Demonstration of the Chainsaw Tool for Windows Event Log Analysis

In previous reports, we explored DeepBlueCLI and Hayabusa, tools used to analyse and investigate Windows Event Logs. This demonstration focuses on Chainsaw, a tool developed by Labswithsecure. As stated on their GitHub page, Chainsaw "provides a powerful 'first-response' capability to quickly identify threats within Windows forensic artefacts such as Event Logs and the MFT file". Chainsaw stands out due to its ability to search through event logs for specific keywords, custom detection rules, and several other functionality not present in other available tools.

Chainsaw provides several features including:

- Hunting for threats using Sigma detection rules and custom rules
- Searching and extracting forensic artefacts by string matches and regex
- Creating execution timelines by analysing Shimcache artefacts and enriching them with Amcache data
- Analysing the SRUM database and provide insights about it
- Dumping the raw content of forensic artefacts, and more.

Chainsaw and the aforementioned tools are all meant to be used for quick forensics, it is not meant to replace other tools and workflows. Searching through and processing event logs is a slow and time-consuming process which is where tools like this come into play. The following event IDs are supported by Chainsaw (not limited to):

Event Type	Event ID
Process Creation (Sysmon)	1
Network Connections (Sysmon)	3
Image Loads (Sysmon)	7
File Creation (Sysmon)	11
Registry Events (Sysmon)	13
Powershell Script Blocks	4104
Process Creation	4688
Scheduled Task Creation	4698
Service Creation	7045

1. Downloading Chainsaw

To download chainsaw, navigate to their releases page and download whatever version supports your OS (in my case I am downloading chainsaw all platforms):

chainsaw_aarch64-apple-darwin.zip	2.83 MB	3 weeks ago
chainsaw_all_platforms+rules+examples.zip	44.1 MB	3 weeks ago
chainsaw_all_platforms+rules.zip	32.9 MB	3 weeks ago
chainsaw_x86_64-apple-darwin.zip	2.97 MB	3 weeks ago
chainsaw_x86_64-pc-windows-msvc.zip	2.99 MB	3 weeks ago
chainsaw_x86_64-unknown-linux-gnu.tar.gz	3.27 MB	3 weeks ago
Source code (zip)		3 weeks ago
Source code (tar.gz)		3 weeks ago

2. Using Chainsaw

Once you have extracted the zip archive, open a CMD prompt and navigate to the installation directory:

```
12/07/2024  07:10 AM    <DIR>          .
04/08/2024  08:55 PM    <DIR>          ..
12/07/2024  07:10 AM         8,010,584 chainsaw_aarch64-apple-darwin
12/07/2024  07:10 AM         8,375,752 chainsaw_x86_64-apple-darwin
12/07/2024  07:10 AM         9,177,088 chainsaw_x86_64-pc-windows-msvc.exe
12/07/2024  07:10 AM        10,175,344 chainsaw_x86_64-unknown-linux-gnu
12/07/2024  07:10 AM    <DIR>          EVTX-ATTACK-SAMPLES
12/07/2024  07:10 AM            35,142 LICENCE
12/07/2024  07:10 AM    <DIR>          mappings
12/07/2024  07:10 AM            50,365 README.md
12/07/2024  07:10 AM    <DIR>          rules
12/07/2024  07:10 AM    <DIR>          sigma
```

To start hunting using the sigma rules and custom Chainsaw rules you can enter the following:

```
chainsaw_x86_64-pc-windows-msvc.exe hunt EVTX-ATTACK-SAMPLES -s sigma/ --mapping mappings/sigma-event-logs-all.yml -r rules/ --csv --output results
```

Please note that you can place any evtx file or directory containing several evtx files after you have entered the binary name, i.e., the syntax is:

- <chainsaw_binary> hunt <evtx_location>/ -s sigma/ --mapping mappings/sigma-event-logs-all.yml -r rules/ --csv --output <output_directory_name>

```
CHAINSAW
    By WithSecure Countercept (@FranticTyping, @AlexKornitzer)

[+] Loading detection rules from: rules/, sigma/
[!] Loaded 3310 detection rules (482 not loaded)
[+] Loading forensic artefacts from: EVTX-ATTACK-SAMPLES (extensions: .evtx, .evt)
[+] Loaded 278 forensic artefacts (48.7 MB)
[+] Hunting: [========================================] 278/278 -
[+] Created account_tampering.csv
[+] Created antivirus.csv
[+] Created lateral_movement.csv
[+] Created log_tampering.csv
[+] Created powershell_script.csv
[+] Created service_installation.csv
[+] Created sigma.csv
[+] Created rdp_attacks.csv

[+] 1433 Detections found on 942 documents
```

