

31st ANNUAL FIRST CONFERENCE

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

2019/06/21

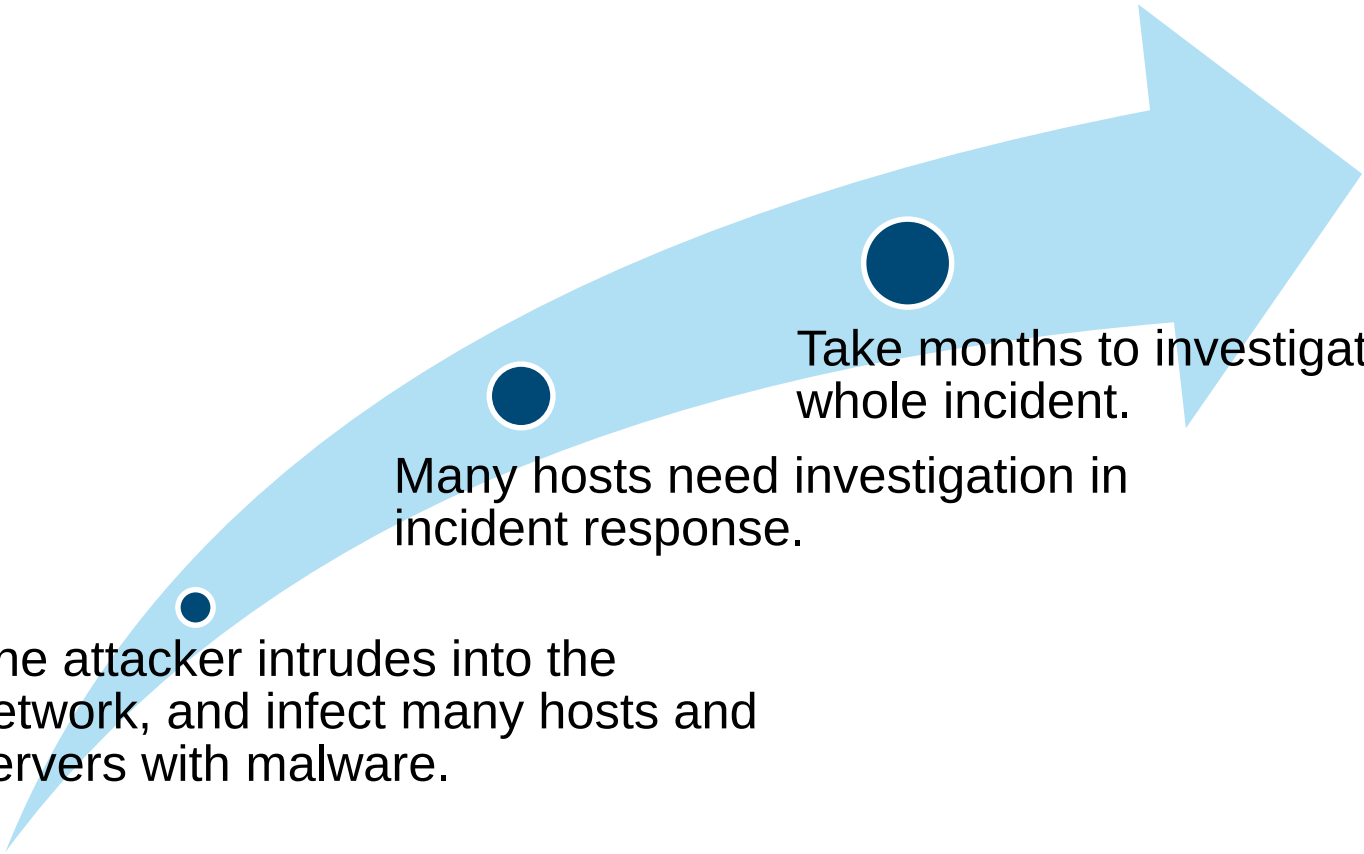
Wataru Takahashi (JPCERT/CC)

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)

