

31st ANNUAL FIRST CONFERENCE

Threat Hunting with SysmonSearch - Sysmon Log Aggregation, Visualization and Investigation

2019/06/21

Wataru Takahashi (JPCERT/CC)

Self-introduction

Wataru Takahashi

- Incident Response Group at JPCERT/CC
- Malware analysis, Forensics investigation.
- Written up posts on findings on this blog and GitHub.
 - <https://blogs.jpCERT.or.jp/en/>
 - <https://github.com/JPCERTCC/>

The Challenges in Current Incident Response



The attacker intrudes into the network, and infect many hosts and servers with malware.

Many hosts need investigation in incident response.

Take months to investigate the whole incident.

Importance of logging

■ Necessity to retain logs on a daily basis:



Application log



Network communication log



System log



Sysmon
(System Monitor)

Sysmon

- Sysmon is a free tool provided by Microsoft.
- Tool to record various Windows OS operations (applications, registry entries, communication etc.)



Sysmon log

■ Example log (Process Create)

```
Information,2017/11/07 16:06:03,Microsoft-Windows-Sysmon,1,Process Create (rule: ProcessCreate),"Process Create:
UtcTime: 2017-11-07 07:06:03.955
ProcessGuid: {02EA0504-5B5B-5A01-0000-00105D741200}
ProcessId: 2412
Image: C:\Windows\SysWOW64\cmd.exe
CommandLine: cmd /c ""net use ¥¥Win7_64JP_03¥c$""
CurrentDirectory: C:\Windows\system32
User: NT AUTHORITY\SYSTEM
LogonGuid: {02EA0504-41A6-5A01-0000-002057020000}
LogonId: 0x3e7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: SHA1=EE8CBF12D87C4D388F09B4F69BED2E91682920B5
ParentProcessGuid: {02EA0504-584C-5A01-0000-0010E1C11000}
ParentProcessId: 2604
ParentImage: C:\Intel\Logs\malware.exe
ParentCommandLine: C:\Intel\Logs\malware.exe"
```

Created process

Executed command

User who created the process (authority)

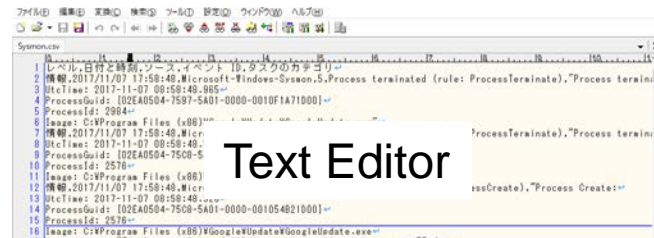
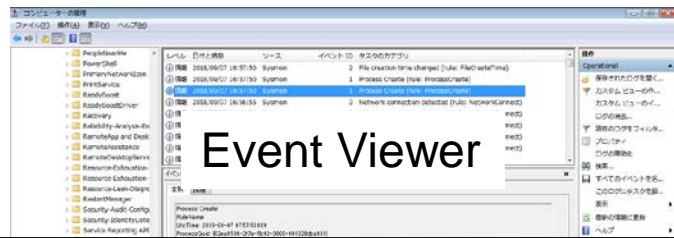
Parent process

■ What you can interpret from the logs

"malware.exe" executes `cmd /c net use ¥¥Win7_64JP_03¥c$` (network sharing) with SYSTEM privilege.

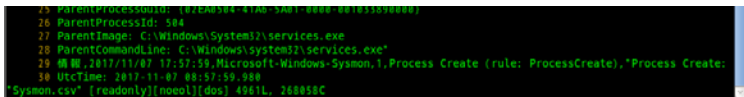
The problems in log analysis

■ No handy tool exists



- Takes time to manually check massive size of data
- Almost impossible to grasp the entire logs
- Difficult to investigate multiple devices at once

Linux commands (grep, awk and others)



The problems in log analysis

- No efficient way to check logs of multiple hosts at the same time
- Difficult to follow the correlation of multiple event IDs
 - you need to check the records of each event ID one by one
 - very time-consuming!

Solution!

- JPCERT/CC created a tool to support Sysmon log analysis.

