Demonstration of the Hayabusa Tool for Windows Event Log Analysis

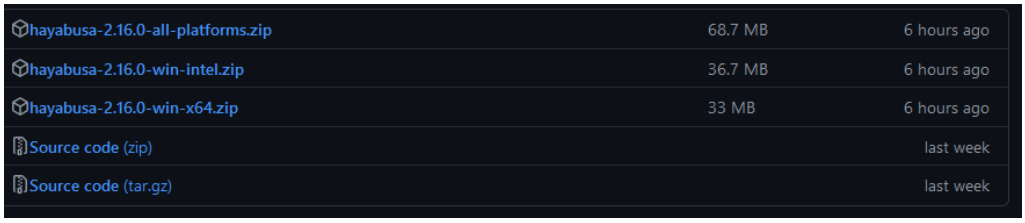
In a previous report, I discussed using the DeepBlueCLI tool for analysing Windows Event logs for the purpose of threat hunting. While DeepBlueCLI is an excellent tool, I recently discovered Hayabusa, developed by the Yamato Security Group. According to its GitHub page, Hayabusa is a "Winsows event log fast forensics timeline generator and threat hunting tool created by the Yamato Security group". Hayabusa supports over 4000 Sigma rules and more than 170 built-in detection rules, facilitating proactive threat hunting and digital forensics and incident response (DFIR). The tool is compatible with Windows, Linux, and macOS.

1. Getting Started with Hayabusa

Download and installation:

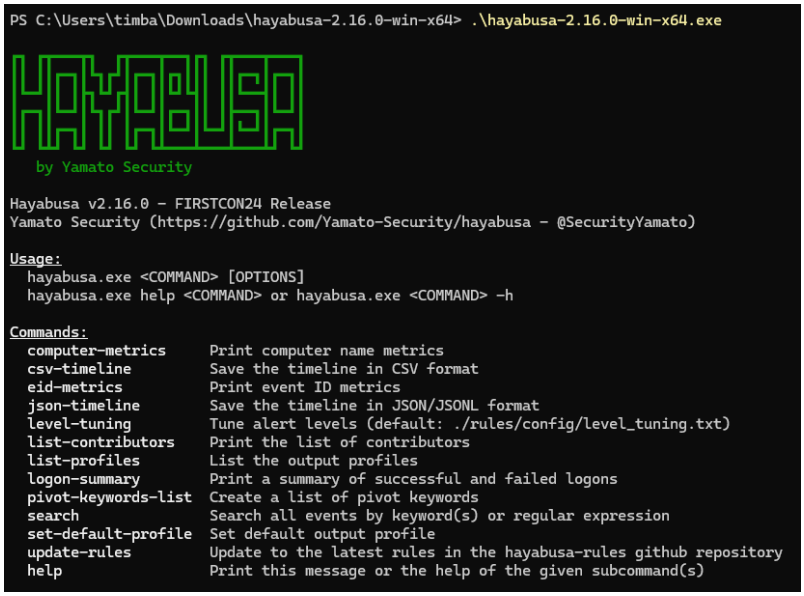
In this demonstration, I will be using Hayabusa on Windows to demonstrate the tool against a series of Windows event logs. To start, navigate to the releases page on their GitHub:

You can then download the newest release (in my case, I chose the win-x64 version):



Once the zip file has downloaded, make sure to extract it. Now open a PowerShell window and navigate to the download directory:

```
PS C:\Users\timba> cd C:\Users\timba\Downloads\hayabusa-2.16.0-win-x64
PS C:\Users\timba\Downloads\hayabusa-2.16.0-win-x64>
```



