dahil), bilinen kötü amaçlı sitelere giden bağlantıların algılanabilmesine yardımcı olabilir. **Sandbox** çözümleri bu bağlantıları algılamak ve kötü amaçlı davranışları belirlemek için otomatik olarak bu sitelere erişim sağlayarak veya bir kullanıcı bağlantıyı ziyaret ederse içeriği beklemek ve yakalamak için kullanılabilir.

Kimlik doğrulama loglarını toplanması ve normal çalışma saatleri dışında olağan dışı/yetkisiz erişimlerin tespit edilmesi gerekmektedir.

Kullanılan uygulama varlık envanterlerinin (web tarayıcıları, bileşenler, eklentiler, ofis ve medya vb.) **düzenli periyotlarda güncelleştirilmesi** önem arz etmektedir.
Tehdit istihbaratı kaynakları tarafından kötü amaçlı olarak sınıflandırılan ağ trafiklerinin **engellenmesi, uyarı oluşturulması sağlanmalıdır.**

TAKTİKLER

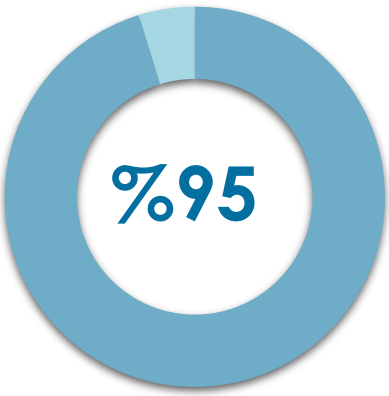
12) YANAL HAREKET (LATERAL MOVEMENT)

Yanal Hareket, saldırganların bir ağdaki uzak sistemlere girmek ve onları kontrol etmek için kullandığı tekniklerden oluşur. Gerçek hedeflerini takip etmek, genellikle hedeflerini bulmak için ağı keşfetmeyi ve ardından ona erişim sağlamayı gerektirir.

Hedeflerine ulaşmak için, genellikle birden fazla sistem ve hesap arasında geçiş yapmayı içerir.

Saldırganlar, yanal hareketi gerçekleştirmek için kendi uzaktan erişim araçlarını kurabilir veya daha gizli olabilecek yerel ağ ve işletim sistemi araçlarıyla meşru kimlik bilgilerini kullanabilir.

Yanal Hareket (Lateral Movement) taktiği kullanılarak yapılan saldırıların **%95'i ADEO MDR Servisi'miz** tarafından tespit edilebilmektedir.



Yanal hareket teknikleri ağ ortamına ve nasıl kullanıldığına bağlı olarak meşru olabilir. **Uzaktan oturum açmadan (RDP)** sonra oluşan erişilen dosyalar ya da gerçekleşen aktiviteler gibi faktörler, bu hareket ile ilgili şüpheli veya kötü amaçlı davranışlara işaret edebilir. Normalde birden çok sisteme nispeten kısa bir süre içinde erişemeyecekleri sistemlerde **oturum açmış kullanıcı hesaplarının izlenmesi önerilir.**

VLAN network ağlarını birbirinden **izole** ederek saldırıların ağda yayılmasına ve veri ihlalerinin önüne geçmektedir.

VPN ile erişilen sistemlerin ya da hizmetlerin sınırlandırılması VPN hesaplarının ele geçmesi durumunda içeride yayılımı minimum düzeyde tutacaktır.

WinRM kullanımı sistem ekipleri tarafından yaygın değilse devre dışı bırakılmalıdır. Eğer yaygın olarak kullanılıyorsa **Windows event logları** yapılandırılmalı ve merkezi olarak **SIEM** üzerinde toplanmalıdır.
Yazılan kurallar ile toplanan bu loglar üzerinden şüpheli erişimler tespit edilmelidir.

SSH kullanımı, ağ ortamına ve nasıl kullanıldığına bağlı olarak meşru olabilir. Uzaktan oturum açmadan sonra oluşan aktiviteler gibi diğer faktörler, **şüpheli veya kötü amaçlı davranışlara** işaret edebilir. Normalde birden çok sisteme nispeten kısa bir süre içinde erişemeyecekleri sistemlerde oturum açmış **kullanıcı hesaplarını izlemek gerekmektedir.**

18) İŞLETİM SİSTEMLERİNE GÖRE KURAL DAĞILIMI

ADEO MDR Servisi olarak **Windows, Linux, MacOS** işletim sistemi ve **türevleri** (*Windows Server, Workstation, Centos, Unix, Debian, Ubuntu tabanlı vb.*) özelinde toplam **2000+** tespit kuralı mevcuttur.

