

Avaddon Ransomware

23.08.2024 – 25.08.2024

Doğukan KAYA

İçerikler

1. Avaddon Ransomware.....	3
1.1. Avaddon Ransomware (Initial Access)	3
1.2. Avaddon Ransomware Koruma ve İzleme Adımları.....	4
1.3. Avaddon Ransomware (Execution)	5
1.4. Avaddon Ransomware (Execution Mitigations)	6
2. Finding a Proof	9
2.1. Avaddon Ransomware Suspicious Registry Activities	9
2.2. Adding Registry Activities.....	11
2.3. SIGMA Rules for Suspicious Registry Activities for Avaddon	12
2.4. Elastic Rules for Detecting Suspicious Registry Activities	14

1. Avaddon Ransomware

Avaddon, 2020 yılından itibaren siber suçluların gerçekleştirdiği bir fidye yazılımıdır. Aynı zamanda RaaS (Ransomware as a Service) olarak çalışır. Bu fidye yazılımı hedef aldığı sistemlerdeki verileri şifreleyerek fidye talebinde bulunur, ödenmediği takdirde bu verileri kamu ile paylaşma tehdidinde bulunur. Kurbanlarını genellikle phishing (Oltalama) saldırıları ile hedef alarak ilk aşamayı bu şekilde başlatır.

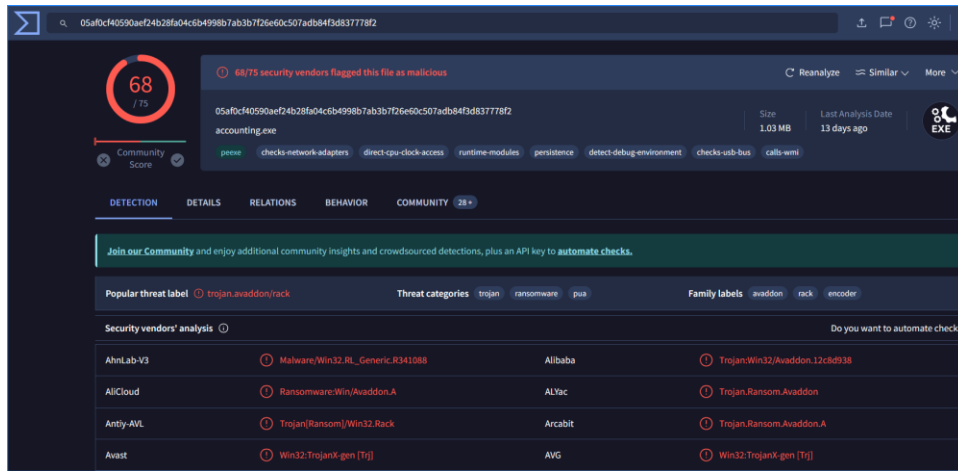


Figure 1 - Avaddon Ransomware VirusTotal

1.1. Avaddon Ransomware (Initial Access)

Avaddon fidye yazılımı, kurbanlarını ilk giriş yöntemi olarak phishing (oltalama) saldırıları ile hedef alır. MITRE ATT&CK Framework' göre Avaddon, T1566 Phishing tekniğini ve bu tekniğin altında bulunan T1566.001 (Spearphishing Attachment) alt tekniğini kullanır.

Phishing			
Sub-techniques (4)			
ID	Name		
T1566.001	Spearphishing Attachment		
T1566.002	Spearphishing Link		
T1566.003	Spearphishing via Service		
T1566.004	Spearphishing Voice		
		ID: T1566	
		Sub-techniques: T1566.001, T1566.002, T1566.003, T1566.004	
		Tactic: Initial Access	
		Platforms: Google Workspace, Linux, Office 365, SaaS, Windows, macOS	
		Contributors: Liora Itkin; Liran Ravich, CardinalOps; Ohad Zaidenberg, @ohad_mz; Philip Winther; Scott Cook, Capital One	

Figure 2 - MITRE ATT&CK Phishing

1.2. Avaddon Ransomware Koruma ve İzleme Adımları

Avaddon fidye yazılımının ilk giriş aşamasında kullandığı Phishing taktiği için üç farklı alanda alınabilecek koruma ve izleme adımları detaylı olarak incelenecektir.

