Escenario de Entrenamiento - Ransomware Firmado

Nombre del Grupo

Datos de Entrenamiento - Ransomware Firmado (Hive)

Escenario

En este escenario de entrenamiento, ejecutaremos una carga útil de ransomware, corriendo como administrador, y con una firma personalizada. Este escenario no es muy diferente de la muestra ‘ **vanilla**’, pero utiliza un ejecutable firmado.

Con frecuencia, los ejecutables firmados son tratados como si estuvieran verificados como benignos. Si bien es cierto que el software certificado *debería* estar todo firmado, esta no es una relación bidireccional, y no debemos confiar en las cosas *solo* porque estén firmadas. Desafortunadamente, a veces se comete ese error.

Identificándolo

Además del hecho de que este nombre de certificado es un poco extraño para fines de entrenamiento, ¿cómo sabe Cyber Crucible que no es confiable? Cyber Crucible actúa con precaución y mantiene una lista (específica del grupo) de certificados de confianza. Esto significa que podemos detectar fácilmente certificados de prueba de firma, así como certificados oficiales de grandes CAs como 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

Podemos ver arriba que aunque el archivo “321d0...” está firmado, sigue sin ser confiable. Dado que no se utilizan otras técnicas de ofuscación complejas para desplegar el ataque, ¡sabemos exactamente de dónde vino!

Para confirmar el método de ejecución, podemos examinar las creaciones de procesos alrededor del momento del incidente. Lo que vemos confirma que no hubo ningún método de explotación complejo, ¡ni siquiera un script! Al igual que con otras muestras, las creaciones de procesos hijos son interesantes, sin embargo. Aunque el método de ejecución del malware en sí mismo fue obvio, se inician muchos procesos en segundo plano que deshabilitan protecciones y otras configuraciones del sistema.

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...

En este punto, el ataque ha sido contenido por Cyber Crucible, pero el análisis de los procesos relacionados es importante para encontrar el alcance de los comportamientos maliciosos. La ejecución del exe no firmado por sí sola parece obvia cuando es expuesta por Cyber Crucible, pero muchas veces los procesos en segundo plano iniciados por algo tan privilegiado y protegido como Defender simplemente serían ignorados.

Documentación relevante

- Mitre T1566 - El phishing puede utilizarse para engañar a un usuario y hacer que realice una acción que de otro modo no habría llevado a cabo, como ejecutar un script o compartir una contraseña.
- Mitre T1091 - El malware puede replicarse a sí mismo en medios extraíbles para que la siguiente máquina que se conecte a ellos pueda ejecutarlo a través de la ejecución automática o vulnerabilidades de controladores.
- Mitre T1204 - La ejecución por parte del usuario, a menudo obtenida mediante phishing, es la forma más simple en que el malware comienza su ejecución.
- Mitre T1587-002 - Los certificados de firma de código son una forma en que una autoridad certifica el código de una aplicación. El malware puede generar un certificado que no proviene de ninguna autoridad certificadora, pero que puede confundir a un usuario haciéndole pensar que es legítimo.

- Mitre T1587-003 - Los certificados SSL se utilizan para garantizar que la transmisión de datos sea confiable. En un entorno mal configurado, el malware puede ser capaz de instalar su propio certificado SSL para facilitar ataques de intermediario (man in the middle).

Revision #1
Created 2026-07-24 01:14:00 UTC by Dennis Underwood
Updated 2026-07-24 01:14:00 UTC by Dennis Underwood