



Hashtag:

#yamasec

#bsidestokyo



# Learn Scalable DFIR with Velociraptor and Hayabusa by Yamato Security

高橋福助

Takahashi Fukusuke (@fukusuket)

古市昌弘

Furuichi Masahiro (D/@hitenkoku)



# Self-introduction

高橋福助    Takahashi Fukusuke (@fukusuket)

NTT Data Group's CSIRT Team (NTT DATA-CERT)  
Yamato Security member

古市昌弘    Furuichi Masahiro (D/@hitenkoku)

Subsidiary of the NTT Group  
Yamato Security member

# About Yamato Security

- A 'Yamato Spirit' security study group that has regularly met since 2012.
- Develops two open-source security programs:



## Project Leader

Zach Mathis (@yamatosecurity)

## Developers

Akira Nishikawa (@nishikawaakira)

DustInDark / hitenkoku

James Takai / hachiyone(@hach1yon)

ItiB (@itiB\_S144)

Kazuminn (@k47\_um1n)

Garigariganzy (@garigariganzy31)

Fukusuke Takahashi / fukuseket

Yusuke Matsui (@apt773)(AD Hacking Group Leader)



## Project Leader

Zach Mathis (@yamatosecurity)

## Developer

DustInDark / hitenkoku

Fukusuke Takahashi / fukusuket

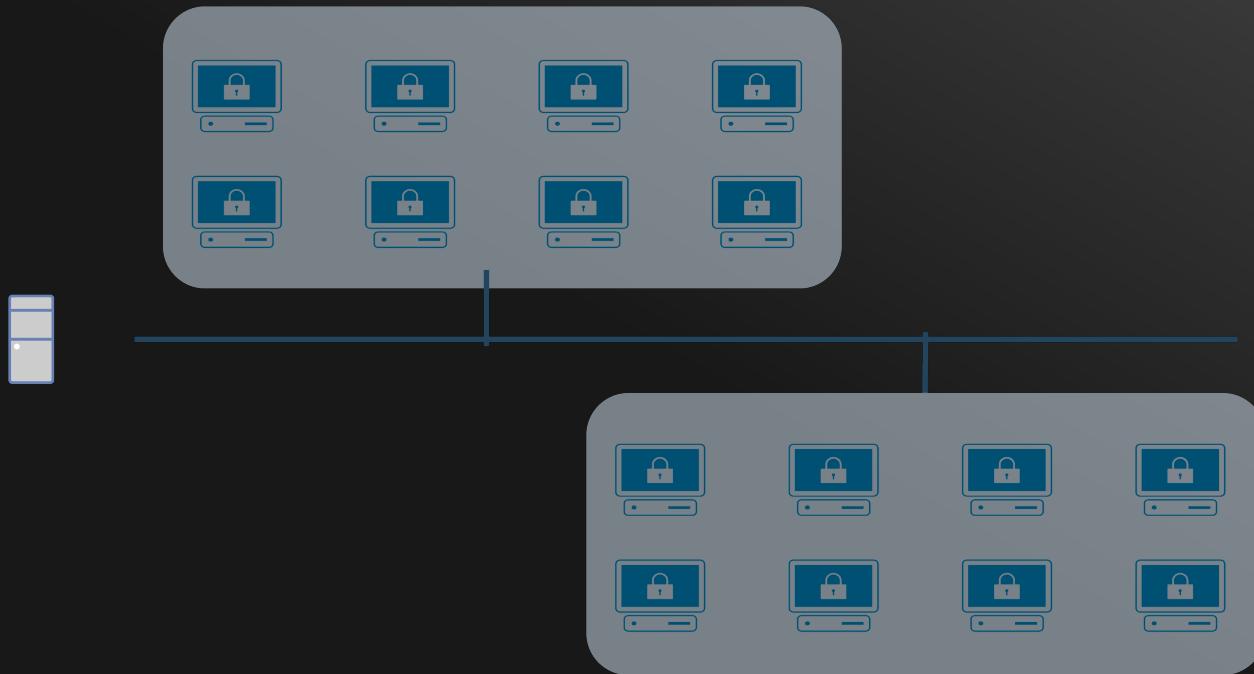


Follow:  
[@SecurityYamato](https://twitter.com/SecurityYamato)

