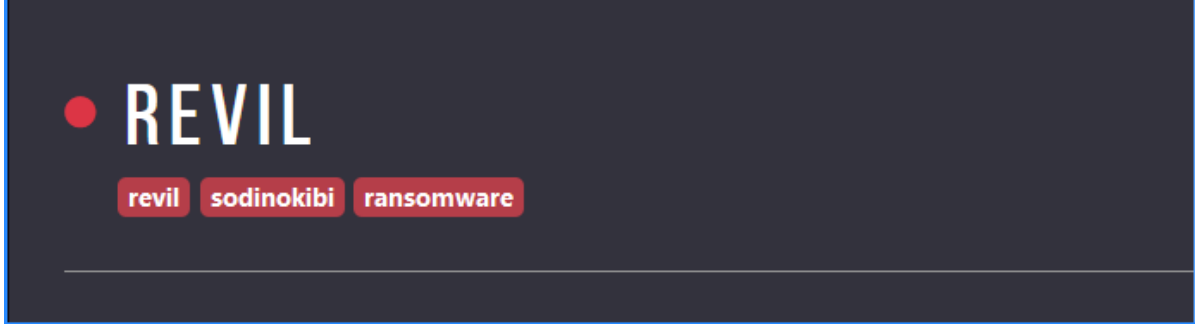


REvil (Sodinokibi) Ransomware Saldırısı



Bu rapor, GOLD SOUTHFIELD APT grubu tarafından gerçekleştirilen ve sarsıcı etkiler yaratan REvil (Sodinokibi) Ransomware saldırısının detaylarını, örnek bir senaryosunu, process incelemesini ve yazılabilecek SIGMA kurallarını içerir.

08.08.2024 – 09.08.2024

Doğukan KAYA

İçindekiler

REvil (Sodinokibi) Ransomware Saldırısı	1
1.1. REvil Ransomware ve GOLD SOUTHFIELD	3
2.1. ANY-RUN Analizi	4
3.1. MITRE ATT&CK Matrix.....	11
4.1. IOC	11
5.1. REvil Ransomware için SIGMA Kuralları	12
6.1. References	17

1.1. REvil Ransomware ve GOLD SOUTHFIELD

REvil bir fidye yazılımıdır. Ransomware + Evil kelimelerinin birleşiminden ortaya çıkmıştır. Aynı zamanda Sodinokibi olarakta bilinir. Kurbanlarının dosyalarını şifreleyerek erişilmez hale getirir ve ardından şifrelerin çözülmesi için genellikle BTC formatında bir ücret talep eder. Aynı zamanda RaaS (Ransomware as a Service) olarak çalışır, Saldırganlar REvil fidye yazılımını kullanarak kendi saldırılarını gerçekleştirebilirler. Ayrıca FIN7 APT grubu da REvil fidye yazılımını kullanmıştır.

REvil Ransomware: <https://attack.mitre.org/software/S0496/>

ID: S0496
① Associated Software: Sodin, Sodinokibi
① Type: MALWARE
① Platforms: Windows
Contributors: Edward Millington
Version: 2.2
Created: 04 August 2020
Last Modified: 11 April 2024

Figure 1 - REvil Info

REvil fidye yazılımının arkasında GOLD SOUTHFIELD isimli APT grubu bulunmaktadır. Bu hacker grubu 2018'den beri aktif olarak saldırılarına devam etmektedir. Motivasyonlarını finansal açıdan ve RaaS (Ransomware as a Service) işleterek sağlarlar. MITRE ATT&CK Framework tablosuna göre T1059.001, T1190, T1133, T1027.010, T1566, T1219, T1113, T1195.002, T1199 olmak üzere kullandığı 9 farklı teknik bulunmaktadır.

GOLD SOUTHFIELD APT GROUP: <https://attack.mitre.org/groups/G0115/>

ID: G0115
① Associated Groups: Pinchy Spider
Contributors: Thijn Bukkems, Amazon
Version: 2.0
Created: 22 September 2020
Last Modified: 28 March 2023

Figure 2 - GOLD SOUTHFIELD Info

2.1. ANY-RUN Analizi

REvil Ransomware saldırı senaryosunun gerçekleştirildiği bir Windows cihazın analizi gerçekleştirilecektir.

Malicious Activity: REvil Ransomware Saldırısı

Date of Compromise: 13.07.2024 - 18:38

Malicious File: sodinokibi.exe

2.1.1. Ransomware Yüklemesi

sodinokibi.exe, hedef sisteme bir .docx dosyası görüntüsü ile yükleniyor. Kurban, dosyayı çalıştırdıktan sonraki analizlerde CPU kullanımı normale göre yüksek bir artış gösteriyor.

