29th ANNUAL FIRST CONFERENCE

SAN JUAN
PUERTO RICO
JUNE 11-16, 2017

FIGHTING PIRATES AND PRIVATEERS

WWW.FIRST.ORG

FIRST
Improving Security Together

APT Log Analysis

- Tracking Attack Tools by Audit Policy and Sysmon -

Shusei Tomonaga

JPCERT Coordination Center

29th ANNUAL FIRST CONFERENCE
SAN JUAN PUERTO RICO

Self-introduction

Shusei Tomonaga

- Analysis Center at JPCERT/CC
- Malware analysis, Forensics investigation.
- Written up posts on malware analysis and technical findings on this blog and Github.
  - http://blog.jpcert.or.jp/
  - https://github.com/JPCERTCC/aa-tools

Challenge of Incident Response

- Many hosts need to be investigated for APT Incident Response.
- Logs required for investigation are not always recorded.
- Difficult to detect Lateral Movement.

Approach

If you know what logs are recorded with the lateral movement tools, IR will be easier.

- For lateral movement, a limited set of tools are used in many different incidents.

- There are some common patterns in the lateral movement methods.

This Presentation Topics

1 Overview of APT Incident and Lateral Movement

2 Tools Used by Attackers for Lateral Movement

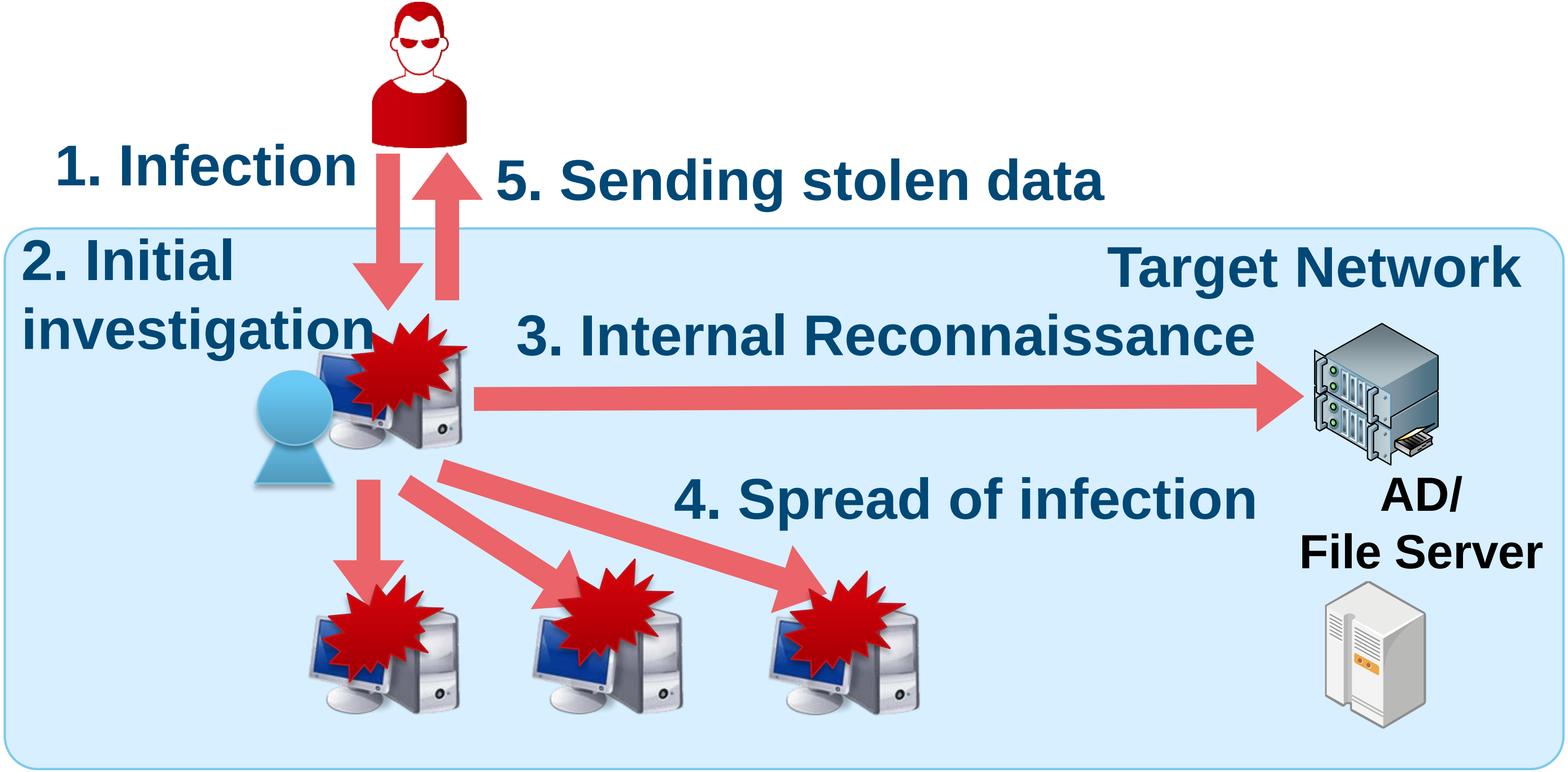
3 How to Track Lateral Movement

1 Overview of APT Incident and Lateral Movement

2 Tools Used by Attackers for Lateral Movement

3 How to Track Lateral Movement

Overview of APT Incident and Lateral Movement



1 Overview of APT Incident and Lateral Movement

2 Tools Used by Attackers for Lateral Movement

3 How to Track Lateral Movement

Tools Used by Attackers at Lateral Movement

Attackers use not only attack tools
but also Windows commands and legitimate tools.

- Why attackers use **Windows commands** and **legitimate tools**?

↓

- They are not detected by antivirus software.

Research of Tools Used by Attackers

Research Methods

Investigating C&C servers in three operations.

- APT17 (named by FireEye)
- Dragon OK (named by Palo Alto)
- Blue Termite (named by Kaspersky)

Lateral Movement: Initial Investigation

Initial investigation

- Collect information of the infected host

- The most used command is **tasklist**.

- If the attacker is not interested in the infected host, they will escape soon.

Windows Command Used by Initial Investigation

Rank	Command	Count
1	**tasklist**	155
2	ver	95
3	ipconfig	76
4	systeminfo	40
5	net time	31
6	netstat	27
7	whoami	22
8	net start	16
9	qprocess	15
10	query	14

Lateral Movement: Internal Reconnaissance

Internal Reconnaissance

- Look for information saved in the machine and remote hosts within the network

- The most used command is **dir**.