Geliştirilen tespit kuralarının dağılımları **Windows işletim sisteminde 1632, Linux 411 ve MacOS ise 407** kural şeklindedir.

Geliştirdiğimiz tespit kuralları **MITRE ATT&CK® Framework**'deki Linux, MacOs, Windows tabanlı tüm işletim sistemleri için oluşturulan **Taktik, Teknik, Prosedürlerin (TTP)** ortalama **%93'ünü** kapsamaktadır.

Bu sayede tüm müşterilemize **3 işletim sistemi** ve türevleri için **%95**'in üzerinde tespit oranıyla destek verebilmekteyiz.

1600+ **400+** **400+**

19) ÖNERİLER

- Olası bir saldırının önüne geçebilmek için **MSSP** veya **MDR** hizmeti ile **7x24x365** gün **izlenmesi gerekmektedir**.

- İkili kimlik doğrulama **MFA aktif edilmesi**, gereksiz yetki verilmesinden kaçınılması, farkındalığın düşük olduğu yerlerde önleyici önlemlerin alınması önemlidir.

- Olası siber olaylara karşın hep güncel bir aksiyon planının oluşturulması ve belli periyotlarla **simülasyonların** tekrar edilerek **farkındalığın** ve hazırlıkların **güncel tutulması gerekmektedir.**

- **IT ve OT** sistemlerinin tamamı kapsayan görünürlük ve sıkılaştırmaların eksiksiz **takip edilmesi önemlidir.**

- Otomatize ürün ve yazılımların, sistemlerin satın alınmasından ziyade **insan temelli servislerin** veya siber güvenlik ekiplerindeki **insanlara olan yatırımın arttırılması** gerekmektedir.

- **Kırmızı Takım (Red Team)** ve **Sızma (Penetrasyon) Testi** aktivitelerinin düzenli periyotlarda uzman ekiplerce gerçekleştirilmesi sağlanmalıdır.

- Saldırıların büyük bir çoğunluğunun yeni çıkan zafiyetlerden kaynaklandığı göz önünde bulundurulmalıdır. Buradan hareketle **"Vulnerability Management"** prosedürlerinin sürekli olarak uygulanması ve bunların sıkı bir şekilde takip edilmesi önem arz etmektedir.

- **Oltalama (Phishing)** saldırılarına karşı kullanıcılar çalışanlara belirli periyotlarda **farkındalık eğitimlerinin** uygulamalı olarak verilmesi, insan kaynaklı saldırıların önüne geçme noktasında faydalı olmaktadır.

- Tespit yeteneklerinin arttırılması ve bunun için öncellikle görünürlüğün arttırılması; ilgili atakları **tespit edecek kuralların** ve **korelasyonların sürekli olarak güncellenmesi** gerekmektedir.

- Siber güvenlik ekiplerinin olgunluk seviyesininin ölçülmesine yönelik Mor Takım **(Purple Team)** aksiyonlarının, uzman ekiplerce alınması sağlanmalıdır.

- **Varlık envanterlerinin** belirli periyotlarda incelenmesi, **dışarıya açık** olan **servislerin kontrollerinin** sağlanması gerekmektedir.

- Kurumlarda var olan **ortam** (Active Directory, Firewall, Network Segmentasyon ve varsa diğer güvenlik cihazlarının) ihtiyaca uygun şekilde sıkılaştırılarak, **atak yüzeyi daraltılmalıdır**.

20) TANIMLAR

MDR (Managed Detection and Response/Yönetilen Tespit ve Müdahale)

MDR, siber saldırıları mümkün olan en hızlı şekilde tespit etmek ve bunlara müdahale etmek için gereken süreçlerin belirlendiği ve yönetildiği servistir.

Gerçek zamanlı siber olay tespiti yapıp, bu saldırılar ile ilgili hızlı aksiyon alarak benzerlerinin gerçekleşmemesi için yapılması gerekenlerin ortaya çıkarılmasını kapsar.

EDR (Endpoint Detection and Response/Uç Nokta Tehdit Algılama ve Yanıt)

Uç noktalarda çalışan tüm işlemleri ve bunların yapmış olduğu aktiviteleri kayıt altına alarak, atomik indikatörlerin yanı sıra davranışsal indikatörlere göre tespit ve tehdit avcılığı imkanı sağlayan ve gerektiğinde şüpheli aktivitelere ait kanıtların toplanabildiği ya da müdahale edilebildiği araçlardır.

XDR (Extended Detection and Response/Genişletilmiş Tespit ve Müdahale)

EDR araçlarına ek olarak başta network olmak üzere cloud, kimlik yönetimi, e-posta güvenliği gibi çeşitli kaynaklardan da kayıtlar analiz edebilen araçlardır.