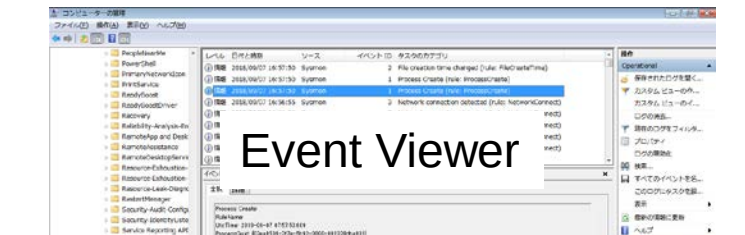
Parent process

■ What you can interpret from the logs

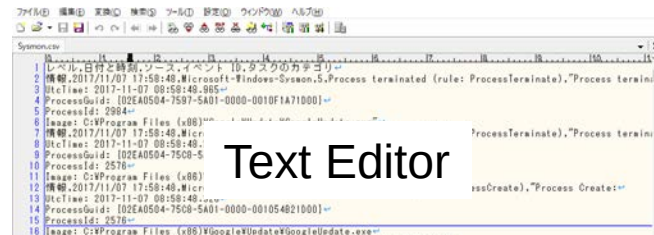
"malware.exe" executes `cmd /c net use ¥¥Win7_64JP_03¥c$` (network sharing) with SYSTEM privilege.

The problems in log analysis

■ No handy tool exists



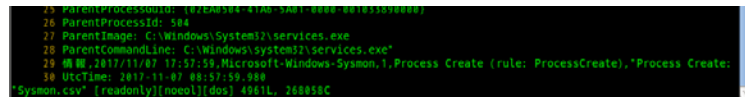
Event Viewer



Text Editor

- 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)



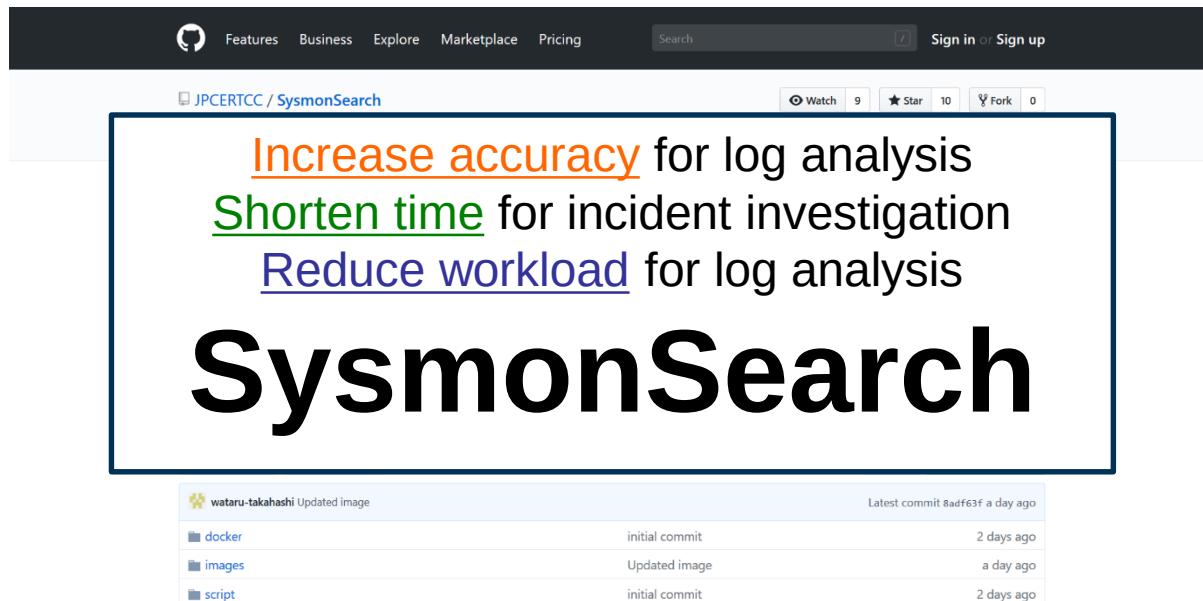
SIEM

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.