Increase accuracy for log analysis
Shorten time for incident investigation
Reduce workload for log analysis

SysmonSearch

| | |
|--------------------------------|--------------------------------|
| wataru-takahashi Updated image | Latest commit 8ad63f a day ago |
| docker | initial commit 2 days ago |
| images | Updated image a day ago |
| script | initial commit 2 days ago |

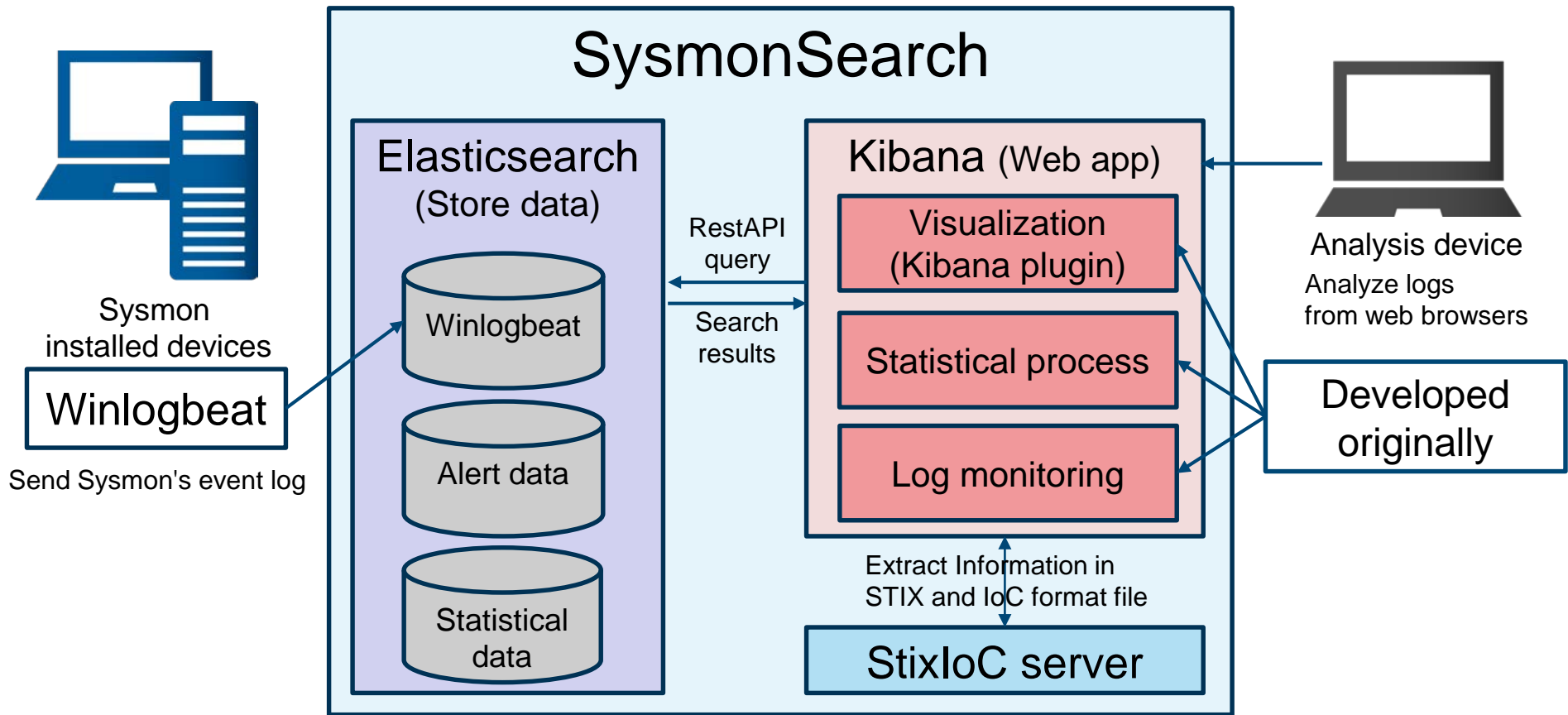
<https://github.com/JPCERTCC/SysmonSearch>

Strength - SysmonSearch -

- Real-time log collection
- Search across multiple logs from multiple hosts
- Visualized Sysmon log correlation
- Comparison with STIX, OpenIOC format indicators

SysmonSearch

System overview



SysmonSearch functions

Search

By hash value,
host names etc.