Çalışan Bazında Koruma ve İzleme Adımları

- Siber farkındalık eğitimlerinin verilmesi.
- Oltalama saldırıları hakkında giriş-gelişme-sonuç olacak şekilde örnek senaryolar ile seminerler düzenlenmesi
- Aralıklı zamanlar ile çalışanlara phishing testlerinin yapıp, ulaşılan sonuca göre farkındalığı en üst seviyeye çıkarana kadar tekrarlanması.

Teknoloji Bazında Koruma ve İzleme Adımları

- Firewall kurulum ve konfigürasyonu ile phishing sitelerine karşı koruma sağlanması.
- IDS/IPS ürünlerini, Firewall ile entegre kullanarak şüpheli aktivitelerin tespitinin sağlanması.
- Kurumların Email Security (Örn. FortiMail) ürünlerini kullanarak e-posta güvenliğini artırması.
- SIEM çözümlerinden yararlanılarak şüpheli trafik analizinin gerçekleştirilmesi ve ilgili kuralların SIEM'e entegre edilmesi.
- Gelen e-postaların sandbox aracılığı ile sanal ortamlarda incelenmesi ve analiz edilmesi.
- Email Security ürünlerinin yanı sıra URL Filtering, SPF ve DKIM gibi prosedürlerin kontrollerinin sağlanması.

Süreç Bazında Koruma Adımları

- Kurum çalışanlarının olası bir oltalama saldırısı şüphesinde acil iletişime geçeceği bir siber güvenlik personeli atanması.
- SOC L1 Analistlerinin olası bir oltalama saldırısında ya da kurum çalışanları tarafından gelen ihbara göre izleyeceği pathway'i adım adım belirlemek ve buna uymak.
- SOC ekiplerinin örnek oltalama saldırısı e-postalarının bilgilerini kurum çalışanlarına bildirmesi ile çalışan farkındalığının artırılması.
- SOC ekiplerinin süreç ile birlikte phishing saldırılarının en aza indirgenmesi için SIEM ile entegreli kurallar oluşturması ve önlemlerin alınması.
- Phishing saldırılarının etkili ve yıkıcı etkileri olması durumunda bir senaryo oluşturulması ve buna karşılık bir yedekleme politikası izleme.

1.3. Avaddon Ransomware (Execution)

Avaddon Ransomware, Initial Access aşamasında kurbanlarına Phishing (T1566) tekniği ve Spearphishing Attachment (T1566.001) alt-tekniki ile yaklaştığı ele alındı.

Bu aşamadan sonra Avaddon, MITRE ATT&CK Framework'e göre Execution (TA0002) taktiğine geçecektir ve bu taktik altında kullandığı çeşitli teknikler ve alt teknikler mevcuttur.

1. Command and Scripting Interpreter: JavaScript (T1059.007)

Avaddon, hedeflediği kullanıcılara Phishing aracılığı ile ilettiği ek dosyalarının içerisine zararlı javascript kodları yerleştirerek bu zararlı .jsp kodlarının hedef sistemde çalışmasını sağlayabilir.

2. Native API (T1106)

S0640	Avaddon	Avaddon has used the Windows Crypto API to generate an AES key. ^[25]
-------	---------	---

Windows Crypto API, veri şifreleme işlemlerini gerçekleştiren bir Windows API'dir. Avaddon hedef sistemdeki verileri AES algoritması ile şifrelemek için bu API kullanır.

3. System Services: Service Execution (T1569.002)

Saldırganlar, kötü amaçlı komutları veya yükleri çalıştırmak için Windows hizmet kontrol yöneticisini kötüye kullanabilirler. Windows hizmet kontrol yöneticisi (services.exe), hizmetleri yönetmek ve manipüle etmek için kullanılan bir arayüzdür.

Avaddon, kendine "sc create" komutu ile yeni bir servis oluşturabilir ve bu oluşturduğu servisi yetki yükseltme yaparak yönetici haklarında çalışmasını sağlayabilir. Hedef sistemdeki bazı servisleri "sc stop" komutu ile durdurabilir. Bunun yanı sıra oluşturduğu ve müdahale edebildiği servisler ile güncellemeler yaparak hedef sistemde kalıcılığını sağlayabilir.

4. Windows Management Instrumentation (T1047)

S0640	Avaddon	Avaddon uses wmic.exe to delete shadow copies. ^[14]
-------	---------	--

“Saldırganlar, kötü amaçlı komutları ve yükleri çalıştırmak için Windows Yönetim Araçlarını (WMI) kötüye kullanabilirler. WMI, programcılar için tasarlanmış olup, Windows sistemlerinde yönetim verileri ve işlemleri için bir altyapıdır. WMI, Windows sistem bileşenlerine erişim sağlamak için standart bir ortam sunan bir yönetim özelliğidir.”

