Detecting Lateral Movement through Tracking Event Logs

JPCERT Coordination Center
June 12, 2017

Table of Contents

1. Introduction

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.

2. Research Method

This chapter describes the method that was used for this research.

2.1. Approach

The research aims to provide basic information which is useful in log analysis by investigating evidence of tools used by many attackers. More specifically, this report aims to be a dictionary that can be used as a guide for effective log analysis by identifying which tools were used based on logs or which log is recorded when a certain tool is executed.

In this research, tools that are used by many attackers were investigated. The specific tools that JPCERT/CC knows are used by many attackers are described in the next section. The following log items were investigated so that persons who are not experts in incident investigation can analyze more easily:

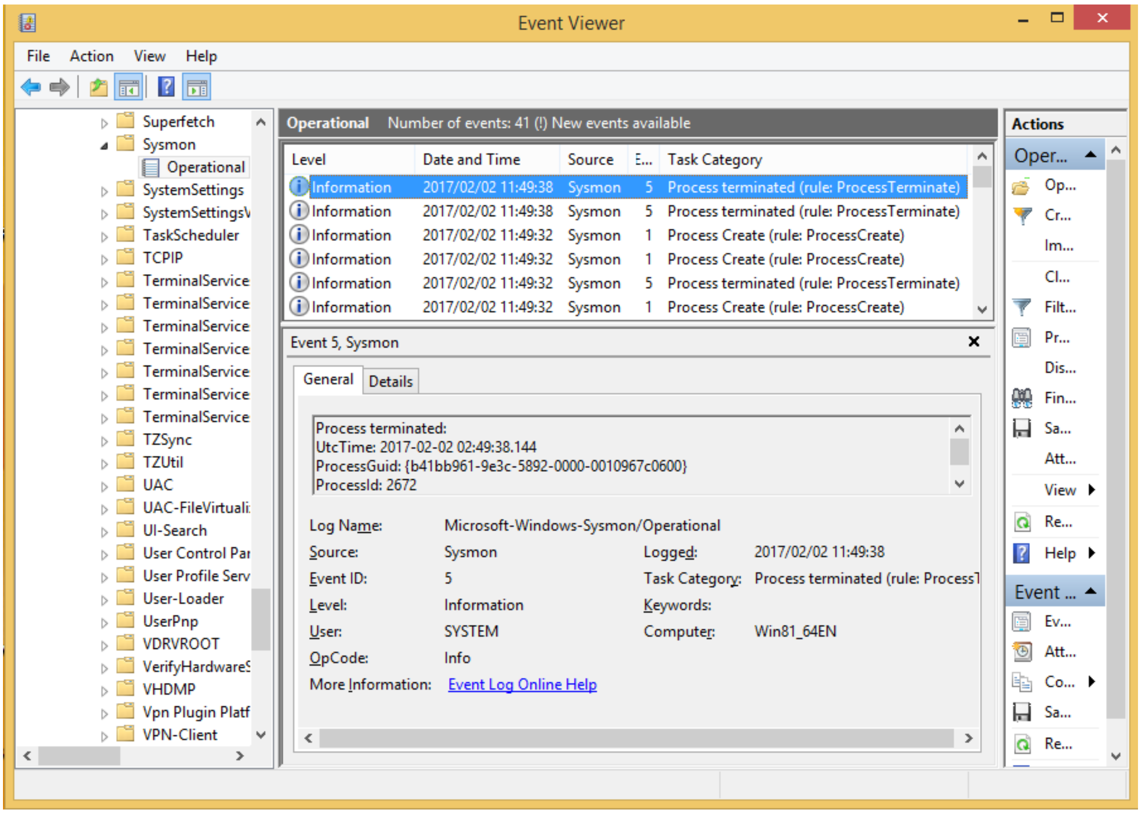
- Event log
- Execution history
- Registry entry

Note that a sufficient amount of event logs cannot be acquired with the default Windows settings. In this research, logs that are recorded with the default setting and the following setting were investigated:

- Enabling the audit policy
- Installing Sysmon

The audit policy is a default Windows setting for acquiring detailed logs about logon, logoff, file access, etc. The audit policy can be confirmed and its settings can be changed from the local group policy.

Sysmon is a tool provided by Microsoft that enables process startup, network communication, file changes, etc., to be recorded in event logs. Installing Sysmon enables recorded logs from Event Viewer to be checked as shown below.



Operational Number of events: 41 (!) New events available

Level	Date and Time	Source	E...	Task Category
Information	2017/02/02 11:49:38	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	2017/02/02 11:49:38	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	2017/02/02 11:49:32	Sysmon	1	Process Create (rule: ProcessCreate)
Information	2017/02/02 11:49:32	Sysmon	1	Process Create (rule: ProcessCreate)
Information	2017/02/02 11:49:32	Sysmon	5	Process terminated (rule: ProcessTerminate)
Information	2017/02/02 11:49:32	Sysmon	1	Process Create (rule: ProcessCreate)

