##### **Liam Smith - October 2019**

##### **Goals:**

* Get participants acquainted with common Windows Event Logs.
* Familiarize participants with Windows Logon Types.
* Demonstrate a successful attack.
* Encourage research of attack.
* Demonstrate the power and importance of Sysmon.

| File | Hash (MD5) |
| --- | --- |
| EventViewer/Microsoft-Windows-Sysmon%4Operational.evtx | 930747a3c50c24c1f83f119bcff29838 |
| BTOBTO/Security.evtx | 801246e4a5305da60f4f118b15153495 |
| BTOBTO/System.evtx | 5654e40fd8b64e4cd4878b4dbef36d50 |
| BTOBTO/$UsnJrnl$J | 0b42a8d3b40cacd5c81604a8b0f1f298 |
| RDP/Microsoft-Windows-Sysmon%4Operational.evtx | 69b6f869b9f039b96da97b160cb7606c |
| RDP/Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx | dd81d647ae31200a9cc8f9724f42d470 |
| RDP/System.evtx | 0485d480a8e02e30049732fd31d17eaf |

##### **EventViewer**

| Question | Difficulty | Hint | Answer |
| --- | --- | --- | --- |
| What is the fully qualified domain name (FQDN) of the computer this log came from? | M | If viewed in Event Viewer, it is in the Details -> System Section. | weakServer.wiredbrain.priv |
| What user is conducting the action in this event log? Format: exampleDomain\Exampleuser | E | It is not SYSTEM. | wiredbrain\weakadmin |
| What is the Process ID of the program launched? | E | View the Log in Event Viewer, or parse it. | 1728 |

##### **BTOBTO**

| Question | Difficulty | Hint | Answer |
| --- | --- | --- | --- |
| What is the name of the service being installed? | E | This is in the System log. | BTOBTO |
| What is the first command that the attacker ran? | M | What are the parts of the code that are changing each attack? | echo cd |
| What two files are being created for every attacker command? | M | When confronted with a long command, break it down part by part. | \_\_output  execute.bat |
| What program is executing the attacker commands? Format: evil.exe | M | What is %COMSPEC%? | cmd.exe |
| What is the Github repository of the tool involved in this attack? | H | We dont care about opsec! Google everything about these logs! | https://github.com/SecureAuthCorp/impacket |
| What is the kind of logon that occurred? (Not a number, but what that number means). | M | Review your logon types. | network |
| What is the Update Sequence Number for the creation of execute.bat? | H | Parse the $J. | 9411576 |
| What is the Update Sequence Number for the last file close of \_\_output? | H | Parse the $J. | 9467064 |

##### **RDP**

| Question | Difficulty | Hint | Answer |
| --- | --- | --- | --- |
| What is the user that was used to conduct this attack? | E | Who authenticated with the RDP attack? | wiredbrain\weakadmin |
| What IP address did the attack come from? | E | A remote desktop connection comes from somewhere. | 10.0.0.3 |
| What is the IP address of the Command and Control (C2) the implant reaches out to? | M | While the attacker came from one place, where does their process go? | 10.0.0.11 |
| What is the encoding algorithm being used in this attack? | M | What does the powershell “-e” flag do? | Base64 |
| What is the hostname of the C2? | M | Sysmon is amazing right? It’ll help you with that. | COMMANDO |
| What is the User the implant is running as? | M | Not who MADE the implant.. But what is the process running AS. | NT AUTHORITY\SYSTEM |
| What is the name of the C2 framework being used? | H | We dont care about OPSec! Google… maybe something more? | PoshC2 |