  - The attacker investigates confidential data stored in the infected host.
- For searching the network, **net** is used.

Windows Command Used by Internal Reconnaissance

Rank	Command	Count
1	**dir**	976
2	**net view**	236
3	ping	200
4	**net use**	194
5	type	120
6	**net user**	95
7	**net localgroup**	39
8	**net group**	20
9	**net config**	16
10	**net share**	11

NET Command

- net view
  - Obtain a list of connectable domain resources
- net user
  - Manage local/domain accounts
- net localgroup
  - Obtain a list of users belonging to local groups
- net group
  - Obtain a list of users belonging to certain domain groups
- net use
  - Access to resources

Example: dir command

Searching Network Drive

```
> dir ¥¥FILESV01¥SECRET > %TEMP%¥a.txt

¥¥FILESV¥SECRET Directory

2014/07/11 09:16 [DIR] Management of Partner Companies
2014/09/04 11:49 [DIR] Management of Intellectual Property
```

Searching Document Files

```
> dir c:¥users¥hoge¥*.doc* /s /o-d

c:¥users¥hoge¥AppData¥Local¥Temp Directory

2014/07/29 10:19 28,672 20140820.doc
1 File 28,672 bytes

c:¥users¥hoge¥Important Information Directory

2015/08/29 10:03 1,214 Design Document.doc
```

/s : Displayed recursively
/o-d : Sorted by date

Lateral Movement: Spread of Infection

Spread of infection

- Infect the machine with other malware or try to access other hosts

- The most used command is **at**.
  - “at” command is not supported on Windows 10, Windows 8.1 etc.
  - If "at" command can not be used, **schtasks** is used.
- Uses password and hash dump tools.

Windows Command Used by Spread of Infection

Rank	Command	Count
1	**at**	103
2	reg	31
3	**schtasks**	29
4	wmic	24
5	wusa	7
6	netsh advfirewall	4
7	sc	4
8	rundll32	2

Remote Command Execute Used Windows Command

at command

```
> at ¥¥[IP Address] 12:00 cmd /c
"C:¥windows¥temp¥mal.exe"
```

schtasks command

```
> schtasks /create /tn [Task Name] /tr C:¥1.bat /sc
onstart /ru System /s [IP Address]
```

Remote Command Execute Used Windows Command

wmic command

```
> wmic /node:[IP Address] /user:”[User Name]”
/password:”[PASSWORD]” process call create “cmd
/c c:¥Windows¥System32¥net.exe user”
```

1 Overview of APT Incident and Lateral Movement

2 Tools Used by Attackers for Lateral Movement

3 How to Track Lateral Movement

How to Track Lateral Movement

The Event logs that can be used for incident response are not recorded with default Windows settings.

- How to get evidence of executed tools?

- We propose a detection method using **Audit Policy** and **Sysmon**.

Research Methods

Testing **44 attack tools** on the host that installed **Sysmon** and enabled **Audit Policy**.

