

## 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 “Windows 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):

📦 hayabusa-2.16.0-all-platforms.zip	68.7 MB	6 hours ago
📦 hayabusa-2.16.0-win-intel.zip	36.7 MB	6 hours ago
📦 hayabusa-2.16.0-win-x64.zip	33 MB	6 hours ago
📄 Source code (zip)		last week
📄 Source code (tar.gz)		last week

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>
```

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

HAYABUSA
by Yamato Security

Hayabusa v2.16.0 - FIRSTCON24 Release
Yamato Security (https://github.com/Yamato-Security/hayabusa - @SecurityYamato)

Usage:
  hayabusa.exe <COMMAND> [OPTIONS]
  hayabusa.exe help <COMMAND> or hayabusa.exe <COMMAND> -h

Commands:
  computer-metrics  Print computer name metrics
  csv-timeline       Save the timeline in CSV format
  eid-metrics        Print event ID metrics
  json-timeline      Save the timeline in JSON/JSONL format
  level-tuning       Tune alert levels (default: ./rules/config/level_tuning.txt)
  list-contributors  Print the list of contributors
  list-profiles      List the output profiles
  logon-summary      Print a summary of successful and failed logons
  pivot-keywords-list Create a list of pivot keywords
  search             Search all events by keyword(s) or regular expression
  set-default-profile Set default output profile
  update-rules       Update to the latest rules in the hayabusa-rules github repository
  help              Print this message or the help of the given subcommand(s)
```

## 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:

```
Scan wizard:

? Which set of detection rules would you like to load? >
> 1. Core (1,935 rules) ( status: test, stable | level: high, critical )
  2. Core+ (3,358 rules) ( status: test, stable | level: medium, high, critical )
  3. Core++ (3,839 rules) ( status: experimental, test, stable | level: medium, high, critical )
  4. All alert rules (4,376 rules) ( status: * | level: low+ )
  5. All event and alert rules (4,487 rules) ( status: * | level: informational+ )
```

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:

```
"Timestamp","RuleTitle","Level","Computer","Channel","EventID","RecordID","Details","ExtraFieldInfo"
"2019-05-03 15:20:28.711 +00:00","Log Cleared","high","SAMS-TBTS70","Sec","1102,2313","SubjectDomainName: SAMS-TBTS70 | SubjectLogonId: 0x42c3d | SubjectUserName: student | SubjectUserSid: S-1-5-21-1552841522-3835366585-4197357653-1001"
"2019-05-03 15:20:27.359 +00:00","Admin Logon","info","SAMS-TBTS70","Sec","4672,23134","TgtUser: tbts70 | LID: 0x1861f7","PrivilegeList: SeSecurityPrivilege SeBackupPrivilege SeRestorePrivilege SeTakeOwnershipPrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeLoadDriverPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege | SubjectDomainName: SAMS-TBTS70 | SubjectUserSid: S-1-5-21-1552841522-3835366585-4197357653-1004"
"2019-05-03 15:20:27.359 +00:00","Logon (Network)","info","SAMS-TBTS70","Sec","4624,23135","Type: 3 - NETWORK | TgtUser: tbts70 | SecComp: WORKSTATION | SrcIP: 127.0.0.1 | LID: 0x1861f7","AuthenticationPackageName: NTLM | ElevatedToken: YES | ImpersonationLevel: DPPESS007100 | IPPort: 1552 | KeyLength: 128 | LpPackageNames: NTLM V2 | LogonGuid: 00000000-0000-0000-0000-000000000000 | LogonProcessName: WinLogon | ProcessId: 0 | ProcessName: - | RestrictedAdminMode: - | SubjectDomainName: - | SubjectLogonId: 0x0 | SubjectUserName: - | SubjectUserSid: S-1-0-0 | TargetDomainName: SAMS-TBTS70 | TargetLinkedLogonId: 0x0 | TargetOutboundDomainName: - | TargetOutboundUserName: - | TargetUserSid: S-1-5-21-1552841522-3835366585-4197357653-1004 | TransmittedServices: - | VirtualAccount: NO"
"2019-05-03 15:20:28.308 +00:00","Logoff","info","SAMS-TBTS70","Sec","4634,23136","User: tbts70 | LID: 0x1861f7 | Type: 3","TargetDomainName: SAMS-TBTS70 | TargetUserSid: S-1-5-21-1552841522-3835366585-4197357653-1004"
```