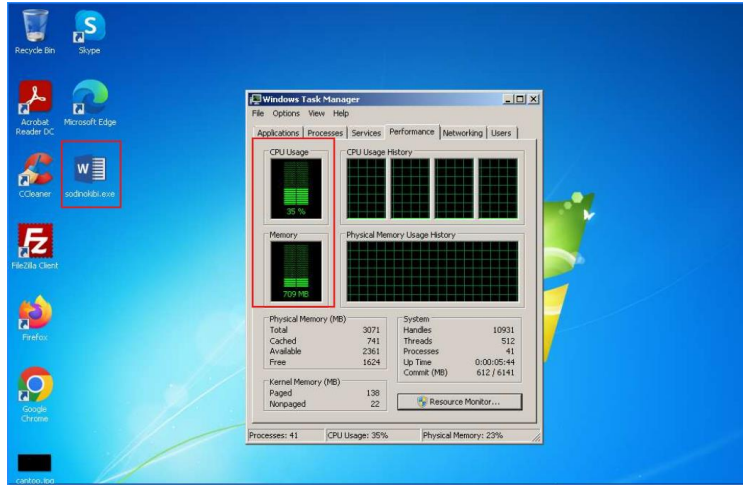
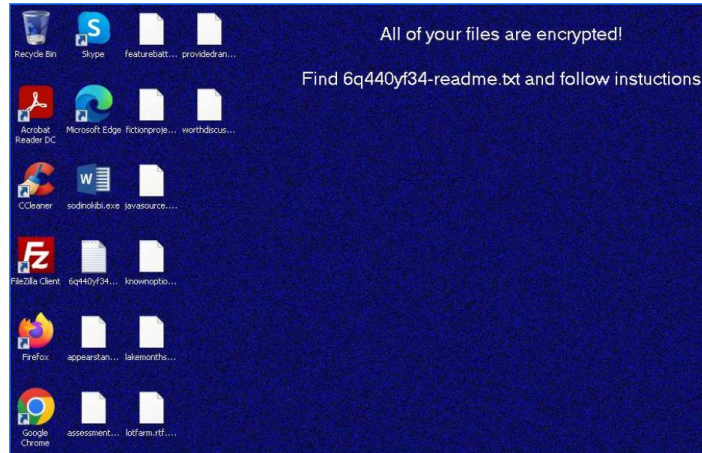


Figure 3 - sodinokibi.exe

İlgili zararlı dosya çalıştırıldıktan sonra kurban bilgisayarındaki tüm dosyalar şifreleniyor. Ardından saldırganlar tarafından 6q440yf34-readme.txt dosyasına taleplerinin karşılanması ve izlemesi gereken yollar için yönlendiriliyor.



2.1.2. Process Detayları

sodinokibi.exe zararlısı çalıştıktan sonra hedef kurban makinede arka planda çalışan processler daha detaylı bir şekilde ele alınacaktır.

