Splunk EVTX Threat Hunting Project

Tyriq McNulty

Project Summary:

Over the course of three weeks, I analyzed a set of EVTX logs using Splunk to investigate and detect malicious activity across key stages of the attack lifecycle. This included indicators of Discovery, Execution, Persistence, and Privilege Escalation. I focused on identifying suspicious behavior through event correlations, process anomalies, unsigned executables, spoofed parent processes, and stealthy registry modifications. Each log was categorized and analyzed with supporting evidence, and I provided tailored mitigation strategies based on real-world detection patterns. The goal was to simulate a realistic threat-hunting scenario and demonstrate my ability to detect, analyze, and respond to advanced threats using Splunk and Windows forensic artifacts.

GitHub: https://github.com/BoyarRiq/Splunk-EVTX-Threat-Hunting-Project
GitHub repo used for EVTX Files: https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES

==========

Tactic Type of EVTX Logs:

- Discovery
- Execution
- Privilege Escalation
- Persistence

==========

Discovery_NamedPipes_Sysmon_Csv: Event Logs Analysis

Data sources: Sysmon, Windows Security

Tactic: Discovery

ATT&CK Technique: T1046: Network Service Scanning | T1047: Windows Admin Shares

Discovery_NamedPipes_Sysmon_Csv: Log Summary

- When analyzing the logs through Splunk. The data suggested Processes communicating through the means of Inter-process communication (IPC). No suspicious activity.

Discovery_NamedPipes_Sysmon_Csv / 2020-09-27T13:20:11.247

- Tactic: Discovery
- Event ID: 18
- Event Record ID: 409616
- Hidden Record: False
- Level: Info

- Map Description: PipeEvent (Pipe Connected)
- Payload:{"EventData":{"Data":[{"@Name":"RuleName"},{"@Name":"EventType", "#text":"ConnectPipe"},{"@Name":"UtcTime","#text":"2020-09-27 13:20:11.245"},{"@Name":"ProcessGuid","#text":"747f3d96-8e29-5f70-0000-001049471000"},{"@Name":"ProcessId","#text":"6096"},{"@Name":"PipeName" ,"#text":"\\browser"},{"@Name":"Image","#text":"C:\\Windows\\system32\\mmc.exe"}]}}
- Process ID: 3320
- Provider: Microsoft-Windows-Sysmon
- Record Number: 20
- Thread ID: 4584
- User ID: S-1-5-18

Payload Data

- Name: Event Type / Text: ConnectPipe
- Name: Process Guid / Text: 747f3d96-8e29-5f70-0000-001049471000
- Name: Process ID / Text: 6096
- Name: PipeName / Text: \\browser
- Name: Image / Text: C:\\Windows\\system32\\mmc.exe

==========

Discovery_NamedPipes_Sysmon_Csv / 2020-09-27T13:20:11.245

- Tactic: Discovery
- Event ID: 18
- Event Record ID: 409615
- Hidden Record: False
- Level: Info
- Map Description: PipeEvent (Pipe Connected)
- Payload:{"EventData":{"Data":[{"@Name":"RuleName"},{"@Name":"EventType", "#text":"ConnectPipe"},{"@Name":"UtcTime","#text":"2020-09-27 13:20:11.229"},{"@Name":"ProcessGuid","#text":"747f3d96-8e29-5f70-0000-001049471000"},{"@Name":"ProcessId","#text":"6096"},{"@Name":"PipeName" ,"#text":"\\wkssvc"},{"@Name":"Image","#text":"C:\\Windows\\system32\\mmc.exe"}]}}
- Process ID: 3320
- Provider: Microsoft-Windows-Sysmon
- Record Number: 19
- Thread ID: 4584
- User ID: S-1-5-18

==========

Discovery_NamedPipes_Sysmon_Csv / 2020-09-27T13:19:54.399

- Tactic: Discovery
- Event ID: 18
- Event Record ID: 409614

- Hidden Record: False
- Level: Info
- Map Description: PipeEvent (Pipe Connected)
- Payload:{"EventData":{"Data":[{"@Name":"RuleName"},{"@Name":"EventType", "#text":"ConnectPipe"},{"@Name":"UtcTime","#text":"2020-09-27 13:19:54.390"},{"@Name":"ProcessGuid","#text":"747f3d96-0c7a-5f71-0000-0010eb030000"},{"@Name":"ProcessId","#text":"4"},{"@Name":"PipeName","#text":"\\wkssvc"},{"@Name":"Image","#text":"System"}]}}
- Process ID: 3320
- Provider: Microsoft-Windows-Sysmon
- Record Number: 18
- Thread ID: 4584
- User ID: S-1-5-18