Monitor

Based on rules

Visualize

In simple graphics

Create statistics

In regular basis

Incident investigation using SysmonSearch

Analysing malware WannaCry

■ Assumption

- we received an alert from the monitoring function

■ Registered monitoring rule

- Filename: tasksche.exe
- Hash: 84C82835A5D21BBCF75A61706D8AB549

Monitoring Screen

The screenshot displays the Kibana SysmonSearch interface. The left sidebar contains navigation options: Discover, Visualize, Dashboard, Timeline, SysmonSearch (selected), Dev Tools, and Management. The main content area is titled 'SysmonSearch' and includes tabs for Alert, Search, Statistics, and Event List. A date range filter is set to '2018/11/21/00:00:00~2018/12/21/00:00:00'. Under 'Detection Rules', five rules are listed with their names and logic, each with a 'Delete file' link. Below this is a 'Results' section with a summary table and a detailed table.

| | Records | Unique Hosts |
|-----------------------------|---------|--------------|
| Overall | 4025 | 8 |
| rule-20181106141408313.json | 3532 | 8 |
| 1.sample | 474 | 7 |
| rule-20181214120140895.json | 10 | 2 |
| rule-20181220103719643.json | 6 | 1 |
| rule-20181220102850449.json | 3 | 1 |

| Computer | Number of Matches |
|-----------------|-------------------|
| Win10_64JP_04 | 3201 |
| Win7_64JP | 267 |
| Win7_64JP_02 | 167 |
| Win10_64JP-Base | 128 |
| Win7_64EN_03 | 128 |
| Win7_64JP_01 | 117 |
| Win7_64JP_2 | 12 |
| Win7_64EN | 5 |

Monitoring Screen - Detection Rules -



Detection Rules

Rule Name:rule-20181106141408313.json | Logic:OR | ProcessName:cmd

[Delete file](#)

Rule Name:1.sample | Logic:AND | Hash:md | ProcessName:net

[Delete file](#)

Rule Name:rule-20181220103719643.json | Logic:OR | Hash:4532f830950aae7e50d1b5b3f1cede2a

[Delete file](#)

Rule Name:rule-20181220102850449.json | Logic:OR | Hash:84C82835A5D21BBCF75A61706D8AB549

[Delete file](#)

Rule Name:rule-20181214120140895.json | Logic:OR | ProcessName:TempNcF88.eXe

[Delete file](#)

MD5 : 84C82835A5D21BBCF75A61706D8AB549

| | |
|-----------------|-----|
| Win7_64JP | 267 |
| Win7_64JP_02 | 167 |
| Win10_64JP-Base | 128 |
| Win7_64EN_03 | 128 |
| Win7_64JP_01 | 117 |
| Win7_64JP_2 | 12 |
| Win7_64EN | 5 |

Monitoring Screen - Results -

The screenshot shows the Kibana interface with the 'Alerts' section selected. The 'Results' table displays the following data:

| | Records | Unique Hosts |
|-----------------------------|---------|--------------|
| Overall | 4025 | 8 |
| rule-20181106141408313.json | 3532 | 8 |
| 1.sample | 474 | 7 |
| rule-20181214120140895.json | 10 | 2 |
| rule-20181220103719643.json | 6 | 1 |
| rule-20181220102850449.json | 3 | 1 |

Below the table, there are two rows of data:

| | |
|-------------|----|
| Win7_64JP_2 | 12 |
| Win7_64EN | 5 |

Monitoring Screen – Check the record -

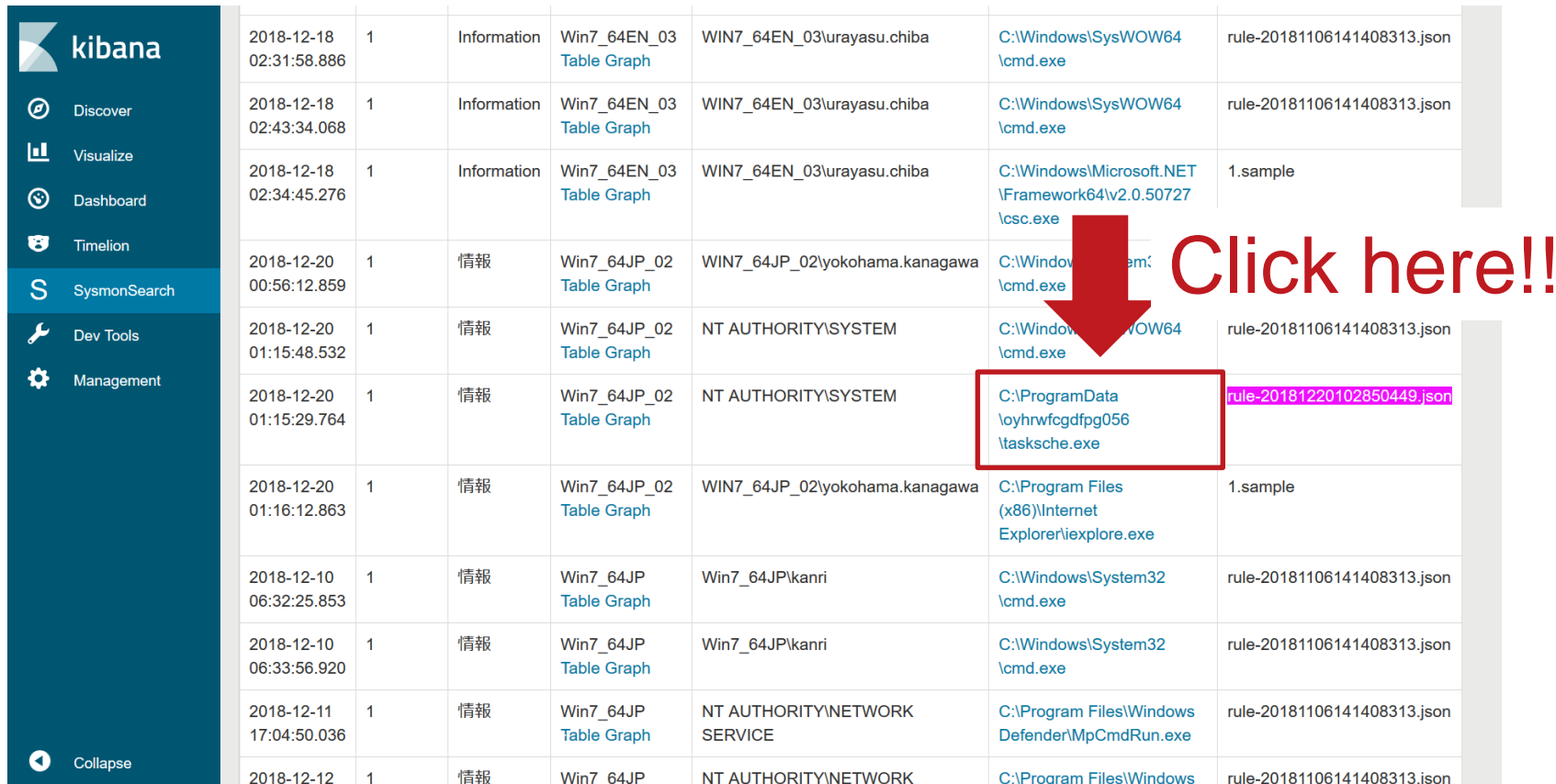
The screenshot shows a Kibana interface with a table of monitoring records. The table has columns for timestamp, priority, level, host, source, process path, and rule ID. A callout box points to a specific process name, and another callout box points to a specific event ID in the table.

| Timestamp | Priority | Level | Host | Source | Process Path | Rule ID |
|-------------------------|----------|-------------|--------------|--------------------------------|---|-----------------------------|
| 2018-12-18 02:31:58.886 | 1 | Information | Win7_64EN_03 | WIN7_64EN_03\urayasu.chiba | C:\Windows\SysWOW64\cmd.exe | rule-20181106141408313.json |
| 2018-12-18 02:43:34.068 | 1 | Information | Win7_64EN_03 | WIN7_64EN_03\urayasu.chiba | C:\Windows\SysWOW64\cmd.exe | rule-20181106141408313.json |
| 2018-12-20 01:15:48.532 | 1 | 情報 | Win7_64JP_02 | NT AUTHORITY\SYSTEM | C:\Windows\SysWOW64\cmd.exe | rule-20181106141408313.json |
| 2018-12-20 01:15:29.764 | 1 | 情報 | Win7_64JP_02 | NT AUTHORITY\SYSTEM | C:\ProgramData\oyhrwfcgdfpg056\tasksche.exe | rule-20181220102850449.json |
| 2018-12-20 01:16:12.867 | 1 | 情報 | Win7_64JP_02 | WIN7_64JP_02\yokohama.kanagawa | C:\Program Files (x86)\Internet Explorer\iexplore.exe | 1.sample |
| 2018-12-10 06:32:25.853 | 1 | 情報 | Win7_64JP | Win7_64JP\kanri | C:\Windows\System32\cmd.exe | rule-20181106141408313.json |
| 2018-12-10 06:33:56.920 | 1 | 情報 | Win7_64JP | Win7_64JP\kanri | C:\Windows\System32\cmd.exe | rule-20181106141408313.json |
| 2018-12-11 17:04:50.036 | 1 | 情報 | Win7_64JP | NT AUTHORITY\NETWORK SERVICE | C:\Program Files\Windows Defender\MpCmdRun.exe | rule-20181106141408313.json |
| 2018-12-12 | 1 | 情報 | Win7_64JP | NT AUTHORITY\NETWORK SERVICE | C:\Program Files\Windows Defender\MpCmdRun.exe | rule-20181106141408313.json |