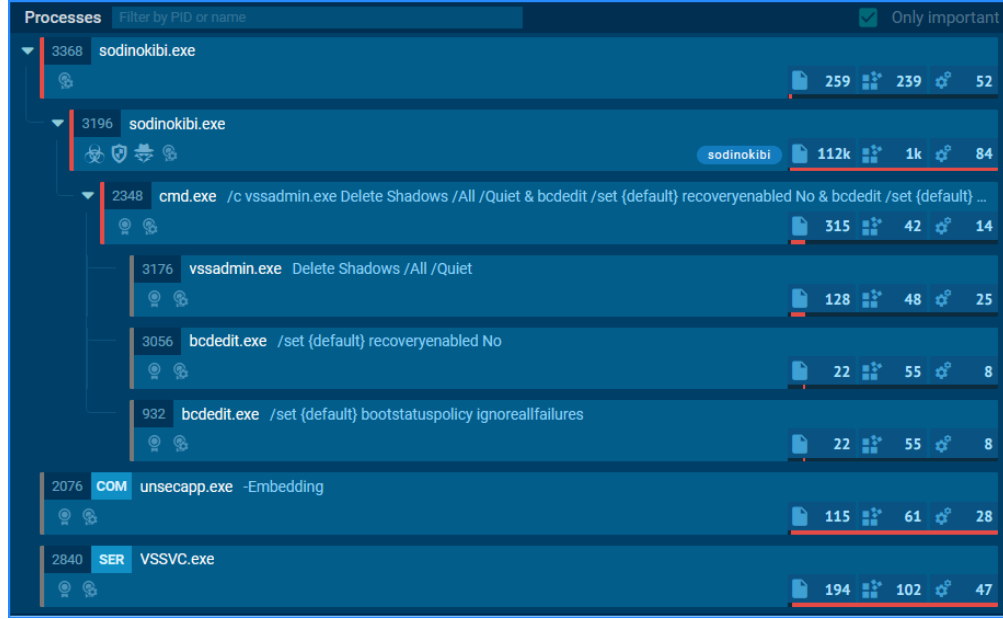


Figure 4 - Process Tree1



Figure 5 - Process Tree2

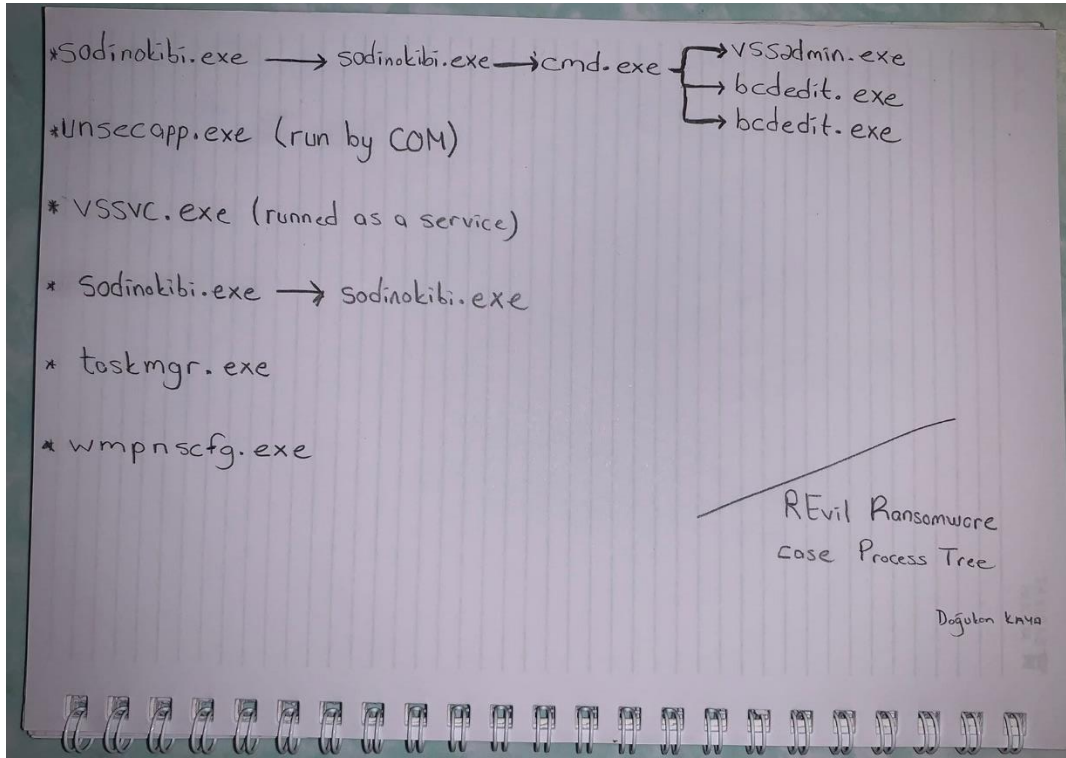


Figure 6 - General Process Tree

General Process Tree (Figure 6) incelenecek olursa, sodinokibi.exe komut satırında ilk çalıştığında kendini launch ederek aynı isimle ikinci bir process oluşturuyor. Bu process ise Figure 7'de görüldüğü üzere 4 tehlikeli, 3 uyarı niteliğinde alarm oluşuyor. Detaylar arasında YARA kuralları sayesinde SODINOKIBI (REvil) Ransomware saldırısının tespit edildiği saptanıyor. Uyarı alanında ise bu process'in CMD.EXE'yi çalıştırdığı tespit ediliyor.



Process information Username: admin SID: S-1-5-21-1302019708-1500728564-335382590-1000 IL: HIGH Start: 3.92 s	Danger 4 T1486 Data Encrypted for Impact (2) - Renames files like ransomware - Sodinokibi ransom note is found SODINOKIBI has been detected (YARA) T1552.001 Credentials In Files (1) - Actions looks like stealing of personal data T1518 Software Discovery (1) - Actions looks like stealing of personal data
File information Command line   "C:\Users\admin\Desktop\sodinokibi.exe"	Warning 3 T1486 Data Encrypted for Impact (1) - Creates files like ransomware instruction T1059.003 Windows Command Shell (1) - Starts CMD.EXE for commands execution T1012 Query Registry (2) - Reads security settings of Internet Explorer - Reads the Internet Settings

Figure 7 - sodinokibi.exe Details

sodinokibi.exe --> cmd.exe --> bcdedit.exe

cmd.exe çalıştıktan sonra Figure 8 de görüldüğü üzere saldırgan bcdedit.exe komutu çalıştırarak RECOVERYENABLED NO seçeneğini aktifleştiriyor. bcdedit.exe, Windows sistemlerde Boot Status Policy ayarlar. Saldırgan bu komut ile işletim sisteminin recovery modunu devre dışı bırakarak hedef sistemin yeniden yüklenmesi ve zararlı yazılımlardan temizlenmesi işlemlerini zorlaştırır.