- OS
  - Windows 7, 8.1, 2008 and 2012
- Sysmon
  - Version 4
- Test tools
  - 17: Windows Commands
  - 27: Attack Tools

Test Tools List

Windows Commands					
wmic	PowerShell	at	winrm	winrs	BITS
RDP	ntdsutil	vssadmin	net user	net use	net share
icacls	wevtutil	csvde	ldifde	dsquery	

Legitimate Tools				
PsExec	sdelete	WebBrowser PassView	Remote Desktop PassView	Mail PassView

Password Dump Tools			
PWDump7	PWDumpX	WCE	Mimikatz
lslsass	Find-GPOPasswords.ps1	gsecdump	Quarks PwDump

Test Tools List

Exploits			
MS14-058	MS15-078	MS14-068	SDB UAC Bypass

Other Tools				
wmiexec.vbs	BeginX	Htran	Fake wpad	timestomp

Results Overview

Detected 37 out of 44 attack tools using **Audit Policy** and **Sysmon**.

Settings	Detect	Not Detect
Default Settings	**6**	**38**
Sysmon / Audit Policy	**37**	**7**

Detected with Default Windows Settings

The tools installed by default in Windows leave execution traces of evidence.

- Detected tools example (Default installed tools only)
  - RDP
  - at
  - WinRM, WinRS
  - wevtutil
  - BITS

Detected with Sysmon and Audit Policy

If Sysmon and Audit Policy are enabled,
many attack tools can be detected.

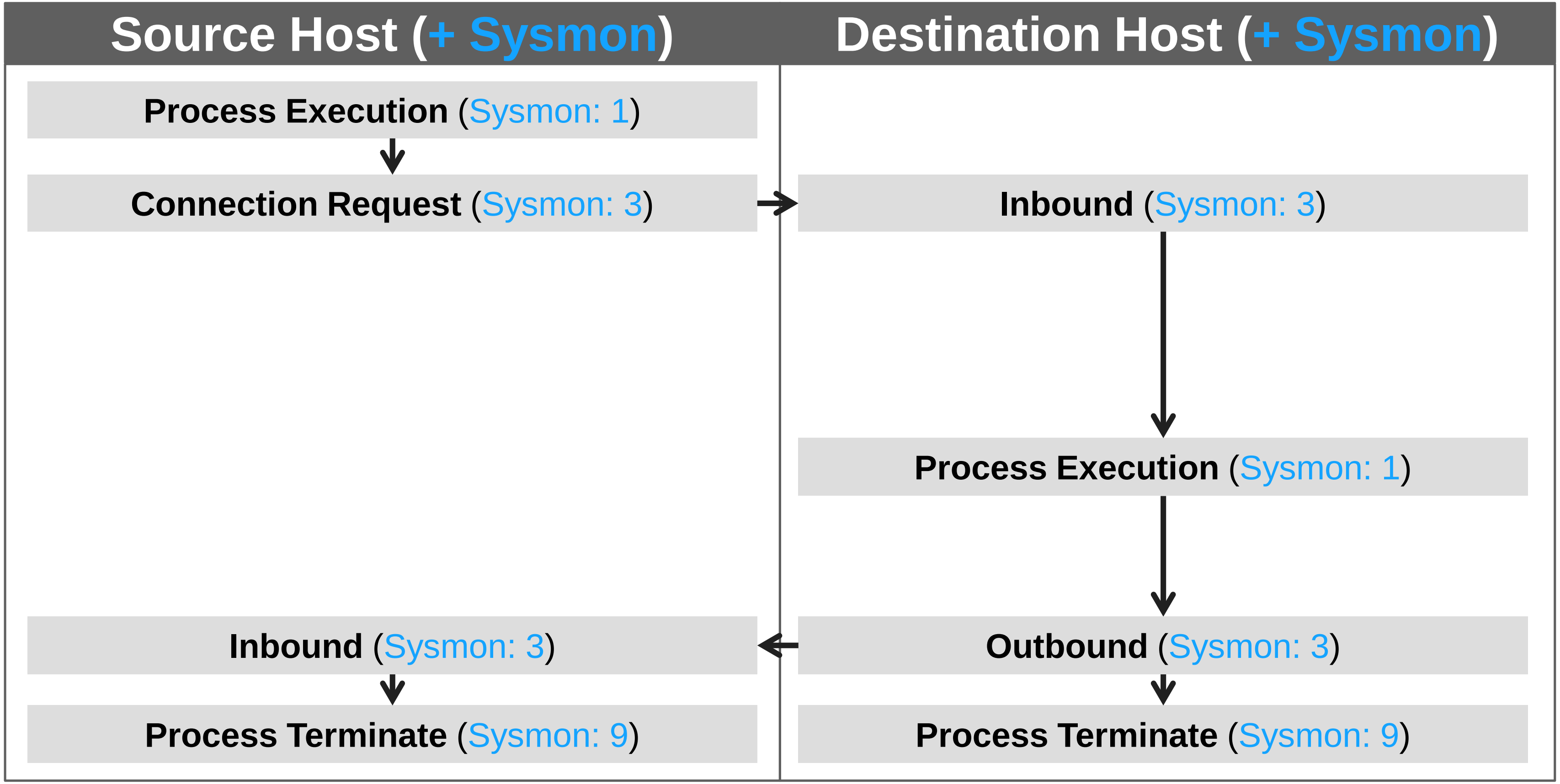
- Detected tools example
  - WCE
  - Mimikatz
  - net command
  - csvde
  - Privilege Escalation Exploit etc.