Process Name :
C:\ProgramData\oyhrwfcgdfpg056\tasksche.exe

Event id : 1 (Process Create)

Monitoring Screen – Check the record -



The screenshot displays the Kibana SysmonSearch interface. On the left is a navigation sidebar with options: Discover, Visualize, Dashboard, Timelion, SysmonSearch (selected), Dev Tools, and Management. A 'Collapse' button is at the bottom of the sidebar. The main area shows a table of system events. A red arrow points to a record where the file path 'C:\ProgramData\oyhrwfcgdfpg056\tasksche.exe' is highlighted with a red box. A red text overlay 'Click here!!' is positioned to the right of the arrow.

| | | | | | | |
|-------------------------|---|-------------|---|--------------------------------|---|-----------------------------|
| 2018-12-18 02:31:58.886 | 1 | Information | Win7_64EN_03 Table Graph | WIN7_64EN_03\urayasu.chiba | C:\Windows\SysWOW64\cmd.exe | rule-20181106141408313.json |
| 2018-12-18 02:43:34.068 | 1 | Information | Win7_64EN_03 Table Graph | WIN7_64EN_03\urayasu.chiba | C:\Windows\SysWOW64\cmd.exe | rule-20181106141408313.json |
| 2018-12-18 02:34:45.276 | 1 | Information | Win7_64EN_03 Table Graph | WIN7_64EN_03\urayasu.chiba | C:\Windows\Microsoft.NET\Framework64\v2.0.50727\lsc.exe | 1.sample |
| 2018-12-20 00:56:12.859 | 1 | 情報 | Win7_64JP_02 Table Graph | WIN7_64JP_02\yokohama.kanagawa | C:\Windows\System32\cmd.exe | rule-20181106141408313.json |
| 2018-12-20 01:15:48.532 | 1 | 情報 | Win7_64JP_02 Table Graph | NT AUTHORITY\SYSTEM | C:\Windows\SysWOW64\cmd.exe | rule-20181106141408313.json |
| 2018-12-20 01:15:29.764 | 1 | 情報 | Win7_64JP_02 Table Graph | NT AUTHORITY\SYSTEM | C:\ProgramData\oyhrwfcgdfpg056\tasksche.exe | rule-20181220102850449.json |
| 2018-12-20 01:16:12.863 | 1 | 情報 | Win7_64JP_02 Table Graph | WIN7_64JP_02\yokohama.kanagawa | C:\Program Files (x86)\Internet Explorer\iexplore.exe | 1.sample |
| 2018-12-10 06:32:25.853 | 1 | 情報 | Win7_64JP Table Graph | Win7_64JP\kanri | C:\Windows\System32\cmd.exe | rule-20181106141408313.json |
| 2018-12-10 06:33:56.920 | 1 | 情報 | Win7_64JP Table Graph | Win7_64JP\kanri | C:\Windows\System32\cmd.exe | rule-20181106141408313.json |
| 2018-12-11 17:04:50.036 | 1 | 情報 | Win7_64JP Table Graph | NT AUTHORITY\NETWORK SERVICE | C:\Program Files\Windows Defender\MpCmdRun.exe | rule-20181106141408313.json |
| 2018-12-12 | 1 | 情報 | Win7_64JP | NT AUTHORITY\NETWORK | C:\Program Files\Windows | rule-20181106141408313.json |

Analysing malware WannaCry

kibana

- Discover
- Visualize
- Dashboard
- Timeline
- S SysmonSearch**
- Dev Tools
- Management