Event 5, Sysmon

```
Process terminated:
UtcTime: 2017-02-02 02:49:38.144
ProcessGuid: {b41bb961-9e3c-5892-0000-0010967c0600}
ProcessId: 2672
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon Logged: 2017/02/02 11:49:38
Event ID: 5 Task Category: Process terminated (rule: ProcessT
Level: Information Keywords:
User: SYSTEM Computer: Win81_64EN
OpCode: Info
More Information: Event Log Online Help

Fig. 2-1: Checking Sysmon Logs from Event Viewer

In this research, the tools listed in Section 2.2 were actually executed on a virtual network made up of Windows Domain Controller and a client. By checking changes in the system before and after executing each tool, execution history, event logs, and registry entry records were collected and summarized in Chapter 3. The network environment used for this research are described in detail in Section 2.3.

2.2. Tested Tools

Among tools observed in multiple incidents that JPCERT/CC handled, 44 tools that are directly related to attack operations were selected as typical tools, such as command execution, obtaining password hash, and remote login. Table 2-1 shows these tools grouped by the attackers' purpose of use.

Table 2-1: List of Tested Tools

Attacker's Purpose of Using Tool	Tool	Chapter Number
Command execution	PsExec	3.2.1
	wmic	3.2.2
	PowerShell	3.2.3
	wmiexec.vbs	3.2.4

Attacker's Purpose of Using Tool	Tool	Chapter Number
	BeginX	3.2.5
	winrm	3.2.6
	at	3.2.7
	winrs	3.2.8
	BITS	3.2.9
Obtaining password hash	PWDump7	3.3.1
	PWDumpX	3.3.2
	Quarks PwDump	3.3.3
	Mimikatz (Obtaining password hash)	3.3.4
	Mimikatz (Obtaining ticket)	3.3.5
	WCE	3.3.6
	gsecdump	3.3.7
	lslsass	3.3.8
	Find-GPOPasswords.ps1	3.3.9
	Mail PassView	3.3.10
	WebBrowserPassView	3.3.11
	Remote Desktop PassView	3.3.12
Malicious communication relay (Packet tunneling)	Htran	3.4.1
	Fake wpad	3.4.2
Remote login	RDP	3.5.1
Pass-the-hash	WCE (Remote login)	3.6.1
Pass-the-ticket	Mimikatz (Remote login)	3.6.2
Escalation to SYSTEM privilege	MS14-058 Exploit	3.7.1
	MS15-078 Exploit	3.7.2
Privilege escalation	SDB UAC Bypass	3.8.1
Capturing domain administrator rights account	MS14-068 Exploit	3.9.1
	Golden Ticket (Mimikatz)	3.9.2
	Silver Ticket (Mimikatz)	3.9.3
Capturing Active Directory database (Creating a domain administrator user or adding it to an administrator group)	ntdsutil	3.10.1
	vssadmin	3.10.2
Adding or deleting a user group	net user	3.11.1
File sharing	net use	3.12.1
	net share	3.12.2
	icacls	3.12.3

Attacker's Purpose of Using Tool	Tool	Chapter Number
Deleting evidence	sdelete	3.13.1
	timestomp	3.13.2
Deleting event log	wevtutil	3.14.1
Obtaining account information	csvde	3.15.1
	ldifde	3.15.2
	dsquery	3.15.3

2.3. Research Environment

A simplified system with a pair of client and server, was built on a virtual network as a target. The selected tools were executed in the environment to observe changes to files and registries resulting from the execution. By installing the following Windows versions on the server and client, a total of four types of system configurations were tested. In each system configuration, Active Directory service was configured on the server to manage the client computer.

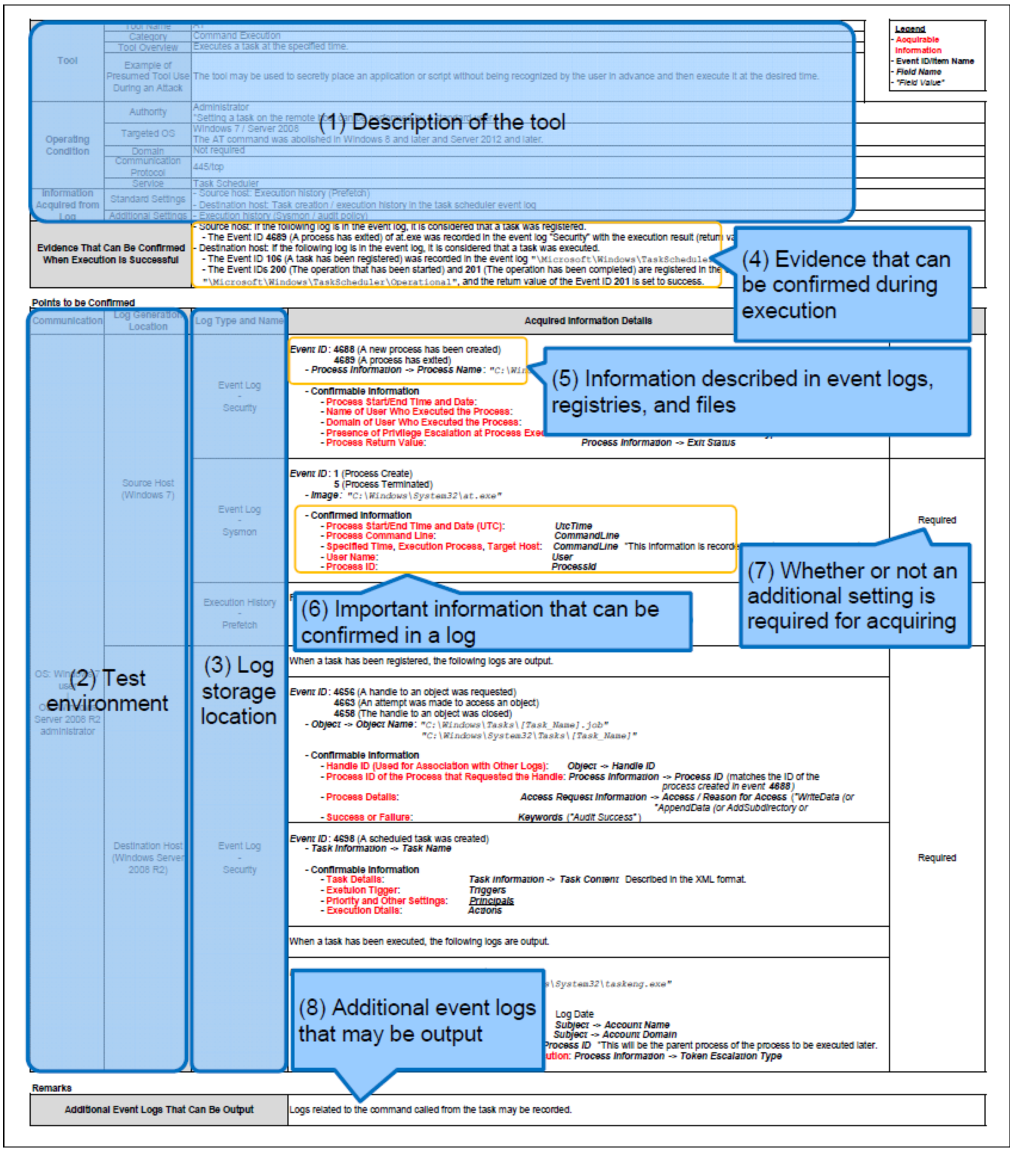
- OS installed on the client
  - Windows 7 Professional Service Pack 1
  - Windows 8.1 Pro
- OS installed on the server
  - Windows Server 2008 R2 Service Pack 1
  - Windows Server 2012 R2

3. Research Results

This chapter summarizes the basic information including functionality of the tools tested in this research and log information recorded when the relevant tools were executed. The attacker's perspective was also taken into account in the description of the basic information so that the significance of each tool in an attack sequence can be easily understood. This chapter also describes the details of logs that can be acquired when the settings described in section 2.1 are configured. (Note that how to set up the audit policy and how to install Sysmon are described in Chapter 7.)

3.1. Layout of This Chapter

The following describes the 44 tools using the table format shown below.



(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
(8) Additional event logs that may be output

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

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 host can be performed by a standard user."
	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\TaskSchedule - 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.

Points to be Confirmed

Communication	Log Generation Location	Log Type and Name	Acquired Information Details	
OS: Windows 7 user OS: Windows 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:\Wi - 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		
	Destination Host (Windows Server 2008 R2)	Event Log - Security	When a task has been registered, the following logs are output.	Required
			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]" - Confirmable Information - Handle ID (Used for Association with Other Logs): *Object -> Handle ID* - Process ID of the Process that Requested the Handle: *Process Information -> Process ID* (matches the ID of the process created in event **4688**) - Process Details: *Access Request Information -> Access / Reason for Access* ("WriteData (or "AppendData (or AddSubdirectory or - Success or Failure: *Keywords* ("Audit Success")	
			Event ID: **4698** (A scheduled task was created) - *Task Information -> Task Name* - Confirmable Information - Task Details: *Task Information -> Task Content* Described in the XML format. - Exetuion Tigger: *Triggers* - Priority and Other Settings: *Principals* - Execution Dtails: *Actions*	
			When a task has been executed, the following logs are output.	
			s\System32\taskeng.exe" Log Date *Subject -> Account Name* *Subject -> Account Domain* rocess ID "This will be the parent process of the process to be executed later. ution: *Process Information -> Token Escalation Type*	

Remarks

Additional Event Logs That Can Be Output	Logs related to the command called from the task may be recorded.

Fig. 3-1: Content of the Descriptions in the Subsequent Sections

The following describes the content described for each item.

(1) Description of the tool

- The impact from the use of the tool, privileges for using the tool, communication protocol, and related services are described.

(2) Test environment

- Information about the OS at the source host and destination host.

(3) Log storage location

- Storage location of registries and event logs.

(4) Evidence that can be confirmed when execution is successful

- The method to confirm successful execution of the tool.

(5) Information described in event logs, registries, and files

- If the record in an event log, registry, or file match the description in this item, it is likely that the record was made by executing the relevant tool and thus investigation is required.

(6) Important information that can be confirmed in a log

- Important information that can be used for the investigation of records in the targeted logs (This does not necessarily mean that all information that is recorded is described.)

(7) Whether or not an additional setting is required for acquiring the relevant log

- Indicated as "-" when the log can be obtained in the standard setting, or "Required" when an additional setting is needed.

(8) Additional event logs that may be output

- Any logs that may be additionally recorded.

3.2.1. PsExec

Basic Information

Tool	Tool Name	PsExec
	Category	Command Execution
	Tool Overview	Executes a process on a remote system
	Example of Presumed Tool Use During an Attack	The tool may be used to remotely execute a command on client and servers in a domain. - Source host: PsExec command execution source - Destination host: The destination logged in by the PsExec command
Operating Condition	Authority	- Source host: Standard user - Destination host: Administrator
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	135/tcp, 445/tcp, a random high port *When executing in a domain environment, communication for Kerberos authentication with the domain controller occurs.
	Service	-
Information Acquired from Log	Standard Settings	- Source host: A registry to the effect that the PsExec License Agreement has been entered is registered. - Destination host: The fact that the "PSEXESVC" service has been installed, started, and ended is recorded.
	Additional Settings	- Execution history (Sysmon/audit policy) - Source host: The fact that the PsExec process was executed and that connection was made to the destination via the network, as well as the command name and argument for a remotely executed command are recorded. - Destination host: The fact that the PSEXESVC's binary was created and accessed, and that connection was made from the source via the network, as well as the command name and argument for a remotely executed command are recorded.
Evidence That Can Be Confirmed When Execution is Successful		If the following is confirmed, it is possible that PsExec was executed. - Source host: If the following log is in the event log - The Event ID **4689** (A process has exited) of psexec.exe was recorded in the event log "Security" with the execution result (return value) of "0x0". - Destination host: PSEXESVC.exe is installed.

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**	**Additional Settings**
OS: Windows user ↓ OS: Windows administrator	Source Host	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[Execution File (psexec.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[Execution File (psexec.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *__The remotely executed command__ is recorded in the argument in the command line. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution history - Registry	Registry Entry: **`HKEY_USERS\[SID]\Software\Sysinternals\PsExec`** - ***EulaAccepted*** *If **PsExec** has not been executed in the past, the registry to the effect that the License Agreement has been entered is output. (If the service was executed in the past, the registry will remain unchanged.)	-
	Destination Host	Event Log - System	***Event ID*** : **7045** (A service was installed in the system) - **Confirmable Information** - **Process Name**: *"PSEXESVC"* - **Path**: *"`%SystemRoot%\PSEXESVC.exe`"*	-
			Event ID : **7036** (The service state has changed) *The *"PSEXESVC"* service enters the *"Executing"* state before executing a remote process, and enters the *"Stopped"* state after the execution.	
		Event Log - Security	***Event ID*** : **5156** (The Windows Filtering Platform has allowed a connection) *Communication occurs from the source host to the destination with destination ports 135 and 445. (Example: *The Windows Filtering Platform has allowed communication from 192.168.0.10:49210 to 192.168.0.2:* ***445***) *Communication occurs from the source host to the destination with a random high port (1024 and higher) as the destination port.	Required
			Event ID : **5140** (A network share object was accessed) - **Confirmable Information** - **Connection Date and Time**: Log Date *The date and time before the start of PSEXESVC.exe - **Account Used for Connection**: ***Subject*** -> ***Security ID*** and ***Account Name*** - **Source Host**: ***Network Information*** -> ***Source Address*** and ***Source Port*** - **Connected Share**: *"`\??\C:\Windows`"* (administrative share)	
			Event ID : **4672** (Special privileges assigned to new logon) *Before this event occurs, the event 4624 occurs. An account logged on when the event **4624** occurs is assigned privileges. - **Confirmable Information** - **Account Used for Connection**: ***Subject*** -> ***Security ID*** and ***Account Name*** - **Assigned Privileges**: ***Privileges***	
			Event ID : **4656** (A handle to an object was requested), **4663** (An attempt was made to access an object) - ***Object*** -> ***Object Name*** :*"`C:\Windows\PSEXESVC.exe`"*	
			Event ID : **5140** (A network share object was accessed) - **Confirmable Information** - **Account Used for Connection**: ***Subject*** -> ***Security ID*** and ***Account Name*** - **Source Host**: ***Network Information*** -> ***Source Address*** and ***Source Port*** - **Connected Share**: *"`\\*\IPC$`"* (administrative share)	
			Event ID : **5145** (A network share object was checked to see whether client can be granted desired access) *The Event ID is recorded several times. - **Confirmable Information** - **Account Used for Connection**: ***Subject*** -> ***Security ID*** and ***Account Name*** - **Source Host Machine**: ***Network Information*** -> ***Source Address*** and ***Source Port*** - **Targeted Share**: ***Share Information*** -> ***Share Path*** *The share path contains *"PSEXESVC"* and "`\\??\C:\Windows`".	

Communication	Log Generation Location	Log Type and Name	Acquired Information Details	Additional Settings
OS: Windows user ↓ OS: Windows administrator (Continued from the previous entry)	Destination Host (Continued from the previous entry)	Event Log - Security (Continued from the previous entry)"	***Event ID*** : **4656** (A handle to an object was requested) **4660** (An object was deleted) **4658** (The handle to an object was closed) - ***Process Information*** -> ***Process ID*** : *"0x4"* (SYSTEM) - **Confirmable Information** - **Targeted File**: ***Object*** -> ***Object Name*** (*"C:\Windows\PSEXESVC.exe"*) - **Handle ID**: ***Object*** -> ***Handle ID*** *This is used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** (*"DELETE", "ReadAttributes"*) - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	Required
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C:\Windows\PSEXESVC.exe"* - ***User*** : *"SYSTEM"* - **Confirmed Information** - **Date and Time PSEXESVC.exe was Executed**: Log Date	Required
			Event ID : **1** (Process Create) **5** (Process Terminated) - **Confirmable Information** - **Remotely Executed Process**: ***Image*** - **Argument**: ***CommandLine*** - **Process Start/End Date and Time (UTC)**: ***UtcTime*** *The date and time after the start of PSEXESVC.exe and before its end - **Account Used for Remote Execution**: ***User***	

Remarks

Additional Event Logs That Can Be Output	Information related to the process execution using **PsExec** may be recorded to the "Destination host".

3.2.2. WMIC (Windows Management Instrumentation Command Line)

Basic Information

Tool	Tool Name	WMIC (Windows Management Instrumentation Command Line)
	Category	Command execution
	Tool Overview	A tool used for Windows system management
	Example of Presumed Tool Use During an Attack	The tool is believed to be used to acquire information on the remote system or to execute a command with WMI. - Source host: wmic command execution source - Destination host: The host accessed by the wmic command
Operating Condition	Authority	Standard user *Depending on the command executed on the remote side, administrator privileges may be required.
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	135/tcp, 445/tcp, a randomly selected TCP port 1024 or higher
	Service	Windows Management Instrumentation, Remote Procedure Call (RPC)
Information Acquired from	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- Process execution details (the argument to wmic) and execution success or failure (the return value) (Sysmon and audit policy)
Evidence That Can Be Confirmed When Execution is Successful		If the following logs that have the same log time are found at "source host" and "destination host", it is possible that a remote connection was made. - Source host: If the following log is in the event log: - The event ID **4689** (A process has exited) of WMIC.exe was recorded in the event log "Security" with the execution result (return value) of "0x0". - Destination host: If the following log is in Sysmon: - It is recorded in the event log "Sysmon" that WmiPrvSE.exe was executed with the event IDs **1** and **5**.

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	Additional Settings
OS: Windows user ↓ OS: Windows administrator	Source Host	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\wbem\WMIC.exe"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C:\Windows\System32\wbem\WMIC.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *Based on the wmic.exe argument, the **remote host** and **executed command** can be confirmed. - **Executing user Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	File Name: **`C:\Windows\Prefetch\WMIC.EXE-98223A30.pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Executed Time***	-