Sysmon and Audit Policy record many logs

Source Host (Default Setting)	Destination Host (Default Setting)

Process Execution, Connection Request, and File Access are not recorded.

Sysmon and Audit Policy record many logs



Source Host (+ Sysmon)

Destination Host (+ Sysmon)

Process Execution (Sysmon: 1)

Connection Request (Sysmon: 3)

Inbound (Sysmon: 3)

Process Execution (Sysmon: 1)

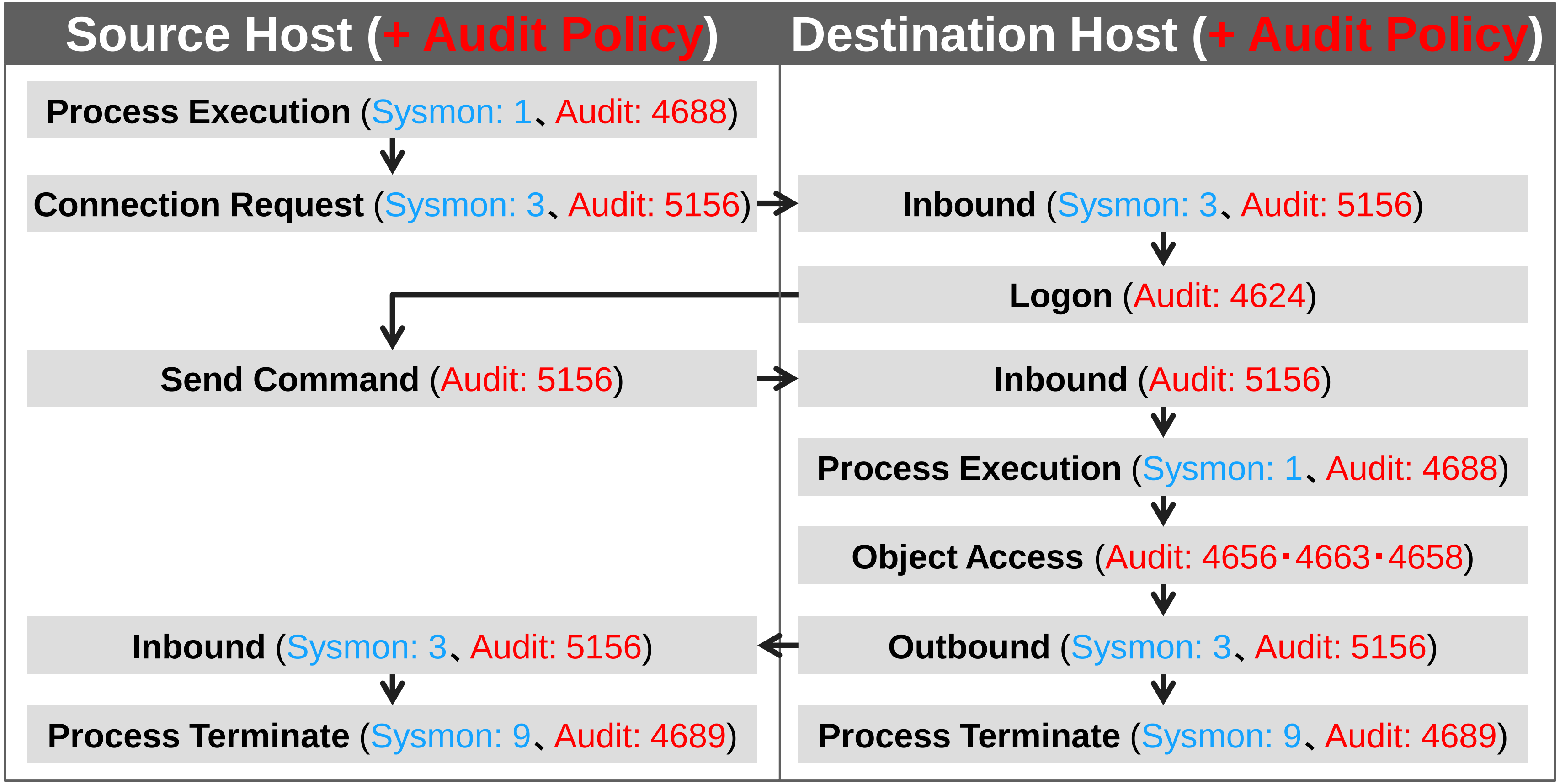
Outbound (Sysmon: 3)