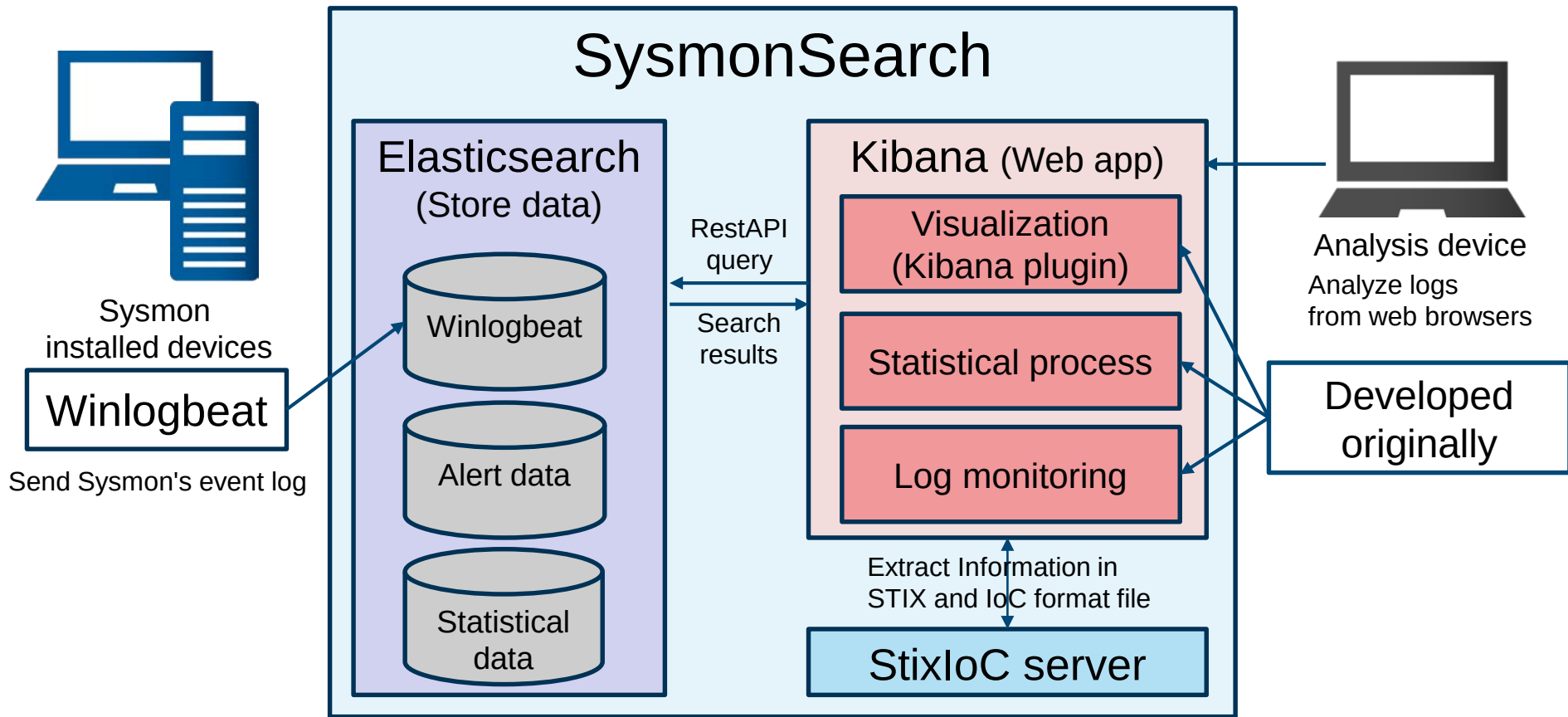
<https://github.com/JPCERTCC/SysmonSearch>

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. On the left is a sidebar with navigation links: Discover, Visualize, Dashboard, Timeline, SysmonSearch (selected), Dev Tools, and Management. The main panel has tabs for Alert, Search, Statistics, and Event List. The 'Alert' tab is active, showing a date range of 2018/11/21/00:00:00~2018/12/21/00:00:00. Below this is a 'Detection Rules' section with a list of rules and their associated actions (Delete file). The 'Results' section shows a summary table with columns for Records and Unique Hosts. Below the summary is a 'result' table with columns for Computer and Number of Matches.

Detection Rules

Rule Name	Action
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:4532f830950aee7e50d1b5b3f1cede2a	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