Payload Data

- Name: Event Type / Text: ConnectPipe
- Name: Process Guid / Text: 747f3d96-0c7a-5f71-0000-0010eb030000
- Name: Process ID / Text: 4
- Name: PipeName / Text: \\wkssvc
- Name: Image / Text: System

==========

Discovery_NamedPipes_Sysmon_Csv / 2020-09-27T13:19:54.385

- Tactic: Discovery
- Event ID: 18
- Event Record ID: 409613
- Hidden Record: False
- Level: Info
- Map Description: PipeEvent (Pipe Connected)
- Payload:{"EventData":{"Data":[{"@Name":"RuleName"},{"@Name":"EventType", "#text":"ConnectPipe"},{"@Name":"UtcTime","#text":"2020-09-27 13:19:54.371"},{"@Name":"ProcessGuid","#text":"747f3d96-0c7a-5f71-0000-0010eb030000"},{"@Name":"ProcessId","#text":"4"},{"@Name":"PipeName","#text":"\\trkwks"},{"@Name":"Image","#text":"System"}]}}
- Process ID: 3320
- Provider: Microsoft-Windows-Sysmon
- Record Number: 17
- Thread ID: 4584
- User ID: S-1-5-18

Payload Data

- Name: Event Type / Text: ConnectPipe
- Name: Process Guid / Text: 747f3d96-0c7a-5f71-0000-0010eb030000
- Name: Process ID / Text: 4

- Name: PipeName / Text: \\trkwks
- Name: Image / Text: System

==========

Discovery_NamedPipes_Sysmon_Csv / 2020-09-27T13:19:54.377

- Tactic: Discovery
- Event ID: 18
- Event Record ID: 409612
- Hidden Record: False
- Level: Info
- Map Description: PipeEvent (Pipe Connected)
- Payload:{"EventData":{"Data":[{"@Name":"RuleName"},{"@Name":"EventType","#text":"ConnectPipe"},{"@Name":"UtcTime","#text":"2020-09-27 13:19:54.371"},{"@Name":"ProcessGuid","#text":"747f3d96-0c7a-5f71-0000-0010eb030000"},{"@Name":"ProcessId","#text":"4"},{"@Name":"PipeName","#text":"\\tapsrv"},{"@Name":"Image","#text":"System"}]}}
- Process ID: 3320
- Provider: Microsoft-Windows-Sysmon
- Record Number: 16
- Thread ID: 4584
- User ID: S-1-5-18

Payload Data

- Name: Event Type / Text: ConnectPipe
- Name: Process Guid / Text: 747f3d96-0c7a-5f71-0000-0010eb030000
- Name: Process ID / Text: 4
- Name: PipeName / Text: \\tapsrv
- Name: Image / Text: System

==========

Discovery_NamedPipes_Sysmon_Csv / 2020-09-27T13:19:54.371

- Tactic: Discovery
- Event ID: 18
- Event Record ID: 409611
- Hidden Record: False
- Level: Info
- Map Description: PipeEvent (Pipe Connected)
- Payload: {"EventData":{"Data":[{"@Name":"RuleName"},{"@Name":"EventType","#text":"ConnectPipe"},{"@Name":"UtcTime","#text":"2020-09-27 13:19:54.356"},{"@Name":"ProcessGuid","#text":"747f3d96-0c7a-5f71-0000-0010eb030000"},{"@Name":"ProcessId","#text":"4"},{"@Name":"PipeName","#text":"\\srvsvc"},{"@Name":"Image","#text":"System"}]}}
- Process ID: 3320
- Provider: Microsoft-Windows-Sysmon

- Record Number: 15
- Thread ID: 4584
- User ID: S-1-5-18

Payload Data

- Name: Event Type / Text: ConnectPipe
- Name: Process Guid / Text: 747f3d96-0c7a-5f71-0000-0010eb030000
- Name: Process ID / Text: 4
- Name: PipeName / Text: \\srvsvc
- Name: Image / Text: System

==========

Discovery_UEFI_Sysmon_Csv: Event Log Analysis

Data sources: Sysmon, Windows Security

Tactic: Discovery

ATT&CK Technique: T1542.001: System Firmware

Discovery_UEFI_Sysmon_Csv: Log Summary

- The following Log indicates RWDrv.sys being malicious. This driver was found in file path C:\Windows\System32\drivers\RwDrv.sys during log analysis. Despite having a legit signature ChongKim Chan, evidence pinpoints to Its SHA-1 Hash being in relation with multiple malicious malware samples, malicious IP's, and tools commonly used in attacks. Examples of malicious intent includes indications of firmware access, malware droppers, and UEFI rootkits.
- But it can be used maliciously for privilege escalation and stealthy operations.