	Destination Host	Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C:\Windows\System32\wbem\WmiPrvSE.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *("C:\Windows\System32\wmiprvse.exe -secured -Embedding")* - **User Name**: ***User*** *("NT AUTHORITY\NETWORK SERVICE")* - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	File Name: **`C:\Windows\Prefetch\WMIPRVSE.EXE-1628051C.pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	- Depending on the process called by wmic, the process-specific logs may be recorded. - If the user exists on the Active Directory, the authentication request may be recorded in the Domain Controller. However, it is not possible to determine whether such an authentication request was made by wmic or others.

3.2.3. PowerShell (Remote Command Execution)

Basic Information

Tool	Tool Name	PowerShell (Remote Command Execution)
	Category	Command Execution
	Tool Overview	A command line tool that can be used for Windows management and settings (it is available by default in Windows 7 or later) In addition to the host that executes PowerShell, this tool enables commands to be executed on other hosts via a network.
	Example of Presumed Tool Use During an Attack	The tool may be used to change settings to enable the Domain Controller and other hosts on the network to perform operations requiring administrator rights. - Source host: PowerShell command execution source - Destination host: The destination logged in by the PowerShell command
	Execution Example (with commands used for verification)	Execute the following commands *The Windows Remote Management (WS-Management) service needs to be started at the destination host. > Enable-PSRemoting -force > Set-Item `WSMan:\localhost\Client\TrustedHosts -Value *` > Enter-PSSession "[Destination Host]" -Credential Administrator
Operating Condition	Authority	PowerShell can be used by standard users. *To execute a script for changing settings, appropriate rights are needed on the host to change settings.
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	Not required to manage within local machines. *To manage other hosts, use 80/tcp or 5985/tcp for HTTP and 443/tcp or 5986/tcp for HTTPS.
	Service	Destination host: Windows Remote Management (WS-Management)
Information Acquired from Log	Standard Settings	Execution history (Prefetch)
	Additional Settings	Execution history (Sysmon, audit policy) *The end event of PowerShell allows execution results to be confirmed. With audit policy, it is possible to confirm the occurence of communication from the source host to the destination host 5985/tcp (HTTP) or 5986/tcp (HTTPS).
Evidence That Can Be Confirmed When Execution is Successful		If the following logs that have the same log time are found, it is possible that a remote command was executed. *This also applies to Prefetch. - Source host: If the following log is in the event log: - The event ID **4689** (A process has exited) of PowerShell was recorded in the event log "Security" with the execution result (return value) of "0x0". - Destination host: If the following log is in the event log: - The event ID **4689** (A process has exited) of wsmprovhost.exe was recorded in the event log "Security" with the execution result (return value) of "0x0".

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	Additional Settings
OS: Windows user ↓ OS: Windows administrator	Source Host	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\Windows PowerShell\v1.0\powershell.exe"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Process Name*** : *"\device\harddiskvolume2\windows\system32\windowspowershell\v1.0\powershell.exe"* - ***Network Information*** -> ***Direction*** : *"Outbound"* - ***Network Information*** -> ***Destination Address*** : *"::1"* - ***Network Information*** -> ***Destination Port / Protocol*** : *"47001" / "6" (TCP)*	
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Process Name*** : *"\device\harddiskvolume2\windows\system32\windowspowershell\v1.0\powershell.exe"* - ***Network Information*** -> ***Direction*** : *"Outbound"* - ***Network Information*** -> ***Destination Address*** : *"[Destination Host]"* ･***Network Information*** -> ***Destination Port / Protocol*** : *"5985"(HTTP) or "5986"(HTTPS) / "6"(TCP)* *A port number can be changed by specifying it on the destination host side.	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C:\Windows\System32\Windows PowerShell\v1.0\powershell.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** : *"C:\Windows\System32\Windows* - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	File Name: **`C:\Windows\Prefetch\POWERSHELL.EXE-920BBA2A.pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-
	Destination Host	Event Log - Security	***Event ID*** : **5156** (The Windows Filtering Platform has allowed a connection) - ***Process ID*** : *"4"* - ***Application Name*** : *"System"* - ***Network Information*** -> ***Direction*** : *"Inbound"* - **Confirmed Information** - **Source Host**: ***Network Information*** -> ***Source Address*** - **Incoming Call Port**: ***Network Information*** -> ***Source Port*** (*"5985"* for HTTP, *"5986"* for HTTPS) - **Protocol**: ***Network Information*** -> ***Protocol*** (*"6"*)	Required
			Event ID : **4624** (An account was successfully logged on) - ***Logon Type*** : *"3"* - **Confirmable Information** - **Date and Time of Successful Logon**: ***Log Date*** *The date immediately after the wsmprovhost.exe process was created (Event ID **4688**) and before it ended (Event ID **4689**). - **Name of Account That Executed the Process on the Destination Host**: ***New Logon*** -> ***Security ID / Account Name***	-
			Event ID : **4634** (An account was logged off) - **Confirmable Information** - **Date and Time of Logoff**: ***Log Date*** *The date after the end of the wsmprovhost.exe process (Event ID **4689**) at the source host.	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image:*** *"C:\Windows\System32\at.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine:*** *"C:\Windows\System32\wsmprovhost.exe -Embedding"* - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	File Name: **`C:\Windows\Prefetch\WSMPROVHOST.EXE-EF06207C.pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	Depending on the command that is executed, logs output by the command may be recorded at the destination host.

3.2.4. wmiexec.vbs

Basic Information

Tool	Tool Name	wmiexec.vbs
	Category	Command Execution
	Tool Overview	A tool used for Windows system management
	Example of Presumed Tool Use During an Attack	This tool executes a script for other hosts. - Source host: The source that executes wmiexec.vbs - Destination host: The machine accessed by the wmiexec.vbs
Operating Condition	Authority	Standard user
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	135/tcp, 445/tcp
	Service	-
Information Acquired from Log	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- File creation/delete history (Audit policy) - Execution history (Sysmon)
Evidence That Can Be Confirmed When Execution is Successful		Destination host: The "WMI_SHARE" share has been created and deleted.

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	Additional Settings
OS: Windows user ↓ OS: Windows user	Source Host	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\cscript.exe"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Process Name*** : *"\device\harddiskvolume2\windows\system32\cscript.exe"* - **Confirmable Information** - **Source Port**: ***Network Information*** -> ***Destination Port*** *A port number can be changed by specifying it on the destination.	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C:\Windows\System32\cscript.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	**File Name: C:\Windows\Prefetch\CSCRIPT.EXE-D1EF4768.pf** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-
	Destination Host	Event Log - Security	***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\Temp\wmi.dll)"* - ***Access Request Information*** -> ***Access / Reason for Access*** : ("WriteData (or AddFile)", "AppendData (or AddSubdirectory or CreatePipeInstance)") - **Confirmable Information** - **Process Name**: *"C:\Windows\System32\cmd.exe"* - **Handle ID**: ***Object*** -> ***Handle ID*** *This is used for association with other logs.	Required
			Event ID : **5142** (A network share object was added.) - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Share Name**: ***Share Information*** -> ***Share Name:*** *("\\*\WMI_SHARE")* - **Share Path**: ***Share Information*** -> ***Share Path:*** *("C:\Windows\Temp")*	
			Event ID : **5145** (A network share object was checked to see whether the client can be granted the desired access) - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Share Name**: ***Share Information*** -> ***Share Name*** (*"\\*\WMI_SHARE"*) - **Share Path**: ***Share Information*** -> ***Share Path*** (*"\??\C:\windows\temp"*) - **Share Path**: ***Share Information*** -> ***Relative Target Name:*** *("wmi.dll")*	
			Event ID : **4656** (A handle to an object was requested) **4660** (An object was deleted) **4658** (The handle to an object was closed) - ***Object*** -> ***Object Name*** : *"(C:\Windows\Temp\wmi.dll)"* - ***Access Request Information*** -> ***Access/Reason for Access*** : *"DELETE"* - **Confirmable Information** - **Process Name**: *"(C:\Windows\System32\cmd.exe)"*	
			Event ID : **5144** (A network share object was deleted.) - **Confirmable Information** - **Share Name**: ***Share Information*** -> ***Share Name*** *("\\*\WMI_SHARE")* - **Share Path**: ***Share Information*** -> ***Share Path:*** *("C:\Windows\Temp")*	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C:\Windows\System32\wbem\WmiPrvSE.exe"* *"C:\Windows\System32\cmd.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required

Communication	Log Generation Location	Log Type and Name	Acquired Information Details	Additional Settings
OS: Windows user ↓ OS: Windows user (Continued from the previous entry)	Destination Host (Continued from the previous entry)	Execution History - Prefetch	**File Name:** `C:\Windows\Prefetch\CSCRIPT.EXE-D1EF4768.pf` `C:\Windows\Prefetch\WMIPRVSE.EXE-1628051C.pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	-

3.2.5. BeginX

Basic Information

Tool	Tool Name	BeginX
	Category	Command Execution
	Tool Overview	Executes a remote command from a client to the server
	Example of Presumed Tool Use During an Attack	This tool is used to change settings on and acquire information from the remote host. - Source host: BeginX client execution source - Destination host: BeginX server execution source
	Reference	https://www.jpcert.or.jp/present/2015/20151028_codeblue_apt-en.pdf
Operating Condition	Authority	Standard user
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	TCP or UDP, and the port number varies depending on the tool.
	Service	-
Information Acquired from Log	Standard Settings	- Both hosts: Execution history (Prefetch) - Destination host: The Windows Firewall settings are changed.
	Additional Settings	- Both hosts: Execution history (Sysmon / audit policy) The fact that communication via a specified port occurred is recorded.
Evidence That Can Be Confirmed When Execution is Successful		- Source host: The fact that communication via a permitted port occurred unintentionally at the destination host is recorded. - Destination host: Unintended communication is permitted for Windows Firewall, and a tool that is listening at the relevant port exists.

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**	**Additional Settings**
OS: Windows user ↓ OS: Windows user	Source host	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	-
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Name*** : *"[File Name]"* - **Confirmable Information** - **Communication Direction**: ***Network Information*** -> ***Direction*** (*"Outbound"*) - **Source Port**: ***Network Information*** -> ***Source Port*** - **Destination Host**: ***Network Information*** -> ***Destination Address*** (the host with a tool name specified during execution) - **Destination Port**: ***Network Information*** -> ***Destination Port*** / ***Protocol***	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *Recorded in Event ID 1. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	File name: `C:\Windows\Prefetch\[File Name]-[RANDOM].pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-
	Destination host	Event Log - Security	The following is recorded immediately after the tool is executed.	-
			Event ID : **5154** (The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections) - ***Application Name*** : *"[File Name]"* - **Confirmable Information** - **Source Port**: ***Network Information*** -> ***Source Port*** - **Protocol to Use**: ***Network Information*** -> ***Protocol***	
			Event ID : **5447** (A Windows Filtering Platform filter has been changed) * Reflection of changes in the firewall settings. **4946** (A change has been made to Windows Firewall exception list. A rule was added) * Reflection of changes in the firewall	
			When the source host executes a command, the following is recorded.	
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Name*** : *"[File Name]"* - **Confirmable Information** - **Communication Direction**: ***Network Information*** -> ***Direction*** (*"Inbound"*) - **Source Port**: ***Network Information*** -> ***Source Port*** - **Destination Host**: ***Network Information*** -> ***Destination Address*** (the remote source host) - **Destination Port**: ***Network Information*** -> ***Destination Port*** / ***Protocol***	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name]","netsh.exe","rundll32.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *The details of the process that was executed are described for each ***Image*** . - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	File name: `C:\Windows\Prefetch\CMD.EXE-4A81B364.pf` `C:\Windows\Prefetch\[File Name]-[RANDOM].pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-
		Execution History - Registry	Registry Entry: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules` *The Windows Firewall settings are changed when a tool is executed, and accordingly, the registry value is changed. The executable file name of a tool is included in the rule.	-

Remarks

Additional Event Logs That Can Be Output	-

3.2.6. WinRM

Basic Information

Tool	Tool Name	WinRM
	Category	Command Execution
	Tool Overview	Executes a command on a remote host
	Example of Presumed Tool Use During an Attack	This tool is used for an investigation before executing a remote command. - Source host: WinRM command execution source - Destination host: The machine accessed by the WinRM command
Operating Condition	Authority	Administrator
	Targeted OS	Windows
	Domain	-
	Communication Protocol	5985/tcp (HTTP) or 5986/tcp (HTTPS)
	Service	Destination host: Windows Remote Management (WS-Management)
Information Acquired from Log	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- Source host: Execution history (Sysmon / audit policy) - Destination host: Connection from the source host
Evidence That Can Be Confirmed When Execution is Successful		- Source host: If the following log exists, it is possible that WinRM was executed. - A log indicating that cscript.exe accessed the destination host with **Event IDs 1** and **5** of the event log "Sysmon" is recorded.

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	Additional Settings
OS: Windows administrator ↓ OS: Windows administrator	Source host	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\cscript.exe"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Name*** : *"\device\harddiskvolume2\windows\system32\cscript.exe"* - **Confirmable Information** - **Communication Direction**: ***Direction*** (*"Outbound"*) - **Destination Host**: ***Network Information*** -> ***Destination Address*** - **Destination Port**: ***Destination Port*** (*"5958"(HTTP) or "5986"(HTTPS)*), ***Protocol*** (*"6"* = TCP)	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C:\Windows\System32\cscript.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Specified Time**, **Execution Process**, **Target Host**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Event Log - Application and Service Microsoft\Windows \Windows Remote Management	***Event ID*** : **166** (The chosen authentication mechanism is Negotiate) - **Confirmable Information** - **Authentication Method**: ***Authentication Mechanism*** (*the selected authentication mechanism is Kerberos*)	-
			Event ID : **80** (Sending the request for operation Get to destination host and port) - **Confirmable Information** - **Send Destination Computer and Port**: *"[Host Name]:[Port]"*	
			Event ID : **143** (Received the response from Network layer) - **Confirmable Information** - **Status**: ***Status*** (*200 (HTTP_STATUS_OK)*)	