Results

	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

result

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 -

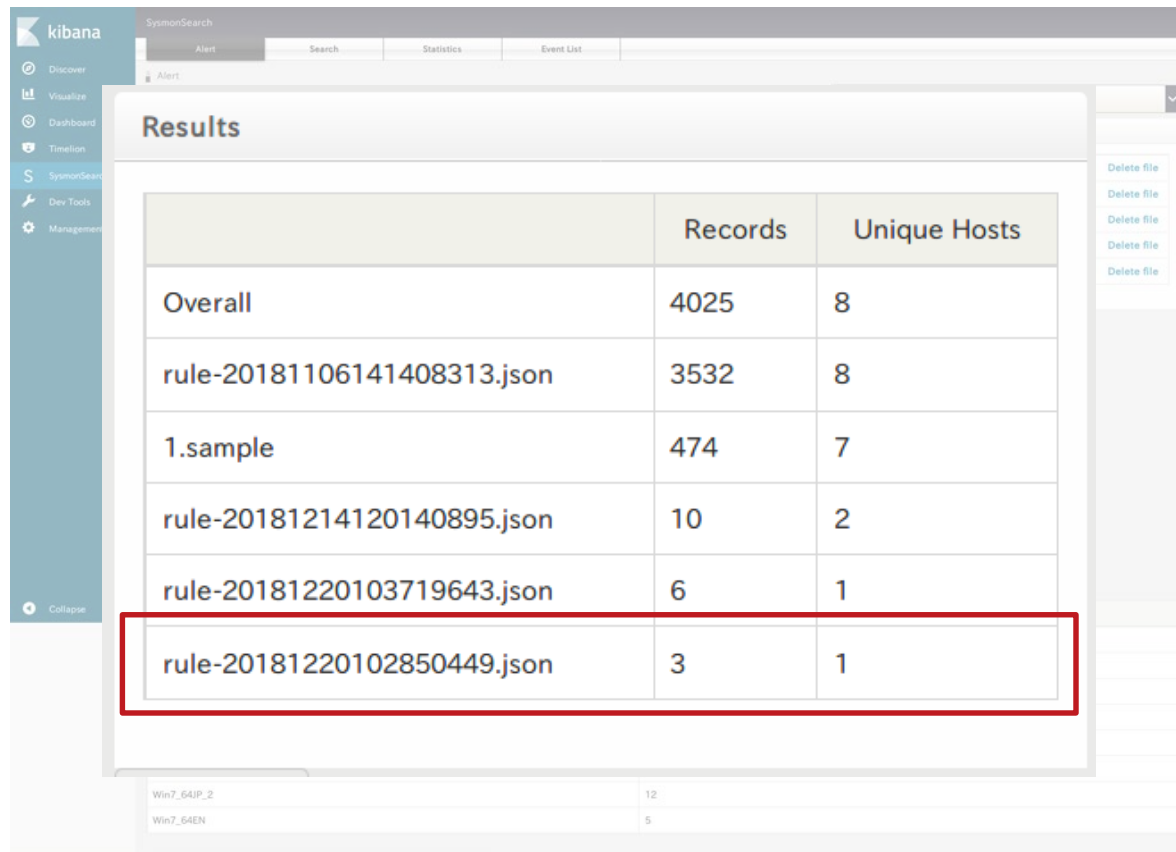


Detection Rules	
Rule Name:rule-20181106141408313.json Logic:OR ProcessName:cmd	Delete file
Rule Name:1.sample Logic:AND Hash:md ProcessName:net	Delete file
Rule Name:rule-20181220103719643.json Logic:OR Hash:4532f830950aae7e50d1b5b3f1cede2a	Delete file
Rule Name:rule-20181220102850449.json Logic:OR 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 SysmonSearch interface. The left sidebar contains navigation links: Discover, Visualize, Dashboard, Timeline, SysmonSearch (selected), Dev Tools, and Management. The top navigation bar includes tabs for Alert, Search, Statistics, and Event List. The main content area is titled 'Results' and displays a table with 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 is a section with two rows of data:

Win7_64JP_2	12
Win7_64EN	5

Monitoring Screen – Check the record -

Discover
Visualize
Dev Tools
Management
Collapse

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
					rosoft.NET 2.0.50727	1.sample
					tem32	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 01:16:12.862	1		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			Table Graph		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

Process Name :

C:\ProgramData\oyhrwfcgdfpg056\tasksche.exe

Event id : 1 (Process Create)