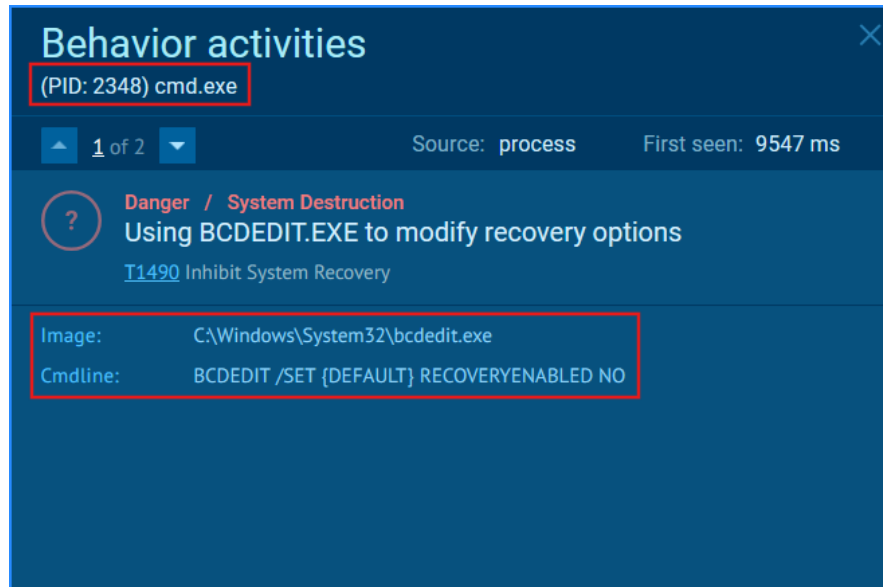


Figure 8 - bcdedit.exe

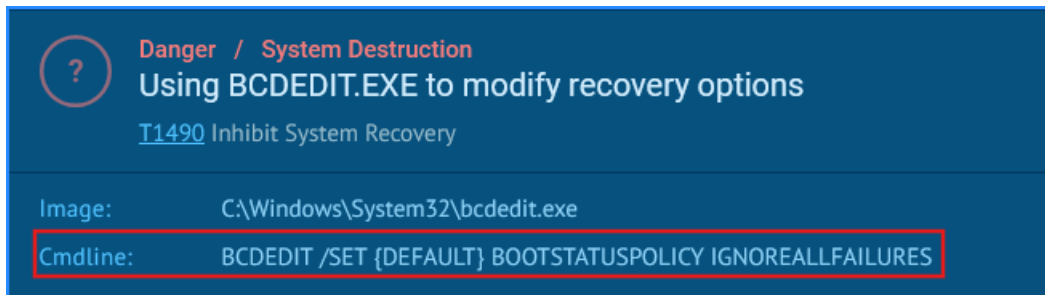


Figure 9 - bcdedit.exe

sodinokibi.exe --> cmd.exe --> vssadmin.exe

cmd.exe'nin çalıştırdığı bir diğer process ise vssadmin.exe. Bu komut satırı aracı, Windows'un yedekleme ve geri yükleme işlemleri için kullanılır. Saldırgan “vssadmin.exe Delete Shadows /All /Quiet” komutu ile Windows'un yedekleme ve geri yükleme için tuttuğu kopyaları (Shadows), /All komutu ile hepsini ve /Quiet komutu ile herhangi bir kullanıcıya bilgi verilmeden yapılmasını sağlar ve kurbanın verileri geri yükleme işlemi bir adımla daha zorlaştırılır.