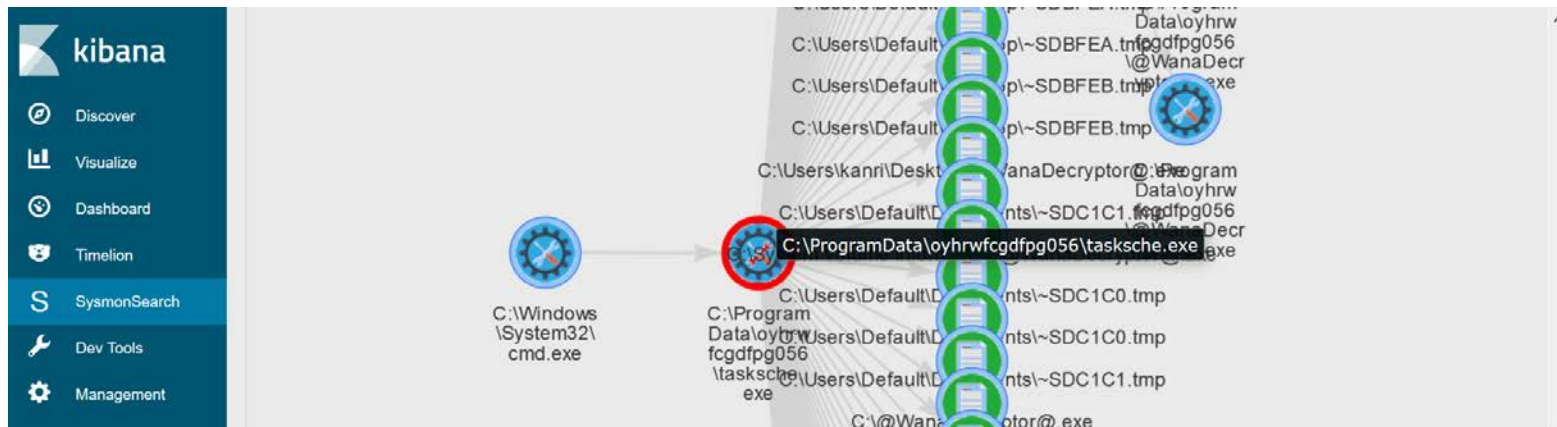
C:\Windows\System32\cmd.exe

C:\ProgramData\oyhrwfcgdfpg056\tasksche.exe

C:\Users\DefaultID\Documents\~SDC1C0.tmp
C:\Users\DefaultID\Documents\~SDC1C0.tmp
C:\Users\DefaultID\Documents\~SDC1C1.tmp
C:\Users\DefaultID\Documents\~SDC1C1.tmp
C:\@WanaDecryptor@.exe
C:\ProgramData\Microsoft\Search\...C:\Temp\~SDC238.tmp
C:\ProgramData\Microsoft\Search\...Data\Temp\~SDC256.tmp
C:\ProgramData\Microsoft\Search\...Temp\usgthrsvc\~SDC257.tmp
C:\ProgramData\Microsoft\Search\...Temp\usgthrsvc\~SDC257.tmp
C:\ProgramData\Microsoft\Search\...C:\Temp\~SDC238.tmp

```
CurrentDirectory:C:\Windows\system32\  
CommandLine:C:\ProgramData\oyhrwfcgdfpg056\tasksche.exe  
Hashes:MD5=84C82835A5D21BBCF75A61706D8AB549, SHA256=ED01EBFC9EB5BBEA545AF4D01BF5F1071661840480439C6E5BABE8E080E41AA  
ParentProcessGuid:{02EA0504-ED31-5C1A-0000-001014C00301}  
ParentCommandLine:cmd.exe /c "C:\ProgramData\oyhrwfcgdfpg056\tasksche.exe"  
ProcessGuid:{02EA0504-ED31-5C1A-0000-0010BBC00301}
```