Shadow copy, Windows sistemlerin belirli aralıklarla anlık olarak aldığı sistem yedekleridir ve herhangi bir recovery durumunda cihazın yeniden yüklenmesi durumunda yardımcı olur. Avaddon bu shadow copy’leri silerek, ransomware saldırısını gerçekleştğinde hedef cihazın backup alabilmesini engeller.

1.4. Avaddon Ransomware (Execution Mitigations)

1. Command and Scripting Interpreter: JavaScript (T1059.007)

Web Server Logs

Web Sunucu logları alınarak, saldırganın hedef sistemde bir javascript kodu çalıştırıp çalıştırmadığını HTTP istekleri incelenerek tespit edilebilir. SIEM ürününe access.log bilgileri entegre edilerek izlenebilir ve şüpheli URL, şüpheli IP adresi gibi bilgiler Kural olarak yazılıp alarm üretilebilir.

AV ve EDR

Son kullanıcılara AV ve EDR çözümlerinin kurulması ile birlikte şüpheli javascript dosyalarının çalıştırılması durumlarında tespitinin sağlanması ve raporlanması ile bir anomali durumunda incelenebilir.

Firewall Logları

Firewall üzerinden traffic logları incelenerek, Ağ üzerinden Javascript içeren şüpheli trafikler incelenebilir. Firewall traffic logları SIEM ürününe entegre edilerek bunun üzerine çeşitli Kural setleri yazılıp alarm üretilebilir.

2. Native API (T1106)

Event Logları

Native API ile yapılabilecek bir saldırıyı tespit etmek için Windows sistemlerde belirli Event

ID'lerin kontrolleri sağlanabilir. Bunlar arasında;

- 4688 (Process creation)
- 4689 (Process has exited)
- 4697 (A service was intalled in the system)

Gibi önemli event ID'ler incelenerek Windows API'lerinin kötüye kullanım ilişkilendirilmesi yapılabilir. SIEM ürününe Windows Event Logları entegre edilerek bunun üzerine Kural yazılıp alarm üretilebilir.

Sysmon Logları

Windows API'lerinin kötüye kullanımında Sysmon logları da toplanabilir. Bunlar arasında

- 1 (Process create)
- 2 (Process terminate)
- 10 (Image Load)

Gibi önemli Event ID'ler bulunur. Bunlar Windows API'lerinin kötüye kullanımı ile ilişkilendirilebilecek bulgular olmakla beraber SIEM ürününe Sysmon logları entegre edilerek bunun üzerine Kural yazılıp alarm üretilebilir.

EDR ve AV Logları

Son kullanıcılara yüklenen EDR ve AV çözümlerinin oluşturduğu detaylı raporlar ve uyarılar incelenebilir ve olası bir tehdit durumunda analizi yapılabilir.

Windows API Monitoring Tools

Windows sistemlere kurulan API monitoring araçları ile API çağrılarını izleyip detaylı bilgiler sağlanabilir (Örn. Procmon). SIEM ürününe bu toollar entegre edilerek izlenimi ve şüpheli bir aktivitede önlem alınması sağlanabilir.

3. System Services: Service Execution (T1569.002)

Event Logs

Windows Event logları bu saldırı tekniği için izlenmelidir ve belirli Event ID'ler bulunur. Bunlar arasında;

- 4697 (A New Security Service Was Installed)
- 7045 (A New Service Was Installed)
- 7030 (Service Start Success)
- 7035 (Service Start Requested)
- 7036 (Service State Changes)

Gibi event ID'ler incelenerek olağan dışı bir servis oluşturması, değiştirilmesi, durdurulması ya da değiştirilmesi kontrolü sağlanabilir. Windows Event logları SIEM ürününe entegre edilerek bu Event ID'ler üzerinden belirli kurallar oluşturularak alarm üretilebilir.

Sysmon Logları

Sistem Servislerinin kötüye kullanımında Sysmon logları da toplanabilir. Bunlar arasında

- 1 (Process create)
- 2 (Process terminate)
- 10 (Image Load)

Gibi önemli Event ID'ler bulunur. Bunlar Sistem servislerinin kötüye kullanımı ile ilişkilendirilebilecek bulgular olmakla beraber SIEM ürününe Sysmon logları entegre edilerek bunun üzerine Kural yazılıp alarm üretilebilir.