Monitoring Screen – Check the record -



kibana

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

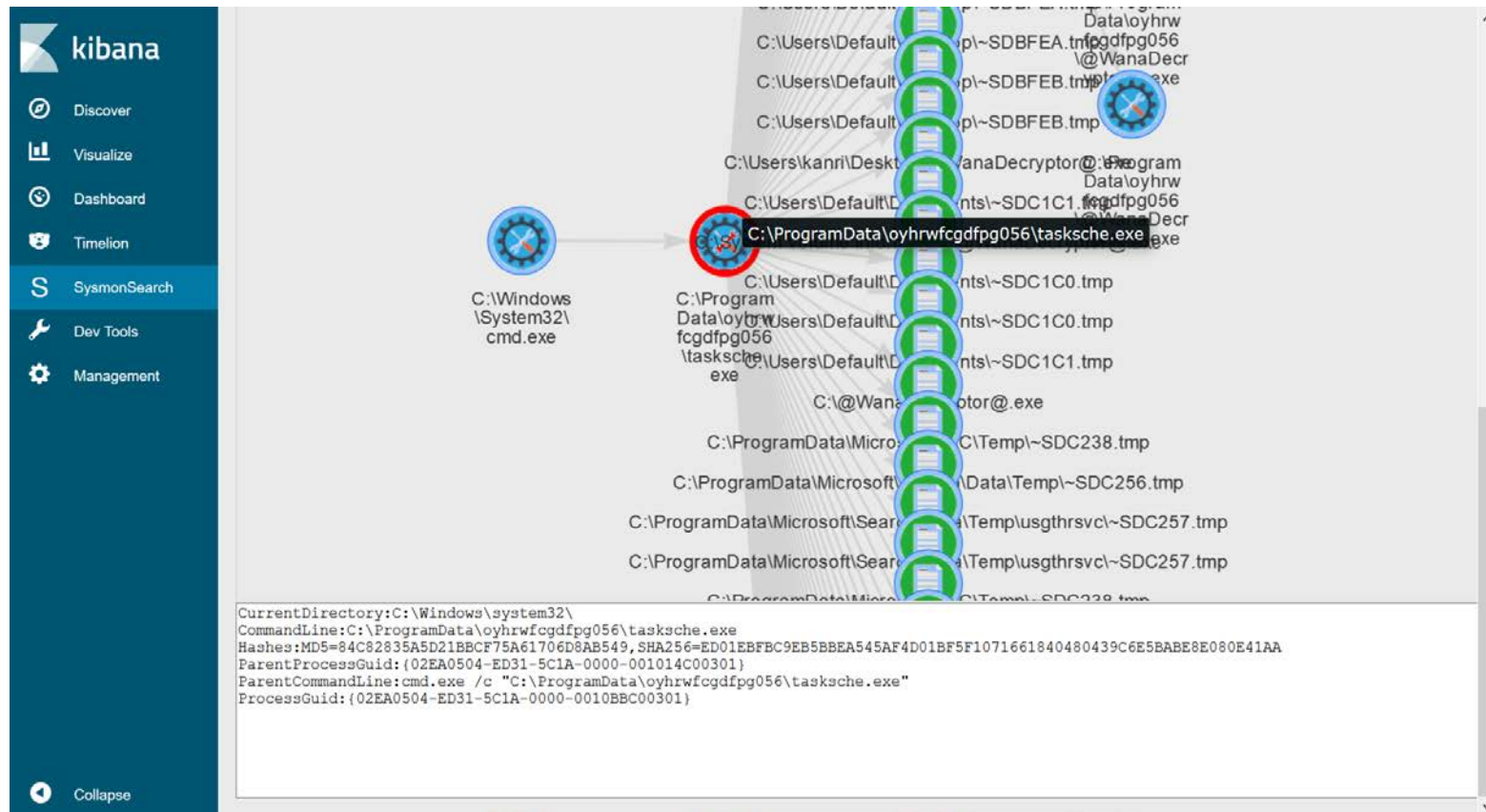
 Collapse

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\csc.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\loyhrwfcgdfpg056\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 Table Graph	NT AUTHORITY\NETWORK	C:\Program Files\Windows	rule-20181106141408313.json



Click here!!

