Cenário de Treinamento - Ransomware Vanilla

Nome do Grupo

Dados de Treinamento - Ransomware Vanilla (Hive)

Cenário

Neste cenário de treinamento, executaremos uma carga útil de ransomware "vanilla", em execução como administrador sem nenhum exploit. Isso simula o exemplo básico de um usuário baixando malware por meio de um link de phishing, USB malicioso, etc.

Embora este seja um método de execução muito simples, se a carga útil for um zero day, ela ainda passará despercebida por produtos de segurança baseados em assinatura, e poderá causar danos irreparáveis antes que produtos comportamentais baseados em nuvem consigam obter uma análise.

Identificando-o

Number of Incidents	Machine Name	Program Path	Program Arguments
3	\\CC-NOAH-TEST	C:\Users\Administrator\Desktop\321d0c4f1bbb44c53cd02186107a18b7a...	321d0c4f1bbb44c53cd02186107a18b7a44c840a9a5f0a7

Created	Response Name	Untrusted Remote Threads	Modified Memory	No Trusted Cert
October 18, 2022 at 11:27:20 AM EDT	Spectacled-Bear Pearly-E\	False	False	True
October 18, 2022 at 11:27:22 AM EDT	Petunia Wisteria Rail 829	False	False	True
October 18, 2022 at 11:27:14 AM EDT	Topi Safety-orange Alyss\	False	False	True

Resposta Automatizada

Identificar este incidente é o mais fácil de todas as amostras. Assim que o nome de arquivo suspeito em um arquivo sem assinatura é percebido, isso já é um sinal de alerta imediato.

Para confirmar o método de execução, podemos analisar as criações de processos em torno do horário do incidente. O que vemos confirma que não houve um método de exploit complexo, nem mesmo um script! Assim como em outras amostras, as criações de processos filhos são

interessantes, no entanto. Mesmo que 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 já foi contido pela 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 apresentada pela 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 a se conectar a ela 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 maneira mais simples de um malware começar a ser executado.

Revision #1
Created 2026-07-24 05:11:57 UTC by Dennis Underwood
Updated 2026-07-24 05:11:57 UTC by Dennis Underwood