Analysing malware WannaCry



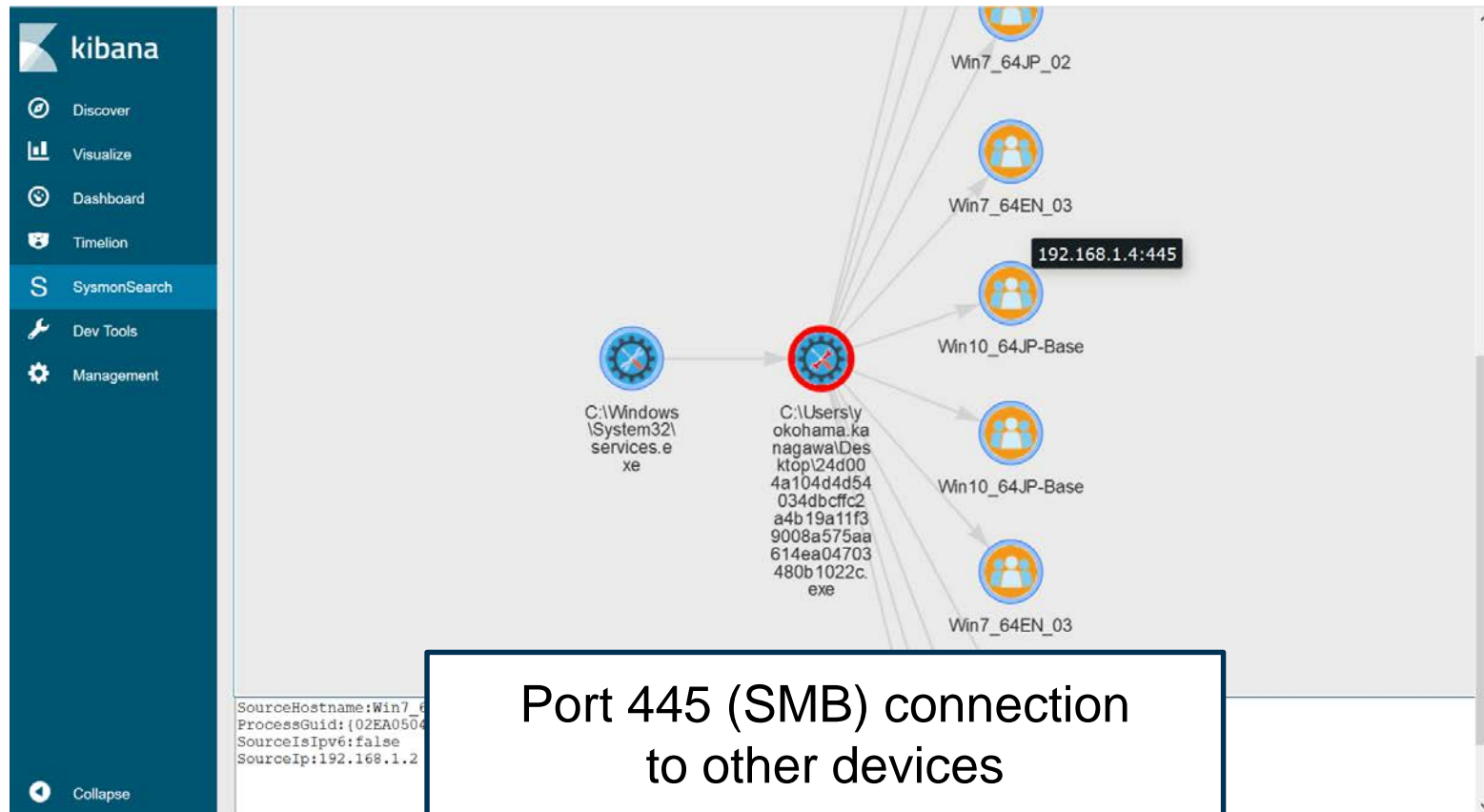
```
CurrentDirectory:C:\Windows\system32\  
CommandLine:C:\ProgramData\oyhrwfcgdfpg056\tasksche.exe  
Hashes:MD5=84C82835A5D21BBCF75A61706D8AB549, SHA256=ED01EBFBC9EB5BBEA545AF4D01BF5F1071661840480439C6E5BABE8E080E41AA  
ParentProcessGuid:{02EA0504-ED31-5C1A-0000-001014C00301}  
ParentCommandLine:cmd.exe /c "C:\ProgramData\oyhrwfcgdfpg056\tasksche.exe"  
ProcessGuid:{02EA0504-ED31-5C1A-0000-0010BBC00301}
```

```
Hashes:MD5=84C82835A5D21BBCF75A61706D8AB549, SHA256=ED01EBFBC9EB5BBEA545AF4D01BF5F1071661840480439C6E5BABE8E080E41AA  
ParentProcessGuid:{02EA0504-ED31-5C1A-0000-001014C00301}  
ParentCommandLine:cmd.exe /c "C:\ProgramData\oyhrwfcgdfpg056\tasksche.exe"  
ProcessGuid:{02EA0504-ED31-5C1A-0000-0010BBC00301}
```

Loading tasksche.exe

The screenshot displays the Kibana SysmonSearch interface. On the left is a dark blue sidebar with the Kibana logo and navigation options: Discover, Visualize, Dashboard, Timelion, SysmonSearch (highlighted), Dev Tools, and Management. A 'Collapse' button is at the bottom of the sidebar. The main content area shows a list of Sysmon events, each with a blue gear icon and a file path. The path `C:\ProgramData\oyhrwfcgdfpg056\tasksche.exe` is highlighted with a black box. A white callout box with a black border and text points to this entry, stating "Loaded 'tasksche.exe'". At the bottom of the list, a hash is visible: `Hashes:MD5=8495400F199AC77853C53B5A3F278F3E,SHA256=2CA2D550E603D74DEDDA03156023135B38DA3630CB014E3D00B1263358C5F00D`.