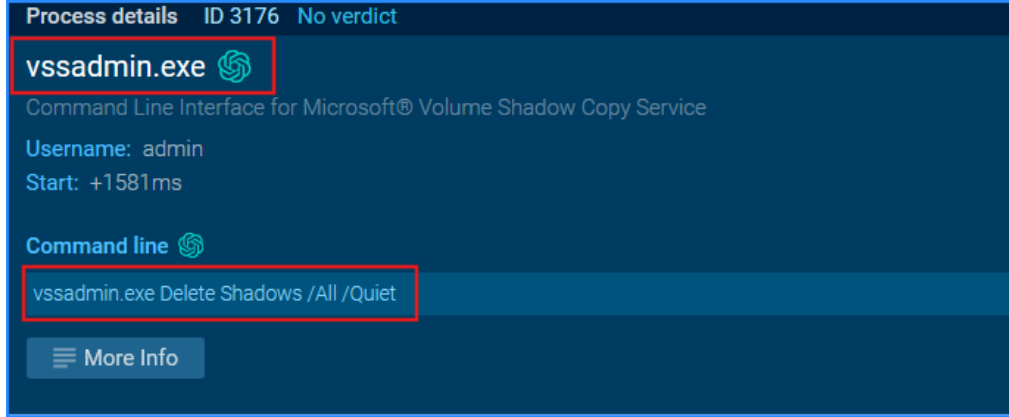


Figure 10 - vssadmin.exe

unsecapp.exe

unsecapp.exe, Windows Management Instrumentation (WMI) ile ilişkilidir. Saldırganın kullandığı komutun içerisinde ki “-Embedding” bunun bir Component Object Model (COM) olarak çalışmasını sağlar. Bu process ile saldırı zararlı faaliyeti gizleme, EDR ve AV gibi ürünleri normal bir process çalışıyormuş tekniği ile atlama, zararlıyı arka planda gizlice çalıştırma gibi bir çok zafiyetten faydalanabilir.

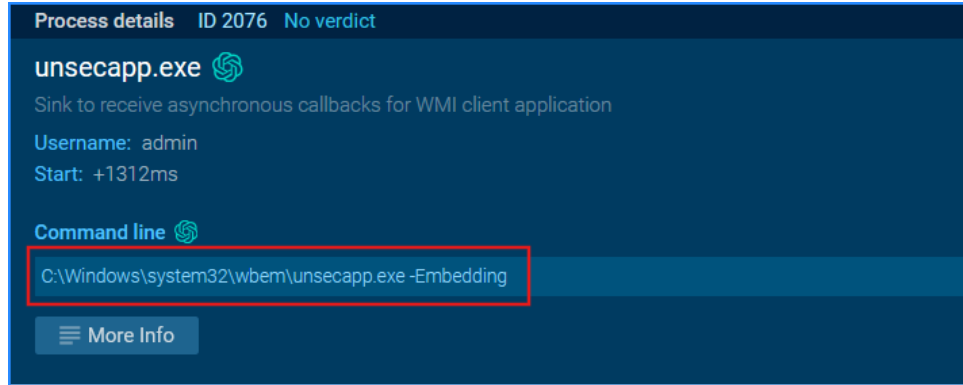


Figure 11 - unsecapp.exe

vssvc.exe

vssvc.exe, Windows'un Volume Shadow Copy Service (VSS) tarafından kullanılan bir sürecidir. Özellikle sistem yedeği ve geri yükleme işlemleri için kullanılan bir hizmettir. Dosyaların durumunu "shadow copy" olarak kaydederek, veri kaybını önler. Saldırganlar vssvc.exe hizmetini system yedeklerini silmek ve geri yükleme işlemlerini önlemek için kullanabilir.

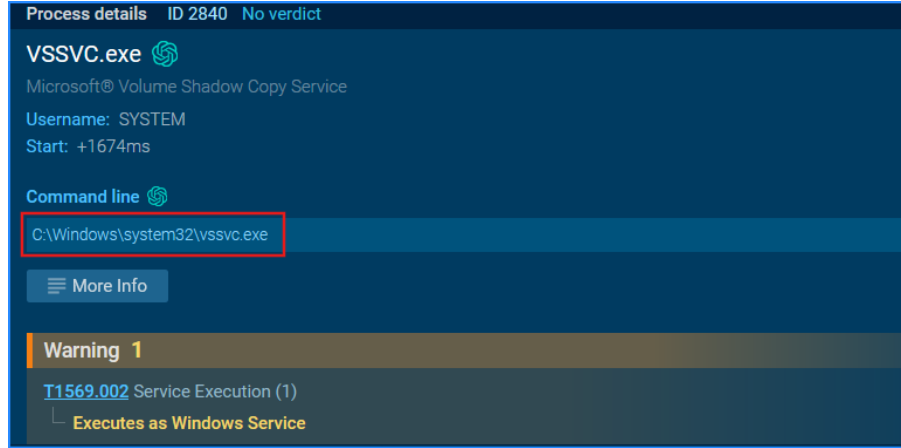


Figure 12 - vssvc.exe

MSFT.VSA.COM.DISABLE.2840, komutu incelendiğinde saldırganın ilgili bileşenin işlevlerinin devre dışı bırakılmasını sağlaması ile ilgili olabileceği saptandı.

