Training Scenario - Signed Ransomware

Group Name

Training Data - Signed Ransomware (Hive)

Scenario

In this training scenario, we will execute a ransomware payload, running as admin, and with a custom signature. This scenario is not too different from the '**vanilla**' sample, but utilizes a signed executable.

Often times signed executables are treated is if they are verified to be benign. While it's true that certified software *should* all be signed, this is not a bidirectional relationship, and we shouldn't trust things *just* because they're signed. Unfortunately, sometimes that mistake is made.

Identifying it

Aside from the fact that this cert name is a bit odd for training purposes, how does Cyber Crucible know it's not trustworthy? Cyber Crucible plays it safe and maintains a (group specific) list of trusted certificates. This means that we can easily catch test signing certs, as well as official certs from large CAs like 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

We can see above that even though the file “321d0…” is signed, it’s still not trusted. Since there are no other complex obfuscation techniques used to deploy the attack, we know exactly where it came from!

To confirm the execution method, we can look into the process creations around the time of the incident. What we see confirms that there was no complex exploit method, or even a script! As with other samples, the child process creations are interesting, though. Even though the execution method of the malware itself was obvious, many background processes are started that disable protections and other system settings.

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...

At this point the attack has been contained by Cyber Crucible, but analysis of the related processes is important to find scope of the malicious behaviors. The execution of the unsigned exe alone looks obvious when its laid out by Cyber Crucible, but many times background processes started by something as privileged and protected as Defender would simply be ignored.

Relevant documentation

- Mitre T1566 - Phishing may be used to trick a user into performing an action they would not have done otherwise such as running a script or sharing a password.
- Mitre T1091 - Malware may replicate itself onto removable media so that the next machine to connect it may execute via autorun or driver vulnerabilities.
- Mitre T1204 - User execution, often gained via phishing, is the simplest way malware to begin execution.
- Mitre T1587-002 - Code signing certificates are a way for an authority to certify that an applications code. Malware may generate a certificate that does not come from any certificate authority but may confuse a user into thinking it is legitimate.
- Mitre T1587-003 - SSL certificates are used to ensure that data transmission is trustworthy. In a poorly configured environment, malware may be able to install its own SSL certificate to facilitate man in the middle attacks.

Revision #2
Created 2026-07-13 18:48:52 UTC by Dennis Underwood
Updated 2026-07-13 18:48:56 UTC by Dennis Underwood