As you can see, 1433 detections were found, and Chainsaw created several csv files for which are the results we want to investigate, let's look at the service_installation.csv file by using Timeline Explorer (note, you can view the CSV file in notepad, excel, etc):

detections	…	…	…	Computer	Service Name	Service File Name
Meterpreter or Cobalt Strike Getsystem Service Installation;Suspicious Commands Service Installation	…	…	…	IEWIN7	WinPwnage	%COMSPEC% /c ping -n 1 127.0.0.1 >nul && echo 'WinPwnage' >

The image above is a snippet of the output. As you can see, Chainsaw was able to correctly identify Meterpreter or Cobalt Strike being installed as a service. The sigma.csv file contains all of the sigma rules matched, meaning there is a lot of logs in this file with no logical order:

timestamp	detections
2017-06-09T19:21:26.968669+00:00	Password Change on Directory Service Restore Mode (DSRM) Account
2017-06-12T23:39:43.512986+00:00	Addition of SID History to Active Directory Object
2017-06-12T23:39:43.512986+00:00	Password Policy Enumerated
2019-02-02T09:17:27.629413+00:00	Powerview Add-DomainObjectAcl DCSync AD Extend Right
2019-02-02T09:17:27.629830+00:00	Powerview Add-DomainObjectAcl DCSync AD Extend Right
2019-02-13T15:26:53.356780+00:00	RDP Login from Localhost
2019-02-13T18:04:58.363696+00:00	Admin User Remote Logon;RDP Login from Localhost
2019-02-16T10:02:21.934438+00:00	Potential Remote Desktop Tunneling;Suspicious Plink Port Forwarding;Tunneling Tool Execution
2019-03-03T09:20:28.621489+00:00	Rare Service Installations
2019-03-03T09:24:24.699653+00:00	Rare Service Installations
2019-03-17T19:09:41.328868+00:00	DMP/HDMP File Creation;Godmode Sigma Rule;LSASS Memory Dump File Creation;LSASS Process Memory Dump Files
2019-03-17T19:09:41.328868+00:00	LSASS Memory Access by Tool With Dump Keyword In Name
2019-03-17T19:10:03.991455+00:00	DMP/HDMP File Creation;Godmode Sigma Rule;LSASS Memory Dump File Creation;LSASS Process Memory Dump Creation Via Taskmgr.EXE;LSASS Process Memory Dump Files
2019-03-17T19:37:11.661930+00:00	HackTool - Generic Process Access;Mimikatz Detection LSASS Access;Uncommon GrantedAccess Flags On LSASS
2019-03-17T20:18:05.086560+00:00	RDP Sensitive Settings Changed;ServiceDll Hijack
2019-03-17T20:18:09.282593+00:00	RDP Sensitive Settings Changed to Zero
2019-03-17T20:20:17.907547+00:00	File or Folder Permissions Modifications
2019-03-17T20:20:17.917561+00:00	File or Folder Permissions Modifications

Let's say you just want to display the results to the terminal and only for critical rules, you can do that by entering the following:

```
chainsaw_x86_64-pc-windows-msvc.exe hunt -r rules/ EVTX-ATTACK-SAMPLES  -s sigma/rules --mapping mappings/sigma-event-logs-all.yml --level critical
```

This provides the output in neat tables formatted by groups:

[+] Group: Antivirus

timestamp	detections	Event ID	Record ID	Computer	Threat Name	Threat Path	SHA1	User	Threat Type
2019-07-18 20:40:00	+ Windows Defender	1116	37	MSEDGEWIN10	Trojan:PowerShell/Powersploit.M	file:_C:\AtomicRedTeam\atomic-red-team-master\atomics\T1056\Get-Keystrokes.ps1		MSEDGEWIN10\IEUser	
2019-07-18 20:40:16	+ Windows Defender	1116	48	MSEDGEWIN10	Trojan:XML/Exeselrun.gen!A	file:_C:\AtomicRedTeam\atomic-red-team-master\atomics\T1086\payloads\test.xsl		MSEDGEWIN10\IEUser	
2019-07-18 20:41:16	+ Windows Defender	1116	75	MSEDGEWIN10	HackTool:JS/Jsprat	file:_C:\AtomicRedTeam\atomic-red-team-master\atomics\T1100\shells\b.jsp->(SCRIPT0005)		MSEDGEWIN10\IEUser	
2019-07-18 20:41:17	+ Windows Defender	1116	76	MSEDGEWIN10	Backdoor:ASP/Ace.T	file:_C:\AtomicRedTeam\atomic-red-team-master\atomics\T1100\shells\cmd.aspx		MSEDGEWIN10\IEUser	
2019-07-18 20:41:48	+ Windows Defender	1116	95	MSEDGEWIN10	Trojan:Win32/Sehyioa.A!cl	file:_C:\AtomicRedTeam\atomic-red-team-master\atomics\T1218\src\Win32\T1218-2.dll		MSEDGEWIN10\IEUser	
2019-07-18 20:51:50	+ Windows Defender	1117	101	MSEDGEWIN10	Trojan:PowerShell/Powersploit.M	file:_C:\AtomicRedTeam\atomic-red-team-master\atomics\T1056\Get-Keystrokes.ps1		MSEDGEWIN10\IEUser	
2019-07-18 20:51:50	+ Windows Defender	1116	102	MSEDGEWIN10	HackTool:JS/Jsprat	containerfile:_C:\AtomicRedTeam\atomic-red-team-master\atomics\T1100\shells\b.jsp; file:_C:\AtomicRedTeam\atomic-red-team-master\atomics\T1100\shells\b.jsp->(SCRIPT0005); file:_C:\AtomicRedTeam\atomic-red-team-master\atomics\T1100\shells\b.jsp->(SCRIPT0037); file:_C:\AtomicRedTeam\atomic-red-team-master\atomics\T1100\shells\b.jsp->(SCRIPT0045); file:_C:\AtomicRedTeam\atomic-red-team-master\atomics\T1100\shells\b.jsp->(SCRIPT0065); file:_C:\AtomicRedTeam\atomic-red-team-master ... (use --full to show all content)		MSEDGEWIN10\IEUser	

3. Searching with Chainsaw

Chainsaw can also be used to search for keywords, in the following example, we are searching for the keyword ‘mimikatz’ which is a popular credential dumping tool:

```
chainsaw_x86_64-pc-windows-msvc.exe search mimikatz -i EVTX-ATTACK-SAMPLES
```

You can put any keyword after the search tag. The results are very long, but the following image is a small snippet showing the Event Logs that contains the keyword:

```
CHAINSAW
   By WithSecure Countercept (@FranticTyping, @AlexKornitzer)

[+] Loading forensic artefacts from: EVTX-ATTACK-SAMPLES
[+] Loaded 345 forensic files (68.6 MB)
[+] Searching forensic artefacts...
---
Event:
  EventData:
    CallTrace: C:\Windows\SYSTEM32\ntdll.dll+4595c|C:\Windows\system32\KERNELBASE.dll
sktop\mimikatz_trunk\Win32\mimikatz.exe+5cbd2|C:\Users\IEUser\Desktop\mimikatz_trunk
    GrantedAccess: '0x1010'
    RuleName: ''
    SourceImage: C:\Users\IEUser\Desktop\mimikatz_trunk\Win32\mimikatz.exe
    SourceProcessGUID: 365ABB72-A1E3-5C8E-0000-0010CEF72200
    SourceProcessId: 3588
    SourceThreadId: 2272
    TargetImage: C:\Windows\system32\lsass.exe
    TargetProcessGUID: 365ABB72-0886-5C8F-0000-001030560000
    TargetProcessId: 476
    UtcTime: 2019-03-17 19:37:11.641
  System:
    Channel: Microsoft-Windows-Sysmon/Operational
    Computer: PC04.example.corp
    Correlation: null
    EventID: 10
    EventRecordID: 4807
    Execution_attributes:
      ProcessID: 344
      ThreadID: 2032
    Keywords: '0x8000000000000000'
    Level: 4
    Opcode: 0
    Provider_attributes:
      Guid: 5770385F-C22A-43E0-BF4C-06F5698FFBD9
      Name: Microsoft-Windows-Sysmon
    Security_attributes:
      UserID: S-1-5-18
    Task: 10
    TimeCreated_attributes:
      SystemTime: 2019-03-17T19:37:11.661930Z
    Version: 3
Event_attributes:
  xmlns: http://schemas.microsoft.com/win/2004/08/events/event
```

The search function can be really handy if you have identified a malicious binary and want to search for all Event Logs containing said binary.

4. Conclusion

Chainsaw is a robust tool for quickly identifying threats in Windows forensic artifacts. It supports various event IDs and offers powerful capabilities. By following the steps outlined, you can efficiently use Chainsaw to enhance your forensic analysis and threat detection workflows.