			Event ID : **132** (WSMan operation Identify completed successfully) - **Confirmable Information** - **Completion Time and Date (UTC)**: ***UtcTime***	
		Execution History - Prefetch	**File name**: ***C:\Windows\Prefetch\CSCRIPT.EXE-D1EF4768.pf*** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-
	Destination host	Event Log - Security	***Event ID*** : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"SYSTEM"* - ***Network Information*** -> ***Direction*** : *"Inbound"* - ***Network Information*** -> ***Source Port*** : *"5985"* (HTTP) or *"5986"* (HTTPS) - ***Network Information*** -> ***Protocol*** : *"6"* (TCP) - **Confirmable Information** - **Source Host**: ***Network Information*** -> ***Destination Address*** - **Source Port**: ***Network Information*** -> ***Destination Port***	Required
			Event ID : **4624** (An account was successfully logged on) - ***Logon Type*** : *"3"* - **Confirmable Information** - **Used Security ID**: ***New Logon*** -> ***Security ID*** - **Logon ID**: ***Subject*** -> ***Logon ID*** - **Account**: ***Account Name*** - ***Account Domain***	
			Event ID : **4656** (A handle to an object was requested) **4658** (The handle to an object was closed) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\svchost.exe"* - ***Object*** -> ***Object Name*** : *"\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN\Client"* - ***Object*** -> ***Object Name*** : *"\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WSMAN\Service"* - **Confirmable Information** - **Handle ID**: ***Object*** -> ***Handle ID*** - **Access Request Details**: ***Access Request Information*** -> ***Access*** ("READ_CONTROL", "Query key value", "Enumerate sub-keys", "Notify about changes to keys") *This process is performed multiple times.	

Communication	Log Generation Location	Log Type and Name	Acquired Information Details	Additional Settings
OS: Windows administrator ↓ OS: Windows administrator (Continued from the previous entry)	Active Directory Domain Controller	Event Log - Security	***Event ID*** : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"\device\harddiskvolume2\windows\system32\lsass.exe"* - ***Network Information*** -> ***Direction*** : *"Inbound"* - ***Network Information*** -> ***Source Port*** : *"88"* - **Confirmable Information** - **Source Host**: ***Network Information*** -> ***Destination Address***	Required
			Event ID : **4769** (A Kerberos service ticket was requested) - ***Network Information*** -> ***Client Address*** : *"[Source Host]"* - **Confirmable Information** - **Used User**: ***Account Information*** -> ***Account Name***	

Remarks

Additional Event Logs That Can Be Output	-

3.2.7. WinRS

Basic Information

Tool	Tool Name	WinRS
	Category	Command Execution
	Tool Overview	Executes a command on a remote host
	Example of Presumed Tool Use During an Attack	This tool is sent by the BITS, etc. and remotely executed using winrs. - Source host: WinRS command execution source - Destination host: The machine accessed by the WinRS command
Operating Condition	Authority	- Source host: Standard user - Destination host: Administrator
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	5985/tcp (HTTP) or 5986/tcp (HTTPS)
	Service	Destination host: Windows Remote Management (WS-Management)
Information Acquired from Log	Standard Settings	- WinRM execution log - Execution history (Prefetch)
	Additional Settings	- Execution history (Sysmon / audit policy) - Recording of communication via Windows Filtering Platform
Evidence That Can Be Confirmed When Execution is Successful		- The execution of WinRS is recorded in the event log "`Application and Service\Microsoft\Windows\Windows Remote Management\Operational`".

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	Additional Settings
OS: Windows standard user ↓ OS: Windows administrator	Source host	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"`C:\Windows\System32\winrs.exe`"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **4648** (A logon was attempted using explicit credentials) - ***Process Information*** -> ***Process Name*** : *"`C:\Windows\System32\winrs.exe`"* - **Confirmable Information** - **Account Used**: ***Account for which a Credential was Used*** -> ***Account Name*** - ***Account Domain*** - **Destination Host**: ***Target Server*** -> ***Target Server Name*** - **Protocol Used**: ***Target Server*** -> ***Additional Information*** (*"[Protocol]/[Target Server Name]"*)	
			- ***Event ID*** : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"`\device\harddiskvolume2\windoows\system32\winrs.exe`"* - ***Network Information*** -> ***Direction*** : *"Outbound"* - ***Network Information*** -> ***Destination Port*** : *"5985"* (HTTP) or *"5986"* (HTTPS) - ***Network Information*** -> ***Protocol*** : *"6"* (TCP) - **Confirmable Information** - **Destination Host**: ***Network Information*** -> ***Destination Address***	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"`C:\Windows\System32\winrs.exe`"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** ***Destination Host**, **Account Used**, **Command Executed**, etc. are recorded. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Event Log - Application and Service `Microsoft\Windows\Windows Remote Management\Operational`	That fact that WinRS was executed is recorded.	-
			Event ID : **80** (Processing of a request) - **Confirmable Information** - **Destination Host**: ***Details Tab*** -> ***`EventData\url`*** - **Destination Port**: ***Details Tab*** -> ***`EventData\port`***	
		Execution History - Prefetch	**File name**: **`C:\Windows\Prefetch\WINRS.EXE-483CEB0F.pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-
	Destination host	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"`C:\Windows\System32\winrshost.exe`"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[Command Specified by Source Host]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"System"* - ***Network Information*** -> ***Direction*** : *"Inbound"* - ***Network Information*** -> ***Source Port*** : *"5985"* (HTTP) or *"5986"* (HTTPS) - ***Network Information*** -> ***Protocol*** : *"6"* (TCP) - **Confirmable Information** - **Source Host**: ***Network Information*** -> ***Destination Address***	

Communication	Log Generation Location	Log Type and Name	Acquired Information Details	Additional Settings
OS: Windows standard user ↓ OS: Windows administrator (Continued from the previous entry)	Destination host (Continued from the previous entry)	Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C:\Windows\System32\winrshost.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
			Event ID : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[Command Specified by Source Host]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	
		Event Log - Application and Service \Microsoft\Windows \Windows Remote	The fact that the WinRS process corresponding to the log at the source host was executed is recorded.	-
			Event ID : **81** (Sending the request for operation Get to destination host and port)	
		Execution History - Prefetch	**File name**: **`C:\Windows\Prefetch\WINRSHOST.EXE-ECE7169D.pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	Logs by a command execution via WinRS may be recorded.

3.2.8. AT Command

Basic Information

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. - Source host: at command execution source - Destination host: The machine for which a task was registered by the AT command
Operating Condition	Authority	Administrator *Setting a task on the remote host can be performed by a standard user.
	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 value) of "0x0". - 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\Operational"`. - The Event IDs **200** (The operation that has been started) and **201** (The operation has been completed) are registered in the event log `"\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	Additional Settings
OS: Windows 7 user ↓ OS: Windows 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:\Windows\System32\at.exe"`* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *`"C:\Windows\System32\at.exe"`* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **Specified Time**, **Execution Process**, **Target Host**: ***CommandLine*** *This information is recorded when the process is executed for the remote host. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	**File name**: **`C:\Windows\Prefetch\AT.EXE-BB02E639.pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-
	Destination host (Windows Server 2008 R2)	Event log - Security	When a task has been registered, the following logs are output.	Required
			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]`* - **Confirmable Information** - **Handle ID (Used for Association with Other Logs)**: ***Object*** -> ***Handle ID*** - **Process ID of the Process that Requested the Handle**: ***Process Information*** -> ***Process ID*** (matches the ID of the *process created in event 4688)* - **Process Details**: ***Access Request Information*** -> ***Access / Reason for Access*** (*"WriteData (or AddFile)" "AppendData (or AddSubdirectory or CreatePipeInstance)")* - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	
			Event ID : **4698** (A scheduled task was created) - ***Task Information*** -> ***Task Name*** - **Confirmable Information** - **Task Details**: ***Task Information*** -> ***Task Content*** Described in the XML format. - **Execution Trigger**: ***Triggers*** - **Priority and Other Settings**: ***Principals*** - **Execution Details**: ***Actions***	
			When a task has been executed, the following logs are output.	
			Event ID : **4688** (A new process has been created) - ***Process Information*** -> ***Process Name*** : *`"C:\Windows\System32\taskeng.exe"`* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Process ID**: ***Process Information*** -> ***New Process ID*** **This will be the parent process of the process to be executed later.* - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type***	
			Event ID : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : Process Executed by the Task - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Process ID** : ***Process Information*** -> ***New Process ID*** *If another child process is executed in the task, this process becomes the parent process. - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Parent Process ID**: ***Process Information*** -> ***Creator Process ID*** *taskeng.exe, which was *executed first, is the parent process.* - **Process Return Value**: ***Process Information*** -> ***Exit Status***	

Communication	Log Generation Location	Log Type and Name	Acquired Information Details	Additional Settings
OS: Windows 7 user ↓ OS: Windows Server 2008 R2 administrator (Continued from the previous entry)	Destination host (Windows Server 2008 R2) (Continued from the previous entry)	Event log - Security (Continued from the previous entry)	***Event ID*** : **4656** (A handle to an object was requested) **4663** (An attempt was made to access an object) - ***Object*** -> ***Object Name*** : *"C:\Windows\Tasks\[Task Name].job"* - ***Access Request Information*** -> ***Access*** / ***Reason for Access*** : *"WriteData (or AddFile)" / "AppendData (or AddSubdirectory or CreatePipeInstance)"* - **Confirmable Information** - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs.	Required
		Event Log - Sysmon	With respect to task registration, no beneficial information is output. When a task has been executed, the following logs are registered.	Required
			Event ID : **1** (Process Create) **5** (Process Terminated) - ***ParentImage*** **Name**: *"C:\Windows\System32\taskeng.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *The execution process and argument are recorded. - **Process ID**: ***ProcessId*** **This can be used for investigating the execution and access history of a* executed by	
		Event Log - Application and Service Log \Microsoft\Windows\TaskScheduler\Operational	When a task has been registered, the following logs are output.	-
			Event ID : **106** (A task has been registered) - **Confirmable Information** - **User Who Registered the Task**: ***Details Tab*** -> ***EventData\UserContext*** - **Task Name**: ***Details Tab*** -> ***EventData\TaskName***	
			When a task has been executed, the following logs are output.	
			Event ID : **200** (The operation that has been started) - **Confirmable Information** - **Task Name**: ***Details Tab*** -> ***EventData\TaskName*** - **Command that was Executed**: ***Details Tab*** -> ***EventData\ActionName*** - **Task Instance ID**: ***Details Tab*** -> ***EventData\TaskInstanceId***	
			Event ID : **129** (A task process has been created) - ***Details Tab*** -> ***EventData\TaskName*** matches ***TaskName*** output to the start event (Event ID **200**). - **Confirmable Information** - **Process that was Executed**: ***Details Tab*** -> ***EventData\Path*** - **Process ID**: ***Details Tab*** -> ***EventData\ProcessID*** *This can be used for investigating the execution history and access history of a process executed	
			Event ID : **201** (The operation has been completed) - ***Details Tab*** -> ***EventData\InstanceId*** matches ***TaskInstanceId*** output to the start event (Event ID **200**). - **Confirmable Information** - **Task Name**: ***Details Tab*** -> ***EventData\TaskName*** - **Command that was Executed**: ***Details Tab*** -> ***EventData\TaskActionName*** - **Execution Results (Return Value)**: ***Details Tab*** -> ***EventData\ResultCode*** *The meaning of a return value varies depending on the process that is executed.	

Remarks

Additional Event Logs That Can Be Output	Logs related to the command called from the task may be recorded.

3.2.9. BITS

Basic Information

Tool	Tool Name	BITS
	Category	Command Execution
	Tool Overview	Sends and receives files in background (the priority, etc. for sending and receiving files can be set)
	Example of Presumed Tool Use During an Attack	This tool is used to send or receive files at a bandwidth that is less noticeable than other communications. - Source host: The machine that sends and receives files by BITS - Destination host: File transmission destination
Operating Condition	Authority	Standard user
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	445/tcp
	Service	Background Intelligent Transfer Service
Information Acquired from Log	Standard Settings	- Source host: It is possible that the use of BITS can be determined based on a change in the execution status of the Background Intelligent Transfer Service. *However, it is not possible when BITS is already running. - Destination host: No beneficial information is recorded.
	Additional Settings	- Source host: Writing to the temporary file created by BITS *"BITF[Random Number].tmp"* is recorded. - Destination host: No beneficial information is recorded.
Evidence That Can Be Confirmed When Execution is Successful		If the following log is in the event log, it is considered that a file was transferred. - The event ID: **60** is recorded in the event log `"Application and Service Log\Microsoft\Windows\Bits-Client"`, and the status code is set to "0x0".

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	Additional Settings
OS: Windows user ↓ OS: Windows user	Source host	Event Log - Security	***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*** : *"[Path to Created File]\BITF[Random Number].tmp"* *Since a temporary file with a name starting with "BITF" is created, it is confirmed that a file transfer by BITS - **Confirmable Information** - **Handle ID (Used for Association with Other Logs)**: ***Object*** -> ***Handle ID*** - **Process ID of the Process that Requested the Handle**: ***Process Information*** -> ***Process ID*** (matches the ID of the process created in event 4688) - **Process Details**: ***Access Request Information*** -> ***Access*** / ***Reason for Access*** (*"WriteData (or AddFile)" / "AppendData (or AddSubdirectory or CreatePipeInstance)" / "DELETE")* - **Success or Failure**: ***Keywords*** ("Audit Success")	Required
		Event Log - Sysmon	***Event ID*** : **2** (File creation time changed) - ***Image Name*** : *"C:\Windows\system32\svchost.exe"* - **Confirmable Information** - **Temporary File for which Time Stamp was Changed**: *"[Path to Created File]\BITF[Random Number].tmp"*	Required
		Event Log - System	***Event ID*** : **7036** (The [Service Name] service entered the [Status] state) - ***Details Tab*** -> ***System\Provider\Name*** is set to *"Service Control Manager"* . - ***Details Tab*** -> ***EventData\param1*** is set to *"Background Intelligent Transfer Service"* . - **Confirmable Information** - **Executing the Service**: ***Details Tab*** -> ***EventData\param2*** (*"Executing"*) - **Remarks** - If a process that uses BITS has been executed after the last startup of the machine, logs may not be output (For example, when BITS is used by Windows Update, logs may not be output after a file is downloaded by Windows Update).	-