Discovery_UEFI_Sysmon_Csv: Mitigation Suggestions

- Avoid clicking on links from unknown or untrusted sources to prevent phishing or drive-by downloads.
- Keep the operating system and firmware (including UEFI/BIOS) updated with the latest security patches.
- Updating Firmware for the BIOS/UEFI, because UEFI rootkits target firmware, which updating the OS system alone won't be fixed.

Discovery_UEFI_Sysmon_Csv / 2020-02-11T11:05:37.148

- Tactic: Discovery
- Event ID: 6
- Event Record ID: 24350
- ExecutableInfo: C:\Windows\System32\drivers\RwDrv.sys
- Hidden Record: False

- Level: Info
- Map Description: Driver loaded
- Payload:
{"EventData":{"Data":[{"@Name":"RuleName"},{"@Name":"UtcTime","#text":"2020-02-11 11:05:36.955"},{"@Name":"ImageLoaded","#text":"C:\\Windows\\System32\\drivers\\RwDrv.sys"},{"@Name":"Hashes","#text":"SHA1=66E95DAEE3D1244A029D7F3D91915F1F233D1916,MD5=60E84516C6EC6DFDAE7B422D1F7CAB06,SHA256=D969845EF6ACC8E5D3421A7CE7E244F419989710871313B04148F9B322751E5D,IMPHASH=955E7B12A8FA06444C68E54026C45DE1"},{"@Name":"Signed","#text":"true"},{"@Name":"Signature","#text":"ChongKim Chan"},{"@Name":"SignatureStatus","#text":"Valid"}]}}
- Process ID: 2844
- Provider: Microsoft-Windows-Sysmon
- Record Number: 1
- Thread ID: 4000
- User ID: S-1-5-18

Payload Data

- Name: ImageLoaded / #Text C:\\Windows\\System32\\drivers\\RwDrv.sys
- Name: Signed / Text: true
- Name: Signature / Text: ChongKim Chan
- Name: Signature Status / Text Valid

Malicious Indicators

- SHA-1: 66e95daee3d1244a029d7f3d91915f1f233d1916
- Contacted IP address: 93.184.221.240 (malicious)
- Execution Parents: malware-sample-library-master.zip, nvflsh64.exe, loader_7a066b03.zip, 4826d957-4425-4b94-8d3f-297d3481bf6d zip, antivirusfalsepositivetest4.exe, RWeverything.exe, LoJaxInfo_EFI.exe, TJprojMain
- PE Resource Parents: iapp_.exe

==========

Persistence_HiddenRun_Sysmon_Csv: Log Analysis

Data sources: Data sources: Sysmon, Windows Security, Registry

Tactic: Persistence

ATT&CK Technique: T1547.001: Registry Run Keys / Startup Folder | T1027: Obfuscated Files or Information

Persistence_HiddenRun_Sysmon_Csv: Summary

- Based off of all the following I've detected in my Splunk log, I believe evidence points to possible compromise. Evidence points to a malware evasion tool ran to have this malware hidden and to automatically start when the PC first boots up. In addition, the taskhost.exe (a Windows program that helps run small background services, like device connections or system notifications.) being in another file path could just be another tool used to evade detection, since there is a public malware evasion tools folder sitting directly on the PC.

Persistence_HiddenRun_Sysmon_Csv: Mitigation Suggestions

- Regularly audit and monitor auto-start registry keys and scheduled tasks for hidden or suspicious entries. This is generally recommended for IT/Security teams to oversee.
- Avoid clicking on links from unknown or untrusted sources to prevent phishing or drive-by downloads.
- Keep the operating system and firmware (including UEFI/BIOS) updated with the latest security patches.

