

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

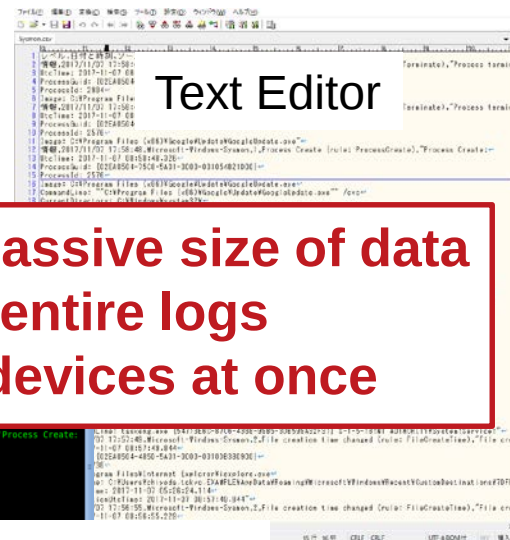
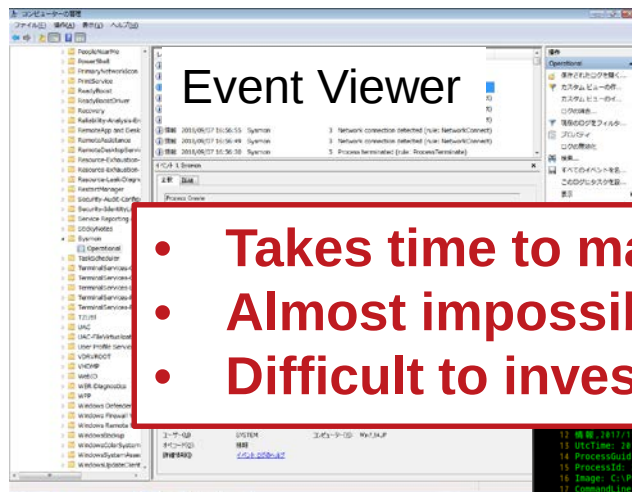
User who created the process (authority)

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)

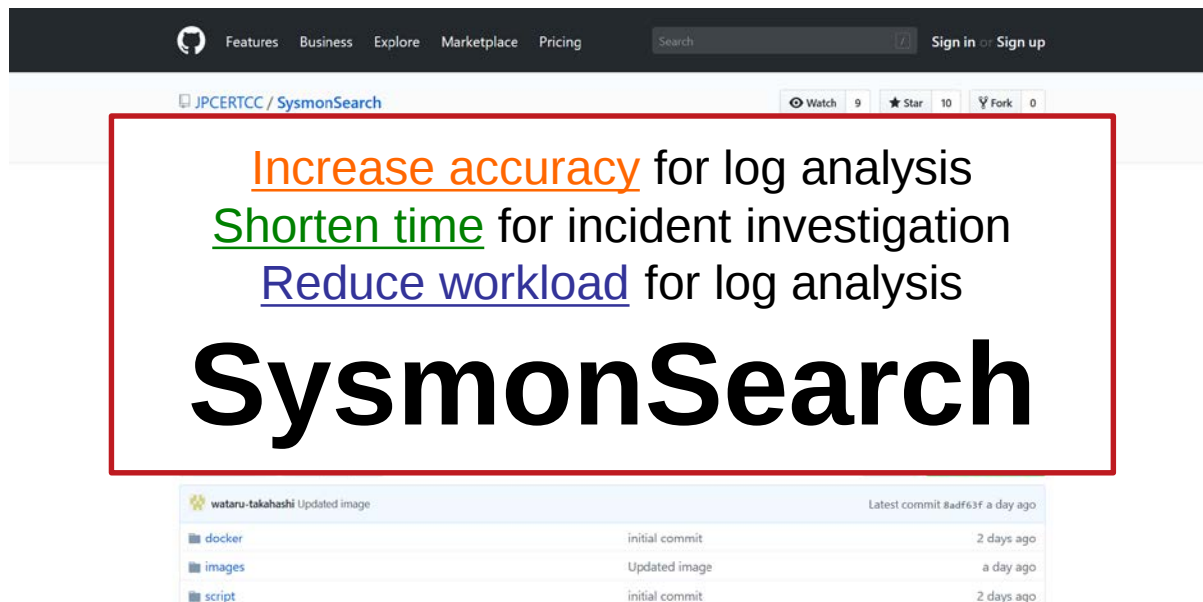
```
12 2017/11/07 17:15:48 Microsoft-Windows-Sysmon,1,Process Create (rule: ProcessCreate),Process Create:  
13 UTCTime: 2017/11/07 00:15:48.125  
14 ProcessId: 0x1A104-71C1-1A01-8000-00101401D0E0  
15 ProcessName: lsass.exe  
16 Image: C:\Program Files (x86)\Google\Update\GoogleUpdate.exe  
17 CommandLine: "C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /svc  
18 CurrentDirectory: C:\Windows\system32  
19 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