Inbound (Sysmon: 3)

Process Terminate (Sysmon: 9)

Process Terminate (Sysmon: 9)

Sysmon and Audit Policy recode many logs



Source Host (+ Audit Policy)	Destination Host (+ Audit Policy)
Process Execution (Sysmon: 1、Audit: 4688)	
Connection Request (Sysmon: 3、Audit: 5156)	Inbound (Sysmon: 3、Audit: 5156)
	Logon (Audit: 4624)
Send Command (Audit: 5156)	Inbound (Audit: 5156)
	Process Execution (Sysmon: 1、Audit: 4688)
	Object Access (Audit: 4656･4663･4658)
Inbound (Sysmon: 3、Audit: 5156)	Outbound (Sysmon: 3、Audit: 5156)
Process Terminate (Sysmon: 9、Audit: 4689)	Process Terminate (Sysmon: 9、Audit: 4689)

Do we need Sysmon?

Answer: YES

Audit Policy can record more logs than Sysmon.

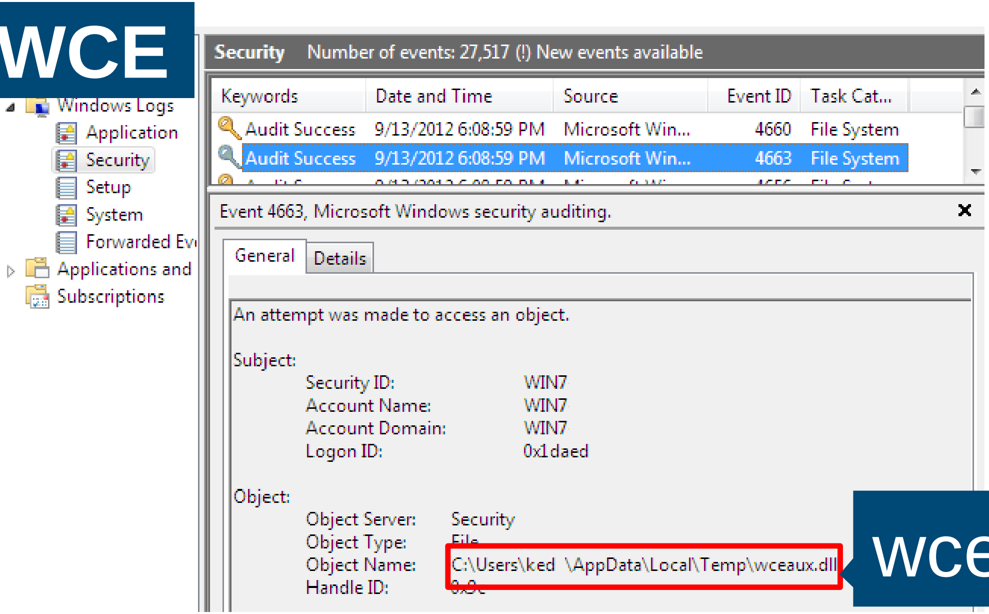
However, Audit Policy can not record command line options.

Sysmon can record all command line.

Example of Detecting with Audit Policy [1]

When the attack tool is executed, the fact that a temporary file may be created is recorded.

Example: WCE



Security Number of events: 27,517 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Cat...
Audit Success	9/13/2012 6:08:59 PM	Microsoft Win...	4660	File System
Audit Success	9/13/2012 6:08:59 PM	Microsoft Win...	4663	File System

Event 4663, Microsoft Windows security auditing.