Persistence_HiddenRun_Sysmon_Csv / 2020-07-04T14:18:58.268-05:00

- Tactic: Persistence
- Event ID: 13
- Event Record ID: 306346
- Hidden Record: False
- Level: Info
- Map Description: RegistryEvent (Value Set)
- Payload: {"EventData":{"Data":[{"@Name":"RuleName","#text":"Persistence - Hidden Run value detected"},{"@Name":"EventType","#text":"SetValue"},{"@Name":"UtcTime","#text":"2020-07-04 14:18:58.231"},{"@Name":"ProcessGuid","#text":"747f3d96-8fd2-5f00-0000-0010c15d2200"},{"@Name":"ProcessId","#text":"3728"},{"@Name":"Image","#text":"C:\\Users\\Public\\tools\\evasion\\a.exe"},{"@Name":"TargetObject","#text":"HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\"},{"@Name":"Details","#text":"\"c:\\windows\\tasks\\taskhost.exe\""}]}}
- Process ID: 3400
- Provider: Microsoft-Windows-Sysmon
- Record Number: 1
- Thread ID: 4136
- User ID: S-1-5-18

Payload Data

- Name: Rule Name / Text: Persistence - Hidden Run value detected
- Name: EventType /Text: SetValue

- Name: ProcessGuid / Text: 747f3d96-8fd2-5f00-0000-0010c15d2200
- Name: ProcessId / Text: 3728
- Name: Image / Text C:\\Users\\Public\\tools\\evasion\\a.exe
- Name: TargetObject / Text: HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\
- Name: Details / Text: \"c:\\windows\\tasks\\taskhost.exe\

Malicious Indicators

HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\

- This registry path is used to auto-start programs at system boot for all users.
- If a suspicious or unknown program is listed here, it's likely being used for persistence, possibly by malware. In this case, we've detected a "Hidden Run value" under this list.
- Always inspect the value name and file path it points to.

Hidden Run value detected

- means a registry key under HKCU\Software\Microsoft\Windows\CurrentVersion\Run (or similar) is set to auto-start a program but is hidden from normal tools or UI.
- often a sign of malware persistence.
- Investigate the value, file path, and related process for suspicious behavior.

C:\Users\Public\tools\evasion\a.exe (highly suspicious)

- The path suggests it's in a shared/public tools folder, often used in malware staging.
- The folder name "evasion" directly implies defensive evasion techniques. In this case, it directly relates to the "Hidden Value" registry key being hidden from normal tools or UI. So, there's definitely some persistence in the picture being directly involved with attacker.
- The file name a.exe is generic—common in malware to avoid detection.
- Tool for Red Teaming

c:\windows\tasks\taskhost.exe (suspicious)

- Legit taskhost.exe runs from C:\Windows\System32, not from \tasks\.
- Malware often copies legit names to alternate paths to evade detection.
- Likely used for persistence or execution impersonating.

==========

Persistence_SilentProcessExit_Sysmon_Csv: Log Analysis

Data sources: Data sources: Sysmon, Windows Security

Tactic: Persistence

ATT&CK Technique: T1055 – Process Injection or T1036.005 – Masquerading: Match Legitimate Name or Location | T1218.005 – Signed Binary Proxy Execution: WerFault.exe

Persistence_SilentProcessExit_Sysmon_Csv: Summary

- I believe we have heavy indications of malware on the remote PC, that's spoofing a legit application "cmd.exe" as unsigned file named "evil.exe". This spoof was executed by a malicious script running the "werfault.exe" command line to maintain silent persistence.
- The file "evil.exe" has known malicious hashes, has contacted bad IP's, and has been used and overall inserted in other malware sample executables (.exe).

Persistence_SilentProcessExit_Sysmon_Csv: Mitigation Suggestions

- Regularly monitor running processes and system logs for unusual or hidden activity. This is recommended for the IT/Security team to oversee.
- Avoid clicking on links from unknown or untrusted sources to prevent phishing or drive-by downloads.
- Keep the operating system and firmware (including UEFI/BIOS) updated with the latest security patches.
- Use endpoint security tools that can detect hidden or silent malware processes.

Persistence_SilentProcessExit_Sysmon_Csv / 2025-01-05T17:23:11.694-06:00

- Tactic: Persistence
- Event ID: 1
- Event Record ID: 8045
- ExecutableInfo: C:\windows\temp\evil.exe
- Hidden Record: False
- Level: Info
- Map Description: Process creation
- Payload:

{"EventData":{"Data":[{"@Name":"RuleName"},{"@Name":"UtcTime","#text":"2019-06-19 17:23:11.678"},{"@Name":"ProcessGuid","#text":"365abb72-6f7f-5d0a-0000-0010b66e1400"},{"@Name":"ProcessId","#text":"3800"},{"@Name":"Image","#text":"C:\\Windows\\Temp\\evil.exe"},{"@Name":"FileVersion","#text":"6.1.7601.17514 (win7sp1_rtm.101119-1850)"},{"@Name":"Description","#text":"Windows Command Processor"},{"@Name":"Product","#text":"Microsoft® Windows® Operating System"},{"@Name":"Company","#text":"Microsoft Corporation"},{"@Name":"CommandLine","#text":"C:\\windows\\temp\\evil.exe"},{"@Name":"CurrentDirectory","#text":"C:\\Windows\\system32\\"},{"@Name":"User","#text":"IEWIN7\\IEUser"},{"@Name":"LogonGuid","#text":"365abb72-6d1b-5d0a-0000-