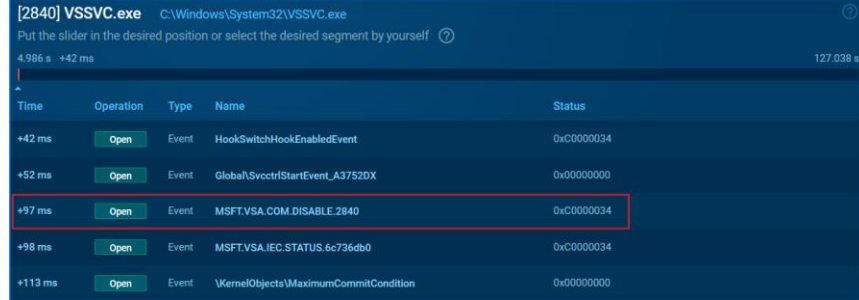


Figure 13 - vssvc.exe Disable

taskmgr.exe

taskmgr.exe, Windows sistemlerde Task Manager'ın çalışmasını sağlar. Saldırganın kullandığı “/4” ise windows sistemlerde “/3”e kadar bir anlam taşıdığı ve “/4”ün saldırganın belirlediği bir komut/zararlıyı çalıştırmak için oluşturulmuş bir komut olabileceği saptandı.

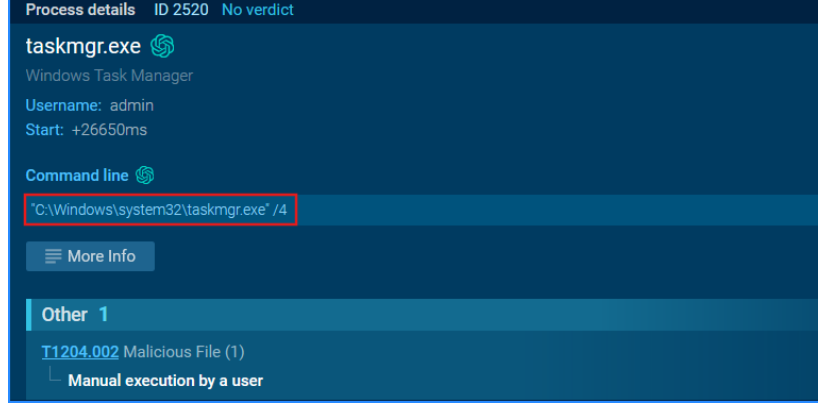


Figure 14 - taskmgr.exe

Taskmgr.exe altında görüntülenen bir Mutex çıktısı. Bu komut birden fazla Görev yöneticisinin aynı anda çalışmasını engellemek için kullanılıyor. Bu aşamada saldırgan kendi Görev Yöneticisi süresini uzatabilir ve kendini gizleyebilir ve zararlı faaliyetlerini sürdürebilir.