2. Using Hayabusa

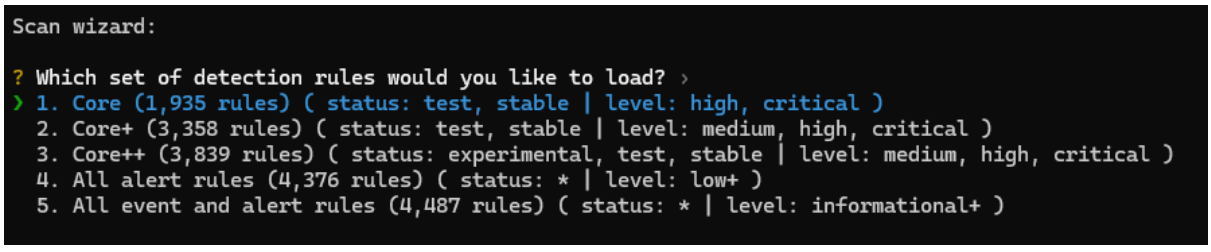
To start using the tool, let's first make sure it has all the updated rules, we can update the rules by entering:

```
.\hayabusa-2.16.0-win-x64.exe update-rules
```

Let's now use Hayabusa to create a csv timeline for a given event log:

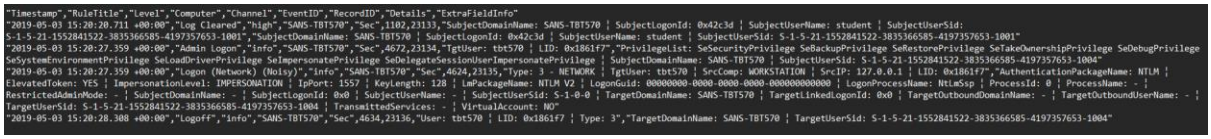
```
.\hayabusa-2.16.0-win-x64.exe csv-timeline -f C:\Users\timba\Downloads\evtx\metasploit-psexec-pwshpayload.evtx -U -o hayabusa_test.csv
```

This command uses the csv-timeline option, -f signifies the evtx file or folder containing a series of evtx files, -U makes the time zone set to UTC, and -o signifies the output file. Run the command by clicking enter:



You will then be prompted asking which set of detection rules would you like to load. This is based off of the sigma rules, in these examples I am going to select all event and alert rules (option 5) and enter y for the other prompts. Once it has analysed the evtx file, it will output the

results to the terminal and the csv file will be saved to the designated location. I opened the results in notepad:



Improved Example

To provide a better example, I downloaded additional sample evtx files, namely one that recorded the logs generated when using the AtomicRedTeam tool. The output produced this time is extremely informative and useful when threat hunting or performing DFIR (some columns have been removed for clarity):

Timestamp	RuleTitle	Level	Computer	Details
2019-07-18 20:40:00.730 +00:00	Antivirus Hacktool Detection	high	MSEDGEWIN10	Threat: Trojan:PowerShell/Powersploit.M Â¦ Severity: Severe Â¦ Type:
2019-07-18 20:40:00.730 +00:00	Antivirus Relevant File Paths Alerts	high	MSEDGEWIN10	Threat: Trojan:PowerShell/Powersploit.M Â¦ Severity: Severe Â¦ Type:
2019-07-18 20:40:00.730 +00:00	Defender Alert (Severe)	crit	MSEDGEWIN10	Threat: Trojan:PowerShell/Powersploit.M Â¦ Severity: Severe Â¦ Type:
2019-07-18 20:40:00.730 +00:00	Antivirus Exploitation Framework Detection	crit	MSEDGEWIN10	Threat: Trojan:PowerShell/Powersploit.M Â¦ Severity: Severe Â¦ Type:
2019-07-18 20:40:16.396 +00:00	Defender Alert (Severe)	crit	MSEDGEWIN10	Threat: Trojan:XML/Exeselrun.gen!A Â¦ Severity: Severe Â¦ Type: Troja
2019-07-18 20:41:16.418 +00:00	Defender Alert (High)	high	MSEDGEWIN10	Threat: HackTool:JS/Jsprat Â¦ Severity: High Â¦ Type: Tool Â¦ User: MS
2019-07-18 20:41:16.418 +00:00	Antivirus Hacktool Detection	high	MSEDGEWIN10	Threat: HackTool:JS/Jsprat Â¦ Severity: High Â¦ Type: Tool Â¦ User: MS
2019-07-18 20:41:17.508 +00:00	Antivirus Relevant File Paths Alerts	high	MSEDGEWIN10	Threat: Backdoor:ASP/Ace.T Â¦ Severity: Severe Â¦ Type: Backdoor Â¦
2019-07-18 20:41:17.508 +00:00	Antivirus Web Shell Detection	high	MSEDGEWIN10	Threat: Backdoor:ASP/Ace.T Â¦ Severity: Severe Â¦ Type: Backdoor Â¦
2019-07-18 20:41:17.508 +00:00	Defender Alert (Severe)	crit	MSEDGEWIN10	Threat: Backdoor:ASP/Ace.T Â¦ Severity: Severe Â¦ Type: Backdoor Â¦
2019-07-18 20:41:48.236 +00:00	Defender Alert (Severe)	crit	MSEDGEWIN10	Threat: Trojan:Win32/Sehyioa.A!cl Â¦ Severity: Severe Â¦ Type: Trojan
2019-07-18 20:51:50.798 +00:00	Defender Alert (High)	high	MSEDGEWIN10	Threat: HackTool:JS/Jsprat Â¦ Severity: High Â¦ Type: Tool Â¦ User: MS
2019-07-18 20:51:50.798 +00:00	Antivirus Hacktool Detection	high	MSEDGEWIN10	Threat: HackTool:JS/Jsprat Â¦ Severity: High Â¦ Type: Tool Â¦ User: MS