0020fc340100"},{"@Name":"LogonId","#text":"0x134FC"},{"@Name":"TerminalSessionId","#text":"1"},{"@Name":"IntegrityLevel","#text":"Medium"},{"@Name":"Hashes","#text":"SHA1=EE8CBF12D87C4D388F09B4F69BED2E91682920B5,MD5=AD7B9C14083B52BC532FBA5948342B98,SHA256=17F746D82695FA9B35493B41859D39D786D32B23A9D2E00F4011DEC7A02402AE,IMPHASH=CEEFB55F764020CC5C5F8F23349AB163"},{"@Name":"ParentProcessGuid","#text":"365abb72-6f7f-5d0a-0000-0010816a1400"},{"@Name":"ParentProcessId","#text":"2856"},{"@Name":"ParentImage","#text":"C:\\Windows\\System32\\WerFault.exe"},{"@Name":"ParentCommandLine","#text":"\"C:\\Windows\\system32\\werfault.exe\" -s -t 3020 -i 2396 -e 2396 -c 0"}]}}

- Process ID: 284
- Provider: Microsoft-Windows-Sysmon
- Record Number: 13
- Thread ID: 2076
- User ID: S-1-5-18
- Username: IEWIN7\IEUser

Payload Data

- Name: ProcessGuid / Text: 365abb72-6f7f-5d0a-0000-0010b66e1400
- Name: ProcessId / Text: 3800
- Name: Image / Text: C:\\Windows\\Temp\\evil.exe
- Name: FileVersion / Text: 6.1.7601.17514 (win7sp1_rtm.101119-1850)
- Name: Description / Text: Windows Command Processor
- Name: Product / Text: Microsoft® Windows® Operating System
- Name: Company / Text: Microsoft Corporation
- Name: CommandLine / Text: C:\\windows\\temp\\evil.exe
- Name: CurrentDirectory / Text: C:\\Windows\\system32\\
- Name: LogonGuid / Text: 365abb72-6d1b-5d0a-0000-0020fc340100
- Name: LogonId / Text: 0x134FC
- Name: TerminalSessionId / Text: 1
- Name: IntegrityLevel / Text: Medium
- Name: ParentProcessGuid / Text: 365abb72-6f7f-5d0a-0000-0010816a1400
- Name: ParentProcessId / Text: 2856
- Name: ParentImage / Text: C:\\Windows\\System32\\WerFault.exe
- Name: ParentCommandLine / Text: \"C:\\Windows\\system32\\werfault.exe\" -s -t 3020 -i 2396 -e 2396 -c 0"

Malicious Indicators

- CommandLine / Text: C:\\windows\\temp\\evil.exe

SHA1=EE8CBF12D87C4D388F09B4F69BED2E91682920B5

- Undetected Hashes on multiple domains via VirusTotal.
- Signature Verification: File is not signed.

- Original File Name: Cmd.Exe
- Malicious IP's contacted: 104.86.182.8 (3 interactions)
- Execution Parents: Several have been used with literal virus Win32 Exe's.
- PE Resource Parents: This file has been embedded in several malicious .exe's even a direct cmd .exe.

Name: ParentImage / Text: C:\\Windows\\System32\\WerFault.exe

- This is actually a legit Windows process named "Windows Error reporting Fault Handler".

  It handles crash reports and app error dialogs. Also, it's located in the System32 Folder under C:/drive, so "normally" that's not suspicious. But the command listed under that same file path should raise the question.

Name: ParentCommandLine / Text: \"C:\\Windows\\system32\\werfault.exe\" -s -t 3020 -i 2396 -e 2396 -c 0"

- This is suspicious, because -s,-t,-I,-e,-c switches aren't used for normal "werfault.exe" usage and isn't publicly noted.
- So, in this case, "werfault.exe" is likely being abused to execute something malicious. Based off the 9.9k execution parents, it could suggest that werfault.exe is the parent file of suspicious children like Cmd.Exe or evil.exe. Which would confirm possibility of execution impersonation.