		Event Log - Application and Service Log `\Microsoft\Windows\Bits-Client`	***Event ID*** : **60** - **Confirmable Information** - **Targeted File**: ***Details Tab*** -> ***ventData\url*** - **Success or Failure**: ***General Tab*** -> ***Status Code***	-
		Execution History - Registry	**Registry Entry**: **`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\BITS`** - **Confirmable Information** - **Service State**: ***StateIndex*** - **Remarks** - The value changes as a result of the BITS status changing to "Executing". - If BITS is already in the executing status when the command is executed, the value does not change.	-
	Destination host	Event Log - Security	***Event ID*** : **5145** (A network share object was checked to see whether client can be granted desired access) - ***Network Information*** -> ***Source Address*** : *"[Source Host]"* - ***Network Information*** -> ***Source Address*** : *"[Source Port]"* - **Confirmable Information** - **Share Name**: ***Shared Information*** -> ***Share Name*** - **Share Path**: ***Shared Information*** -> ***Share Path*** - **Placed File Name**: ***Shared Information*** -> ***Relative Target Name***	Required

Remarks

Additional Event Logs That Can Be Output	- If an audit of object reading is conducted, reading of transferred files may be recorded.

3.3.1. PwDump7

Basic Information

Tool	Tool Name	PwDump7
	Category	Password and Hash Dump
	Tool Overview	Displays a list of password hashes in the system
	Example of Presumed Tool Use During an Attack	This tool is used to perform logon authentication on other hosts using the acquired hash information.
Operating Condition	Authority	Administrator
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	-
	Service	-
Information Acquired from	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- Execution history (Sysmon / audit policy)
Evidence That Can Be Confirmed When Execution is Successful		The successful execution of the tool cannot be determined from event logs or execution history.

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	Additional Settings
-	Host (Windows)	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name (PwDump7.exe)]"* - **Points to be Confirmed** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (PwDump7.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *The used option is recorded as an argument. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	File name: `C:\Windows\Prefetch\[Executable File(PWDUMP7.EXE)]-[RANDOM].pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	-

3.3.2. PWDumpX

Basic Information

Tool	Tool Name	PWDumpX
	Category	Password and Hash Dump
	Tool Overview	Acquires a password hash from a remote host
	Example of Presumed Tool Use During an Attack	This tool uses the acquired hash to perform attacks such as pass-the-hash. - Source host: PWDumpX execution source - Destination host: The destination logged in by PWDumpX
Operating Condition	Authority	- Source host: Standard user - Destination host: Administrator
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	135/tcp, 445/tcp
	Service	-
Information Acquired from Log	Standard Settings	- Both hosts: Execution history (Prefetch) - Destination host: The fact that the PWDumpX service has been installed and executed is recorded.
	Additional Settings	- The fact that the PWDumpX service has been sent from the source host to the destination host and then executed is recorded. - The fact that a text file is used to create and receive hash information is recorded.
Evidence That Can Be Confirmed When Execution is Successful		- Source host: If "[Path to Tool]\[Destination Address]-PWHashes.txt" has been created, it is considered that it was successfully executed.

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	Additional Settings
OS: Windows user ↓ OS: Windows administrator	Source host	Event Log - Security	Event ID : 4688 (A new process has been created) 4689 (A process has exited) - Process Information -> Process Name : " [File Name (PWDumpX.exe)]" - Confirmable Information - Process Start/End Time and Date: Log Date - Name of User Who Executed the Process: Subject -> Account Name - Domain of User Who Executed the Process: Subject -> Account Domain - Presence of Privilege Escalation at Process Execution: Process Information -> Token Escalation Type - Process Return Value: Process Information -> Exit Status	Required
			A temporary file is created.	
			Event ID : 4663 (An attempt was made to access an object) - Process Information -> Process Name : " [File Name (PWDumpX.exe)]" - Object -> Object Name : "[Path to Tool]\[Destination Address]-PWHashes.txt" *Data is written to the above file multiple times.	
			Event ID : 4663 (An attempt was made to access an object) - Process Information -> Process Name : " [File Name (PWDumpX.exe)]" - Object -> Object Name : "[Path to Tool]\[Destination Address]-PWHashes.txt.Obfuscated" - Confirmable Information - Handle ID: Object -> Handle ID *Used for association with other logs. *Data is written to the above file multiple times.	
			The temporary file is deleted.	
			Event ID : 4663 (An attempt was made to access an object) - Process Information -> Process Name : " [File Name (PWDumpX.exe)]" - Object -> Object Name : "[Path to Tool]\[Destination Address]-PWHashes.txt.Obfuscated" - Confirmable Information - Handle ID: Object -> Handle ID *Used for association with other logs. - Process Details: Access Request Information -> Access ("DELETE")	
		Event Log - Sysmon	Event ID : 1 (Process Create) 5 (Process Terminated) - Image: " [File Name (PWDumpX.exe)]" - Confirmable Information - Process Start/End Time and Date (UTC): UtcTime - Process Command Line: CommandLine *The destination host or used account is taken as an argument. - User Name: User - Process ID: ProcessId	Required
		Execution History - Prefetch	File name: C:\Windows\Prefetch\[File Name (PWDUMPX.EXE)]-[File Name].pf - Confirmable Information (the following can be confirmed using this tool: WinPrefetchView) - Last Execution Time and Date: Last Execution Time	-
	Destination host	Event Log - Security	Event ID : 4688 (A new process has been created) 4689 (A process has exited) - Process Information -> Process Name : "[File Name (DumpSvc.exe)]" - Confirmable Information - Process Start/End Time and Date: Log Date - Name of User Who Executed the Process: Subject -> Account Name - Domain of User Who Executed the Process: Subject -> Account Domain - Presence of Privilege Escalation at Process Execution: Process Information -> Token Escalation Type - Process Return Value: Process Information -> Exit Status	Required
			Event ID : 5145 (A network share object was checked to see whether client can be granted desired access) - Network Information -> Source Address : "[Source host]" - Shared Information -> Share Name : "\\*\ADMIN$" - Shared Information -> Relative Target Name : "system32\DumpSvc.exe"/"system32\DumpExt.dll"	
			Event ID : 4663 (An attempt was made to access an object) - Process Information -> Process Name : "C:\Windows\System32\lsass.exe" - Object -> Object Name : "C:\Windows\System32\PWHashes.txt" "C:\Windows\System32\PWHashes.txt.Obfuscated" - Confirmable Information - Handle ID (Used for Association with Other Logs): Object -> Handle ID *Data is written to the above file multiple times.	

Communication	Log Generation Location	Log Type and Name	Acquired Information Details	Additional Settings
OS: Windows user ↓ OS: Windows administrator (Continued from the previous entry)	Destination host (Continued from the previous entry)	Event Log - Security (Continued from the previous entry)	***Event ID*** : **4663** (An attempt was made to access an object) - ***Process Information*** -> ***Process Name*** : *`"C:\Windows\System32\lsass.exe"`* - ***Object*** -> ***Object Name*** : *`"C:\Windows\System32\PWHashes.txt.Obfuscated"/"C:\Windows\System32\PWHashes.txt"`* *`"C:\Windows\System32\DumpExt.dll"/"C:\Windows\System32\DumpSvc.exe"`* - **Confirmable Information** - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** (*"DELETE"*)	Required
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *`"C:\Windows\System32\DumpSvc.exe"`* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
			Event ID : **8** (CreateRemoteThread detected:) - ***Image*** : *`"C:\Windows\System32\DumpSvc.exe"`* - ***TargetImage*** : *`"C:\Windows\System32\lsass.exe"`*	
		Event Log - System	***Event ID*** : **7045** (A service was installed in the system) - ***Service Name*** : (*"PWDumpX Service"*) - ***Service File Name*** : (*`"%windir%\system32\DumpSvc.exe"`*)	-
			Event ID : **7036** (The [Service Name] service entered the [Status] state) - ***Service Name*** : (*"PWDumpX Service"*) * The *"PWDumpX Service"* service enters the *"Executing"* state before executing a remote process, and enters the "Stopped" state after the execution.	
		Execution History Prefetch	**File name**: **`C:\Windows\Prefetch\DUMPSVC.EXE-DB3A90FA.pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	-

3.3.3. Quarks PwDump

Basic Information

Tool	Tool Name	Quarks PwDump
	Category	Password and Hash Dump
	Tool Overview	Acquires the NTLM hash of a local domain account and cached domain password. Information in a machine including NTDS.DIT files can be specified and analysed.
	Example of Presumed Tool Use During an Attack	This tool is used to perform logon authentication on other hosts using the acquired hash information.
Operating Condition	Authority	Administrator
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	-
	Service	-
Information Acquired from Log	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- Execution history (Sysmon / audit policy) - A record that the temporary file (*"SAM-[Random Number].dmp"*) has been created
Evidence That Can Be Confirmed When Execution is Successful		- A temporary file (*"SAM-[Random Number].dmp")* was created and deleted.

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	Additional Settings
-	Host (Windows)	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name (QuarksPwDump.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status*** *"0x0" if successful, or another value if failed.	Required
			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) - ***Process Information*** -> ***Process Name*** : *"[File Name (QuarksPwDump.exe)]"* - **Confirmable Information** - **Targeted File**: ***Object*** -> ***Object Name*** (`"C:\Users\[User Name]\AppData\Local\Temp\SAM-[Random Number].dmp"`) - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** (*"WriteData (or AddFile)"*)	
			Event ID : **4656** (A handle to an object was requested) **4660** (An object was deleted) **4658** (The handle to an object was closed) - ***Process Information*** -> ***Process Name*** : *"[File Name (QuarksPwDump.exe)]"* - ***Process Information*** -> ***Process ID*** : *"[Process ID of the Tool]"* - ***Object*** -> ***Object Name*** : `"C:\Users\[User Name]\AppData\Local\Temp\SAM-[Random Number].dmp"` - **Confirmable Information** - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Requested Process**: ***Access Request Information*** -> ***Access*** / ***Reason for Access*** (*"DELETE"*) - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (QuarksPwDump.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *The specified option (**the type of the acquired password**) is recorded as an argument. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	**File name**: `C:\Windows\Prefetch\[File Name (QUARKSPWDUMP.EXE)]-[RANDOM].pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	-

3.3.4. Mimikatz (Obtaining Password Hash)

Basic Information

Tool	Tool Name	mimikatz > sekurlsa::logonpasswords mimikatz > lsadump::sam
	Category	Password and Hash Dump
	Tool Overview	Steals recorded authentication information
	Example of Presumed Tool Use During an Attack	This tool is executed to acquire passwords or escalate the privileges to the domain Administrator privileges.
Operating Condition	Authority	Administrator
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	-
	Service	-
Information Acquired from	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- Execution history (Sysmon / audit policy)
Evidence That Can Be Confirmed When Execution is Successful		The successful execution of the tool cannot be determined from event logs or execution history.

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**	**Additional Settings**
-	Host (Windows)	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name (mimikatz.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (mimikatz.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *The used option is recorded as an argument. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	File name: `C:\Windows\Prefetch\[Executable File(MIMIKATZ.EXE)]-[RANDOM].pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	**-**

Remarks

Additional Event Logs That Can Be Output	-

3.3.5. Mimikatz (Obtaining Ticket)

Basic Information

Tool	Tool Name	mimikatz > sekurlsa::tickets
	Category	Password and Hash Dump
	Tool Overview	Acquires tickets for all sessions in a host
	Example of Presumed Tool Use During an Attack	This tool is used to acquire tickets to remotely execute a command.
Operating Condition	Authority	Administrator
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	-
	Service	-
Information Acquired from	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- Execution history (Sysmon / audit policy) *The fact that a file that output a ticket was generated is recorded.
Evidence That Can Be Confirmed When Execution is Successful		- If a file that output a ticket is generated, it is considered that the process was successful.

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	Additional Settings
-	Host (Windows)	Event Log - Security	***Event ID***: **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name***: *"[File Name (mimikatz.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account*** **Name** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account*** ***Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Until all tickets are processed, the processing of the **Event IDs: 4656, 4663, and 4658** are repeated.	
			Event ID: **4656** (A handle to an object was requested) - ***Process Information*** -> ***Process Name***: *"[File Name (mimikatz.exe)]"* - **Confirmable Information** - **Targeted File**: ***Object*** -> ***Object Name*** (*"[Ticket File Name]"*) - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** (*"READ_CONTROL", "SYNCHRONIZE", "WriteData (or AddFile)", "AppendData (or AddSubdirectory or CreatePipeInstance)", "WriteEA", "ReadAttributes", "WriteAttributes"*)	
			Event ID: **4663** (An attempt was made to access an object) - **Confirmable Information** - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** (*"WriteData (or AddFile)", "AppendData (or AddSubdirectory or CreatePipeInstance)"*)	
			Event ID: **4658** (The handle to an object was closed) - **Confirmable Information** - **Handle ID**: ***Object*** -> ***Handle ID***	
		Event Log - Sysmon	***Event ID***: **1** (Process Create) **5** (Process Terminated) - ***Image***: *"[File Name (mimikatz.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *The used option is recorded as an argument (it is recorded in Event ID 1). - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	File name: `C:\Windows\Prefetch\[Executable File (MIMIKATZ.EXE)]-[RANDOM].pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	-

3.3.6. WCE (Windows Credentials Editor)

Basic Information

Tool	Tool Name	WCE (Windows Credentials Editor)
	Category	Password and Hash Dump
	Tool Overview	Acquires password hash information in the memory of a logged in host
	Example of Presumed Tool Use During an Attack	This tool uses the acquired hash information to perform pass-the-hash and other attacks.
Operating Condition	Authority	Administrator
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	-
	Service	-
Information Acquired from Log	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- The fact that a tool was executed, and the option used during tool execution (Sysmon). - Reference of lsass.exe by the tool (Sysmon) - Creation / deletion of a file (audit policy)
Evidence That Can Be Confirmed When Execution is Successful		- The *`"C:\Users\[User Name]\AppData\Local\Temp\wceaux.dll"`* file was created and deleted.

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**	**Additional Settings**