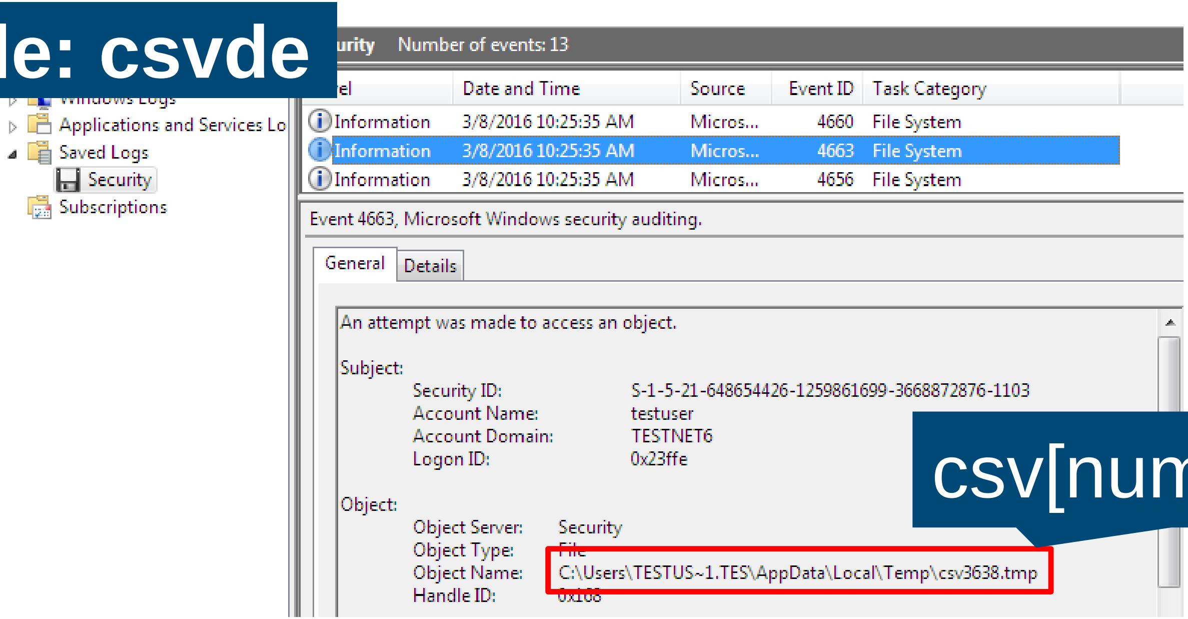
```
An attempt was made to access an object.

Subject:
        Security ID:            WIN7
        Account Name:           WIN7
        Account Domain:         WIN7
        Logon ID:               0x1daed

Object:
        Object Server:      Security
        Object Type:        File
        Object Name:        C:\Users\ked  \AppData\Local\Temp\wceaux.dll
        Handle ID:          0x3c
```

wceaux.dll

Example of Detecting with Audit Policy [2]

When the attack tool is executed, the fact that a temporary file may be created is recorded.

Example: csvde



urity Number of events: 13

Windows Logs
Applications and Services Lo
Saved Logs
Security
Subscriptions

el	Date and Time	Source	Event ID	Task Category
Information	3/8/2016 10:25:35 AM	Micros...	4660	File System
Information	3/8/2016 10:25:35 AM	Micros...	4663	File System
Information	3/8/2016 10:25:35 AM	Micros...	4656	File System

Event 4663, Microsoft Windows security auditing.

```
An attempt was made to access an object.

Subject:
        Security ID:            S-1-5-21-648654426-1259861699-3668872876-1103
        Account Name:           testuser
        Account Domain:         TESTNET6
        Logon ID:               0x23ffe

Object:
        Object Server:  Security
        Object Type:    File
        Object Name:    C:\Users\TESTUS~1.TES\AppData\Local\Temp\csv3638.tmp
        Handle ID:      0x108
```

csv[number].tmp

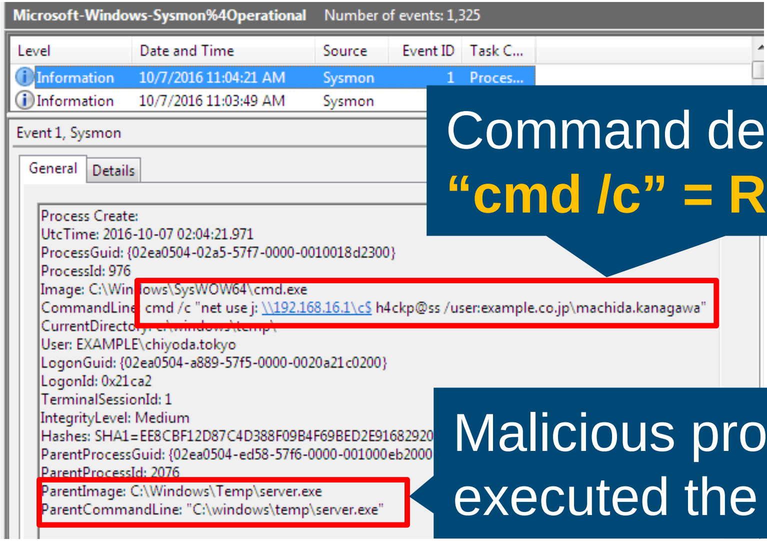
Event ID for Audit Policy

ID	Overview	ID	Overview
4624	Account logon	4689	Process termination
4634	Account logoff	4720	Account creation
4648	A specified logon attempt by a particular account	4726	Account deletion
4656	A handle request for reading or writing an object	4728	Addition of a member to a group
4658	Ending the use of and releasing of a handle	4729	Removal of a member from a group
4690	Duplication of an existing handle for use in other processes	4768/ 4769	An authentication request for an account
4660	Deleting an object	4946	Addition of a Windows Firewall rule
4663	Access made to an object	5140	Access to network share
4661	A handle request to SAM	5142	Creation of a new network share
4672	Assignment of special privileges to a particular logon instance	5144	Deletion of a network share
4673	Execution of a process requiring particular privileges	5145	Confirmation of whether a file share point can be used
4688	Startup of a process	5154	Port listening by an application or service