## 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/Exeserlrun.gen!A Â; Severity: Severe Â; Type: Troje
2019-07-18 20:41:16.418 +00:00	Defender Alert (High)	high	MSEDGEWIN10	Threat: HackTool:JS/Jspratt Â; Severity: High Â; Type: Tool Â; User: M:
2019-07-18 20:41:16.418 +00:00	Antivirus Hacktool Detection	high	MSEDGEWIN10	Threat: HackTool:JS/Jspratt Â; Severity: High Â; Type: Tool Â; User: M:
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/Jspratt Â; Severity: High Â; Type: Tool Â; User: M:
2019-07-18 20:51:50.798 +00:00	Antivirus Hacktool Detection	high	MSEDGEWIN10	Threat: HackTool:JS/Jspratt Â; Severity: High Â; Type: Tool Â; User: M:

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_AtomRedTeam.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:

Timeline Explorer v2.0.0.1										
File Tools Tabs View Help										
test4.csv										
Drag a column header here to group by that column										
	Line	Tag	Timestamp	Rule Title	Level	Computer	Channel	Event Id	Record Id	Details
Y	=	<input type="checkbox"/>	=	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	=	=	<input type="checkbox"/>
▾	11	<input type="checkbox"/>	2019-07-19 06:41:48	Defender Alert (Severe)	crit	MSEDGEWIN10	Defender	1116	95	Threat: Trojan:Win32/Sehyioa.A!cl
	5	<input type="checkbox"/>	2019-07-19 06:40:16	Defender Alert (Severe)	crit	MSEDGEWIN10	Defender	1116	48	Threat: Trojan:XML/Exeselrun.gen!A
	4	<input type="checkbox"/>	2019-07-19 06:40:00	Antivirus Exploitation Framework Detection	crit	MSEDGEWIN10	Defender	1116	37	Threat: Trojan:PowerShell/Powersploit.M
	3	<input type="checkbox"/>	2019-07-19 06:40:00	Defender Alert (Severe)	crit	MSEDGEWIN10	Defender	1116	37	Threat: Trojan:PowerShell/Powersploit.M
	2	<input type="checkbox"/>	2019-07-19 06:40:00	Antivirus Relevant File Paths Alerts	high	MSEDGEWIN10	Defender	1116	37	Threat: Trojan:PowerShell/Powersploit.M
	1	<input type="checkbox"/>	2019-07-19 06:40:00	Antivirus Hacktool Detection	high	MSEDGEWIN10	Defender	1116	37	Threat: Trojan:PowerShell/Powersploit.M
	10	<input type="checkbox"/>	2019-07-19 06:41:17	Defender Alert (Severe)	crit	MSEDGEWIN10	Defender	1116	76	Threat: Backdoor:ASP/Ace.T
	9	<input type="checkbox"/>	2019-07-19 06:41:17	Antivirus Web Shell Detection	high	MSEDGEWIN10	Defender	1116	76	Threat: Backdoor:ASP/Ace.T
	8	<input type="checkbox"/>	2019-07-19 06:41:17	Antivirus Relevant File Paths Alerts	high	MSEDGEWIN10	Defender	1116	76	Threat: Backdoor:ASP/Ace.T
	7	<input type="checkbox"/>	2019-07-19 06:41:16	Antivirus Hacktool Detection	high	MSEDGEWIN10	Defender	1116	75	Threat: HackTool:JS/Jsprat
	6	<input type="checkbox"/>	2019-07-19 06:41:16	Defender Alert (High)	high	MSEDGEWIN10	Defender	1116	75	Threat: HackTool:JS/Jsprat
	13	<input type="checkbox"/>	2019-07-19 06:51:50	Antivirus Hacktool Detection	high	MSEDGEWIN10	Defender	1116	102	Threat: HackTool:JS/Jsprat
	12	<input type="checkbox"/>	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.