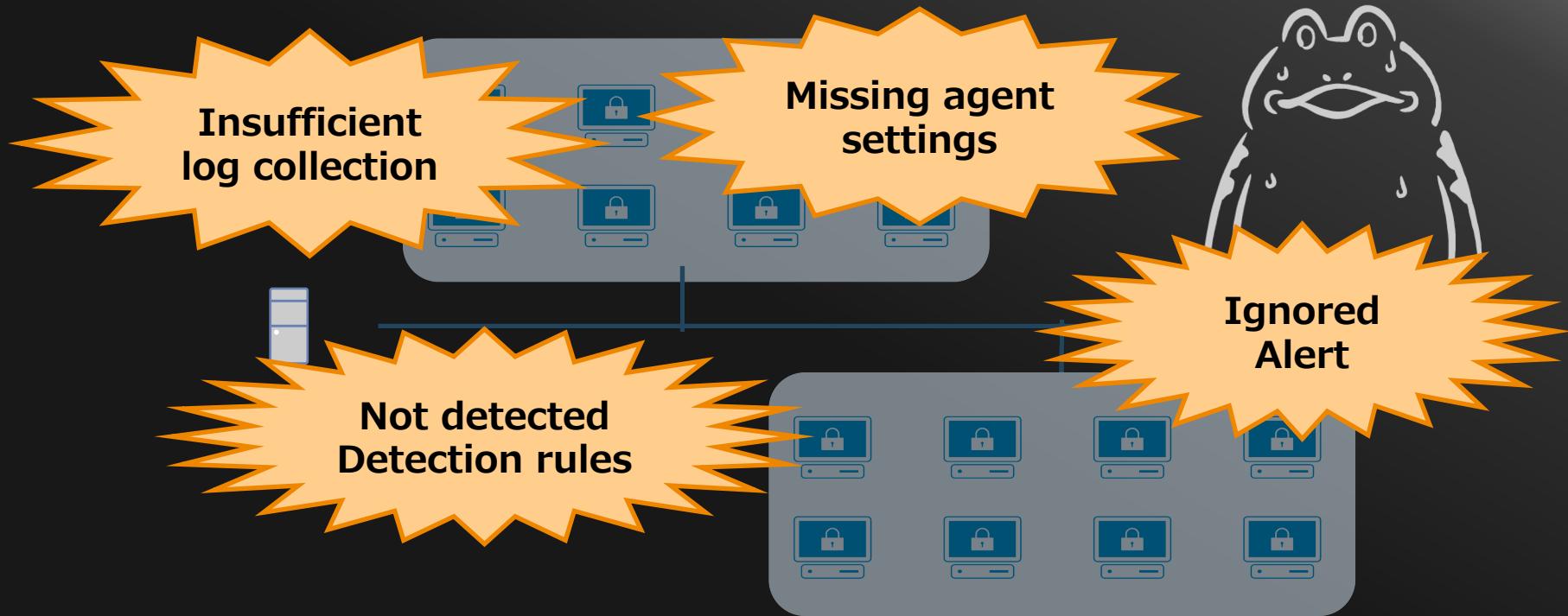
# Agenda

- DFIR in environments where EDR and SIEM operations are insufficient
- About Velociraptor
- About Hayabusa
- Community Knowledge
- Scalable DFIR built with Velociraptor & Hayabusa & Takajo

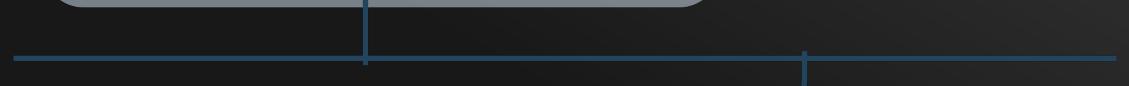
# An environment where EDR and SIEM operations are insufficient?



# An environment where EDR and SIEM operations are insufficient?



# Scalable DFIR with Velociraptor, Hayabusa and Takajo!

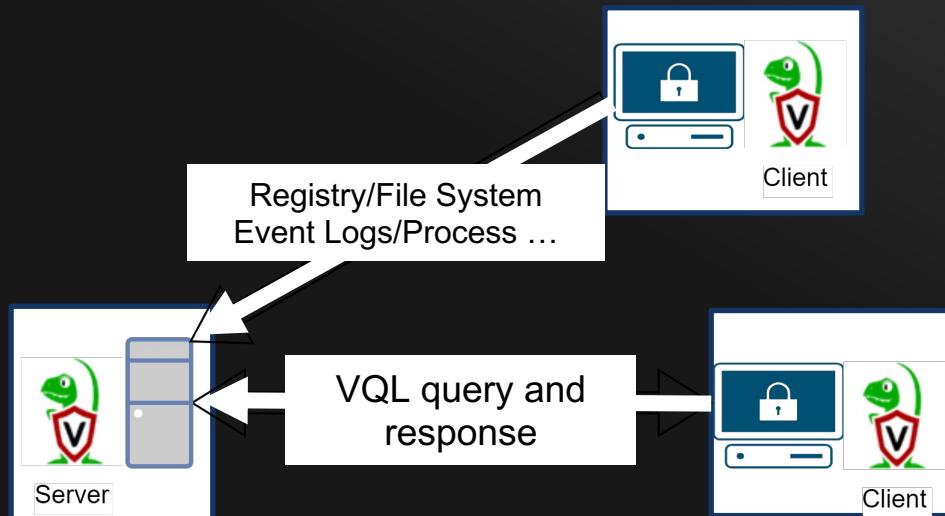


- Go back in time and recreate SIEM!
- Fast forensics on many machines!

# About Velociraptor

<https://docs.velociraptor.app>

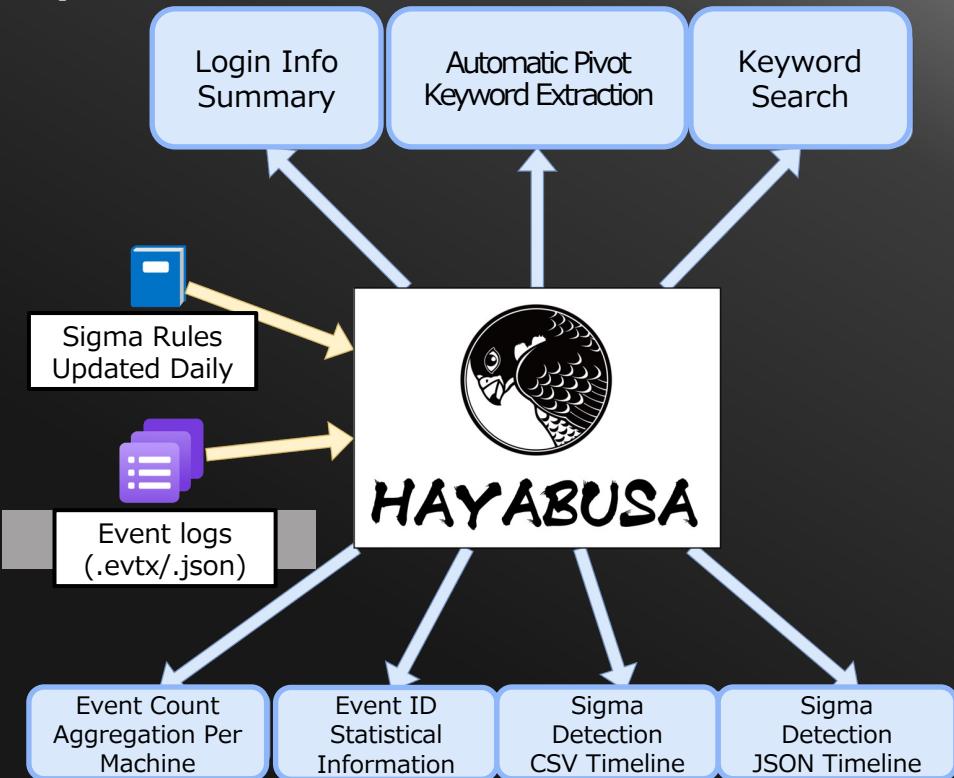
- An OSS EDR-like DFIR tool developed by Mike Cohen.
- Strength in collecting forensic artifacts.
- Can execute queries (VQL) from server-to-client and aggregate data to a server.
- Leverage knowledge by importing queries (VQL) shared by the community.