wataru-takahashi Updated image		Latest commit 8adf63f 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>

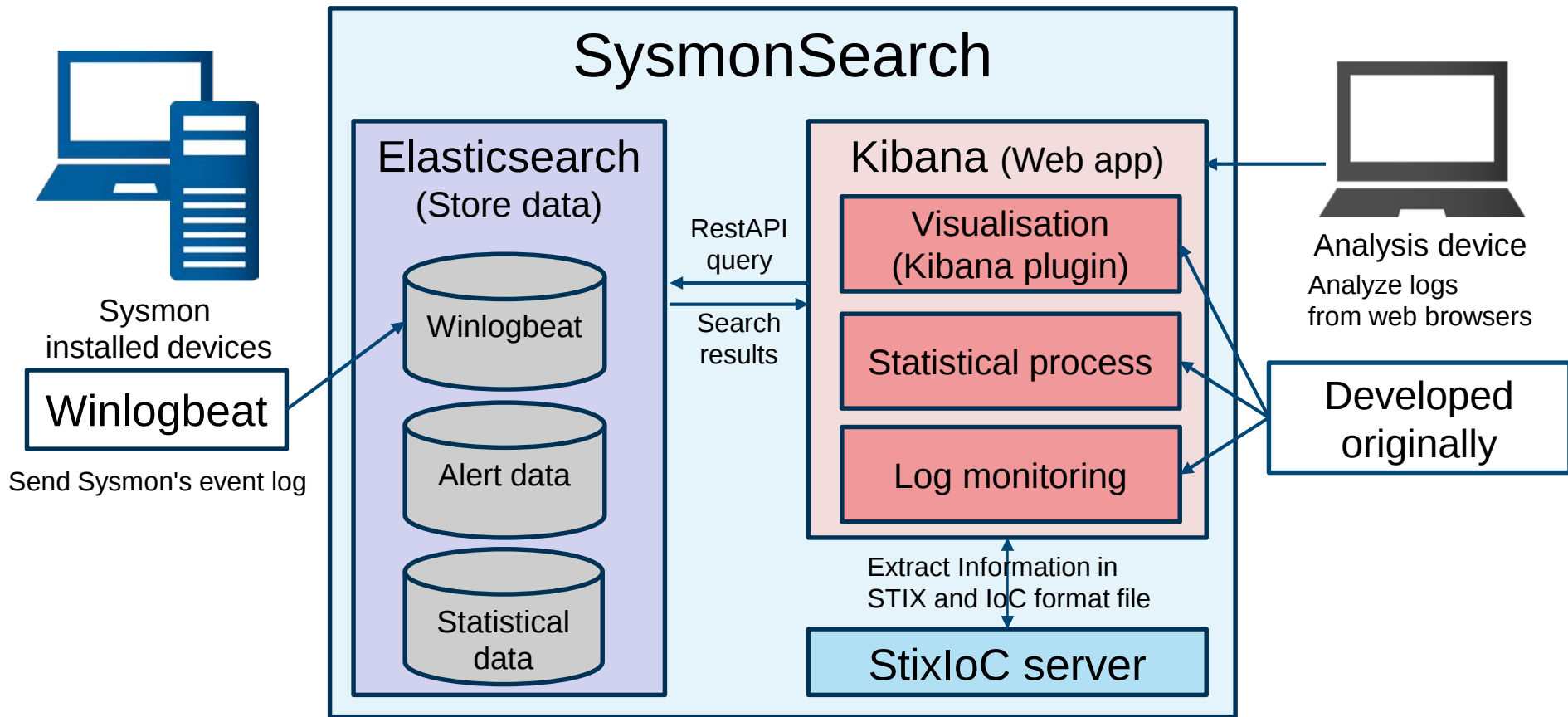
SysmonSearch

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 links: Discover, Visualize, Dashboard, Timeline, SysmonSearch (selected), Dev Tools, and Management. The main panel is titled 'SysmonSearch' and has tabs for Alert, Search, Statistics, and Event List. The 'Search' tab is active, showing a search condition input area with a date range and a field 'Process Name' set to 'powershell'. Below this, a table of results is shown, containing 23 records and 2 unique hosts. The results table has columns for UtcTime, EventId, Level, Computer, UserName, and Image. The first five rows of the table are visible, showing events related to powershell.exe execution on various Windows systems.

