TLP:CLEAR

Hayabusa & Takajō

隼  ×  鷹匠

*For an **Easier** DFIR Life*

Agenda

1) Problems with Windows Event Log Analysis
2) Solution: Yamato Security OSS Tools!
   - Hayabusa
   - Takajō

Problems with Windows Event Log Analysis

- Tough to read
- Tough to process
- Tough to filter quickly
- Tough to analyze quickly

Event logs are Evil

Solution: Yamato Security OSS Tools!

- **Easy** to read
- **Easy** to process
- **Easy** to filter quickly

HAYABUSA

- **Easy** to analyze quickly

鷹匠

Takajō

Event log analysis made **Easy**

About **Hayabusa** (隼)

- Motivation: Get the most use out of Sigma rules and make Windows event log analysis as quick and easy as possible.
- Language: Rust (fast and memory safe!)
- Started development in 2021
- Contributors: 14
- Releases / Major updates: 44!!!
- Major update released almost monthly for 2.5 years!
- Downloads: 97,000+
- Hayabusa detection rules: ~200
- Sigma detection rules: 4000+

About **Hayabusa** (隼)

~~Tough~~ **Easy** to **Filter Quickly**!

Results saved in **CSV** for **easy analysis** with **Timeline Explorer**!

```
> hayabusa  csv-timeline -d <evtx directory> -o result.csv
```

Timestamp	Computer	Channel	Event ID	Level	Record …	Rule Title	Details
2013-10-23 12:2…	IE8Win7	Sec	4624	info	124	Logon (Interactive) *Cr…	Type: 2 ¦ TgtUser: IEUser ¦
2013-10-23 12:2…	IE8Win7	Sec	4624	info	125	Logon (Interactive) *Cr…	Type: 2 ¦ TgtUser: IEUser ¦
2013-10-23 12:2…	IE8Win7	Sec	4648	info	123	Explicit Logon	TgtUser: IEUser ¦ SrcUser: W
2013-10-23 12:2…	IE8Win7	Sec	4672	info	126	Admin Logon	TgtUser: IEUser ¦ LID: 0x298
2013-10-23 12:2…	IE8Win7	Sys	20001	info	367	New Non-USB PnP Device	DeviceID: UMB\UMB\1&841921D8
2013-10-23 12:2…	IE8Win7	Sys	20001	info	369	New Non-USB PnP Device	DeviceID: SW\{EEAB7790-C514-
2013-10-23 12:2…	IE8Win7	Sec	4616	low	129	Unauthorized System Tim…	PrevTime: 2013-10-23T16:23:5
2013-10-23 12:2…	IE8Win7	Sys	20001	info	391	New Non-USB PnP Device	DeviceID: STORAGE\VOLUMESNAP

~~Tough~~ **Easy** to **Process**!

You can also output in **JSON(L)** for analysis **with JQ!**

```
> hayabusa  json-timeline -d <evtx directory> -o result.json -L
```


```
cat results.json | jq ' .Timestamp | .[:10] ' -r | sort | uniq -c
```

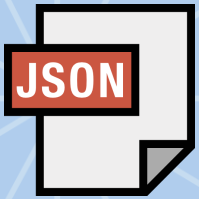
```
1066 2021-12-12
1093 2016-09-02
1571 2021-04-22
1750 2016-09-03
2271 2016-08-19
```

This will give us the dates with the most events!

Hayabusa 2.16.0 is released today!!

- **Loads of new features and enhancements!**
- **15%~10x faster with Channel filtering!**
- **Splunk REST API exported log support!**
- **Initial support for Sigma Correlations!**
- **Easier to read/process output**

For an easier DFIR life with Takajo!