Analysing malware WannaCry



Analysing malware WannaCry

kibana

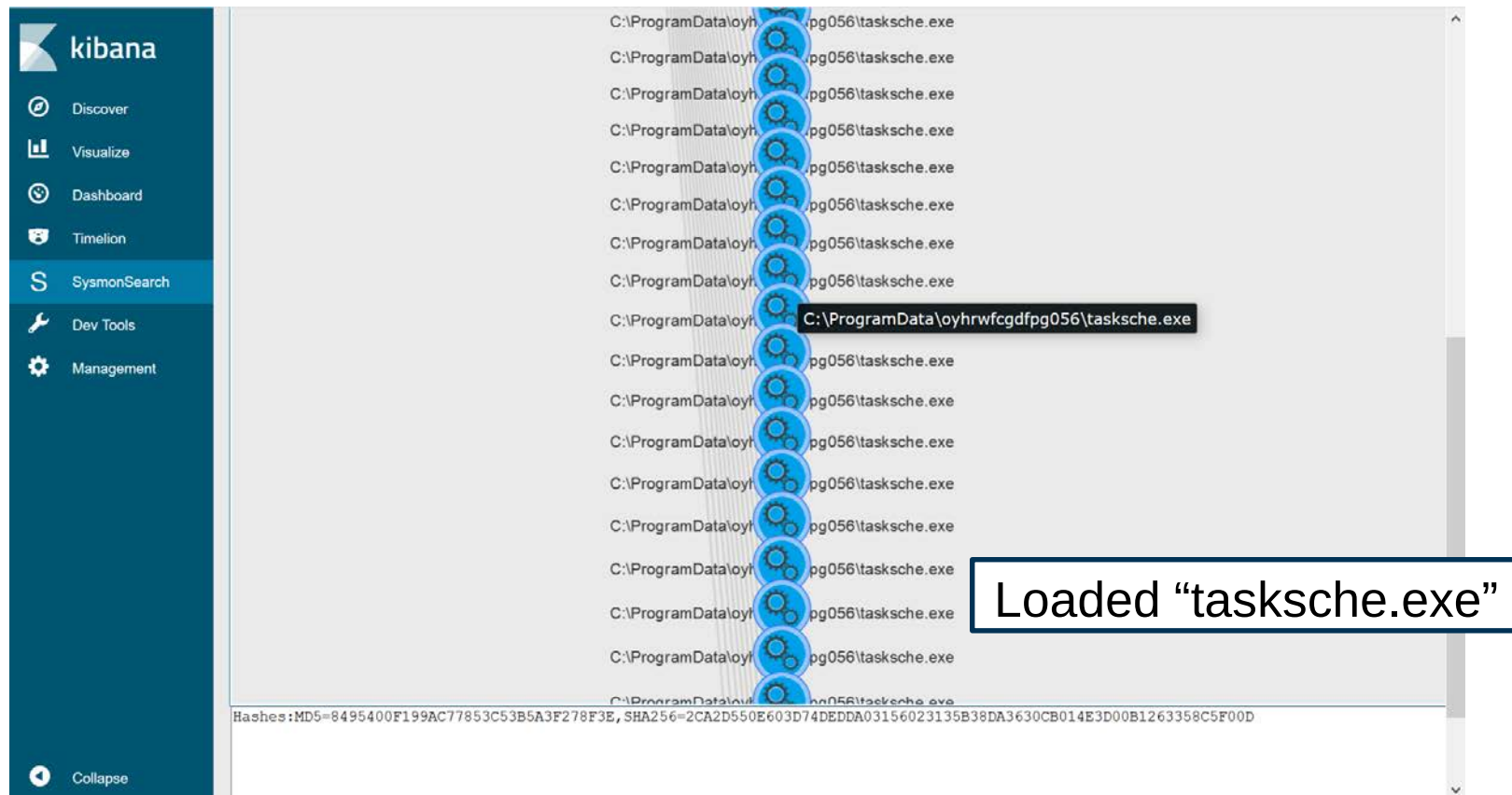
- Discover
- Visualize
- Dashboard
- Timeline
- S SysmonSearch**
- Dev Tools
- Management

Process Tree:

- C:\Windows\System32\cmd.exe
 - C:\ProgramData\oyhrwfcgdfpg056\tasksche.exe

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}

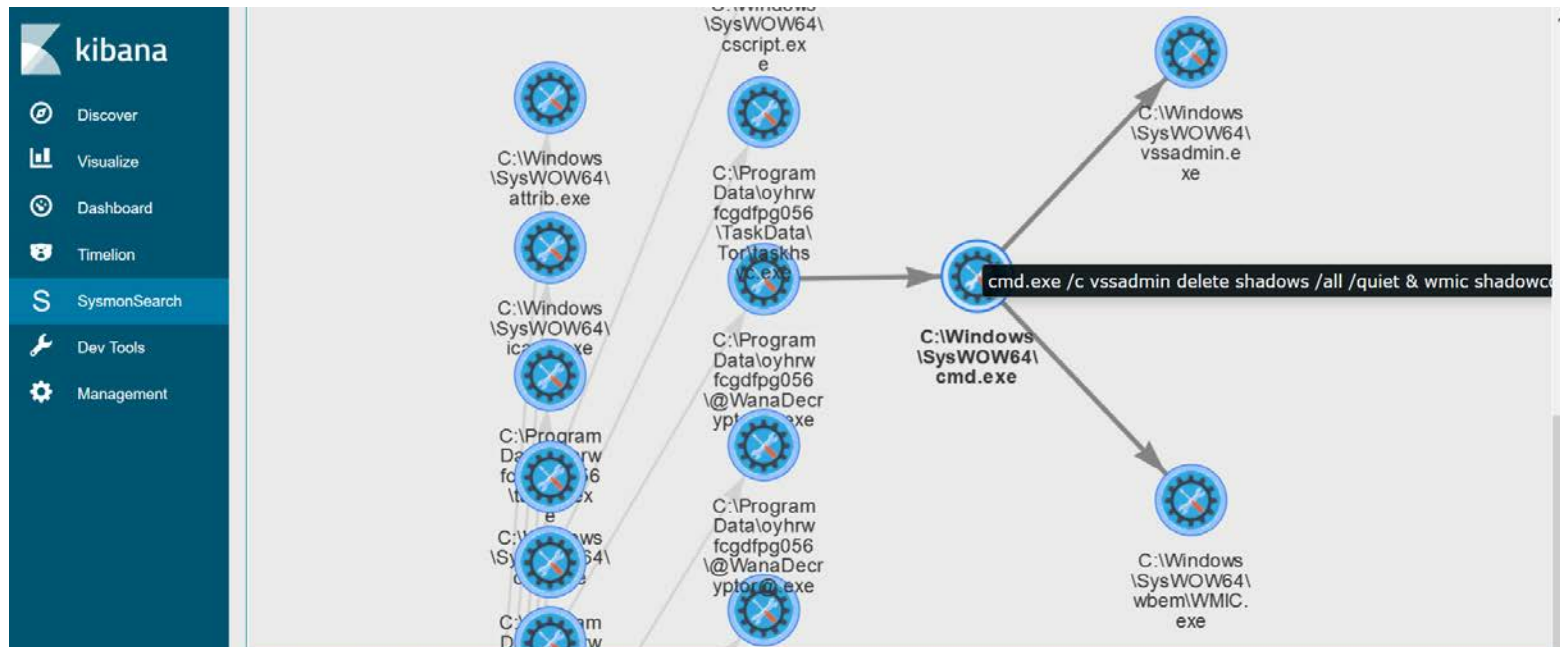
Loading tasksche.exe



The screenshot displays the Kibana SysmonSearch interface. On the left is a dark blue sidebar with the Kibana logo and navigation links: 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 entry consists of a blue circular icon with a gear, followed by a file path. The path 'C:\ProgramData\oyhrwfcgdfpg056\tasksche.exe' is highlighted in black. At the bottom of the list, a hash is displayed: Hashes:MD5=8495400F199AC77853C53B5A3F278F3E, SHA256=2CA2D550E603D74DEDDA03156023135B38DA3630CB014E3D00B1263358C5F00D. A white box with a black border and the text 'Loaded "tasksche.exe"' is overlaid on the right side of the list.

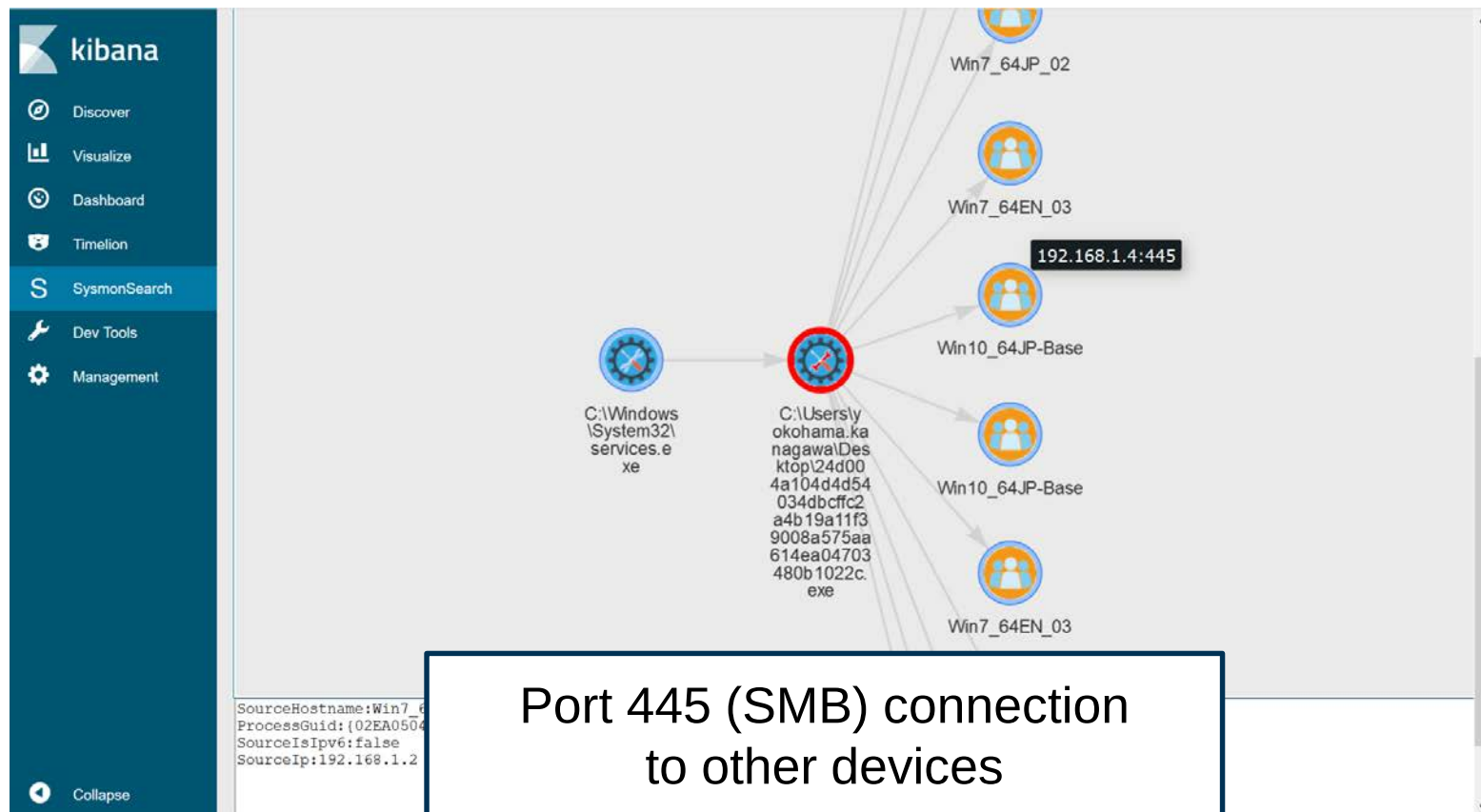
Loaded "tasksche.exe"