==========

Execution_Msxsl_Sysmon_Csv: Log Analysis

Data sources: Data sources: Sysmon, Windows Security

Tactic: Execution

ATT&CK Technique: T1220 – XSL Script Processing | T1105 – Ingress Tool Transfer

Execution_Msxsl_Sysmon_Csv: Summary

- The file with SHA1 EE8CBF12D87C4D388F09B4F69BED2E91682920B5 is malicious, matching the suspicious evil.exe from the "Persistence_SilentProcessExit_Sysmon_Csv" log, disguised as cmd.exe and unsigned.
- The attacker has full access to the user’s VirtualBox VM and uses the host shared folder (\vboxsrv\HTools) to deliver tools from their PC into the VM.
- Malware like test.dat (a disguised malicious XSL file) is executed inside the VM via msxsl.exe, run under the spoofed cmd.exe.
- The attacker is likely trying to escalate privileges, gather credentials, and find ways to escape the VM to the host PC, but so far only controls the VM.

Execution_Msxsl_Sysmon_Csv: Mitigation Suggestions

- Regularly monitor running processes and system logs for unusual or hidden activity. This is recommended for the IT/Security team to oversee.

- Avoid clicking on links from unknown or untrusted sources to prevent phishing or drive-by downloads.
- Keep the operating system and firmware (including UEFI/BIOS) updated with the latest security patches.
- Use endpoint security tools that can detect hidden or silent malware processes.

Execution_Msxsl_Sysmon_Csv / 2025-01-05T17:26:09.437-06:00

- Execution
- Event ID: 1
- Event Record ID: 1019
- ExecutableInfo: "C:\Windows\System32\cmd.exe"
- Hidden Record: False
- Level: Info
- Map Description: Process creation
- Payload:

{"EventData":{"Data":[{"@Name":"RuleName"},{"@Name":"UtcTime","#text":"2019-05-23 17:26:09.417"},{"@Name":"ProcessGuid","#text":"365abb72-d7b1-5ce6-0000-00102cd76d00"},{"@Name":"ProcessId","#text":"2240"},{"@Name":"Image","#text":"C:\\Windows\\System32\\cmd.exe"},{"@Name":"FileVersion","#text":"6.1.7601.17514 (win7sp1_rtm.101119-1850)"},{"@Name":"Description","#text":"Windows Command Processor"},{"@Name":"Product","#text":"Microsoft® Windows® Operating System"},{"@Name":"Company","#text":"Microsoft Corporation"},{"@Name":"CommandLine","#text":"\"C:\\Windows\\System32\\cmd.exe\" "},{"@Name":"CurrentDirectory","#text":"D:\\"},{"@Name":"User","#text":"IEWIN7\\IEUser"},{"@Name":"LogonGuid","#text":"365abb72-ce6c-5ce6-0000-002047f30000"},{"@Name":"LogonId","#text":"0xF347"},{"@Name":"TerminalSessionId","#text":"1"},{"@Name":"IntegrityLevel","#text":"High"},{"@Name":"Hashes","#text":"SHA1=EE8CBF12D87C4D388F09B4F69BED2E91682920B5,MD5=AD7B9C14083B52BC532FBA5948342B98,SHA256=17F746D82695FA9B35493B41859D39D786D32B23A9D2E00F4011DEC7A02402AE,IMPHASH=CEEFB55F764020CC5C5F8F23349AB163"},{"@Name":"ParentProcessGuid","#text":"365abb72-d7b0-5ce6-0000-001077c56d00"},{"@Name":"ParentProcessId","#text":"3388"},{"@Name":"ParentImage","#text":"\\\\vboxsrv\\HTools\\msxsl.exe"},{"@Name":"ParentCommandLine","#text":"msxsl.exe c:\\Users\\IEUser\\AppData\\Roaming\\Adobe\\test.dat c:\\Users\\IEUser\\AppData\\Roaming\\Adobe\\test.dat"}]}}