As you can see, the information provided by Hayabusa would be extremely helpful as we can immediately determine malicious activities are occurring on the MSEDGEWIN10 machine.

HTML Results Summary

Hayabusa can also output results in HTML format. To output the results in HTML format, we can use the -H option like as follows:

```
.\hayabusa-2.16.0-win-x64.exe csv-timeline -f C:\Users\timba\Downloads\evtx\WinDefender_Events_1117_1116_AtomicRedTeam.evtx -U -o test3.csv -H report.html
```

The image below shows some of the output, if you click the hyperlinks, you are also provided with the sigma rule that matched:

Computers with most unique critical detections:

- MSEDGEWIN10 (2)

Computers with most unique high detections:

- MSEDGEWIN10 (4)

Computers with most unique medium detections:

Computers with most unique low detections:

Computers with most unique informational detections:

All critical alerts:

- Defender Alert (Severe) (4) - Zach Mathis, Fukusuke Takahashi
- Antivirus Exploitation Framework Detection (1) - Florian Roth, Arnim Rupp

All high alerts:

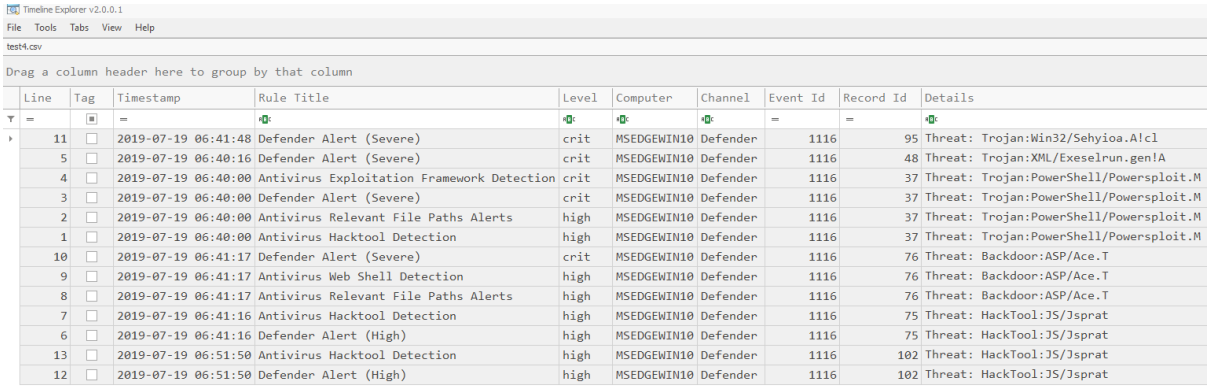
- Antivirus Hacktool Detection (3) - Florian Roth, Arnim Rupp
- Antivirus Relevant File Paths Alerts (2) - Florian Roth, Arnim Rupp
- Defender Alert (High) (2) - Zach Mathis, Fukusuke Takahashi
- Antivirus Web Shell Detection (1) - Florian Roth, Arnim Rupp