4. Windows Management Instrumentation (T1047)

Event Logs

Windows Event logları bu saldırı tekniği için izlenmelidir ve belirli Event ID'ler bulunur. Bunlar arasında;

- 4697 (A New Security Service Was Installed)
- 4688 (A New Process Has Been Created)
- 4689 (A Process Has Been Terminated)

Gibi event ID'ler incelenebilir. WMI komutları genellikle yeni işlemler oluşturur, WMI üzerinden yeni bir güvenlik servisi yüklenmiş olabilir ve şüpheli WMI işlemlerinin sonlandırılması gibi olaylar ele alınabilir. SIEM ürününe Windows Event Logları entegre edilerek bunun üzerine Kural yazılıp alarm üretilebilir.

Sysmon Logları

WMI kullanılarak başlatılan işlemler bu loglar aracılığı ile görüntülenebilir. "wmic.exe" veya "powershell.exe" ile başlatılan komutlar bu aşamada değerlendirmeye alınabilir.

- 1 (Process create)
- 10 (Image Load)

Sysmon Logları, SIEM ürününe entegre edilerek bunun üzerine Kural yazılıp alarm üretilebilir.

WMI Monitoring Araçları

Windows sistemler üzerine kurulabilen WMI izleme araçları kullanılarak şüpheli aktivitelerin izlenmesi sağlanabilir. Burada "wmic" veya "powershell" kullanılarak yapılan sorgular, yetkisiz erişim durumları incelenerek SIEM ürününe entegre edilip bunun üzerine Kural seti geliştirilip alarm üretilebilir.

2. Finding a Proof

2.1. Avaddon Ransomware Suspicious Registry Activities

Avaddon Ransomware MITRE: <https://attack.mitre.org/software/S0640/>

Avaddon, sistemin ele geçirilmesi sırasında aşağıdaki registry değerlerini değiştirir.

Registry: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System EnableLUA=0
Mitre: Persistence (TA0003) and Privilege Escalation (TA0004)
Description: Windows'un kullanıcı hesap denetimi (UAC) sistemi, kullanıcıların sistemlerde yüksek izin gerektiren işlemleri gerçekleştirmeleri durumunda onay vermelerini sağlar. Bu registry ile Avaddon "EnableLUA" değerini "0" yaparak kullanıcıların yönetici yetkisi gerektiren işlemlerini daha kolay gerçekleştirmelerini sağlar.

Registry: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System EnableLinkedConnections=1
Mitre: Persistence (TA0003) and Privilege Escalation (TA0004)
Description: Windows işletim sistemlerinde bulunan Linked Connections özelliğini "EnableLinkedConnections" değerini "1" konumuna getirerek etkinleştirme aşamasını gerçekleştirir. Avaddon fidye yazılımı ağ sürücülerine ve paylaşımlarına erişimini sağlamak için emin olur. Bu değişiklik, fidye yazılımının ağ üzerindeki tüm mevcut konumlarda dosyaları şifreleyerek veya başka şekilde etkileyerek zararını artırmasına yardımcı olur.

Registry: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System ConsentPromptBehaviorAdmin=0
Mitre: Abuse Elevation Control Mechanism: Bypass User Account Control - T1548.002
Description: Avaddon, "ConsentPromptBehaviorAdmin" değerini "0" konumuna getirerek, Windows sistemlerde bulunan izin ve kimlik doğrulama ayarlarını en basite indirger. Bu değer "0" konumuna gelmesi ile herhangi bir kimlik doğrulama ya da onay penceresi olmadan yönetici haklarıyla işlem gerçekleştirilebilir ve sistemi sömürmesi daha da kolay bir hale gelir.

Avaddon, sistem başlangıcında otomatik olarak çalışmasını sağlamak için aşağıdaki registry değerlerini ekler.

Registry: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run update = %Application Data%\{avaddon}.exe
Mitre: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder - T1547.001
Description: Avaddon, Bu registry değerini HKEY_CURRENT_USER altına ekleyerek aktif kullanıcı her oturum açtığına kendi zararlı yazılımının çalışmasını sağlar. Böylelikle hedef cihaz her açılıp kullanıcı girişi olduğunda zararlı kendini yeniden çalıştıracaktır ve kalıcılık sağlanacaktır.