–	Host (Windows)	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name (wce.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			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) - ***Process Information*** -> ***Process Name*** : *"[File Name (wce.exe)]"* - **Confirmable Information** - **Targeted File**: ***Object*** -> ***Object Name*** : *`("C:\Users\[User Name]\AppData\Local\Temp\wceaux.dll")`* - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** (*"READ_CONTROL"* , *"SYNCHRONIZE"* , *"ReadData (or "WriteData (or AddFile)"* , *"AppendData (or AddSubdirectory or CreatePipeInstance)"* , *"ReadEA"* , *"WriteEA"* , *"ReadAttributes"* , *"WriteAttributes")* - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	
			Event ID : **4656** (A handle to an object was requested) **4660** (An attempt was deleted) **4658** (The handle to an object was closed) - ***Process Information*** -> ***Process Name*** : *"[File Name (wce.exe)]"* - **Confirmable Information** - **Targeted File**: ***Object*** -> ***Object Name*** : *`("C:\Users\[User Name]\AppData\Local\Temp\wceaux.dll")`* - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** (*"DELETE"*) - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (wce.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
			Event ID : **8** (CreateRemoteThread detected) - ***Image*** : *"[File Name (wce.exe)]"* - ***TargetImage*** : *`"C:\Windows\System32\lsass.exe"`* - **Confirmable Information** - **Process Start Time and Date (UTC)**: ***UtcTime***	
		Execution History - Prefetch	**File name: `C:\Windows\Prefetch\[File Name (WCE.EXE)]-[RANDOM].pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	-

3.3.7. gsecdump

Basic Information

Tool	Tool Name	gsecdump
	Category	Password and Hash Dump
	Tool Overview	Extracts hash from SAM/AD or logon sessions
	Example of Presumed Tool Use During an Attack	This tool is used to log on to other hosts using acquired hash information.
Operating Condition	Authority	Administrator
	Targeted OS	Windows 32-bit (a tool that operates in the 64-bit environment has yet to be confirmed)
	Domain	Not required
	Communication Protocol	-
	Service	-
Information Acquired from	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- Execution history (Sysmon / audit policy)
Evidence That Can Be Confirmed When Execution is Successful		The successful execution of the tool cannot be determined from event logs or execution history.

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	Additional Settings
-	Host (Windows)	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account*** **Name** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account*** ***Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *The used option is recorded as an argument. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	**File name:** `C:\Windows\Prefetch\[File Name (GSECDUMP.EXE)]-[RANDOM].pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	-

3.3.8. lslsass

Basic Information

Tool	Tool Name	lslsass
	Category	Password and Hash Dump
	Tool Overview	Acquires a password hash of active logon sessions from the lsass process
	Example of Presumed Tool Use During an Attack	This tool is used to perform logon authentication on other hosts using the acquired hash information.
Operating Condition	Authority	Administrator
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	-
	Service	-
Information Acquired from	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- Execution history (Sysmon/access history)
Evidence That Can Be Confirmed When Execution is Successful		The successful execution of the tool cannot be determined from event logs or execution history.

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	Additional Settings
-	Host (Windows)	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name (lslsass[Bit Number].exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (lslsass[Bit Number].exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *The used option is recorded as an argument. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History Prefetch	**File name:** `C:\Windows\Prefetch\[Executable File(LSLSASS[Number of Bits].EXE)]-[RANDOM].pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	

3.3.9. Find-GPOPasswords.ps1

Basic Information

Tool	Tool Name	Find-GPOPasswords.ps1
	Category	Password and Hash Dump
	Tool Overview	Acquires any password descriptions in a group policy file
	Example of Presumed Tool Use During an Attack	This tool attempts to infiltrate other hosts using acquired passwords (by executing the tool on Active Directory).
Operating Condition	Authority	Administrator
	Targeted OS	Windows Server This investigation is conducted on the Domain Controller.
	Domain	Required
	Communication Protocol	-
	Service	-
Information Acquired from Log	Standard Settings	- Execution history (Prefetch) *The information is not of use when PowerShell is used in regular operations.
	Additional Settings	- The fact that PowerShell was started is recorded. - The fact that a file in which passwords are dumped (GPPDataReport-[Domain Name]-[Time and Date].csv) is output is recorded.
Evidence That Can Be Confirmed When Execution is Successful		- A file in which a password was dumped (GPPDataReport-[Domain Name]-[Time and Date].csv) is output.

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	Additional Settings
-	Active Directory Domain Controller (Windows Server)	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account*** **Name** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **4656** (A handle to an object was requested) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"* - **Confirmable Information** - **Targeted File**: ***Object*** -> ***Object Name*** : *("C:\Users\[User Name]\AppData\Local\Microsoft\Windows\SchCache \[Domain Controller FQDN].sch")* - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** *("READ_CONTROL", "SYNCHRONIZE", "WriteData (or AddFile)", "AppendData (or AddSubdirectory or CreatePipeInstance)","WriteEA","ReadAttributes","WriteAttributes")*	
			Event ID : **4663** (An attempt was made to access an object) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"* - **Confirmable Information** - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** *("WriteData (or AddFile)", "AppendData (or AddSubdirectory or CreatePipeInstance)")*	
			Event ID : **4658** (The handle to an object was closed) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"* - **Confirmable Information** - **Handle ID**: ***Object*** -> ***Handle ID*** *The same as the ***handle ID*** recorded in event **4663** that is output first.	
			Event ID : **4656** (A handle to an object was requested) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"* - **Confirmable Information** - **Targeted File**: ***Object*** -> ***Object Name*** : *("GPPDataReport-[Domain Name]-[Time and Date].csv")* - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** *("READ_CONTROL", "SYNCHRONIZE", "WriteData (or AddFile)", "AppendData (or AddSubdirectory or CreatePipeInstance)","WriteEA","ReadAttributes","WriteAttributes")*	
			Event ID : **4663** (An attempt was made to access an object) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"* - **Confirmable Information** - **Targeted File**: ***Object*** -> ***Object Name*** : *("GPPDataReport-[Domain Name]-[Time and Date].csv")* - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** *("WriteData (or AddFile)", "AppendData (or AddSubdirectory or CreatePipeInstance)")*	
			Event ID : **4658** (The handle to an object was closed) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"* - **Confirmable Information** - **Handle ID**: ***Object*** -> ***Handle ID*** *The same as the ***handle ID*** recorded in event **4663** that is output first.	
			Event ID : **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"* - **Confirmable Information** - **Process End Time and Date**: Log Date - **Process Return Value**: ***Process Information*** -> ***Exit Status***	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C:\Windows\System32\Windows PowerShell\v1.0\powershell.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required

Remarks

Additional Event Logs That Can Be Output	-

3.3.10. Mail PassView

Basic Information

Tool	Tool Name	Mail PassView
	Category	Password and Hash Dump
	Tool Overview	Extracts account information saved in the mail client settings on the machine
	Example of Presumed Tool Use During an Attack	E-mails are transmitted using information obtained with this tool. If the same user name and password obtained with this tool are used for others, they might have been misused.
Operating Condition	Authority	Standard user
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	-
	Service	-
Information Acquired from Log	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- Execution history (Sysmon / audit policy)
Evidence That Can Be Confirmed When Execution is Successful		The successful execution of the tool cannot be determined from event logs or execution history. *If the extracted password is saved, it is considered that the execution was successful. If the saved information is protected by a password, it cannot be read with this tool. Therefore, a successful execution and successful collection of information do not always match.

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**	**Additional Settings**
-	Host (Windows)	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***New Process Name*** : *"[File Name (mailpv.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account*** **Name** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **4663** (An attempt was made to access an object) **4656** (A handle to an object was requested) **4658** (The handle to an object was closed) - ***Process Information*** -> ***Process Name*** : *"[File Name (mailpv.exe)]"* - **Confirmable Information** - **Targeted File**: ***Object*** -> ***Object Name*** : *"[File Specified in Argument]"* - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** (*"WriteData (or AddFile)"*)	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (mailpv.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *The text file name used as the output destination is specified in the argument. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	**File name**: `C:\Windows\Prefetch\[File Name (MAILPV.EXE)]-[RANDOM].pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	A read access could occur to the profile of an e-mail client that Mail PassView supports.

3.3.11. WebBrowserPassView

Basic Information

Tool	Tool Name	WebBrowserPassView
	Category	Password and Hash Dump
	Tool Overview	Extracts user names and passwords saved in the web browser of a machine
	Example of Presumed Tool Use During an Attack	This tool is used to extract and use account information entered for accessing an intranet or external services.
Operating Condition	Authority	Standard user
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	-
	Service	-
Information Acquired from	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- Execution history (Sysmon / audit policy)
Evidence That Can Be Confirmed When Execution is Successful		The successful execution of the tool cannot be determined from event logs or execution history. *If the extracted password is saved, it is considered that the execution was successful. If the saved information is protected by a password, it cannot be read with this tool. Therefore, a successful execution and successful collection of information do not always match.

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**	**Additional Settings**
-	Host (Windows)	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name (WebBrowserPassView.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **4663** (An attempt was made to access an object) **4656** (A handle to an object was requested) **4658** (The handle to an object was closed) - ***Process Information*** -> ***Process Name*** : *"[File Name (WebBrowserPassView.exe)]"* - **Confirmable Information** - **Targeted File**: ***Object*** -> ***Object Name*** : *"[File Specified in Argument]"* - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** (*"WriteData (or AddFile)"*)	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (WebBrowserPassView.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *The text file name used as the output destination is specified in the argument. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History Prefetch	**File name**: **`C:\Windows\Prefetch\[File Name (WEBBROWSERPASSVIEW.EXE)]-[RANDOM].pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	- If browsers supported by WebBrowserPassView are installed on the system, the profile of each browser is read. - The latest WebBrowserPassView is designed for GUI and saves settings in "[Tool Name].cfg" after it is executed.

3.3.12. Remote Desktop PassView

Basic Information

Tool	Tool Name	Remote Desktop PassView
	Category	Password and Hash Dump
	Tool Overview	Extracts account information saved in the RDP settings on the machine
	Example of Presumed Tool Use During an Attack	This tool is used to extract passwords saved in the settings file for Remote Desktop and to log in to other hosts with such passwords.
Operating Condition	Authority	Standard user
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	-
	Service	-
Information Acquired from	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- Execution history (Sysmon / audit policy)
Evidence That Can Be Confirmed When Execution is Successful		The successful execution of the tool cannot be determined from event logs or execution history. *If the extracted password is saved, it is considered that the execution was successful.

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	Additional Settings
-	Host (Windows)	Event Log - Security	*Event ID* : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name (rdpv.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account*** **Name** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account*** ***Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **4656** (A handle to an object was requested) - ***Process Name in Process Information*** : *"[File Name (rdpv.exe)]"* - **Confirmable Information** - **Targeted File**: ***Object*** -> ***Object Name*** : *("The file name of the target tool is specified to the tool in the argument")* - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** *("READ_CONTROL","SYNCHRONIZE","WriteData (or AddFile)","AppendData (or AddSubdirectory or CreatePipeInstance)","WriteEA","ReadAttributes","WriteAttributes"*)	
			Event ID : **4663** (An attempt was made to access an object) - **Confirmable Information** - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** *("WriteData (or AddFile)","AppendData (or AddSubdirectory or CreatePipeInstance)")*	
			Event ID : **4658** (The handle to an object was closed) - **Confirmable Information** - **Handle ID**: ***Object*** -> ***Handle ID***	
		Event Log - Sysmon	*Event ID* : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (rdpv.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *The used option is recorded as an argument. (It is recorded in Event ID 1.) - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	File name: `C:\Windows\Prefetch\[Executable File(RDPV.EXE)]-[RANDOM].pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	-

3.4.1. Htran

Basic Information

Tool	Tool Name	Htran
	Category	Malicious Communication Relay
	Tool Overview	Creates a TCP session and tunnel other port communications
	Example of Presumed Tool Use During an Attack	Pass communication from unallowed ports through whitelisted ports. - Source host: Htran execution source - Destination host: the machine connected by Htran
Operating Condition	Authority	Standard user
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	Any TCP port
	Service	-
Information Acquired from Log	Standard Settings	- Source host: Execution history (Prefetch) - Destination host: Depends on the application that uses the communication made via a tunnel
	Additional Settings	- Source host: Execution of the tool (Audit of process tracking) Presence or absence of communications with the tunnel host (attacker) and tunnel destination host (destination host) (Audit of object access) - Destination host: Depends on the application that uses the communications made via a tunnel
Evidence That Can Be Confirmed When Execution is Successful		- Source host: If the following log is in the event log, it is possible that communication occurred: - It is recorded in the event ID **5156** in the event log "Security" that a communication occurred with the tunnel host and tunnel destination host.

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

Points to be Confirmed

*In this report, "the machine on which Htran was executed" and "the machine connected via Htran" are referred to as "the source host" and "the destination host", respectively.