# About Hayabusa

<https://github.com/Yamato-Security/hayabusa>

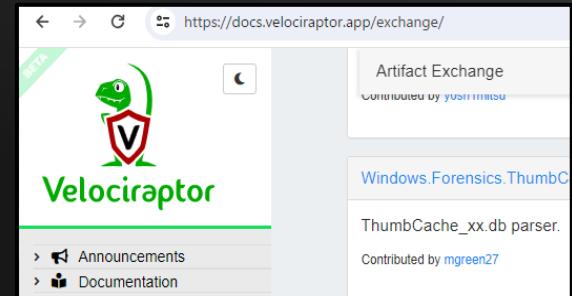
- An application that quickly analyzes large amounts of Windows event logs.
- Has various commands specialized for Windows event log analysis
- Synchronize with Sigma repository with one command. Over 4000 Sigma rules built-in





# Hayabusa - Sigma - Velociraptor Community knowledge

- **Hayabusa and Sigma**
  - You can apply the latest rules from the Sigma repository with 'update-rules'.
  - The Sigma repository updates rules daily and contains the latest knowledge.
- **Velociraptor**
  - **Velociraptor Artifact Exchange**
    - ~ Mechanism for sharing queries (VQL) created by the community~
  - **Import Server.Import.ArtifactExchange**
    - easily use community collection queries (VQL)



# Hayabusa - Sigma - Velociraptor Community knowledge



```
Windows PowerShell x + 
PS C:\tmp\hayabusa-2.13.0-win-x64> .\hayabusa-2.13.0-win-x64.exe update-rules

HAYABUSA
by Yamato Security

Start time: 2024/03/28 10:31

- File Was Not Allowed To Run (Modified: 2021/11/27 | Path: rules\sigma\builtin\applocker\win...
- Pingback Backdoor File Indicators (Modified: 2023/02/17 | Path: rules\sigma\sysmon\emerg...
- Potential PlugX Activity (Modified: 2023/02/03 | Path: rules\sigma\builtin\emerging-threats...
- New Root Certificate Installed Via CertMgr.EXE (Modified: 2023/03/05 | Path: rules\sigma\bu...
- Potential DLL Sideloaded Via ClassicExplorer32.dll (Modified: 2022/12/13 | Path: rules\sig...
- Suspicious PowerShell Invocation From Script Engines (Modified: 2023/01/05 | Path: rules\sig...
- Enumeration via the Global Catalog (Modified: 2023/02/24 | Path: rules\sigma\builtin\unsupp...
- Potential Product Class Reconnaissance Via Wmic.EXE (Modified: 2023/03/07 | Path: rules\sig...
- Suspicious Process Discovery With Get-Process (Modified: 2022/03/17 | Path: rules\sigma\bu...
- Potentially Suspicious GoogleUpdate Child Process (Modified: 2023/05/22 | Path: rules\sigma\...
- Sensitive File Access Via Volume Shadow Copy Backup (Modified: 2024/01/18 | Path: rules\sig...
- Dynamic .NET Compilation Via Csc.EXE - Hunting (Modified: 2023/08/02 | Path: rules\sigma\sv...

Updated Sigma rules: 4201
Updated Hayabusa rules: 4
Rules updated successfully.

PS C:\tmp\hayabusa-2.13.0-win-x64>
```

Just one command!

A screenshot of a Microsoft Edge browser window displaying the GitHub repository for Sigma. The URL is https://github.com/SigmaHQ/sigma. The page shows the README file, which contains the title "Sigma - Generic Signature Format for SIEM Systems" and the Sigma logo. Below the README, there is a green "Sigma Rule Tests" button with "passing", a "Sigma Official" button, a "Stars" button with "7.5k", a "downloads" button with "57k", and an "Open Source Security Index" badge.



# Scalable DFIR environment with Velociraptor + Hayabusa + Takajo

# A scalable DFIR environment?



## Scalable DFIR environment

Environment

Easy to setup/distribute/collect!

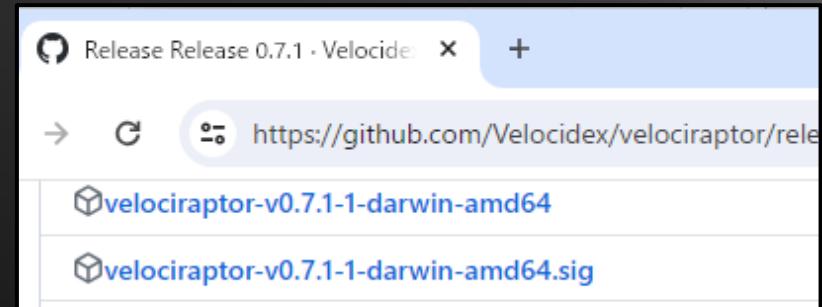
Knowledge

Bulk analysis by Takajo!

# Velociraptor environment setup

Set up in 3 easy steps:

1. Server module startup
  - velociraptor gui
2. Create MSI package for distribution
  - Run Server.Utils.CreateMSI artifact
3. Distribute to client terminal
  - Distribute the MSI package created in <Step 2> using AD Group Policy, Intune, EDR, etc.



… And the setup is now complete!

# Velociraptor environment setup



Screenshot of the Velociraptor Response and More application interface:

The top navigation bar shows the title "Velociraptor Response and More" and the URL "https://127.0.0.1:8889/app/index.html#/dashboard". The user is logged in as "admin".