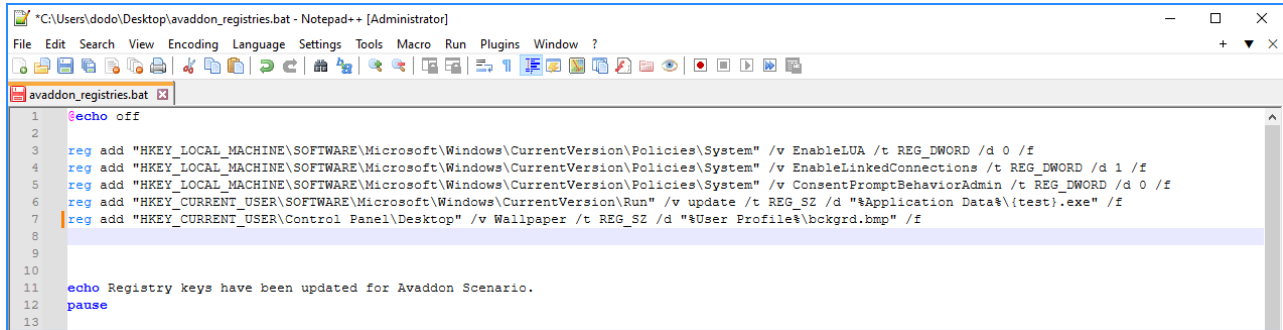
Registry: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run update = %Application Data%\{avaddon}.exe
Mitre: Persistence (TA0003) - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder(T1547.001)
Description: Avaddon, Bu registry değerini HKLM altına ekleyerek bilgisayar her açıldığında zararlı yazılımının çalışmasını sağlar. HKLM altına eklenerek belirli bir kullanıcı yerine sistem açıldığında tüm kullanıcılar için çalışmasıdır. Böylelikle hedef cihaz her açıldığında zararlı kendini yeniden çalıştıracaktır ve kalıcılık sağlanacaktır.

Avaddon, masaüstü arka plan fotoğrafını değiştirmek için aşağıdaki registry değerini değiştirir.

Registry: HKEY_CURRENT_USER\Control Panel\Desktop Wallpaper = %User Profile%\bckgrd.bmp
Description: Avaddon, HKCU altına ransomware saldırı bilgisinin sağlanması ve masaüstü arka plan fotoğrafını kendi istekleri üzerinde değiştirilmesi için bu registry değerinin eklemesini yapar.

2.2. Adding Registry Activities

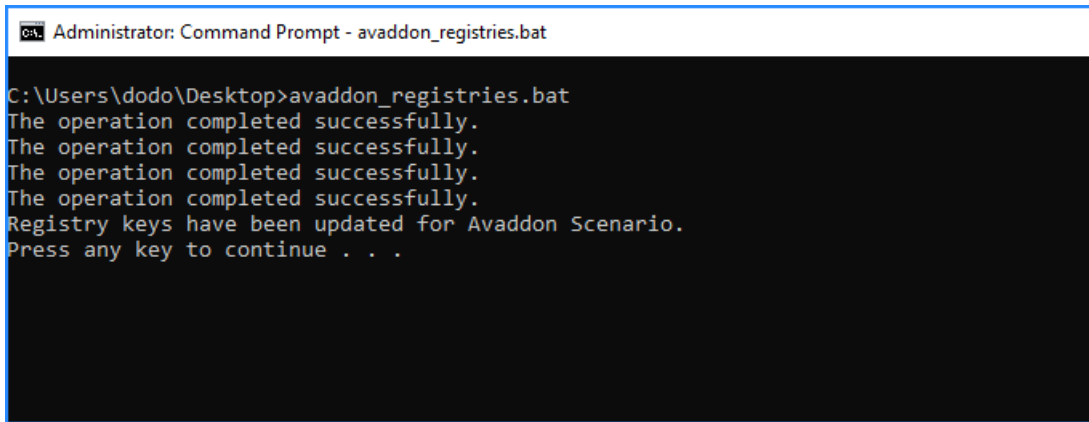
Avaddon Ransomware'ın, sistem üzerinde çalıştığı, eklediği ve değiştirdiği registry kayıtlarını hedef cihazda topluca çalıştırmak için ilgili bir .bat dosyayı oluşturulacaktır ve tüm registry hedef cihaza eklenecektir.



```
*C:\Users\dodo\Desktop\avaddon_registries.bat - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
avaddon_registries.bat
1  @echo off
2
3  reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v EnableLUA /t REG_DWORD /d 0 /f
4  reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v EnableLinkedConnections /t REG_DWORD /d 1 /f
5  reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v ConsentPromptBehaviorAdmin /t REG_DWORD /d 0 /f
6  reg add "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v update /t REG_SZ /d "%Application Data%\test.exe" /f
7  reg add "HKEY_CURRENT_USER\Control Panel\Desktop" /v Wallpaper /t REG_SZ /d "%User Profile%\bckgrd.bmp" /f
8
9
10
11 echo Registry keys have been updated for Avaddon Scenario.
12 pause
13
```