Communication	**Log Generation Location**	**Log Type and Name**	**Acquired Information Details**	**Additional Settings**
OS: Windows user ↓ OS: Windows user	Source host	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			A communication from the "source host" to two locations occurs.	
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"[File Name]"* - ***Network Information*** -> ***Direction*** : *"Inbound"* - ***Network Information*** -> ***Source Address*** : *"[IP Address of Source Host]"* - ***Network Information*** -> ***Protocol*** : *"6"* (TCP) - **Confirmable Information** - **Tunnel Host**: ***Destination Address*** - **Port Used for Tunneling**: ***Destination Port***	
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"[File Name]"* - ***Network Information*** -> ***Direction*** : *"Inbound"* - ***Network Information*** -> ***Source Address*** : *"[IP Address of Source Host]"* ･***Network Information*** -> ***Protocol*** : *"6"* (TCP) - **Confirmable Information** - **Tunnel Host**: ***Destination Address*** - **Port Used for Tunneling**: ***Destination Port***	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **Specified Time**, **Execution Process**, **Targeted Host**: ***CommandLine*** *The following is recorded in the argument: **The IP address and port number of the tunnel host (attacker) and the tunnel destination host (destination host)** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	**File name: `C:\Windows\Prefetch\[File Name]-[RANDOM].pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-
	Destination host	Various Logs	Multiple logs could be recorded by applications using communications made via a tunnel. Remote Desktop (RDP) is an example of applications often used via Htran. In this case, a communication on the destination port 3389/tcp with the source host IP address of the "source host" where Htran was executed is recorded in the "destination host", which is the tunnel destination. *For details on RDP logs, see the separate RDP document.	Required

Remarks

Additional Event Logs That Can Be Output	When a version that supports a HTTP proxy is used, HTTPS communication is recorded in the proxy. If SSL cannot be decoded due to HTTPS, only the CONNECT method is recorded.

3.4.2. Fake wpad

Basic Information

Tool	Tool Name	Fake wpad
	Category	Malicious Communication Relay
	Tool Overview	Acquires and changes communication content by operating as the wpad server
	Example of Presumed Tool Use During an Attack	This tool modifies the response so that the attacker's site is embedded without the user noticing. - Source host: Receives a spoofed wpad file - Destination host: Becomes the proxy of the source host by sending the spoofed wpad file to the source host
	Reference Information	https://www.jpcert.or.jp/present/2015/20151028_codeblue_apt-en.pdf
Operating Condition	Authority	- Destination host (wpad server): Listens on 80/tcp and 8888/tcp. Administrator privileges are required because changes, such as to Windows Firewall to allow files to be received, need to be made. - Source host: Standard user
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	80/tcp, 8888/tcp
	Service	-
Information Acquired from Log	Standard Settings	- Source host: The last acquired proxy setting (registry) is recorded. *The setting cannot be distinguished if wpad is used in regular operations. - Destination host: Execution history (Prefetch)
	Additional Settings	- Source host: The fact that communications were made via 80/tcp and 8888/tcp to the host that executes the tool is recorded (audit object access). The fact that a wpad.dat cache was created is recorded (audit object access).
		- Destination host: The fact that 80/tcp and 8888/tcp were listened to is recorded (audit object access). Handle requests to wpad.dat and the proxy log proxy.log are recorded (audit object access).
Evidence That Can Be Confirmed When Execution is Successful		- Source host: Communication via 80/tcp and 8888/tcp was made with a host that is originally neither a proxy nor HTTP server. - Destination host: A host that is originally neither a proxy nor HTTP server was listening to 80/tcp and 8888/tcp. wpad.dat and proxy.log were created.

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	Additional Settings
OS: Windows user ↓ OS: Windows user	Source host	Event Log - Security	The following is recorded when wpad is acquired. (The following shows an example using Internet Explorer. The storage location and behavior are different when using other browsers.) Note that because event IDs **4656**, **4663**, and **4658** are recorded when wpad is used, malicious communication cannot be distinguished if wpad is used in normal operations. ***Event ID*** : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"\device\harddiskvolume2\program files\internet explorer\iexplore.exe"* - ***Network Information*** -> ***Direction*** : *"Outbound"* - ***Network Information*** -> ***Destination Port / Protocol*** : *"80"* / *"6"* (TCP) - **Confirmable Information** - **Connected Host**: ***Network Information*** -> ***Destination Address*** ***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) - **Confirmable Information** - **Target File**: ***Object*** -> ***Object Name*** (*"C:\Users\[User Name]\AppData\Local\Microsoft\Windows* \Temporary Internet Files\Content.IE5\[Text]\wpad[1].htm") - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** (*"WriteAttributes"/"WriteData (or AddFile)"/* "AppendData (or AddSubdirectory *or CreatePipeInstance"*) - **Success or Failure**: ***Keywords*** (*"Audit Success"*) The following is recorded if a proxy is used. If a condition that the relevant host is not to be used as a proxy is defined in wpad.dat, the ***Destination Address*** is the host at the destination to be actually connected. ***Event ID*** : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"\device\harddiskvolume2\program files\internet explorer\iexplore.exe"* - ***Network Information*** -> ***Direction*** : *"Outbound"* - ***Network Information*** -> ***Destination Port / Protocol*** : *"8888"* / *"6"* (TCP) - **Confirmable Information** - **Host Used as the Proxy**: ***Network Information*** -> ***Destination Address***	Required
		Access History - Registry	Registry Entry: **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\ SavedLegacySettings** **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\ DefaultConnectionSettings** - **Confirmable Information** - **Last Acquired Proxy Setting** *The setting cannot be distinguished if wpad is used in regular operations.	-
	Destination host	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***New Process Name*** : *"[File Name (wpad.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status*** The following is recorded immediately after the tool is executed. ***Event ID*** : **5154** (The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections) - ***Application Information*** -> ***Process ID*** : The ***Process ID*** recorded in event ID **4688**. - ***Application Information*** -> ***Application Name*** : *"\device\harddiskvolume2\[File Name (wpad.exe)]"* - **Confirmable Information** - **Port Listened to**: ***Network Information*** -> ***Source Port*** (*"80"*/*"8888"*) - **Protocol**: ***Network Information*** -> ***Protocol*** (*"6"* = TCP) ***Event ID*** : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Process ID*** : *"4"* - ***Application Information*** -> ***Application Name*** : *"System"* - ***Network Information*** -> ***Direction*** : *"Outbound"* - ***Network Information*** -> ***Source Address*** : *"[Host that Executed the Tool]"* - ***Network Information*** -> ***Address Port Source Port Protocol*** : *"137"* (both destination and source) / *"17"* The following is recorded when the source host acquires wpad.	Required

Communication	Log Generation Location	Log Type and Name	Acquired Information Details	Additional Settings
OS: Windows user ↓ OS: Windows user (Continued from the previous entry)	Destination host (Continued from the previous entry)	Event Log - Security	***Event ID***: **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Process ID***: The ***Process ID*** recorded in event **4688**. - ***Application Information*** -> ***Application Name***: *"\device\harddiskvolume2\[File Name (wpad.exe)]"* - ***Network Information*** -> ***Direction***: *"Inbound"* - ***Network Information*** -> ***Source Port / Protocol***: *"80"* / *"6"* (TCP) - **Confirmable Information** - **Connected Host**: ***Network Information*** -> ***Destination Address***	Required
			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) - ***Process Information*** -> ***Process Name***: *"[File Name (wpad.exe)]"* - **Confirmable Information** - **Target File**: ***Object*** -> ***Object Name*** (*"[Path to Tool]\wpad.dat"*) - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** (*"SYNCHRONIZE"* / *"ReadData (or ListDirectory)"* / *"WriteData (or "AppendData (or AddSubdirectory or CreatePipeInstance)"* / *"ReadEA"* / *"WriteEA"* / *"ReadAttributes"* / - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	Required
			The following is recorded when the source host uses the host as a proxy. The log file (proxy.log) is created on the same path as that of the executable file (a handle for the log is requested and closed each time).	
			Event ID: **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Process ID***: The ***Process ID*** recorded in event **4688**. - ***Application Information*** -> ***Application Name***: *"\device\harddiskvolume2\[File Name (wpad.exe)]"* - ***Network Information*** -> ***Direction***: *"Inbound"* - ***Network Information*** -> ***Source Port / Protocol***: *"8888"* / *"6"* (TCP) - **Confirmable Information** - **Connected Host**: ***Network Information*** -> ***Destination Address***	
			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) - ***Process Information*** -> ***Process Name***: *"[File Name (wpad.exe)]"* - **Confirmable Information** - **Target File**: ***Object*** -> ***Object Name*** (*"[Path to Tool]\proxy.log"*) - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs. - **Process Details**: ***Access Request Information*** -> ***Access*** (*"WriteData (or AddFile)"*) - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	
			Event ID: **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Process ID***: The ***Process ID*** recorded in event **4688**. - ***Application Information*** -> ***Application Name***: *"\device\harddiskvolume2\[File Name (wpad.exe)]"* - ***Network Information*** -> ***Direction***: *"Outbound"* - ***Network Information*** -> ***Source Address***: *"[Host that Executed the Tool]"* - ***Network Information*** -> ***Source Port / Protocol***: *"[Destination Server Port] (80 if nothing is specified)"* / *"6"* (TCP) - **Confirmable Information** - **Destination Host**: ***Network Information*** -> ***Destination Address***	
		Event Log - Sysmon	***Event ID***: **1** (Process Create) **5** (Process Terminated) - ***Image***: *"[File Name (wpad.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *If iframe, etc. is used, it can be read from the argument. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History Prefetch	**File name: `C:\Windows\Prefetch\WPAD.EXE-[RANDOM].pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	-

3.5.1. RDP (Remote Desktop Protocol)

Basic Information

Tool	Tool Name	RDP (Remote Desktop Protocol)
	Category	Remote Login
	Tool Overview	A protocol to connect to a server on which Remote Desktop Service (RDS) is running
	Example of Presumed Tool Use During an Attack	- View files on the logged in machine - Collect information (required) for connecting to other servers and clients - Use as a stepping stone to connect to other equipment
Operating Condition	Authority	Standard user
	Targeted OS	- Source host: Windows - Destination host: Windows with Remote Desktop enabled
	Domain	Not required
	Communication Protocol	3389/tcp
	Service	- Destination host: Remote Desktop Services
Information Acquired from Log	Standard Settings	- Destination host: RDP session connection start/end time and date Source host IP address Logged in user name, and Success or failure of account domain connection
	Additional Settings	- Source host: mstsc.exe execution history, file access history
Evidence That Can Be Confirmed When Execution is Successful		- Destination host: If the following logs are in the event log, it is considered that the connection was successful. - Event ID: **4624** is recorded in the event log "Security". - Event IDs **21** and **24** are recorded in the event log `"Microsoft\Windows\TerminalServices-LocalSessionManager\Operational"`

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	Additional Settings
OS: Windows user ↓ OS: Windows user	Source host	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information -> New Process Name*** : *`"C:\Windows\System32\mstsc.exe`* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject -> Account Name*** - **Domain of User Who Executed the Process**: ***Subject -> Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information -> Token Escalation Type*** - **Process Return Value**: ***Process Information -> Exit Status***	Required
			Event ID : **4663** (An attempt was made to access an object) **4656** (A handle to an object was requested) **4658** (The handle to an object was closed) - ***Process Information -> Process Name*** : *`"C:\Windows\System32\mstsc.exe"`* - **Confirmable Information** - **Target File**: ***Object -> Object Name*** (Example: *`"C:\Users\[User Name]\Documents\Default.rdp"`*) - **Handle ID (Used for Association with Other Logs)**: ***Object -> Handle ID*** - **Process Details**: ***Access Request Information -> Access*** (*"WriteData (or AddFile)"* *"AppendData (or AddSubdirectory or* - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	
		Execution history - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *`"C:\Windows\System32\mstsc.exe"`* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	**File name**: **`C:\Windows\Prefetch\MSTSC.EXE-76A46E8A.pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-
		Access History - Registry	**Registry Entry**: **`HKEY_USERS\[SID]\Software\Microsoft\Terminal Server Client\Default\`** - **Confirmable Information** - **Remote Desktop Connection History**: ***Value Name*** = *"MRU0"* to *"MRU9"* *As ***the data of the above value*** , **an IP address that was connected to in the past** is recorded. MRU0 is the last connected history As ***the last write time*** for a key, **the update time and date** (time of the first connection to a destination host not found in the connection history) for the *"MRU0"* ***value data*** is recorded.	-
			Registry Entry: `HKEY_USERS\[SID]\Software\Microsoft\Terminal Server Client\Servers\[Destination Host IP Address]\` - **Confirmable Information** - **The Last Accessed Account Domain and User Name: *Value Name*** = *"UsernameHint"* *As the value data, the last accessed account domain and user name are recorded for each IP address that was connected to in the past.	
	Destination host	Access History - Audit Policy	***Event ID*** : **4624** (An account was successfully logged on) - ***Logon Type*** : *"10"* - ***Network Information -> Source Network Address*** : ***Destination Address*** for event **5156** - ***Network Information -> Source Port*** : ***Destination Port*** recorded in event **5156** - ***Detailed Authentication Information -> Logon Process*** : *"Kerberos"* - **Confirmable Information** - **Connection Source Host**: ***Network Information -> Source Network Address*** - **Used User**: ***New Logon -> Account Name / Account Domain*** - **New Logon ID (used for association with other logs)**: ***New Logon -> Logon ID***	Required
		Event Log - Application and Service Log `\Microsoft\Windows\TerminalServices-LocalSessionManager\Operational`	**Event ID: 21** (Remote Desktop Services: Session logon succeeded) - **Confirmable Information** - **Session Connection Start Time and Date**: ***Log Date*** - **Logged in Account Domain and User Name**: ***User*** - **Connection Source IP Address**: ***Source Network Address***	-
			Event ID: 24 (Remote Desktop Services: Session has been disconnected) - **Confirmable Information** - **Session Connection Start Time and Date**: ***Log Date*** of an Event Log with the Same ***Session ID*** in **Event ID: 21** - **Logged in Account Domain and User Name**: ***User*** - **Connection Source IP Address**: ***Source Network Address***	

Remarks

Additional Event Logs That Can Be Output	Depending on the environment, the following log may be recorded in the destination host event log "Security". ***Event ID*** : **4624** (An account was successfully logged on) - ***Logon Type*** : *"12"*

