Trainingsszenario - Signierte Ransomware

Gruppenname

Trainingsdaten - Signierte Ransomware (Hive)

Szenario

In diesem Trainingsszenario führen wir eine Ransomware-Payload aus, die als Administrator läuft und eine benutzerdefinierte Signatur verwendet. Dieses Szenario unterscheidet sich nicht sonderlich vom „**Standard**“-Beispiel, verwendet jedoch eine signierte ausführbare Datei.

Oft werden signierte ausführbare Dateien so behandelt, als sei bestätigt, dass sie harmlos sind. Zwar sollte zertifizierte Software *eigentlich* immer signiert sein, doch handelt es sich dabei nicht um eine bidirektionale Beziehung, und wir sollten Dingen nicht *allein deshalb* vertrauen, weil sie signiert sind. Leider unterläuft dieser Fehler manchmal doch.

Erkennung

Abgesehen davon, dass dieser Zertifikatsname für Trainingszwecke etwas seltsam ist, wie erkennt Cyber Crucible, dass er nicht vertrauenswürdig ist? Cyber Crucible geht auf Nummer sicher und führt eine (gruppenspezifische) Liste vertrauenswürdiger Zertifikate. Dadurch können wir sowohl Test-Signaturzertifikate als auch offizielle Zertifikate großer Zertifizierungsstellen wie DigiCert problemlos erkennen.

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

Created	Response Name	Untrusted Remote Threads	Modified Memory	No Trusted Cert
October 18, 2022 at 1:51:54 PM EDT	Worm Geum Indigo 180	False	False	True

Wie oben zu sehen ist, ist die Datei „321d0…“ zwar signiert, aber dennoch nicht vertrauenswürdig. Da keine weiteren komplexen Verschleierungstechniken zur Verbreitung des Angriffs verwendet wurden, wissen wir genau, woher er stammt!

Um die Ausführungsmethode zu bestätigen, können wir uns die Prozesserstellungen im Zeitraum des Vorfalls ansehen. Was wir sehen, bestätigt, dass es keine komplexe Exploit-Methode gab, nicht einmal ein Skript! Wie bei anderen Beispielen sind jedoch die Erstellungen von Kindprozessen interessant. Obwohl die Ausführungsmethode der Schadsoftware 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, doch die Analyse der zugehörigen Prozesse ist wichtig, um den Umfang der bösartigen Verhaltensweisen zu ermitteln. Die Ausführung der unsignierten EXE-Datei allein wirkt offensichtlich, wenn sie von Cyber Crucible dargestellt 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 Handlung auszuführen, die er sonst nicht ausgeführt hätte, wie z. B. das Ausführen eines Skripts oder das Weitergeben eines Passworts.
- Mitre T1091 - Schadsoftware kann sich selbst auf Wechselmedien replizieren, sodass sie beim Anschließen an den nächsten Rechner über Autorun oder Treiber-Schwachstellen ausgeführt werden kann.
- Mitre T1204 - Benutzerausführung, die häufig durch Phishing erlangt wird, ist der einfachste Weg für Schadsoftware, mit der Ausführung zu beginnen.
- Mitre T1587-002 - Code-Signaturzertifikate sind eine Möglichkeit für eine Autorität, den Code einer Anwendung zu zertifizieren. Schadsoftware kann ein Zertifikat erzeugen, das von keiner Zertifizierungsstelle stammt, aber einen Benutzer glauben lassen, es sei legitim.

- Mitre T1587-003 - SSL-Zertifikate werden verwendet, um sicherzustellen, dass die Datenübertragung vertrauenswürdig ist. In einer schlecht konfigurierten Umgebung kann Schadsoftware in der Lage sein, ihr eigenes SSL-Zertifikat zu installieren, um Man-in-the-Middle-Angriffe zu ermöglichen.

Revision #1
Created 2026-07-24 03:55:20 UTC by Dennis Underwood
Updated 2026-07-24 03:55:20 UTC by Dennis Underwood