Figure 1 - .bat File for Registry Activities

.bat dosyası içerisine eklenen tüm registry komutları başarılı bir şekilde çalıştırılmıştır.



```
C:\Users\dodo\Desktop>avaddon_registries.bat
The operation completed successfully.
The operation completed successfully.
The operation completed successfully.
The operation completed successfully.
Registry keys have been updated for Avaddon Scenario.
Press any key to continue . . .
```

Figure 2 - Executing the .bat File

2.3. SIGMA Rules for Suspicious Registry Activities for Avaddon

title: Şüpheli UAC Disabled Tespiti

id: 48437c39-9e5f-47fb-af95-3d663c3f2919

related:

- id: c5f6a85d-b647-40f7-bbad-c10b66bab038

type: similar

- id: 0d7ceef-3539-4392-8953-3dc664912714

type: similar

status: stable

description: |

Saldırgan UAC'yi registry değerleri ile devre dışı bırakmak, "EnableLUA" değerini "0" konumuna getirdiğinde tespit sağlar.

author: Doğukan KAYA

date: 2024-08-29

modified: 2024-08-29

tags:

- attack.privilege-escalation

- attack.defense-evasion

- attack.t1548.002

logsource:

category: registry_set

product: windows

detection:

selection:

TargetObject|contains: '\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\EnableLUA'

Details: 'DWORD (0x00000000)'

condition: selection

level: High

title: Registry üzerinden Şüpheli Masaüstü arka planı Değişikliği

id: 85b88e05-dadc-430b-8a9e-53ff1cd30aae

related:

- id: 8cbc9475-8d05-4e27-9c32-df960716c701

type: similar

status: experimental

description: |

Kullanıcının masaüstü arka planının yerini alacak kayıt defteri değeri ayarlarını algılar.

Bu, kötü amaçlı yazılımların masaüstü arka planını fidye notu veya başka bir görüntüyle değiştirmek için kullandığı yaygın bir tekniktir.

author: Doğukan KAYA

date: 2024-08-29

tags:

- attack.defense-evasion
- attack.impact
- attack.t1112
- attack.t1491.001

logsource:

product: windows

category: registry_set

detection:

selection_keys:

TargetObject | contains:

- 'Control Panel\Desktop'
- 'CurrentVersion\Policies\ActiveDesktop'
- 'CurrentVersion\Policies\System'

selection_values_1:

TargetObject | endswith: 'NoChangingWallpaper'

Details: 'DWORD (0x00000001)' # Prevent changing desktop background

selection_values_2:

TargetObject | endswith: '\\Wallpaper'

selection_values_3:

TargetObject|endswith: '\\WallpaperStyle'

Details: '2' # Stretch

filter_main_svchost:

Note: Excluding GPO changes

Image|endswith: '\\svchost.exe'

condition: selection_keys and 1 of selection_values_* and not 1 of filter_main_*

level: medium

2.4. Elastic Rules for Detecting Suspicious Registry Activities

Şüpheli Registry Aktivitesi için yazılan Kural çıktısı;

About

Sistemlerde genellikle ransomware saldırılarında kullanılan "EnableLUA=0", "EnableLinkedConnections=1" ve "ConsentPromptBehaviorAdmin=0" zararlı registry aktivitelerinin tespitini sağlar.

Author Doğukan KAYA

Severity High

Risk score 73

Max alerts per run 100

Definition

Index patterns apm-* transaction* auditbeat-* endgame-* filebeat-* logs-* packetbeat-* traces-apm* winlogbeat-* -*elastic-cloud-logs-*

Custom query host.name : "desktop-f23lll8" and registry.path : "HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System" and registry.value : "EnableLUA" or "EnableLinkedConnections" or "ConsentPromptBehaviorAdmin" and process.name : "regedit.exe"

Rule type Query

Timeline template None

Figure 3 - SIEM Rule