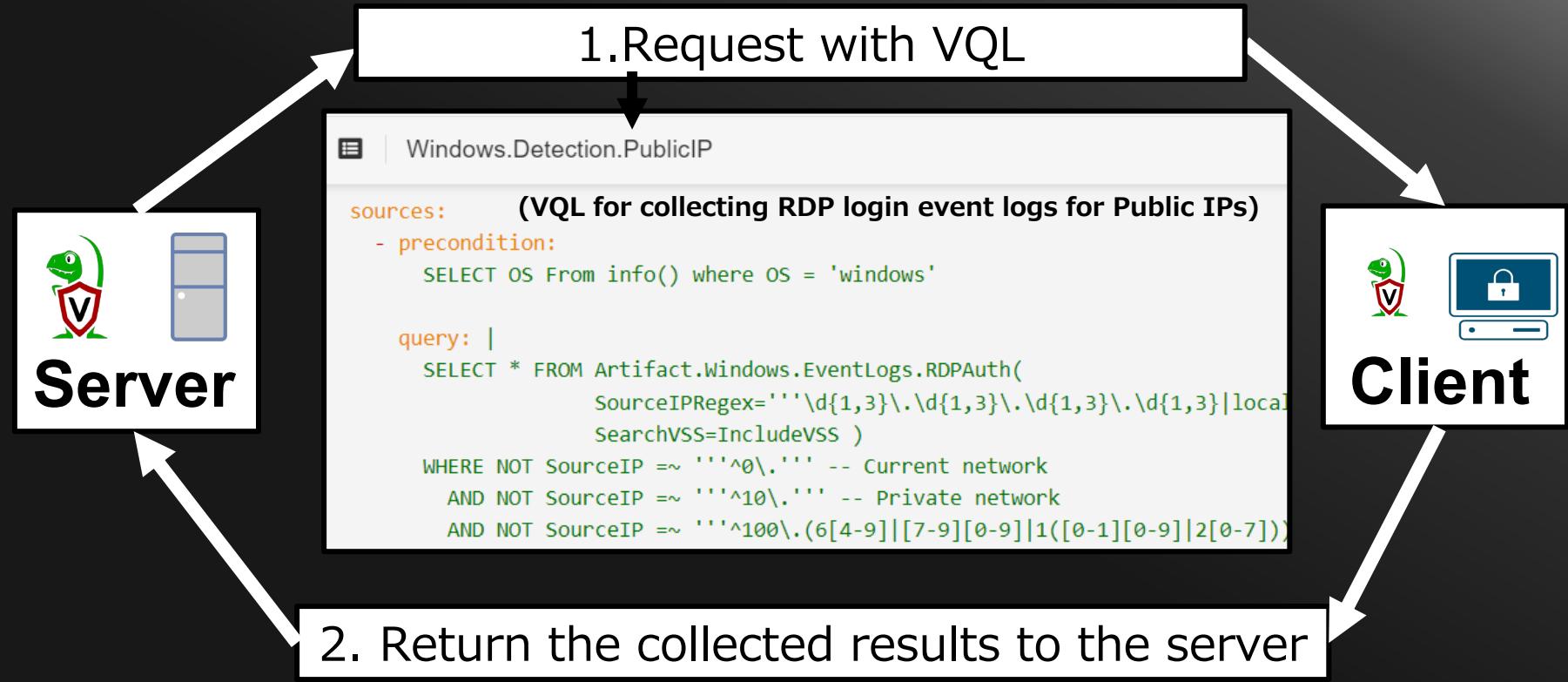
The main dashboard displays the following information:

- Search clients:** A search bar with placeholder "Search clients" and a dropdown menu showing "admin".
- Client Config:** A table showing client configurations:

Name	OrgId	ClientConfig
<root>	root	root
ACME Inc	0123	0123
- Disk Space:** A section showing disk usage for "C:" drive.
- Users:** A section showing user information.
- Client Overview:** A summary table:

Query: all		Total Matching Clients 1
	Client ID	Hostname
<input type="checkbox"/>	C.632a4ab99b91b03b	mouse

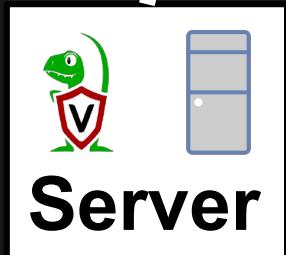
# Velociraptor Basics



# Distribution, execution, and collection of Hayabusa using VQL

1. Request Hayabusa distribution + execution with VQL

<https://docs.velociraptor.app/exchange/artifacts/pages/windows.eventlogs.hayabusa/>



```
Windows.EventLogs.Hayabusa
name: Windows.EventLogs.Hayabusa
description: |
    [Hayabusa](https://github.com/Yamato-Security/hayabusa) is a
    Windows event log fast forensics timeline generator and threat
    hunting tool.

tools:
- name: Hayabusa-2.13.0
url: https://github.com/Yamato-Security/hayabusa/releases/download/v2.13.0/hayabusa-2.13.0-win-x64.exe
expected_hash: c350ba83ffb02391115d2d5e1236a6a1cd79e9c49be8296f485819e7b20be8fa
version: 2.13.0

precondition: SELECT OS From info() where OS = 'Windows'
```

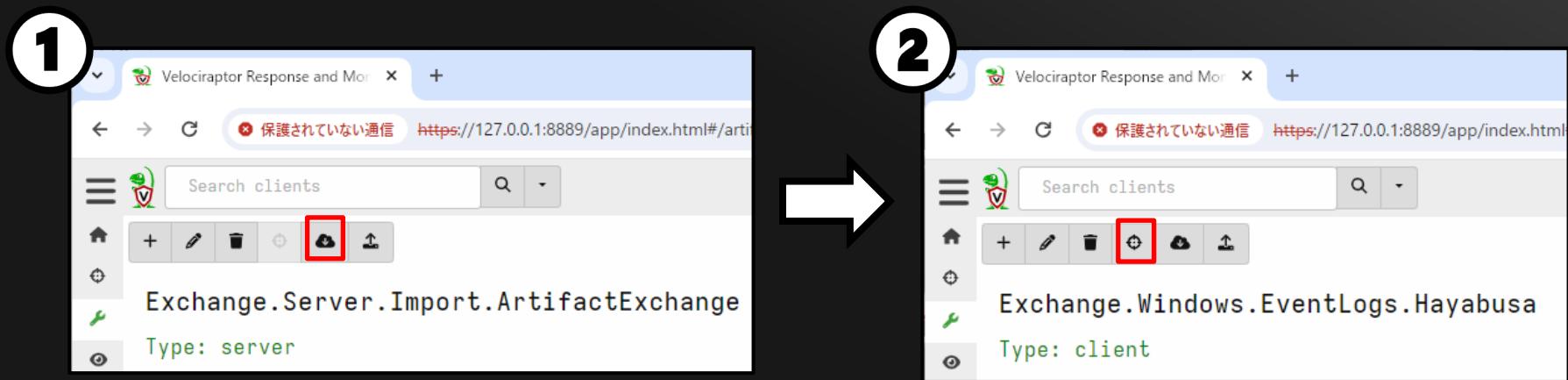


2. Return the collected results to the server

# Distribution, execution, and collection of Hayabusa using VQL

Can be started in 2 easy steps!

1. Run Server.Import.ArtifactExchange. Import community VQL
2. Run Exchange.Windows.EventLogs.Hayabusa !



# Collecting Windows event log timeline with Hayabusa



Screenshot of the BSIDES TOKYO interface showing the results of a Windows event log scan with Hayabusa.

The interface includes a toolbar with icons for home, add, delete, and search, and a sidebar with navigation links for Home, Artifacts, Requests, Results, Log, and Notebook.