Hayabusa's JSONL results

鷹匠 Takajō

./takajo --help

```
fukusuke@fukusukenoAir hayabusa-2.15.0-mac-arm % ./takajo -h
Version: 2.5.0 BSides Tokyo Release
Usage: takajo.exe <COMMAND>

Commands:
  help                          print comprehensive or per-cmd help
  automagic                     automatically executes as many commands as possible and output results to a new folder
  extract-scriptblocks          extract and reassemble PowerShell EID 4104 script block logs
  list-domains                  create a list of unique domains to be used with vt-domain-lookup
  list-hashes                   create a list of process hashes to be used with vt-hash-lookup
  list-ip-addresses             create a list of unique target and/or source IP addresses to be used with vt-ip-lookup
  list-undetected-evtx          create a list of undetected evtx files
  list-unused-rules             create a list of unused sigma rules
  split-csv-timeline            split up a large CSV file into smaller ones based on the computer name
  split-json-timeline           split up a large JSONL timeline into smaller ones based on the computer name
  stack-cmdlines                stack executed command lines
  stack-computers               stack computers
  stack-dns                     stack DNS queries and responses
  stack-ip-addresses            stack the target IP addresses (TgtIP field) or source IP addresses (SrcIP field)
  stack-logons                  stack logons by target user, target computer, source IP address and source computer
  stack-processes               stack executed processes
  stack-services                stack service names and paths from System 7040 and Security 4697 events
  stack-tasks                   stack new scheduled tasks from Security 4698 events and parse out XML task content
  stack-users                   stack target users (TgtUser field) or source users (SrcUser field)
  sysmon-process-tree           output the process tree of a certain process
  timeline-logon                create a CSV timeline of logon events
  timeline-partition-diagnostic create a CSV timeline of partition diagnostic events
  timeline-suspicious-processes create a CSV timeline of suspicious processes
  timeline-tasks                create a CSV timeline of scheduled tasks
  ttp-summary                   summarize tactics and techniques found in each computer
  ttp-visualize                 extract TTPs and create a JSON file to visualize in MITRE ATT&CK Navigator
  ttp-visualize-sigma           extract TTPs from Sigma and create a JSON file to visualize in MITRE ATT&CK Navigator
  vt-domain-lookup              look up a list of domains on VirusTotal
```

Easy to process **Quickly**!

Just one easy command to automate everything!

```
> takajo automagic –d <Hayabusa JSONL result file directory> -o case
```

All processed by Takajo's automagic!

```
PS C:\tmp\takajo-2.4.0-win> .\takajo automagic -t .\timeline.jsonl -q
Started the automagic command

Automatically executes as many commands as possible and output results to a new folder.

File: .\timeline.jsonl (45.27 MB)
Counting total lines. Please wait.
Total lines: 34,940

Scanning the Hayabusa timeline. Please wait.

100%|████████████████████| 34940/34940 [ 3.0s< 0.0s,  61.55k/sec]
```

Command	Results	Saved Files
extract-scriptblocks	PowerShell logs: 108	case-1/scriptblock-logs/Summary.csv (19.92 case-1/scriptblock-logs/*.txt
list-domains	Domains: 0	case-1/ListDomains.txt (0 Bytes)
list-domains(detailed)	Domains: 2	case-1/ListDomainsDetailed.txt (16 Bytes)
list-hashes	MD5: 1,038 SHA1: 976 SHA256: 978 Import: 1,038	case-1/ListHashes-MD5.txt (4.88 KB) case-1/ListHashes-SHA1.txt (5.66 KB) case-1/ListHashes-SHA256.txt (9.02 KB) case-1/ListHashes-ImportHashes.txt (4.28 KB
list-ip-addresses	IP adddresses: 0	case-1/ListIP-Addresses.txt (0 Bytes)
stack-cmdlines	Unique cmdlines: 1,411	case-1/StackCmdlines.csv (814.13 KB)
stack-computers	Unique computers: 54	case-1/StackTargetComputers.csv (49.51 KB)
stack-computers	Unique computers: 3,571	case-1/StackSourceComputers.csv (383.32 KB)

Logon Timeline!