Example of Detecting with Sysmon

All Windows commands can be recorded by Sysmon.

Example: net use



Microsoft-Windows-Sysmon%4Operational   Number of events: 1,325

Level	Date and Time	Source	Event ID	Task C...
Information	10/7/2016 11:04:21 AM	Sysmon	1	Proces...
Information	10/7/2016 11:03:49 AM	Sysmon		

Event 1, Sysmon

```
Process Create:
UtcTime: 2016-10-07 02:04:21.971
ProcessGuid: {02ea0504-02a5-57f7-0000-0010018d2300}
ProcessId: 976
Image: C:\Windows\SysWOW64\cmd.exe
CommandLine: cmd /c "net use j: \\192.168.16.1\c$ h4ckp@ss /user:example.co.jp\machida.kanagawa"
CurrentDirectory: c:\windows\temp\
User: EXAMPLE\chiyoda.tokyo
LogonGuid: {02ea0504-a889-57f5-0000-0020a21c0200}
LogonId: 0x21ca2
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=EE8CBF12D87C4D388F09B4F69BED2E91682920
ParentProcessGuid: {02ea0504-ed58-57f6-0000-001000eb2000
ParentProcessId: 2076
ParentImage: C:\Windows\Temp\server.exe
ParentCommandLine: "C:\windows\temp\server.exe"
```

Command details
“cmd /c” = Remote shell

Malicious process name that executed the command.

Event ID for Sysmon

ID	Overview	Supported Version
1	Process creation	
2	A process changed a file creation time	
3	Network connection	
4	Sysmon service state changed	
5	Process terminated	
6	Driver loaded	
7	Image loaded	
8	CreateRemoteThread	
9	RawAccessRead	
10	ProcessAccess	
11	FileCreate	5.0
12	RegistryEvent (Object create and delete)	5.0
13	RegistryEvent (Value Set)	5.0
14	RegistryEvent (Key and Value Rename)	5.0
15	FileCreateStreamHash	5.0

Tools not Detected with Sysmon and Audit Policy

- Example
  - PWDump7
  - gsecdump
  - lslsass
  - Mail PassView
  - WebBrowserPassView
  - Remote Desktop PassView
  - dsquery