A table displays the collected artifacts:

State	FlowId	Artifacts	Created	Last Active
✓	F.C024QK3P077AA	Exchange.Windows.EventLogs.Hayabusa	2024-03-27T16:46:08Z	2024-03-27T16:47:18Z

The "Results" tab is selected, showing the output of the scan:

Exchange.Windows.EventLogs.Hayabusa/Results

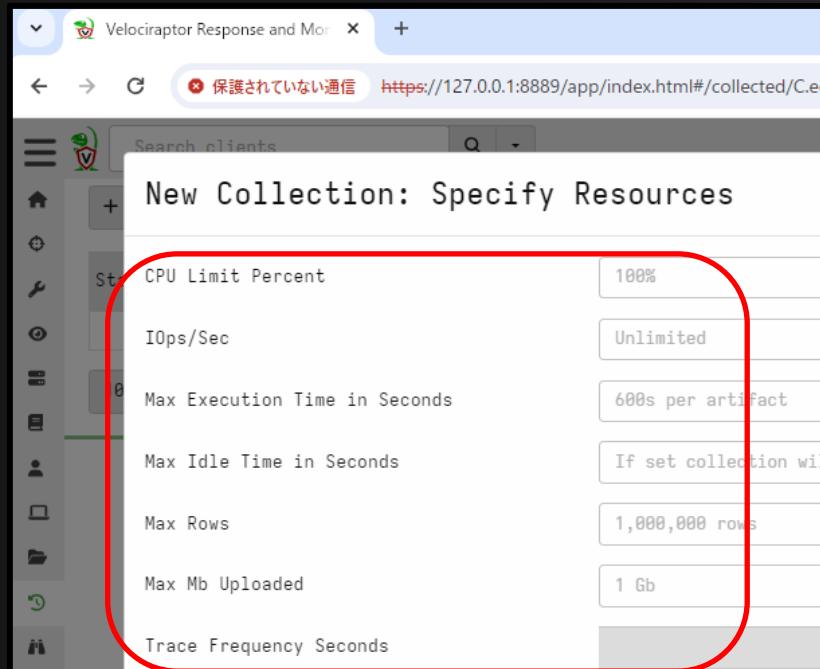
**Hayabusa's result  
(Windows event logs scanned with Sigma)**

The results table shows two events:

Timestamp	RuleTitle	Level	Computer	Channel	EventID	RecordID	Details
2023-10-13T04:06:52Z	Important Log File Cleared	high	DESKTOP-CNG7416	Sys	104	2645	Log: System   User: defaultuser0
2023-10-15T03:56:01Z	Windows Defender Real-time Protection Disabled	high	mouse	Defender	5001	99	Product Name: Microsoft Defender ウイルス対策   Product Version: 4.18.2201.11

A red box highlights the second event in the results table.

# Tip! Specify client resource limits with Velociraptor

A screenshot of a web browser window showing the Velociraptor interface. The title bar says "Velociraptor Response and More". The URL is https://127.0.0.1:8889/app/index.html#/collected/C.ed0. The main content area shows a form titled "New Collection: Specify Resources". A red box highlights the first six input fields: "CPU Limit Percent" (100%), "IOPS/Sec" (Unlimited), "Max Execution Time in Seconds" (600s per artifact), "Max Idle Time in Seconds" (If set collection will), "Max Rows" (1,000,000 rows), and "Max Mb Uploaded" (1 Gb).

CPU Limit Percent	100%
IOPS/Sec	Unlimited
Max Execution Time in Seconds	600s per artifact
Max Idle Time in Seconds	If set collection will
Max Rows	1,000,000 rows
Max Mb Uploaded	1 Gb

But it can only be used with the Velociraptor built-in module...

Resource limit specification does not work for Hayabusa, which is not built-in...

So, we are releasing new features today!

New Hayabusa features released!



--low-memory-mode!!

Special Thanks to: James Takai

Achieving advanced detection  
while reducing average client load!

# New Hayabusa features released!



## Analyzing Windows event logs in JSON format exported with Splunk!

Special Thanks to: DustInDark

Even in SIEM environments with insufficient detection rules,  
advanced Sigma scans are possible later!

The next step...

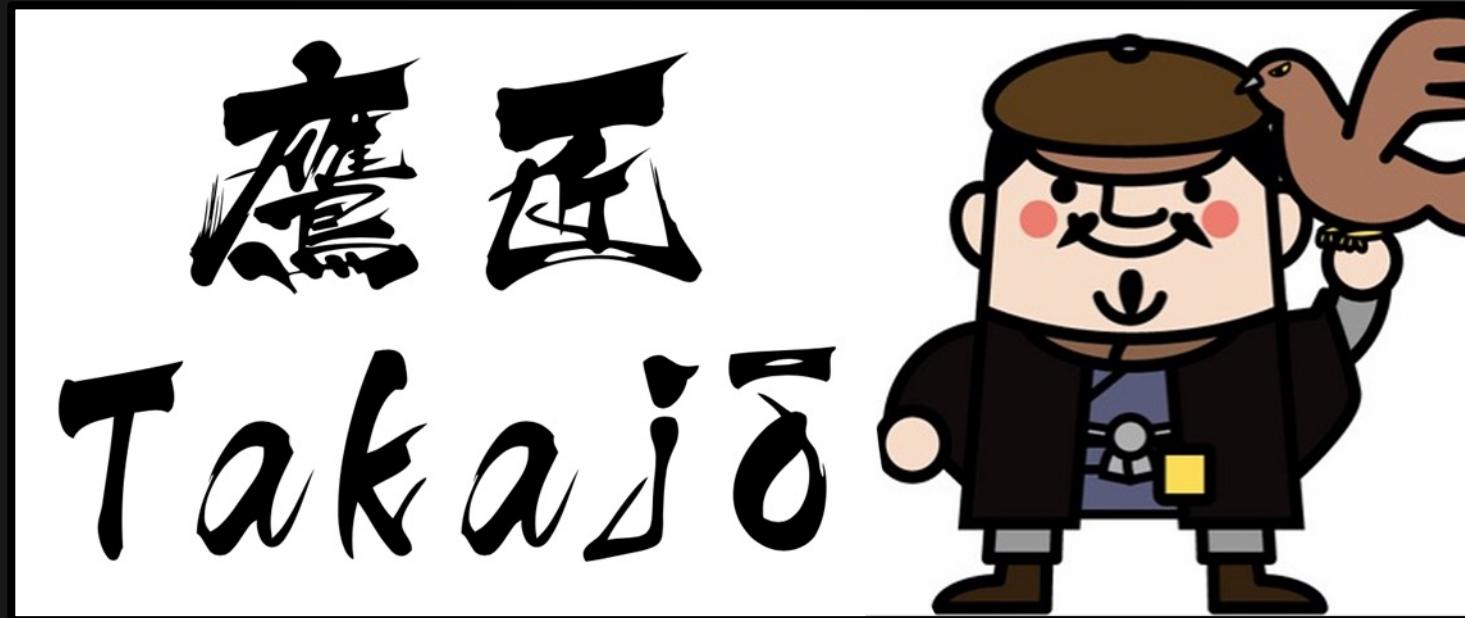
We collected event log analysis results from multiple clients at once using Velociraptor and Hayabusa!