Deleting VSS



```
CurrentDirectory:C:\ProgramData\oyhrwfcgdfpg056\  
CommandLine:cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures /set {default} recoveryenabled no & wbadm delete catalog -quiet  
Hashes:MD5=AD7B9C14083B52BC532FBA5948342B98,SHA256=17F746D82695FA9B35493B41859D39D786D32B23A9D2E00F4011DEC7A02402AE  
ParentProcessGuid:{02EA0504-ED3A-5C1A-0000-0010F1520401}  
ParentCommandLine:@WanaDecryptor@.exe vs  
ProcessGuid:{02EA0504-ED44-5C1A-0000-0010EE830401}
```

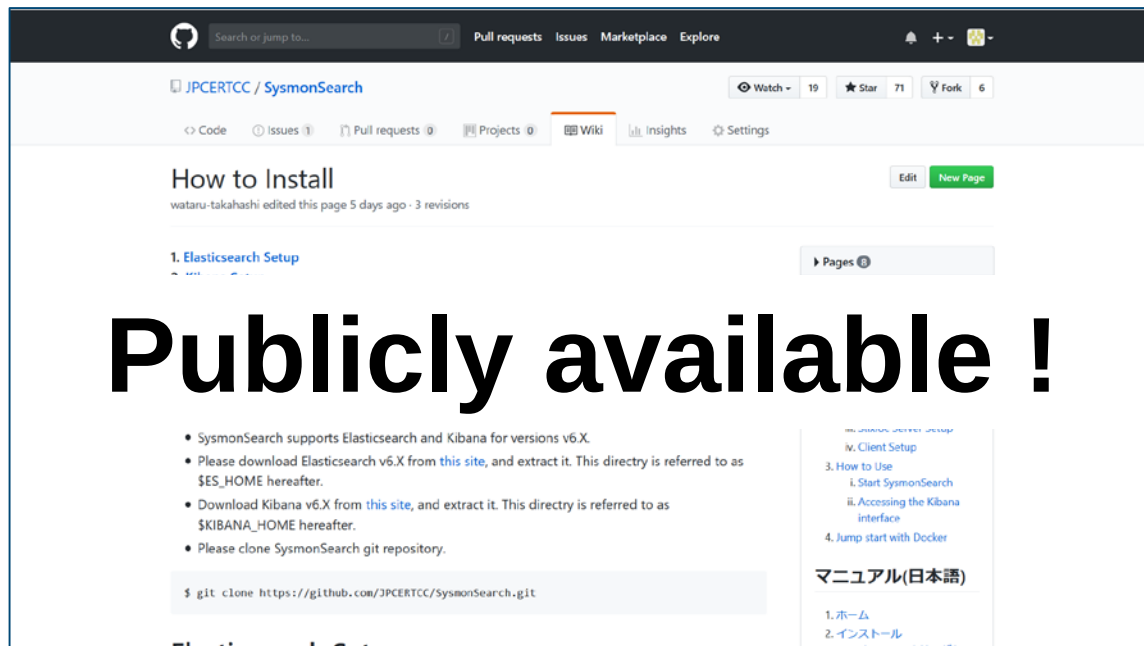
SMB communication to other devices



How to Install

■ SysmonSearch wiki

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



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