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 links: Discover, Visualize, Dashboard, Timeline, 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, the 'Detection Rules' section lists two rules with 'Delete file' links. The 'Results' section shows a table with 'Records' and 'Unique Hosts' for overall and rule-specific data. The 'Number of Matches' section shows a table with 'Computer' and 'Number of Matches' for 'Win7_64JP'.

Monitor rules

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

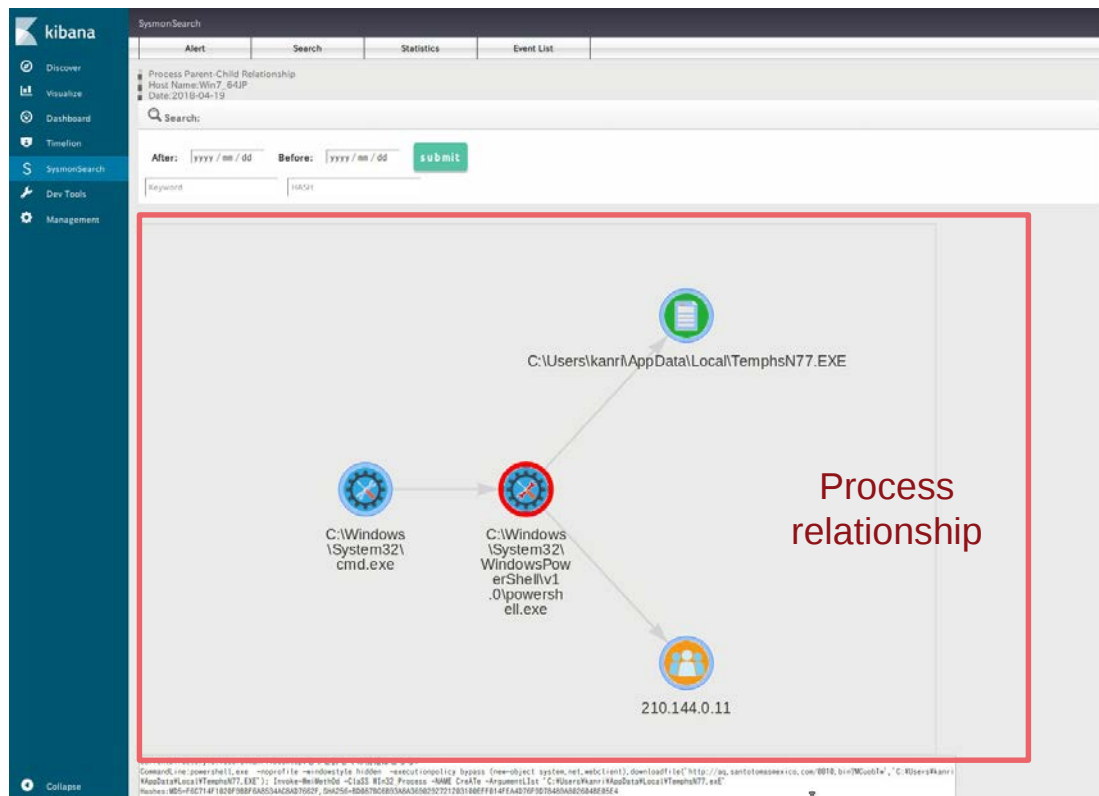
Detection results

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

Number of matches

Computer	Number of Matches
Win7_64JP	4