ALARM

Siber saldırıları tespit edebilmek için kullanılan güvenlik araçlarına düşen uyarı mesajlarına denir. Bu alarmlar kritiklik seviyelerine göre gruplandırılırlar.

TANIMLAR

TTP

Bir tehdit aktörünün işleyişini açıklamak/tanımlamakta kullanılan Teknik, Taktik ve Prosedürler başlıklarının kısaltmasıdır. TTP'ler belirli bir tehdit aktörünün profilini çıkarmak için kullanılmaktadır.

TRUE POSITIVE ALARM

Gerçek bir saldırı ya da istenmeyen/illegal davranış belirten alarmlardır.

FALSE POSITIVE ALARM

Yapılan analizler sonucunda gerçek bir saldırı işaret etmediği belirlenen ya da hatalı yazılan kurallar doğrultusunda oluşan alarmlardır.

VAKA (INCIDENT)

Tespit edilen true bir alarmın analiz edilmesi sonucunda derinlemesine analiz ve olay müdahalesi süreçlerinin işletilmesini gerektiren saldırgan aktiviteleridir. Çoğunlukla kısa süre içerisinde birden fazla makinede yayılım ve kalıcılık gösteren aktivitelerdir.

TAKTİK

Saldırgan tarafından gerçekleştirilen aktivitelerin amacını belirtir. Saldırının aşamasını belirlemede büyük önem arz etmektedir.

TESPİT SÜRESİ

Saldırının gerçekleşmesi ile saldırının MDR ekibi tarafından görülüp, saldırı olarak tanımlanması arasında geçen süreye denir.

TANIMLAR

MÜDAHALE SÜRESİ

Saldırının gerçekleşmesi ile, ilgili saldırının MDR Ekibi tarafından görülüp, tanımlanmasının ardından gerekli aksiyonun alındığı zaman aralığına denir.

PURPLE TEAM

Mor Takım, Kırmızı Takım ve Mavi Takım'ın birlikte çalışması, iş birliğidir. Kırmızı Takım ve Mavi Takım'ın her ikisinin de beceri ve süreçlerinin geliştirilmesi hedeflenir.

Managed Security Service Providers (MSSP) - Yönetilen Güvenlik Hizmet Sağlayıcısı

(MSSP), bir kuruluşa uzaktan yazılım/donanım tabanlı bilgi veya ağ güvenliği hizmetleri sağlayan bir tür hizmet sağlayıcısıdır. Bir MSSP, bir veya daha fazla istemciye aynı anda bilgi güvenliği (IS) hizmetleri sağlayarak bir güvenlik altyapısını barındırır, dağıtır ve yönetir.

Operasyonel Teknolojiler (OT)

İdari operasyonların aksine endüstriyel operasyonları yönetmek için kullanılan bilgisayar sistemlerini ifade eder. OT, fiziksel cihazların nasıl çalıştığını izleyen ve kontrol eden bir donanım ve yazılım kategorisi olarak da tanımlanabilir. Üretim (proses) sistemine ve/veya depolama ve dağıtım sistemlerine sahip işletmeler IT'den tamamen farklı ağ ve cihaz yapısı kullanır. Aynı cihaz anahtar (switch), kablo ve yönlendiriciler kullanıldığı için bu yapının farklılığını anlamak ilk bakışta zordur. PLC'ler, kontrolcüler, sensörler, operatör istasyonlarının hepsinin bir araya gelmesinden oluşan bu yapıya OT (Operasyonel Teknoloji) denilmektedir.

ADEO

MANAGED DETECTION AND RESPONSE

MDR Servis Hizmeti'miz ile ilgili detaylı bilgi almak için

mdr@adeo.com.tr

üzerinden bizimle iletişime geçebilirsiniz.

İstanbul Merkez

Fetih Mah. Tahralı Sk.
Tahralı Sitesi Kavakyeli Plaza
C Blok D16/17
Ataşehir / İSTANBUL / TÜRKİYE

Telefon: +90 (216) 472 35 35
Fax: +90 (216) 472 35 36

Ankara Şube

Kabil Cad. (Eski 4.Cad)
1335. Sokak No:58 D:9-10
Aşağı Öveçler
Çankaya / ANKARA / TÜRKİYE

Telefon: +90 (312) 482 12 35
Fax: +90 (312) 482 12 36

Email: **info@adeo.com.tr**

adeo.com.tr
mxdrturkiye.com

/adeosecurity /adeodfir
/adeocomtr

/ADEOcomtr

/ADEO Cyber Security Services

/adeocomtr