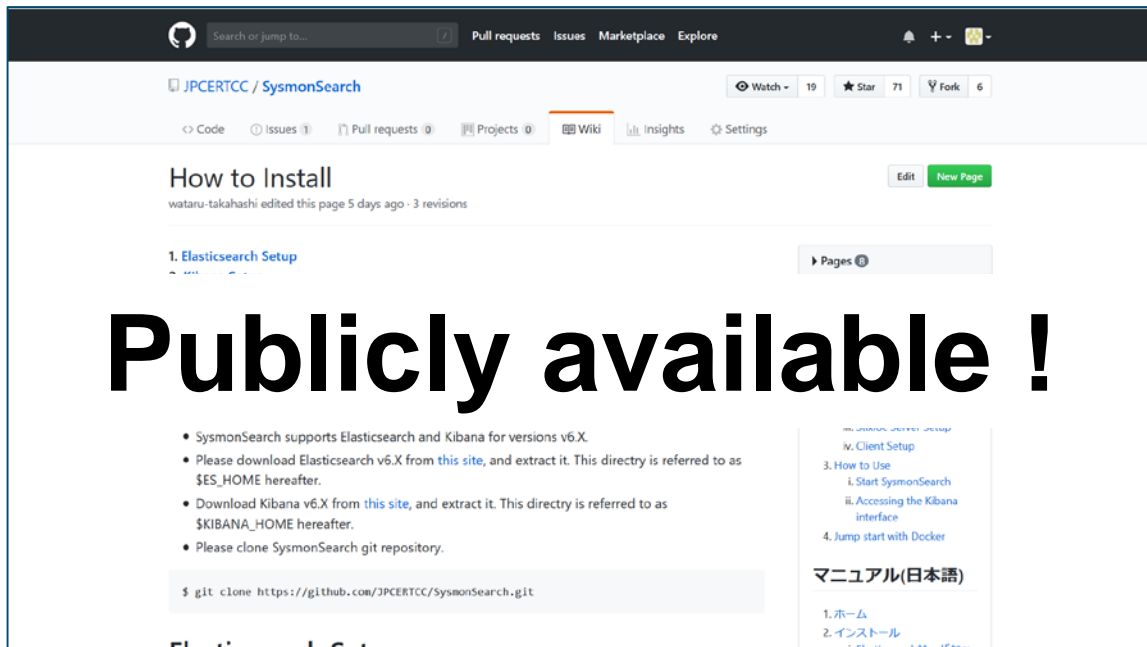
SMB communication to other devices



How to Install

■ SysmonSearch wiki

— <https://github.com/JPCERTCC/SysmonSearch/wiki>



The screenshot shows the GitHub Wiki page for SysmonSearch. The page title is "How to Install" and it was last edited 5 days ago. The main content features a large, bold heading "Publicly available!". Below this, there is a list of instructions for installation, including downloading Elasticsearch and Kibana, and cloning the repository. A terminal command is provided: `$ git clone https://github.com/JPCERTCC/SysmonSearch.git`. The page also includes a sidebar with a table of contents and a link to the Japanese manual.

Publicly available !

- SysmonSearch supports Elasticsearch and Kibana for versions v6.X.
- Please download Elasticsearch v6.X from [this site](#), and extract it. This directory is referred to as \$ES_HOME hereafter.
- Download Kibana v6.X from [this site](#), and extract it. This directory is referred to as \$KIBANA_HOME hereafter.
- Please clone SysmonSearch git repository.

```
$ git clone https://github.com/JPCERTCC/SysmonSearch.git
```

1. ElasticSearch Setup

iv. Client Setup

3. How to Use

- i. Start SysmonSearch
- ii. Accessing the Kibana interface

4. Jump start with Docker

マニュアル(日本語)

1. ホーム
2. インストール

Note

- Sysmon log output configuration
 - Besides installing the tool, you will need to change Sysmon configurations to record logs

- Network events recorded in Sysmon
 - Under proxy environment
 - Recorded destination IP address will be set to the proxy
 - Investigation required in line with the proxy server logs

What's learned from the pilot version

- JPCERT installed the pilot version of SysmonSearch onto 50 devices
 - SysmonSearch Server
 - CPU: 2 core
 - Memory: 4GB
 - SysmonSearch does not require a server with high spec
 - Log amount : 100MB/day
 - Room for Improvement
 - Sysmon log is not enough to analyze the network with proxy server.

Future Works

- Extended functions
 - Import Sysmon logs
 - Raise alert upon detection

- Link between Sysmon logs and network logs

Takeaway

- SysmonSearch can be used for investigation of device operations and log monitoring in peacetime based on rules
 - Investigate suspicious operation by visualizing Sysmon logs
 - Detect suspicious operations based on rules

Thank you!!

Please give us feedback.
e-mail: ir-info@jpcert.or.jp