Timestamp	Cha	Event	Event	LogoffTime	ElapsedTime	FailureReason	TargetComputer	TargetUser	AdminLog	SourceC
2016-08-18 23:47:04.676 +09:00	Sec	4624	Successful Logon				IE10Win7	IEUser	Yes	127.0.0.1
2016-08-18 23:47:04.676 +09:00	Sec	4624	Successful Logon	2016-08-18 23:47:20.053 +09:00	0d 0h 0m 15s 377ms		IE10Win7	IEUser		127.0.0.1
2016-08-18 23:47:36.671 +09:00	Sec	4624	Successful Logon				IE10Win7	SYSTEM		-
2016-08-18 23:47:36.671 +09:00	Sec	4624	Successful Logon				IE10Win7	SYSTEM		-
2016-08-18 23:47:38.430 +09:00	Sec	4624	Successful Logon				IE10Win7	IEUser	Yes	127.0.0.1
2016-08-18 23:47:38.430 +09:00	Sec	4624	Successful Logon	2016-08-18 23:48:31.289 +09:00	0d 0h 0m 52s 859ms		IE10Win7	IEUser		127.0.0.1
2016-08-18 23:47:38.430 +09:00	Sec	4624	Successful Logon				IE10Win7	IEUser	Yes	127.0.0.1
2016-08-18 23:47:38.430 +09:00	Sec	4624	Successful Logon	2016-08-18 23:48:31.289 +09:00	0d 0h 0m 52s 859ms		IE10Win7	IEUser		127.0.0.1
2016-08-18 23:49:38.281 +09:00	Sec	4624	Successful Logon				IE10Win7	SYSTEM		-
2016-08-18 23:49:38.281 +09:00	Sec	4624	Successful Logon				IE10Win7	SYSTEM		-
2016-08-18 23:49:40.000 +09:00	Sec	4624	Successful Logon				IE10Win7	IEUser	Yes	127.0.0.1
2016-08-18 23:49:40.000 +09:00	Sec	4624	Successful Logon	2016-08-19 00:28:28.043 +09:00	0d 0h 38m 48s 43ms		IE10Win7	IEUser		127.0.0.1
2016-08-18 23:49:40.000 +09:00	Sec	4624	Successful Logon				IE10Win7	IEUser	Yes	127.0.0.1
2016-08-18 23:49:40.000 +09:00	Sec	4624	Successful Logon	2016-08-19 00:28:28.043 +09:00	0d 0h 38m 48s 43ms		IE10Win7	IEUser		127.0.0.1
2016-08-19 00:29:27.609 +09:00	Sec	4624	Successful Logon				IE10Win7	SYSTEM		-
2016-08-19 00:29:27.609 +09:00	Sec	4624	Successful Logon				IE10Win7	SYSTEM		-
2016-08-19 00:29:29.859 +09:00	Sec	4624	Successful Logon				IE10Win7	IEUser	Yes	127.0.0.1
2016-08-19 00:29:29.859 +09:00	Sec	4624	Successful Logon				IE10Win7	IEUser		127.0.0.1
2016-08-19 00:29:29.859 +09:00	Sec	4624	Successful Logon				IE10Win7	IEUser	Yes	127.0.0.1
2016-08-19 00:29:29.859 +09:00	Sec	4624	Successful Logon				IE10Win7	IEUser		127.0.0.1
2016-08-19 03:46:19.937 +09:00	Sec	4624	Successful Logon				IE10Win7	SYSTEM		-
2016-08-19 03:46:19.937 +09:00	Sec	4624	Successful Logon				IE10Win7	SYSTEM		-
2016-09-20 01:50:06.477 +09:00	Sec	4625	Failed Logon			Unknown - UNKNOWN USER	DESKTOP-M5SN04R	JcDfcZTc		6hgtmVlr
2016-09-20 01:50:06.477 +09:00	Sec	4625	Failed Logon			Unknown - UNKNOWN USER	DESKTOP-M5SN04R	JcDfcZTc		6hgtmVlr