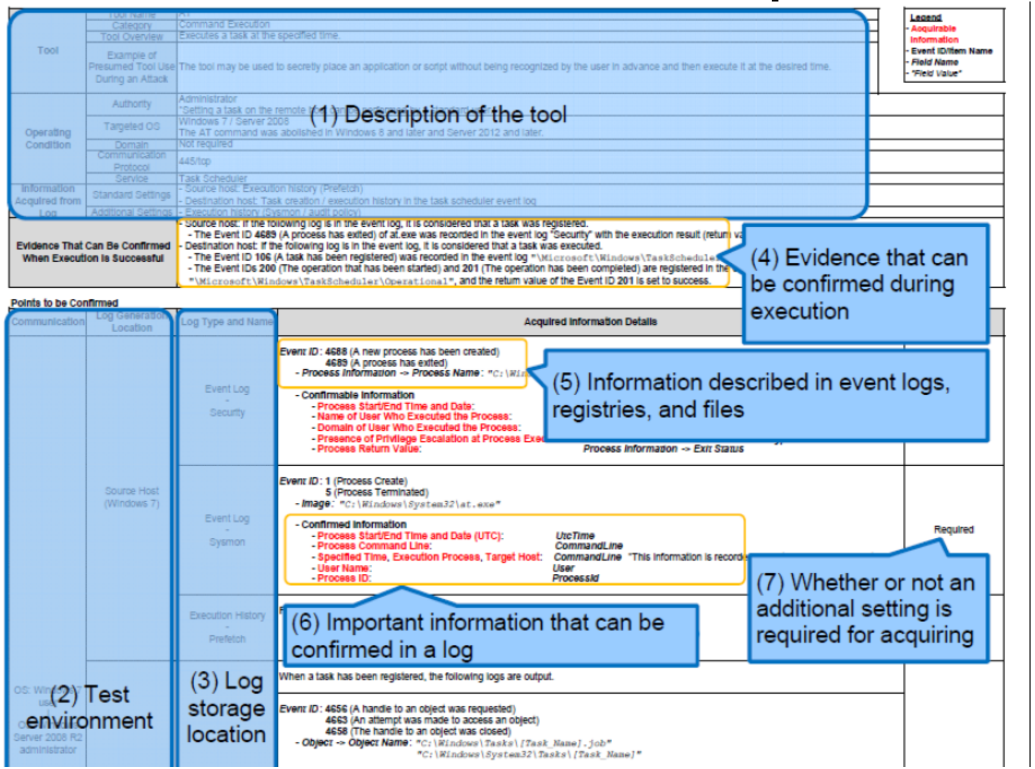
More Details About This Research

Released a research report.
“Detecting Lateral Movement through Tracking Event Logs”

- How to download.
  - https://www.jpcert.or.jp/english/pub/sr/ir_research.html

More Details About This Research

- Describes the 44 tools in this report.



Tool	Tool Name	AT
	Category	Command Execution
	Tool Overview	Executes a task at the specified time.
	Example of Presumed Tool Use During an Attack	The tool may be used to secretly place an application or script without being recognized by the user in advance and then execute it at the desired time.
Operating Condition	Authority	Administrator *Setting a task on the remote
	Targeted OS	Windows 7 / Server 2008 The AT command was abolished in Windows 8 and later and Server 2012 and later.
	Domain	Not required
	Communication Protocol	445/tcp
	Service	Task Scheduler
Information Acquired from Log	Standard Settings	- Source host: Execution history (Prefetch) - Destination host: Task creation / execution history in the task scheduler event log
	Additional Settings	- Execution history (Sysmon / audit policy)
Evidence That Can Be Confirmed When Execution Is Successful		- Source host: If the following log is in the event log, it is considered that a task was registered. - The Event ID 4689 (A process has exited) of at.exe was recorded in the event log "Security" with the execution result (return va - Destination host: If the following log is in the event log, it is considered that a task was executed. - The Event ID 106 (A task has been registered) was recorded in the event log "\Microsoft\Windows\TaskScheduler - The Event IDs 200 (The operation that has been started) and 201 (The operation has been completed) are registered in the "\Microsoft\Windows\TaskScheduler\Operational", and the return value of the Event ID 201 is set to success.

Legend
- Acquirable Information
- Event ID/Item Name
- Field Name
- "Field Value"

Points to be Confirmed

Communication	Log Generation Location	Log Type and Name	Acquired Information Details	
OS: Win[illegible] us[illegible] O[illegible] Server 2008 R2 administrator	Source Host (Windows 7)	Event Log - Security	*Event ID*: 4688 (A new process has been created) 4689 (A process has exited) - *Process Information -> Process Name*: "C:\Win - Confirmable Information - Process Start/End Time and Date: - Name of User Who Executed the Process: - Domain of User Who Executed the Process: - Presence of Privilege Escalation at Process Exe - Process Return Value: *Process Information -> Exit Status*	
		Event Log - Sysmon	*Event ID*: 1 (Process Create) 5 (Process Terminated) - *Image*: "C:\Windows\System32\at.exe" - Confirmed Information - Process Start/End Time and Date (UTC): *UtcTime* - Process Command Line: *CommandLine* - Specified Time, Execution Process, Target Host: *CommandLine* "This information is record - User Name: *User* - Process ID: *ProcessId*	Required
		Execution History - Prefetch		
			When a task has been registered, the following logs are output.	
			Event ID: 4656 (A handle to an object was requested) 4663 (An attempt was made to access an object) 4658 (The handle to an object was closed) - *Object -> Object Name*: "C:\Windows\Tasks\[Task_Name].job" "C:\Windows\System32\Tasks\[Task_Name]"	

(1) Description of the tool
(2) Test environment
(3) Log storage location
(4) Evidence that can be confirmed during execution
(5) Information described in event logs, registries, and files
(6) Important information that can be confirmed in a log
(7) Whether or not an additional setting is required for acquiring

Notes

- **The amount of logs increases** when the audit policy is enabled, and log rotation accelerates.

- When enabling the audit policy, consider **changing the maximum size of event logs to be stored**.

- The maximum size of event logs can be changed with **Event Viewer** or the **wevtutil** command.

Future Work

- This report will be updated.
  - Support Windows 10
  - Update Sysmon version 5
  - Add forensic architecture
    - USN Journal, AppCompatCache, UserAssist etc.
  - Add network architecture
    - Proxy, Firewall etc.
  - Add other attack tools

Conclusion

- Typically, limited set of tools and commands are used for Lateral Movement.

- Many attack tools can be detected with audit policy and Sysmon.

- Our report would be helpful if you are investigating APT incidents.

Thank you!

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