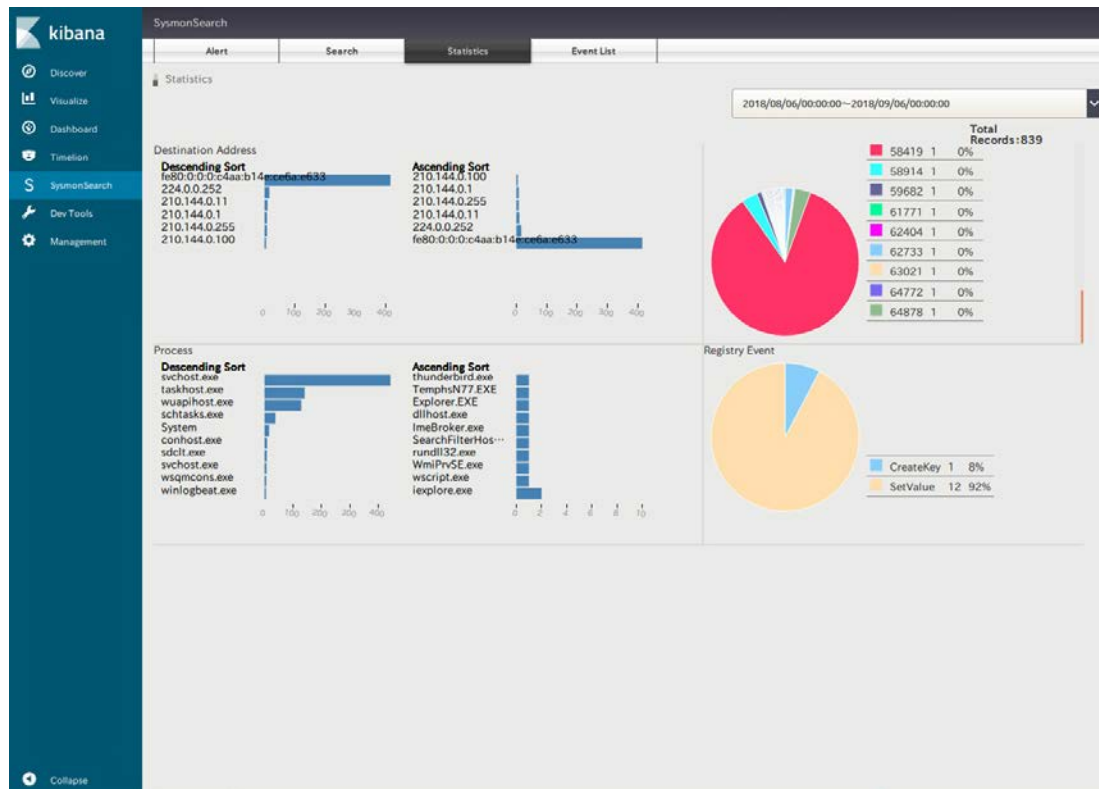
Visualise



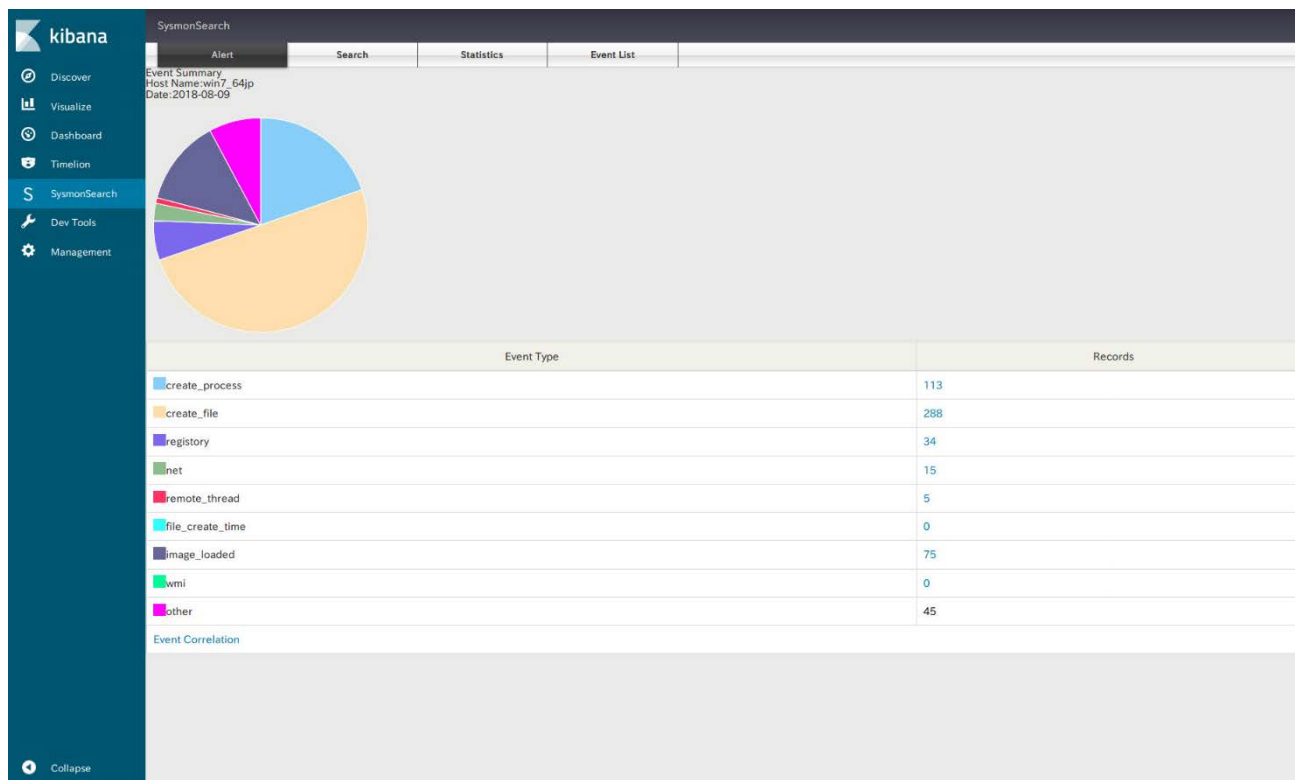
Corresponding icons to IDs

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



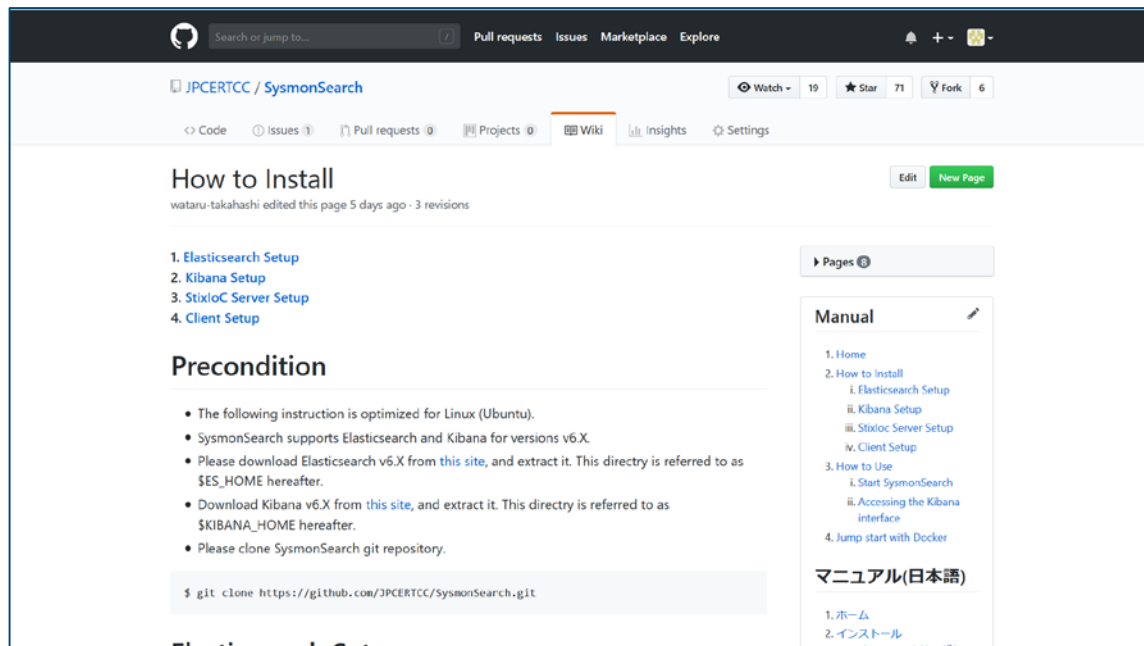
Create statistics



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 edited by wataru-takahashi 5 days ago. The page content includes a list of steps: 1. Elasticsearch Setup, 2. Kibana Setup, 3. StixIoC Server Setup, and 4. Client Setup. Below this is a "Precondition" section with a list of requirements: the instructions are optimized for Linux (Ubuntu), SysmonSearch supports Elasticsearch and Kibana for versions v6.X, users should download Elasticsearch v6.X from a specific site and extract it, download Kibana v6.X from another site and extract it, and clone the SysmonSearch git repository. A terminal command is provided: `$ git clone https://github.com/JPCERTCC/SysmonSearch.git`. On the right side, there is a "Manual" section with a list of links: 1. Home, 2. How to Install (with sub-links for Elasticsearch Setup, Kibana Setup, StixIoC Server Setup, and Client Setup), 3. How to Use (with sub-links for Start SysmonSearch and 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 links for 1. ホーム and 2. インストール.

■ JPCERT/CC Blog

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



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