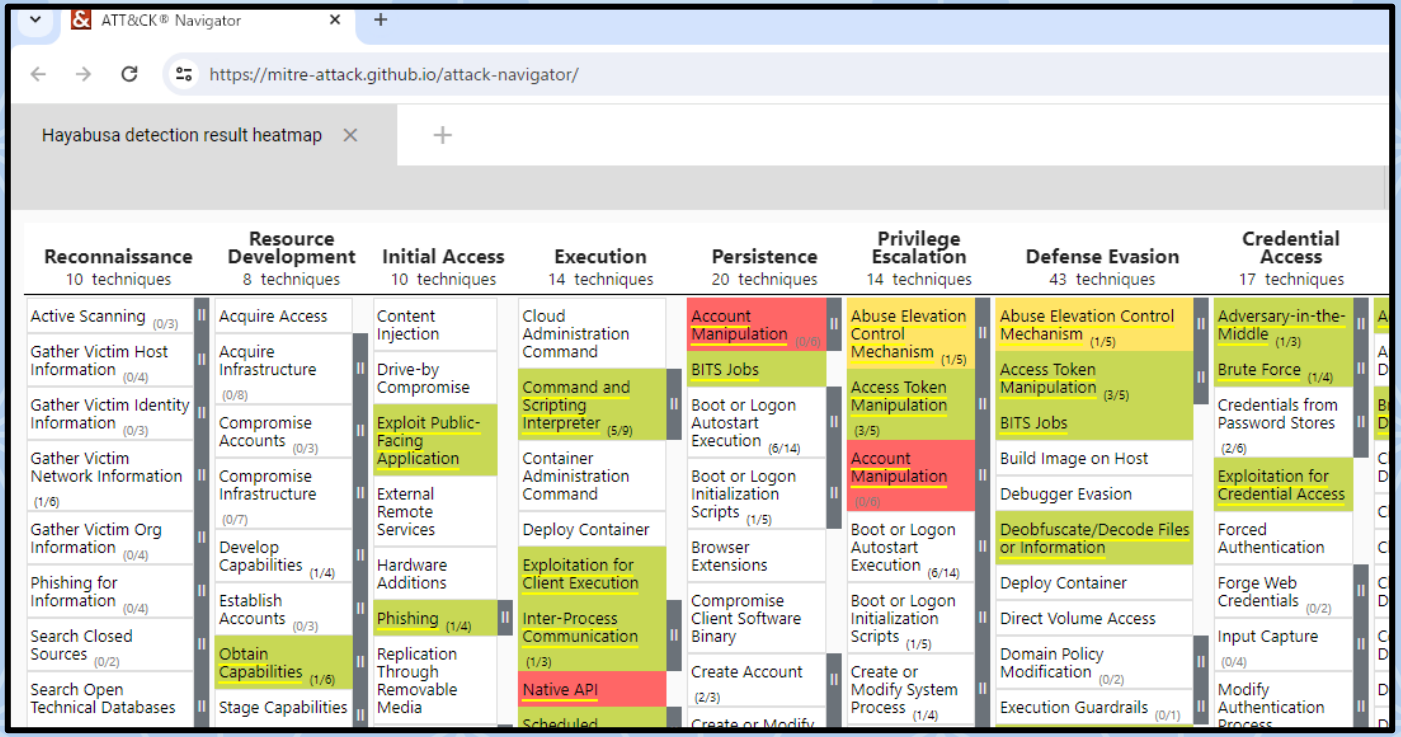
PowerShell Execution Timeline!