The next step is to analyze this all at once 🤔



# Knowledge scalability

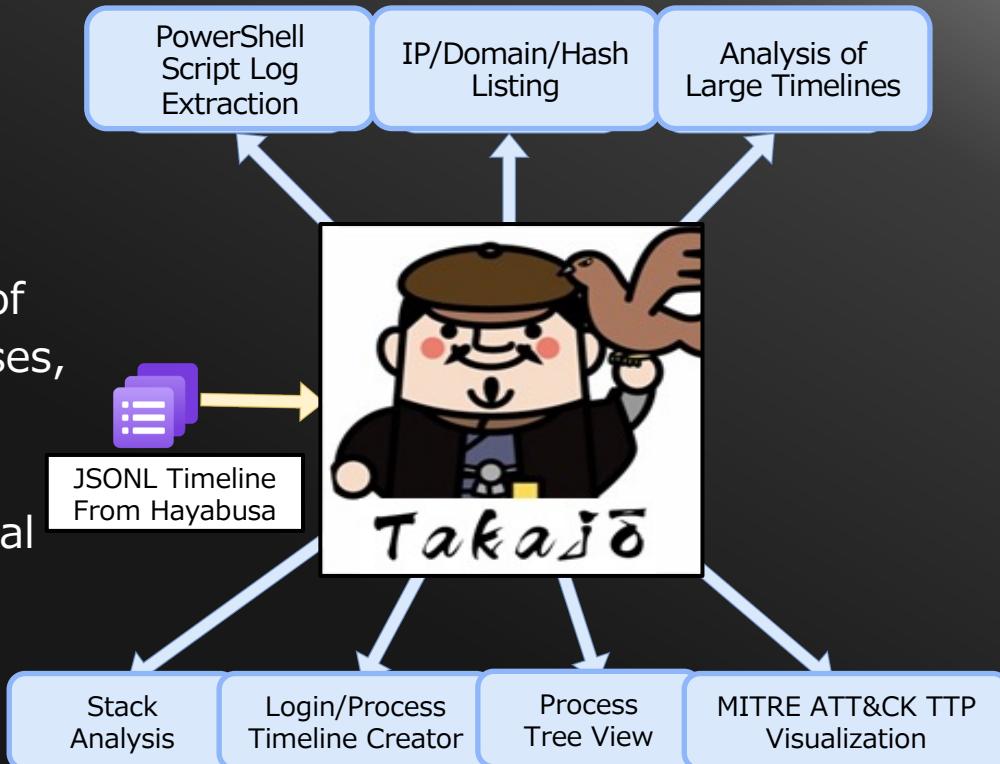
Yamato Security's analysis know-how with commands!



# About Takajo

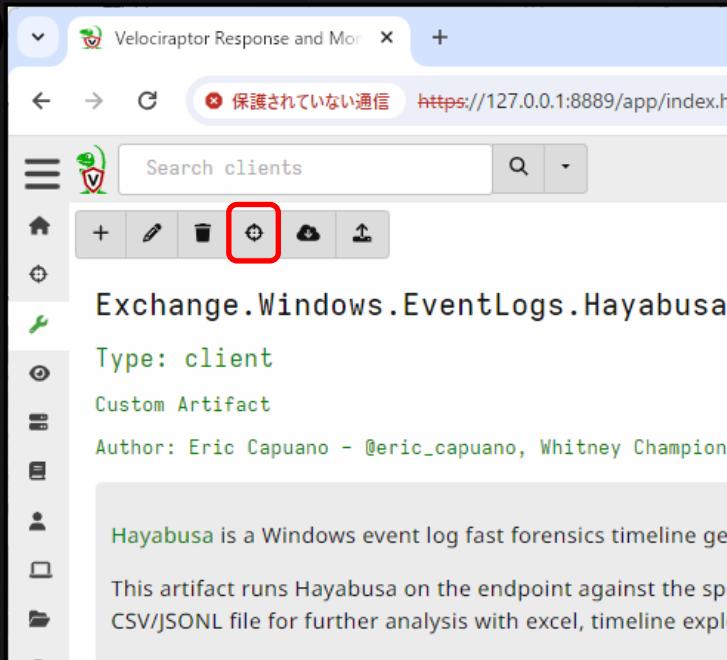
<https://github.com/Yamato-Security/takajo>

- Tool to analyze Hayabusa timeline (JSONL format)
- Aggregation and stacking analysis of command line, DNS, logon, processes, services, scheduled tasks, etc.
- IP/Domain/Hash lookup in VirusTotal
- MITER ATT&CK TTP visualization



# Collect Hayabusa timelines from multiple client at once

1

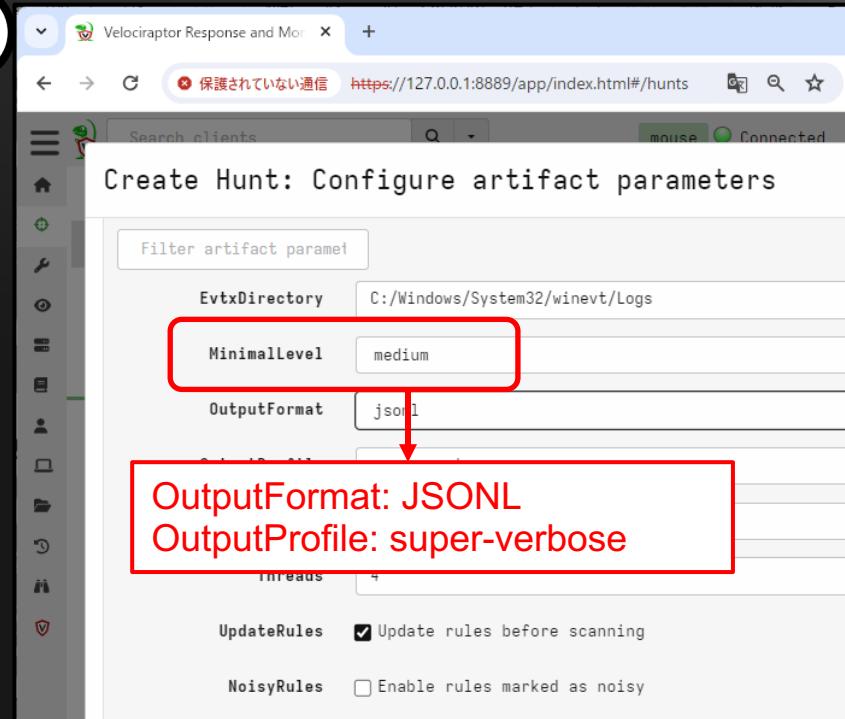


Screenshot of the Velociraptor Response and More interface. The top navigation bar shows a warning about an unencrypted connection and the URL <https://127.0.0.1:8889/app/index.html#/>. Below the bar is a search bar labeled "Search clients". On the left, there's a sidebar with various icons. In the center, there's a section titled "Exchange.Windows.EventLogs.Hayabusa" with the following details:

- Type: client
- Custom Artifact
- Author: Eric Capuano - @eric\_capuano, Whitney Champion

A note below states: "Hayabusa is a Windows event log fast forensics timeline generator. This artifact runs Hayabusa on the endpoint against the specified CSV/JSONL file for further analysis with excel, timeline explorer, etc." A red box highlights the "New Hunt" button (a plus sign icon) in the toolbar.

2

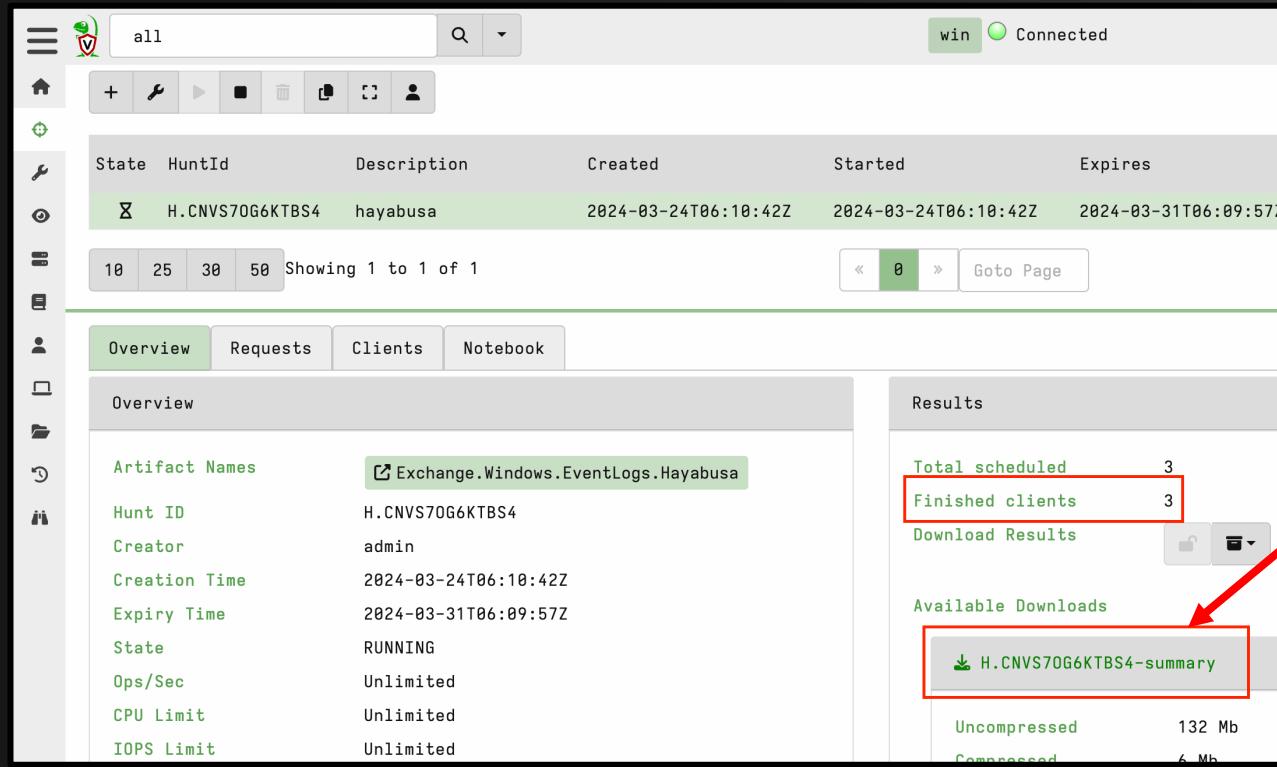


Screenshot of the "Create Hunt: Configure artifact parameters" dialog. The dialog has several input fields:

- EvtxDirectory: C:/Windows/System32/winevt/Logs
- MinimalLevel: medium (highlighted by a red box)
- OutputFormat: jsonl (highlighted by a red box)

Below these fields, a red box highlights the text "OutputFormat: JSONL" and "OutputProfile: super-verbose". At the bottom of the dialog, there are checkboxes for "UpdateRules" (checked) and "NoisyRules" (unchecked). A note at the bottom says "Threads: 4".

# Collect Hayabusa timelines from multiple client at once



The screenshot shows the Red Canary interface with a hunt titled "hayabusa" running. The hunt details include:

State	HuntId	Description	Created	Started	Expires
X	H.CNVS70G6KTBS4	hayabusa	2024-03-24T06:10:42Z	2024-03-24T06:10:42Z	2024-03-31T06:09:57Z

Below the hunt table, there are buttons for page size (10, 25, 30, 50) and a search bar showing "Showing 1 to 1 of 1".

The interface has tabs for Overview, Requests, Clients, and Notebook. The Overview tab is selected, displaying hunt metadata:

Artifact Names	Exchange.Windows.EventLogs.Hayabusa
Hunt ID	H.CNVS70G6KTBS4
Creator	admin
Creation Time	2024-03-24T06:10:42Z
Expiry Time	2024-03-31T06:09:57Z
State	RUNNING
Ops/Sec	Unlimited
CPU Limit	Unlimited
IOPS Limit	Unlimited

The Results section shows the status of scheduled clients:

Total scheduled	3
Finished clients	3

There is a "Download Results" button and a link to "H.CNVS70G6KTBS4-summary".

Hayabusa results for multiple clients can be downloaded in one file!



Takajo new feature released!

**'automagic' command !**

= Batch analysis of multiple files !

Takajo's various analysis commands and  
Analyze multiple files in one go!



# All analyzed by Takajo automagic!

Batch analysis only requires the following two steps!

- 1. Download Hunt result JSON from Velociraptor GUI**
- 2. takajo.exe automagic -t <Step 1> .jsonl**

With the above,  
you can analyze Hayabusa timeline results from multiple clients at once!