- Process ID: 2032
- Provider: Microsoft-Windows-Sysmon
- Record Number: 3

- Thread ID: 2092
- User ID: S-1-5-18
- Username: IEWIN7\IEUser

Payload Data

- Name: ProcessGuid / Text: 365abb72-d7b1-5ce6-0000-00102cd76d00
- Name: ProcessId / Text: 2240
- Name: Image / Text: C:\\Windows\\System32\\cmd.exe
- Name: FileVersion / Text: 6.1.7601.17514 (win7sp1_rtm.101119-1850)
- Name: Description / Text: Windows Command Processor
- Name: Product / Text: Microsoft® Windows® Operating System
- Name: Company / Text: Microsoft Corporation
- Name: CommandLine / Text: \"C:\\Windows\\System32\\cmd.exe\
- Name: CurrentDirectory / Text: D:\\
- Name: LogonGuid / Text: 365abb72-ce6c-5ce6-0000-002047f30000
- Name: LogonId / Text: 0xF347
- Name: TerminalSessionId / Text: 1
- Name: IntegrityLevel / Text: High
- Name: ParentProcessGuid / Text: 365abb72-d7b0-5ce6-0000-001077c56d00
- Name: ParentProcessId / Text: 3388
- Name: ParentImage / Text: \\\vboxsrv\\HTools\\msxsl.exe
- Name: ParentCommandLine / Text: msxsl.exe c:\\Users\\IEUser\\AppData\\Roaming\\Adobe\\test.dat c:\\Users\\IEUser\\AppData\\Roaming\\Adobe\\test.dat

Malicious Indicators

SHA1=EE8CBF12D87C4D388F09B4F69BED2E91682920B5

- This is the same file from the "Persistence_SilentProcessExit_Sysmon_Csv". Which suggests that this file is malicious as well.
- Signature Verification: File not signed
- Original File Name: Cmd.Exe
- Malicious IP's contacted: 104.86.182.8 (3 interactions)
- Execution Parents: Several have been used with literal virus Win32 Exe's.
- PE Resource Parents: This file has been embedded in several malicious .exe's even a direct cmd .exe.

Name: ParentImage / Text: \\\vboxsrv\\HTools\\msxsl.exe

- The attacker has complete access to the primary user's VirtualBox environment (VM).
- so, he's essentially pushing malware into the VM with hopes to get information from the VM that will hopefully reveal a vulnerability to get information from the host pc or get into host PC altogether, but overall, he's not there yet, the attacker only has access to the host's VM.
- The attacker is using the host shared folder in the VM to bring in tools from his PC to execute malware.

- Executing malware (test.dat, cmd.exe) within the guest VM. From the "Persistence_SilentProcessExit_Sysmon_Csv" we know the cmd.exe is a disguise for the real file name "evil.exe". And once the user moved his tools onto the primary user's VM environment. He ran a script that used a malicious XSL file and disguised it as a harmless .dat file. In this case the .dat file was named "test.dat".
- He's likely trying to escalate privileges, gather crediential and discover overall vulnerabilities that can allow him to escape the host machine and land onto the host's primary computer.

```
 Name: ParentCommandLine / Text: msxsl.exe
c:\\Users\\IEUser\\AppData\\Roaming\\Adobe\\test.dat
c:\\Users\\IEUser\\AppData\\Roaming\\Adobe\\test.dat
```

- This is the script that the attacker ran inside the spoofed cmd.exe to push a malicious XSL file into the VM environment disguised as a harmless file named "test.dat". Which attacker is using for persistence . Spoofing the cmd.exe and covering the malicious .xsl file helps the attacker significantly go unnoticed on the VM.

==========

PE_UACME_Sysmon_Csv: Log Analysis

Data sources: Data sources: Sysmon, Windows Security

Tactic: Privilege Escalation

ATT&CK Technique: T1055 / T1059.003 – Command and Scripting Interpreter: Windows Command Shell | T1547 / T1059.003 / T1036 – Multiple overlapping techniques

PE_UACME_Sysmon_Csv: Summary

- Throughout multiple logs, I've noticed a recurring pattern: an unsigned cmd.exe that is not only malicious, but also acts as a loader for malware, enabling persistence and privilege escalation. Based on earlier logs, this spoofed cmd.exe is likely masking a file named evil.exe.
- I will also note that one of the parent executables for this cmd.exe is a.exe, which is used to hide an application auto-starting upon UEFI, allowing persistence for the attacker.
- Following Ive noticed the parent command line was C:\windows\system32\taskmgr.exe. And the child command line was cmd.exe. This is also suspicious and shows indications of possibly the taskmgr.exe used to start command prompt is spoofed, and overall malicious. Reasoning being that there are No legitimate scenarios where Task Manager opens Command Prompt by itself. Additionally, No standard CLI commands run through Task Manager that would launch cmd.exe.
- Concluding, I believe that the primary user PC shows indications of being compromised.

PE_UACME_Sysmon_Csv: Mitigation Suggestions

- Regularly monitor running processes and system logs for unusual or hidden activity. This is recommended for the IT/Security team to oversee.
- Avoid clicking on links from unknown or untrusted sources to prevent phishing or drive-by downloads.
- Keep the operating system and firmware (including UEFI/BIOS) updated with the latest security patches.
- Use endpoint security tools that can detect hidden or silent malware processes.