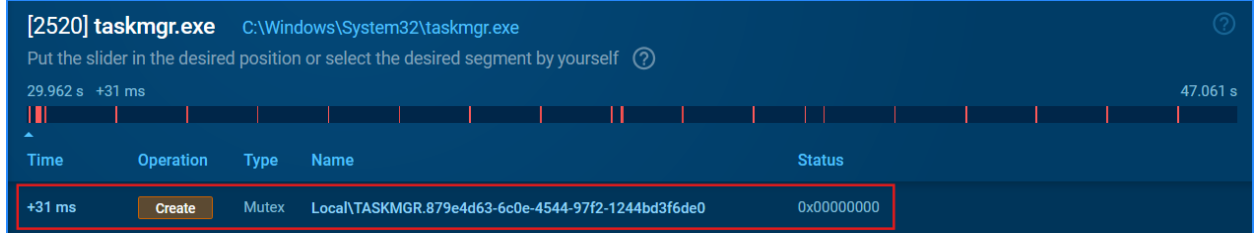


Figure 15 - taskmgr.exe Mutex

3.1. MITRE ATT&CK Matrix

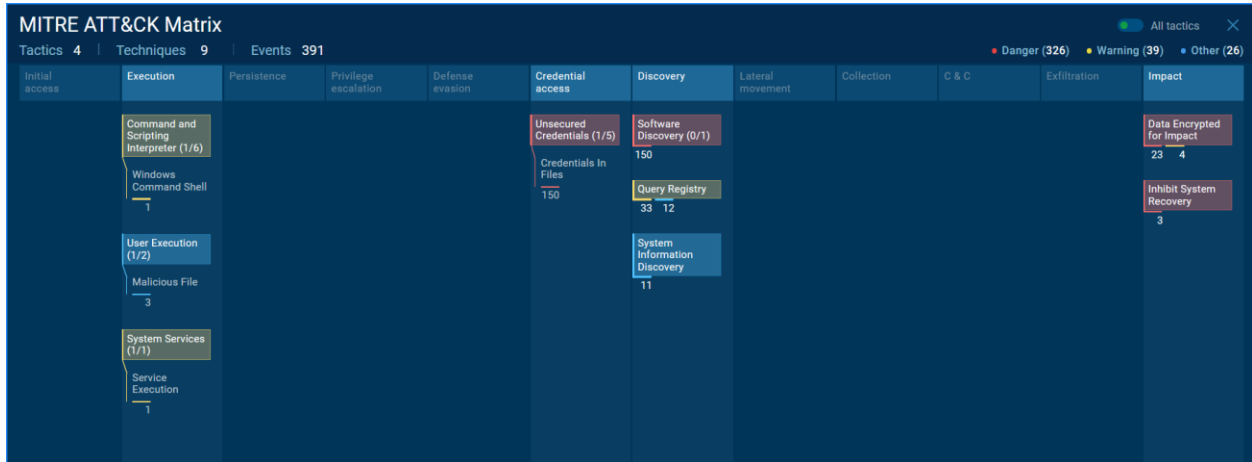


Figure 16 - MITRE Taktik ve Teknikler

4.1. IOC

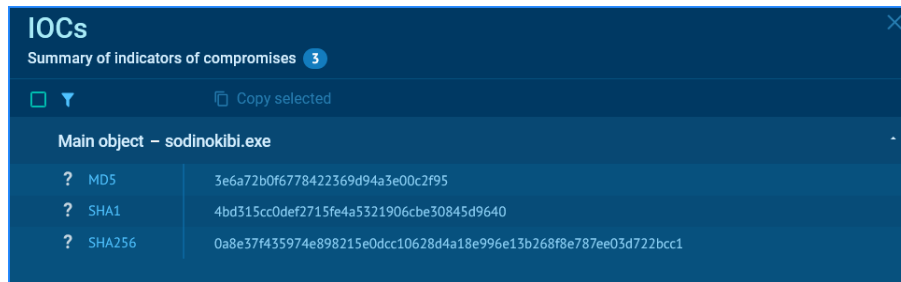


Figure 17 - Hash Değerleri

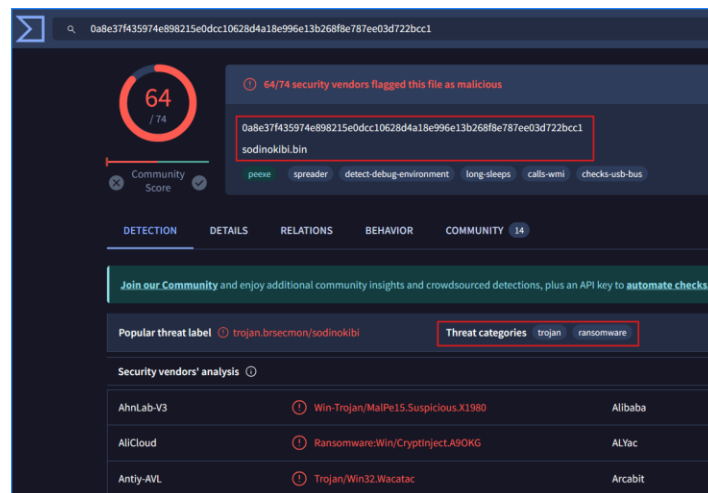


Figure 18 - VirusTotal1

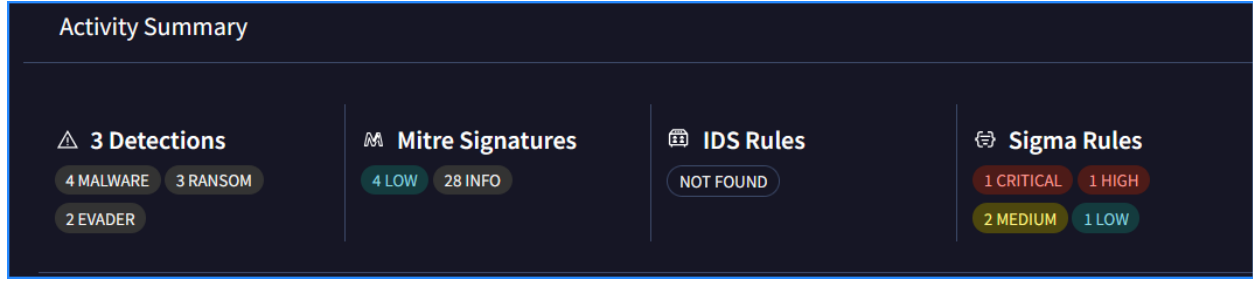


Figure 19 - VirusTotal2

5.1. REvil Ransomware için SIGMA Kuralları

Critical

SIGMA Kuralı ile eşleşen komut: CMD.EXE - "C:\Windows\System32\cmd.exe" /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignoreallfailures

title: REvil (Sodinokibi) Ransomware Tespiti

id:

status: test

description: REvil Ransomware Saldırı Tespiti

references: Florian Roth from Nextron Systems

author: Doğukan KAYA

date: 2024/08/09

tags:

- Ransomware
- REvil
- Sodinokibi
- attack.t1210
- attack.discovery
- attack.t1083
- attack.defense_evasion
- attack.t1222.001
- attack.impact
- attack.t1486

- attack.t1490
- detection.emerging_threats

logsource:

category: process_creation

product: windows

detection:

selection1:

- EventID: 4688
- Image|endswith:
 - '\tasksche.exe'
 - '\taskmgr.exe'
 - '\taskhsvc.exe'
 - '\sodinokibi.exe'

selection2:

- CommandLine|contains|all:
 - 'bcdedit'
 - '/set'
 - '{default}'
 - 'recoveryenabled'
 - 'no'
- CommandLine|contains|all:
 - 'delete'
 - 'catalog'
 - '-quiet'

condition: 1 of selection*

fields:

- CommandLine
- ParentCommandLine
- Process Creation
- NewProcessName
- NewProcessId

falsepositives:

level: critical

High

SIGMA Kuralı ile Eşleşen Komut: VSSADMIN.EXE - ParentCommandLine:"C:\Windows\System32\cmd.exe" /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignoreallfailures

title: Shadow Kopyalarının Silinmesi

id:

status: stable

description: Shadow Kopyalarının Silinmesi için İşletim Sistemi Araçları Kullanımı

references: Florian Roth from Nextron Systems

author: Doğukan KAYA

date: 2024/08/09

tags:

- attack.defense_evasion
- attack.impact
- attack.t1070
- attack.t1490

logsource:

category: process_creation

product: windows

detection:

selection1_img:

- Image|endswith:
 - '\powershell.exe'
 - '\cmd.exe'
 - '\wmic.exe'
 - '\vssadmin.exe'
 - '\diskshadow.exe'
- OriginalFileName:
 - 'PowerShell.EXE'
 - 'pwsh.dll'
 - 'wmic.exe'
 - 'VSSADMIN.EXE'

- 'diskshadow.exe'

selection1_cli:

CommandLine|contains|all:

- 'shadow' # will match "delete shadows" and "shadowcopy delete" and "shadowstorage"
- 'delete'

selection2_cli:

CommandLine|contains|all:

- 'delete'
- 'catalog'
- 'quiet' # will match -quiet or /quiet

selection3_img:

- Image|endswith: '\vssadmin.exe'
- OriginalFileName: 'VSSADMIN.EXE'

selection3_cli:

CommandLine|contains|all:

- 'resize'
- 'shadowstorage'

condition: (all of selection1*) or (all of selection2*) or (all of selection3*)

fields:

- CommandLine
- ParentCommandLine

falsepositives:

level: high

Medium

SIGMA Kuralı ile eşleşen komut: BCDEDIT.EXE - :C:\Windows\system32\cmd.exe /c C:\Windows\Sysnative\bcdedit.exe 1>bcdedit 2>&1

title: Sysnative Kullanılarak Process Creation

id:

status: test

description: Sysnative klasörünü kullanan işlem oluşturma olaylarını tespit eder.

references: Max Altgelt from Nextron Systems

author: Doğukan KAYA

date: 2024/08/09

tags:

- attack.defense_evasion
- attack.privilege_escalation
- attack.t1055

logsource:

category: process_creation

product: windows

detection:

EventID: 4688

sysnative:

- CommandLine|contains: ':\Windows\Sysnative\'
- Image|contains: ':\Windows\Sysnative\'

condition: sysnative

falsepositives:

level: medium

6.1. References

REvil Ransomware Analizi: <https://www.cybereason.com/blog/research/the-sodinokibi-ransomware-attack>

<https://attack.mitre.org/software/S0496/>

<https://attack.mitre.org/groups/G0115/>

https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/documentation/logsource-guides/windows/category/process_creation.md

<https://virustotal.readme.io/docs/crowdsourced-sigma-rules>

<https://www.nextron-systems.com/tag/sigma/>