Creation Time	Computer Name	Script ID	Script Name	Records	Level	Alerts
2019-09-09 22:35:08.655 +09:00	MSEDGEWIN10	37f6d110-cfdf-4118-8748-17638e258531	no-path	1/1	med	"Suspicious FromBase64String Usage On Archive - Ps Script", "Potentially Malicious PwSh"
2019-09-09 22:35:09.315 +09:00	MSEDGEWIN10	c7ca7056-b317-4fff-b796-05d8ef896dcd	no-path	1/1	high	"Suspicious PowerShell Get Current Us "PowerShell Credential Prompt", "Manipulation of User Computer or Gro Security Principals Across AD", "Potentially Malicious PwSh"
2020-06-30 23:24:08.254 +09:00	MSEDGEWIN10	27f08bda-c330-419f-b83b-eb5c0f699930	C:\Users\Public\lsass_wer_ps.ps1	1/1	high	"PowerShell Get-Process LSASS in ScriptBlock", "Malicious PowerShell Keywords", "Suspicious Process Discov With Get-Process", "WinAPI Function C Via PowerShell Scripts", "Use Remove- to Delete File", "Potentially Malicio PwSh"
2020-08-26 14:09:28.845 +09:00	DESKTOP-RIPCLIP	fdd51159-9602-40cb-839d-c31039ebbc3a	no-path	1/1	high	"Usage Of Web Request Commands And Cm - ScriptBlock", "Powershell Token Obfuscation - Powershell"

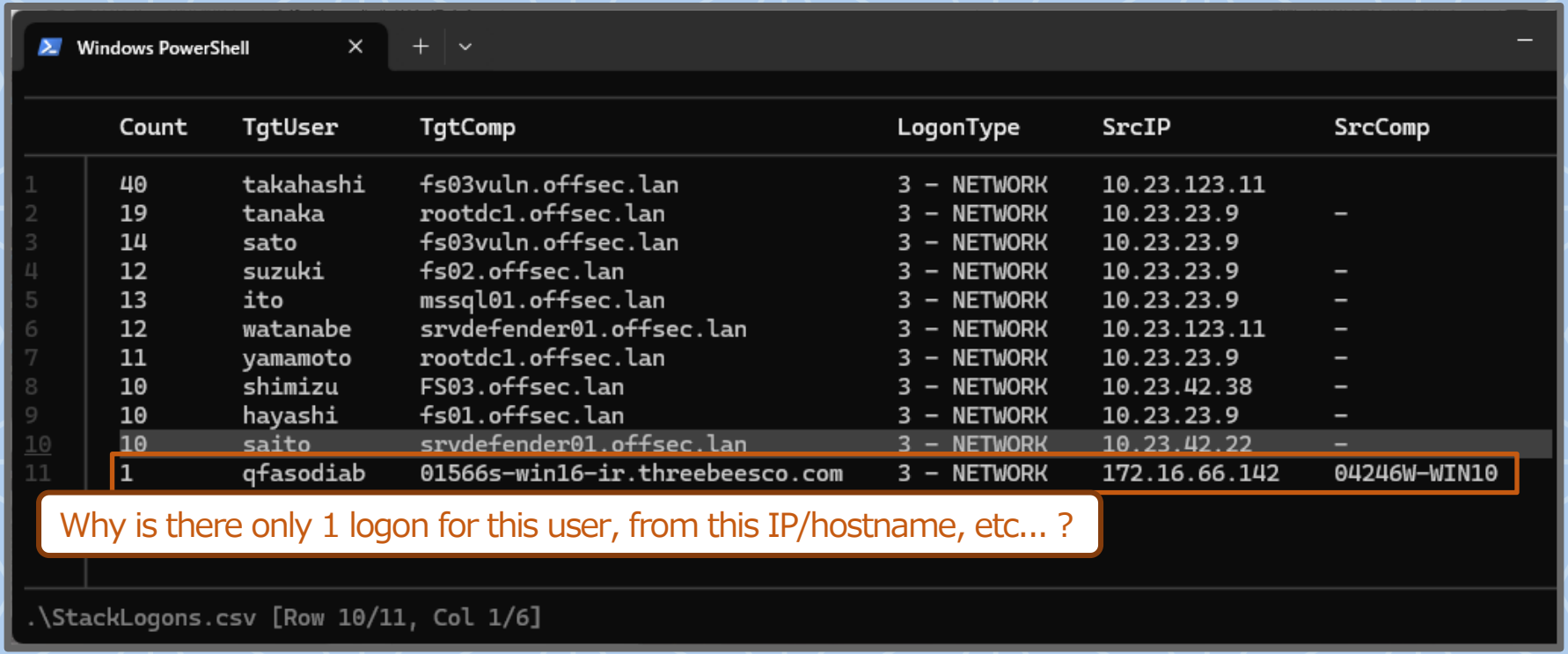
Suspicious Process Timeline!