Multiline Output

If you want to import the results into tools like LibreOffice or Timeline Explorer, use the -M option:

```
.\hayabusa-2.16.0-win-x64.exe csv-timeline -f C:\Users\timba\Downloads\evtx\WinDefender_Events_1117_1116_AtomicRedTeam.evtx -U -o test4.csv -M
```

In this case, I am going to import the output into Timeline Explorer, which is a wonderful Eric Zimmerman tool:



Line	Tag	Timestamp	Rule Title	Level	Computer	Channel	Event Id	Record Id	Details
11		2019-07-19 06:41:48	Defender Alert (Severe)	crit	MSEDGEWIN10	Defender	1116	95	Threat: Trojan:Win32/Sehyioa.A!cl
5		2019-07-19 06:40:16	Defender Alert (Severe)	crit	MSEDGEWIN10	Defender	1116	48	Threat: Trojan:XML/Exeselrun.gen!A
4		2019-07-19 06:40:00	Antivirus Exploitation Framework Detection	crit	MSEDGEWIN10	Defender	1116	37	Threat: Trojan:PowerShell/Powersploit.M
3		2019-07-19 06:40:00	Defender Alert (Severe)	crit	MSEDGEWIN10	Defender	1116	37	Threat: Trojan:PowerShell/Powersploit.M
2		2019-07-19 06:40:00	Antivirus Relevant File Paths Alerts	high	MSEDGEWIN10	Defender	1116	37	Threat: Trojan:PowerShell/Powersploit.M
1		2019-07-19 06:40:00	Antivirus Hacktool Detection	high	MSEDGEWIN10	Defender	1116	37	Threat: Trojan:PowerShell/Powersploit.M
10		2019-07-19 06:41:17	Defender Alert (Severe)	crit	MSEDGEWIN10	Defender	1116	76	Threat: Backdoor:ASP/Ace.T
9		2019-07-19 06:41:17	Antivirus Web Shell Detection	high	MSEDGEWIN10	Defender	1116	76	Threat: Backdoor:ASP/Ace.T
8		2019-07-19 06:41:17	Antivirus Relevant File Paths Alerts	high	MSEDGEWIN10	Defender	1116	76	Threat: Backdoor:ASP/Ace.T
7		2019-07-19 06:41:16	Antivirus Hacktool Detection	high	MSEDGEWIN10	Defender	1116	75	Threat: HackTool:JS/Jsprat
6		2019-07-19 06:41:16	Defender Alert (High)	high	MSEDGEWIN10	Defender	1116	75	Threat: HackTool:JS/Jsprat
13		2019-07-19 06:51:50	Antivirus Hacktool Detection	high	MSEDGEWIN10	Defender	1116	102	Threat: HackTool:JS/Jsprat
12		2019-07-19 06:51:50	Defender Alert (High)	high	MSEDGEWIN10	Defender	1116	102	Threat: HackTool:JS/Jsprat

The output is much easier to read using a tool like Timeline Explorer compared to something like Excel or notepad.

Conclusion

I tested Hayabusa with various Windows event log files, including those containing Mimikatz activity, privilege escalation, password spraying, and Metasploit. The tool proved extremely valuable for threat hunting and DFIR, providing detailed and actionable insights.

Hayabusa is a robust tool that enhances the capability to quickly and effectively analyse Windows Event logs. Its compatibility across different platforms and extensive support for Sigma rules make it a must-have for any security professional's toolkit. Please note that this only touches the surface of this tool, it can be integrated with other popular tools such as Velociraptor and has several other features that weren't explored in this report.