# All analyzed by Takajo 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.

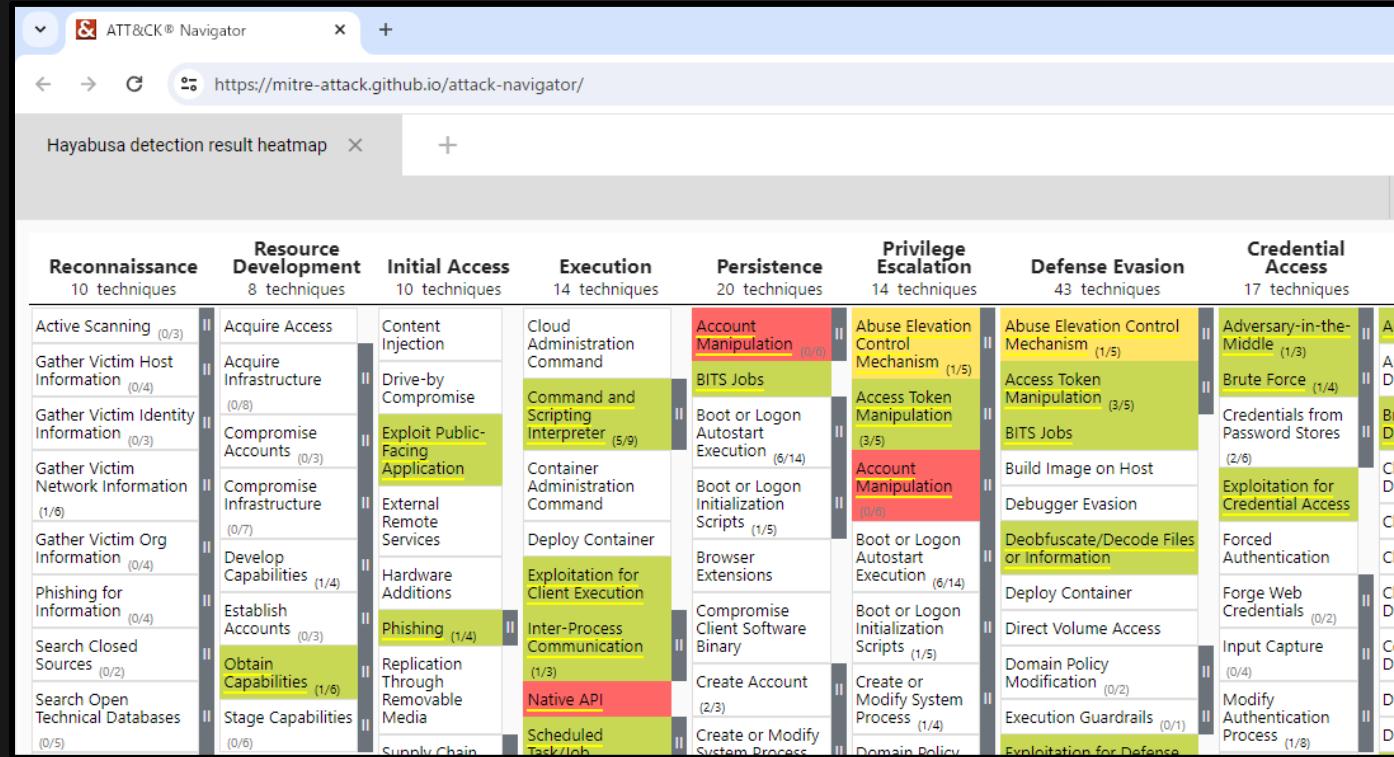
File: .\timeline.jsonl (45.27 MB)
Counting total lines. Please wait.
Total lines: 34,940

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 KB) 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 addresses: 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)

# Visualization of MITRE ATT&CK TTPs with automagic results





# Stack analysis with automagic results

Windows PowerShell

Count	TgtUser	TgtComp	LogonType	SrcIP	SrcComp
1	40	takahashi	fs03vuln.offsec.lan	3 - NETWORK	10.23.123.11
2	19	tanaka	rootdc1.offsec.lan	3 - NETWORK	10.23.23.9
3	14	sato	fs03vuln.offsec.lan	3 - NETWORK	10.23.23.9
4	12	suzuki	fs02.offsec.lan	3 - NETWORK	10.23.23.9
5	13	ito	mssql01.offsec.lan	3 - NETWORK	10.23.23.9
6	12	watanabe	srvdefender01.offsec.lan	3 - NETWORK	10.23.123.11
7	11	yamamoto	rootdc1.offsec.lan	3 - NETWORK	10.23.23.9
8	10	shimizu	FS03.offsec.lan	3 - NETWORK	10.23.42.38
9	10	hayashi	fs01.offsec.lan	3 - NETWORK	10.23.23.9
10	10	saito	srvdefender01.offsec.lan	3 - NETWORK	10.23.42.22
11	1	qfasodiab	01566s-win16-ir.threebeesco.com	3 - NETWORK	172.16.66.142
					04246W-WIN10

You can also analyze outliers that have different naming conventions than other users, suspicious...

.\\StackLogons.csv [Row 10/11, Col 1/6]



# All analyzed by Takajo automagic!

Many other analysis results can be output with a single run of automagic:

- List Domain/IP/Hash
- Stacking Scheduled Tasks
- Stacking Users
- Stacking Service names
- Task scheduler timeline
- Logon timeline
- Process timeline
- PowerShell execution history
- MITRE ATT&CK TTPs
- …etc.

# Takeaways

Velociraptor + Hayabusa + Takajo gives you two “scalables”

- Scalable environment
  - Simply set up Velociraptor and collect forensic artifacts via the client.
  - Analyze logs from multiple clients with Hayabusa.
    - You can get forensic artifacts quickly
- Scalable knowledge
  - Takajo is packed with Yamato Security know-how
  - Takajo can get analysis results with a single command.
    - Deeper analysis possible in less time.

# Thank you so much for listening!

A screenshot of a GitHub repository page for "Yamato Security". The repository has 227 followers, is located in Japan, and the user handle is @SecurityYamato. The README.md file contains the text "Hi there まいど ! 🙌".

https://github.com/Yamato-Security

Yamato Security 大和セキュリティ

227 followers Japan @SecurityYamato

README.md

Hi there まいど ! 🙌

If you like our tools, please consider supporting us with a GitHub star!

Check out the latest release information on X!



Follow:  
[@SecurityYamato](https://twitter.com/@SecurityYamato)

## Thank you for your attention!