Timestamp	Computer	Type	Level	Rule	Cmdline
2019-05-20 02:32:00.482 +09:00	DC1.inse…	Sysmon 1	high	Proc Exec (Sysmon Alert)	attrib +h nbtscan.exe
2019-05-22 00:32:57.286 +09:00	IEWIN7	Sysmon 1	high	Rundll32 Execution Without DLL File	rundll32.exe javascript:"\..\mshtml,RunHTMLApp
2019-05-22 00:32:57.286 +09:00	IEWIN7	Sysmon 1	high	Rundll32 Execution Without DLL File	rundll32.exe javascript:"\..\mshtml,RunHTMLApp
2019-05-22 00:32:57.286 +09:00	IEWIN7	Sysmon 1	high	Mshtml DLL RunHTMLApplication Abuse	cmd.exe /C rundll32.exe javascript:"\..\mshtml
2019-05-22 00:32:57.286 +09:00	IEWIN7	Sysmon 1	high	Mshtml DLL RunHTMLApplication Abuse	rundll32.exe javascript:"\..\mshtml,RunHTMLApp
2019-05-22 00:32:57.286 +09:00	IEWIN7	Sysmon 1	high	Mshtml DLL RunHTMLApplication Abuse	cmd.exe /C rundll32.exe javascript:"\..\mshtml
2019-05-22 00:32:57.286 +09:00	IEWIN7	Sysmon 1	high	Mshtml DLL RunHTMLApplication Abuse	rundll32.exe javascript:"\..\mshtml,RunHTMLApp
2019-05-22 00:32:57.867 +09:00	IEWIN7	Sysmon 1	high	Remotely Hosted HTA File Executed Via Mshta…	"C:\Windows\System32\mshta.exe" https://hotele
2019-05-22 00:32:57.867 +09:00	IEWIN7	Sysmon 1	high	Remotely Hosted HTA File Executed Via Mshta…	"C:\Windows\System32\mshta.exe" https://hotele
2019-05-22 00:32:57.867 +09:00	IEWIN7	Sysmon 1	high	Windows Shell/Scripting Processes Spawning …	"C:\Windows\System32\mshta.exe" https://hotele
2019-05-22 00:32:57.867 +09:00	IEWIN7	Sysmon 1	high	Windows Shell/Scripting Processes Spawning …	"C:\Windows\System32\mshta.exe" https://hotele
2019-05-22 00:32:59.769 +09:00	IEWIN7	Sysmon 1	high	Suspicious Command Patterns In Scheduled Ta…	"C:\Windows\System32\schtasks.exe" /Create /sc
2019-05-22 00:32:59.769 +09:00	IEWIN7	Sysmon 1	high	Suspicious Command Patterns In Scheduled Ta…	"C:\Windows\System32\schtasks.exe" /Create /sc

MITRE ATT&CK Heatmap Visualizations



Various stack analysis to identify outliers and abnormalities.



Features of Takajo's automagic!

Automagic will output many useful results:

- Listing up domains, IP addresses, hashes
- VirusTotal lookups
- Stacking tasks, users, services, etc…
- Logon timeline
- Suspicious process timeline
- Scheduled tasks timeline
- PowerShell timeline
- PowerShell script extraction and reassembly
- MITRE ATT&CK TTP visualizations
- and more!

Thank you for listening!

大和セキュリティ

HAYABUSA

鷹匠
Takajō

@SecurityYamato