Scénario de formation - Ransomware signé

Nom du groupe

Données de formation - Ransomware signé (Hive)

Scénario

Dans ce scénario de formation, nous allons exécuter une charge utile de ransomware, s'exécutant en tant qu'administrateur, et avec une signature personnalisée. Ce scénario n'est pas très différent de l'échantillon « **classique** », mais utilise un exécutable signé.

Souvent, les exécutables signés sont traités comme s'ils étaient vérifiés comme étant bénins. Bien qu'il soit vrai que les logiciels certifiés *devraient* tous être signés, cela n'est pas une relation bidirectionnelle, et nous ne devrions pas faire confiance aux éléments *uniquement* parce qu'ils sont signés. Malheureusement, cette erreur est parfois commise.

Identification

Mis à part le fait que ce nom de certificat est un peu étrange à des fins de formation, comment Cyber Crucible sait-il qu'il n'est pas digne de confiance ? Cyber Crucible joue la carte de la prudence et maintient une liste (spécifique au groupe) de certificats de confiance. Cela signifie que nous pouvons facilement détecter les certificats de test de signature, ainsi que les certificats officiels provenant de grandes autorités de certification comme digicerts.

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

Nous pouvons voir ci-dessus que même si le fichier « 321d0... » est signé, il n'est toujours pas fiable. Étant donné qu'aucune autre technique d'obfuscation complexe n'est utilisée pour déployer l'attaque, nous savons exactement d'où elle provient !

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'exploitation 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 démarrés 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 mise en évidence par Cyber Crucible, mais bien souvent, les processus en arrière-plan démarrés par un élément aussi privilégié et protégé que Defender seraient 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 exécuter un script ou partager un mot de passe.
- Mitre T1091 - Un logiciel malveillant peut se répliquer sur un support amovible afin que la prochaine machine à laquelle il est connecté puisse l'exécuter via l'exécution automatique ou des vulnérabilités de pilote.
- Mitre T1204 - L'exécution par l'utilisateur, souvent obtenue via le phishing, est le moyen le plus simple pour un logiciel malveillant de commencer son exécution.
- Mitre T1587-002 - Les certificats de signature de code sont un moyen pour une autorité de certifier le code d'une application. Un logiciel malveillant peut générer un certificat qui ne provient d'aucune autorité de certification mais peut induire un utilisateur en erreur en lui faisant croire qu'il est légitime.

- Mitre T1587-003 - Les certificats SSL sont utilisés pour garantir que la transmission des données est fiable. Dans un environnement mal configuré, un logiciel malveillant peut être en mesure d'installer son propre certificat SSL pour faciliter les attaques de type « homme du milieu ».

Revision #1
Created 2026-07-24 06:20:31 UTC by Dennis Underwood
Updated 2026-07-24 06:20:31 UTC by Dennis Underwood