PE_UACME_Sysmon_Csv / 2020-10-05T20:43:58.451-05:00

- Privilege Escalation
- Event ID: 1
- Event Record ID: 2164892
- ExecutableInfo: cmd.exe
- Hidden Record: False
- Level: Info
- Map Description: Process creation
- Payload: {"EventData":{"Data":[{"@Name":"RuleName"},{"@Name":"UtcTime","#text":"2020-10-05 20:43:58.450"},{"@Name":"ProcessGuid","#text":"00247c92-858e-5f7b-0000-0010e741202b"},{"@Name":"ProcessId","#text":"6636"},{"@Name":"Image","#text":"C:\\Windows\\System32\\cmd.exe"},{"@Name":"FileVersion","#text":"10.0.18362.449 (WinBuild.160101.0800)"},{"@Name":"Description","#text":"Windows Command Processor"},{"@Name":"Product","#text":"Microsoft® Windows® Operating System"},{"@Name":"Company","#text":"Microsoft Corporation"},{"@Name":"OriginalFileName","#text":"Cmd.Exe"},{"@Name":"CommandLine","#text":"cmd.exe"},{"@Name":"CurrentDirectory","#text":"C:\\windows\\"},{"@Name":"User","#text":"LAPTOP-JU4M3I0E\\bouss"},{"@Name":"LogonGuid","#text":"00247c92-8c36-5f75-0000-002034e39103"},{"@Name":"LogonId","#text":"0x391E334"},{"@Name":"TerminalSessionId","#text":"2"},{"@Name":"IntegrityLevel","#text":"High"},{"@Name":"Hashes","#text":"SHA1=8DCA9749CD48D286950E7A9FA1088C937CBCCAD4,MD5=D7AB69FAD18D4A643D84A271DFC0DBDF,SHA256=FF79D3C4A0B7EB191783C323AB8363EBD1FD10BE58D8BCC96B07067743CA81D5,IMPHASH=272245E2988E1E430500B852C4FB5E18"},{"@Name":"ParentProcessGuid","#text":"00247c92-858e-5f7b-0000-00105241202b"},{"@Name":"ParentProcessId","#text":"18404"},{"@Name":"ParentImage","#text":"C:\\Windows\\System32\\Taskmgr.exe"},{"@Name":"ParentCommandLine","#text":"C:\\windows\\system32\\taskmgr.exe"}]}}
- Process ID: 5424

- Provider: Microsoft-Windows-Sysmon
- Record Number: 7
- Thread ID: 6708
- User ID: S-1-5-18
- Username: LAPTOP-JU4M3I0E\bouss

Payload Data

- Name: ProcessGuid /Text: 00247c92-858e-5f7b-0000-0010e741202b
- Name: ProcessId / Text: 6636
- Name: Image / Text: C:\\Windows\\System32\\cmd.exe
- Name: FileVersion / Text: 10.0.18362.449 (WinBuild.160101.0800)
- Name: Description / Text: Windows Command Processor
- Name: Product / Text: Microsoft® Windows® Operating System
- Name: Company / Text: Microsoft Corporation
- Name: OriginalFileName / Text: Cmd.Exe
- Name: CommandLine / Text: cmd.exe
- Name: CurrentDirectory / Text: C:\\windows\\
- Name: LogonGuid /Text: 00247c92-8c36-5f75-0000-002034e39103
- Name: LogonId / Text: 0x391E334
- Name: TerminalSessionId / Text: 2
- Name: IntegrityLevel / Text: High
- Name: ParentProcessGuid / Text: 00247c92-858e-5f7b-0000-00105241202b
- Name: ParentProcessId / Text: 18404
- Name: ParentImage / Text: C:\\Windows\\System32\\Taskmgr.exe
- Name: ParentCommandLine / Text: C:\\windows\\system32\\taskmgr.exe

Malicious Indicators

SHA1 = 8DCA9749CD48D286950E7A9FA1088C937CBCCAD4

- Signature Verification: File not signed
- Original Name: Cmd.Exe
- Several Malicious Execution Parents: neshta.exe, sd.exe, Glenmore.exe, salinesh.exe, neshta.exe, Wextract, a.exe, cmd22.exe, E1614A878888EDDB3296E856DC5F4E63A926B9E4C899CF09DA12A8F477ACE4CF.EXE, a.exe.exe