Scénario de formation - Ransomware classique

Nom du groupe

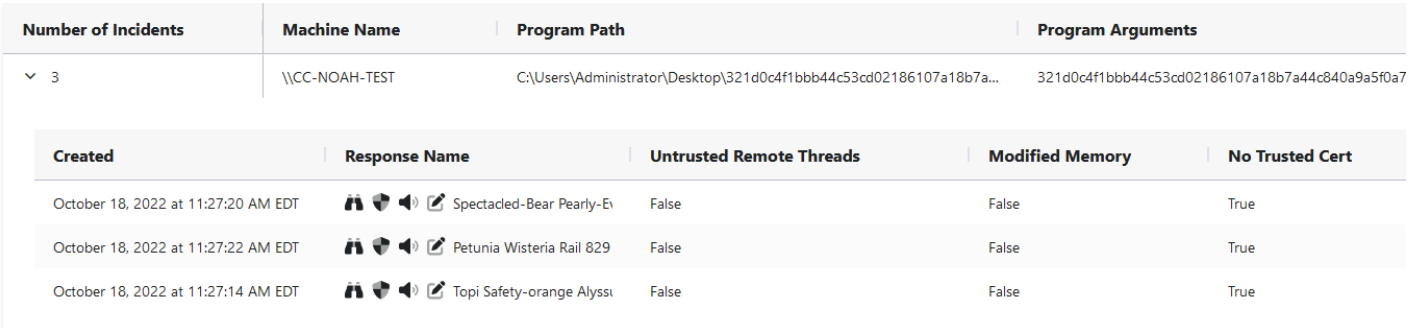
Données de formation - Ransomware classique (Hive)

Scénario

Dans ce scénario de formation, nous allons exécuter une charge utile de ransomware « classique », s'exécutant en tant qu'administrateur sans aucun exploit. Cela simule l'exemple de base d'un utilisateur téléchargeant un logiciel malveillant via un lien de phishing, une clé USB malveillante, etc.

Bien qu'il s'agisse d'une méthode d'exécution très simple, si la charge utile est un zero-day, elle passera tout de même inaperçue par les produits de sécurité basés sur les signatures, et pourra causer des dommages irréparables avant que les produits comportementaux basés sur le cloud ne puissent obtenir une analyse en retour.

Identification



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

Réponse automatisée

Identifier cet incident est le plus simple de tous les exemples. Une fois que le nom de fichier suspect d'un fichier sans signature a été remarqué, il s'agit d'un signal d'alarme immédiat.

Pour confirmer la méthode d'exécution, nous pouvons examiner les créations de processus autour du moment de l'incident. Ce que nous voyons confirme qu'il n'y avait pas de méthode d'exploit

complexe, ni même de script ! Comme pour les autres échantillons, les créations de processus enfants sont néanmoins intéressantes. Même si la méthode d'exécution du logiciel malveillant lui-même était évidente, de nombreux processus en arrière-plan sont lancés pour désactiver les protections et d'autres paramètres système.

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...

À ce stade, l'attaque a été contenue par Cyber Crucible, mais l'analyse des processus associés est importante pour déterminer l'étendue des comportements malveillants. L'exécution de l'exe non signé seule semble évidente lorsqu'elle est présentée par Cyber Crucible, mais bien souvent, les processus en arrière-plan lancés par un élément aussi privilégié et protégé que Defender seraient tout simplement ignorés.

Documentation pertinente

- Mitre T1566 - Le phishing peut être utilisé pour inciter un utilisateur à effectuer une action qu'il n'aurait pas effectuée autrement, comme l'exécution d'un script ou le partage d'un mot de passe.
- Mitre T1091 - Un logiciel malveillant peut se répliquer sur un support amovible afin que la prochaine machine qui s'y connecte puisse l'exécuter via l'exécution automatique ou des vulnérabilités de pilotes.
- Mitre T1204 - L'exécution par l'utilisateur, souvent obtenue via le phishing, est le moyen le plus simple pour un logiciel malveillant de commencer à s'exécuter.

Revision #1
Created 2026-07-24 06:20:06 UTC by Dennis Underwood
Updated 2026-07-24 06:20:06 UTC by Dennis Underwood