3.6.1. WCE (Remote Login)

Basic Information

Tool	Tool Name	WCE (Remote Login)
	Category	pass-the-hash, pass-the-ticket
	Tool Overview	Executes a command with higher privileges using the hash of the acquired password
	Example of Presumed Tool Use During an Attack	Remotely executes a command on another machine by using a password hash for a user with Administrator privileges who belongs to Active Directory - Source host: WCE execution source - Destination host: The destination logged in by WCE
Operating Condition	Authority	Local administrator
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	A random 5-digit port (WMIC)
	Service	-
Information Acquired from Log	Standard Settings	- Source host: Execution history (Prefetch) A record of the fact that WCESERVICE was installed and executed
	Additional Settings	- Both source host and destination host: WMI execution history and Windows Filtering Platform log - Destination host: Login has occurred remotely.
Evidence That Can Be Confirmed When Execution is Successful		- Source host: The fact that WCESERVICE was installed and executed is recorded. - Destination host: The fact that a logon was made from a remote host is recorded. - Both source host and destination host: The fact that communication using WMI occurred is recorded.

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	Additional Settings
OS: Windows administrator ↓ OS: Windows administrator	Source host (Windows)	Event Log - Security	***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\Temp\wceaux.dll)"* - ***Access Request Information*** -> ***Access / Reason for Access*** : (*"WriteData (or AddFile)"*) - **Confirmable Information** - **Process Name**: *"[File Name (wce.exe)]"* - **Handle ID**: ***Object*** -> ***Handle ID***	Required
			Event ID : **4656** (A handle to an object was requested) **4660** (An attempt was deleted) **4658** (The handle to an object was closed) - ***Object*** -> ***Object Name*** : *"(C:\Windows\Temp\wceaux.dll)"* - ***Access Request Information*** -> ***Access / Reason for Access*** : (*"DELETE"*) - **Confirmable Information** - **Process Name**: *"[File Name (wce.exe)]"* - **Handle ID**: ***Object*** -> ***Handle ID***	
			Processes for events **4656**, **4663**, and **4658** are performed for multiple files.	
			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:\Users\[User Name]\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5)"* - ***Access Request Information*** -> ***Access / Reason for Access*** : (*"SYNCHRONIZE"* ,*"WriteAttributes"* ,*"WriteData (or AddFile)"*) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\wbem\WMIC.exe"* - **Confirmable Information** - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs.	
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** :(*"C:\Windows\System32\wbem\WMIC.exe"*) - ***Network Information*** -> ***Direction*** : *"Outbound"* - **Confirmable Information** - **Destination Host**: ***Destination Address*** - **Destination Port**: ***Destination Port***	
		Event Log - System	***Event ID*** : **7045** (A service was installed in the system) - ***Service Name*** : *"WCESERVICE"* - **Confirmable Information** - **Process Start Time and Date**: Log Date - **Service File Name**: *"[File Name (wce.exe)] -S"*	-
			Event ID : **7036** - ***Detailed Tab*** -> ***System\Provider\Name*** : *"Service Control Manager"* - ***Details Tab*** -> ***EventData\param1*** : *"WCESERVICE"* - **Confirmable Information** - **Running the Service**: ***Details Tab*** -> ***EventData\param2*** (*"Running"*) / (*"Stopped"*)	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (wce.exe)]"* - ***Image*** : *"C:\Windows\System32\wbem\WMIC.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
			Event ID : **8** (CreateRemoteThread detected) - ***SourceImage*** : *"[File Name (wce.exe)]"* - ***TargetImage*** : (*"C:\Windows\System32\lsass.exe"*) - **Confirmable Information** - **Process Start Time and Date (UTC)**: ***UtcTime***	
			Event ID : **9** (RawAccessRead detected) - ***Image*** : *"C:\Windows\System32\cmd.exe"* - **Confirmable Information** - **Process Start Time and Date (UTC)**: ***UtcTime*** - **Access Destination**: ***Device***	

Communication	Log Generation Location	Log Type and Name	Acquired Information Details	Additional Settings
OS: Windows administrator ↓ OS: Windows administrator (Continued from the previous entry)	Destination host (Windows)	Execution History - Registry	**File name:** `C:\Windows\Prefetch\[File Name (WCE.EXE)]-[RANDOM].pf` `C:\Windows\Prefetch\WMIC.EXE-A7D06383.pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-
		Event Log - Security	***Event ID*** : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *("\device\harddiskvolume2\windows\system32\svchost.exe")* - ***Network Information*** -> ***Direction*** : *"Inbound"* - **Confirmable Information** - **Source Host**: ***Destination Address*** - **Source Port**: ***Destination Port***	Required
			Event ID : **4624** (An account was successfully logged on) **4634** (An account was logged off) - **Confirmable Information** - **Process Start Time and Date**: Log Date - **Source Host Account Name**: ***New Logon*** -> ***Account Name / Domain Name*** - **Source Host**: ***Network Information*** -> ***Source Network Address***	
			Event ID : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\wbem\WmiPrvSE.exe"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status*** - **Parent Process ID**: ***Process Information*** -> ***Creator Process ID*** :	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C:\Windows\System32\wbem\WmiPrvSE.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
			Event ID : **9** (RawAccessRead detected) - ***Image*** : *"C:\Windows\System32\wbem\WmiPrvSE.exe"* - **Confirmable Information** - **Process Start Time and Date (UTC)**: ***UtcTime*** - **Access Destination**: ***Device***	
		Execution History - Prefetch	**File name:** `C:\Windows\Prefetch\WMIPRVSE.EXE-1628051C.pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	-

3.6.2. Mimikatz (Remote Login)

Basic Information

Tool	Tool Name	Mimikatz (Remote Login)
	Category	pass-the-hash, pass-the-ticket
	Tool Overview	Executes a command with another user's privileges using a hash of the acquired password
	Example of Presumed Tool Use During an Attack	Remotely executes a command on another machine by using a password hash for a user with Administrator privileges - Source host: Mimikatz execution source - Destination host: The destination logged in by Mimikatz
Operating Condition	Authority	Source host: Administrator Destination host: Privileges of the user whose hash was used
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	A random 5-digit port (WMIC)
	Service	Windows Management Instrumentation
Information Acquired from Log	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- Communication logs during a remote connection - Process logs when a connection occurs
Evidence That Can Be Confirmed When Execution is Successful		- Destination host: If the following log is in the event log, it is considered that a remote login was made. - The event ID **4624** is recorded in the event log "Security" regarding access from an unintended source host.

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	Additional Settings
OS: Windows administrator ↓ OS: Windows user	Source host	Event Log - Security	*Event ID* : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name (mimikatz.exe)]"* *"C:\Windows\System32\cmd.exe"* *"C:\Windows\System32\wbem\WMIC.exe"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"C:\Windows\System32\wbem\WMIC.exe"* - ***Network Information*** -> ***Direction*** : *"Outbound"* - **Confirmable Information** - **Source Port**: ***Source Port*** - **Destination Host**: ***Destination Address*** - **Destination Port**: ***Destination Port*** (5-digit port)	
			Event ID : **4648** (A logon was attempted using explicit credentials) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\wbem\WMIC.exe"* - **Confirmable Information** - **Process Start Time and Date**: Log Date - **Account Name that Executed the Process on the Destination Host**: ***Account for which Credentials were Used*** -> ***Account Name /*** - **Destination Host**: ***Target Server*** -> ***Target Server Name***	
		Event Log - Sysmon	*Event ID* : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C:\Windows\System32\at.exe"* *"C:\Windows\System32\cmd.exe"* *"C:\Windows\System32\wbem\WMIC.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Registry	**File name: C:\Windows\Prefetch\CMD.EXE-4A81B364.pf** **C:\Windows\Prefetch\[File Name (MIMIKATZ.EXE)]-[RANDOM].pf** **C:\Windows\Prefetch\WMIC.EXE-A7D06383.pf** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-
	Destination host	Event Log - Security	*Event ID* : **4624** (An account was successfully logged on) - ***Logon Type*** : *"3"* - **Confirmable Information** - **Process Start Time and Date**: Log Date - **Source Host Account Name**: ***New Logon*** -> ***Account Name / Domain Name*** - **Source Host**: ***Network Information*** -> ***Source Network Address***	Required
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"\device\harddiskvolume2\windows\system32\svchost.exe"* - ***Network Information*** -> ***Direction*** : *"Inbound"* - **Confirmable Information** - **Source Host**: ***Destination Address*** - **Source Port**: ***Destination Port*** *Matches the ***source port*** at the source host. - **Destination Port**: ***Source Port*** *Matches the **destination port** at the source host.	
		Event Log - Sysmon	*Event ID* : **1** (Process Create) - ***Image*** : *"C:\Windows\System32\wbem\WmiPrvSE.exe"* - **Confirmable Information** - **Process Start Time and Date (UTC)**: ***UtcTime*** - **Process ID**: ***ProcessId***	Required
		Execution History - Registry	**File name: C:\Windows\Prefetch\WMIPRVSE.EXE-1628051C.pf** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	-

3.7.1. MS14-058 Exploit

Basic Information

Tool	Tool Name	MS14-058 Exploit
	Category	Escalation to SYSTEM Privileges
	Tool Overview	Executes a specified command with SYSTEM privileges
	Example of Presumed Tool Use During an Attack	This tool is used for a user with standard privileges to execute a command that normally requires administrator privileges.
Operating Condition	Authority	Standard user
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	-
	Service	-
Information Acquired from Log	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- The name of a process executed by the tool with SYSTEM privileges, and argument (Sysmon / audit of process tracking)
Evidence That Can Be Confirmed When Execution is Successful		If the following log is in the event log, it is considered that privilege escalation was successful. - The event ID: **4688** is recorded regarding a process executed with SYSTEM privileges, whose parent process cannot be the parent of the tool or that process.

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**	**Additional Settings**
-	Host (Windows)	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***New Process Name*** : *"[Process Executed with SYSTEM Privileges]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** (*"[Computer Name]$"*) - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** ***A command executed with SYSTEM privileges** is recorded in the argument. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
			Event ID : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[Process Executed with SYSTEM Privileges]"* - **Confirmable Information** - **Process Start Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** ***An argument for the command** is recorded. - **User Name**: ***User*** (*"NT AUTHORITY\SYSTEM"*) - **Process ID**: ***ProcessId*** - **Parent Process Name**: ***ParentImage*** (*"[File Name]"*) - **Command Line Specified as the Parent Process**: ***ParentCommandLine***	
		Execution History - Prefetch	**File name**: **`C:\Windows\Prefetch\[File Name]-[RANDOM].pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Executed Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	Other logs that are related to processes executed with SYSTEM privileges may be recorded.

3.7.2. MS15-078 Exploit

Basic Information

Tool	Tool Name	MS15-078 Exploit
	Category	Escalation to SYSTEM Privileges
	Tool Overview	Executes a specified command with SYSTEM privileges
	Example of Presumed Tool Use During an Attack	This tool is used for a user with standard privileges to execute a command that normally requires administrator privileges.
Operating Condition	Authority	Standard user
	Targeted OS	Windows 7 / 8 / 2008 This tool cannot be executed in a test environment with Windows Server 2012.
	Domain	Not required
	Communication Protocol	-
	Service	-
Information Acquired from	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- The name of a process executed by the tool with SYSTEM privileges, and argument (Sysmon / audit of process tracking)
Evidence That Can Be Confirmed When Execution is Successful		If the following log is in the event log, it is considered that privilege escalation was successful. - The event ID: **4688** is recorded regarding a process executed with SYSTEM privileges, whose parent process cannot be the parent of the tool or that process.

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	Additional Settings
-	Host (Windows)	Event Log - Security	*Event ID* : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***New Process Name*** : *"[File Name]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***New Process Name*** : *"[Process Executed with SYSTEM Privileges]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** (*"[Computer Name]$"*) - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	
		Event Log - Sysmon	*Event ID* : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** ***A command executed with SYSTEM privileges** is recorded in the argument. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
			Event ID : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[Process Executed with SYSTEM Privileges]"* - **Confirmable Information** - **Process Start Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** ***An argument for the command** is recorded. - **User Name**: ***User*** (*"NT AUTHORITY\SYSTEM"*) - **Process ID**: ***ProcessId*** - **Parent Process Name**: ***ParentImage*** (*"[File Name]"*) - **Command Line Specified as the Parent Process**: ***ParentCommandLine***	
		Execution History - Prefetch	**File name**: `C:\Windows\Prefetch\[File Name]-[RANDOM].pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Executed Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	Other logs that are related to processes executed with SYSTEM privileges may be recorded.

3.8.1. SDB UAC Bypass

Basic Information

Tool	Tool Name	SDB UAC Bypass
	Category	Privilege Escalation
	Tool Overview	Uses Application Compatibility Database (SDB) to execute applications that are normally controlled by User Account Control (UAC) as a user with administrator privileges
	Example of Presumed Tool Use During an Attack	This tool is used to execute an application that is not normally executed by pretending to execute a typical application. In doing so, the tool is capable of executing an application that normally requires administrator privileges without obtaining the permission of the relevant user.
	Reference Information	http://blog.jpcert.or.jp/2015/02/a-new-uac-bypass-method-that-dridex-uses.html
Operating Condition	Authority	A user who has authority to use administrator privileges according to UAC without entering an administrator password. (A user who belongs to the Administrators group in the client)
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	-
	Service	-
Information Acquired from Log	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- Execution history (Sysmon / audit policy) - A process whose parent process name includes an application that is normally assumed not to be a parent process starts. - "The application used for a bypass" and "The application executed as a bypass" are recorded.
Evidence That Can Be Confirmed When Execution is Successful		- The fact that a process whose parent process name includes an application that is normally assumed not to be a parent process was executed is recorded.

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	Additional Settings
-	Host (Windows)	Event Log - Security	The following is recorded when an SDB file is installed. ***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\sdbinst.exe"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status*** ***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) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\sdbinst.exe"* - **Confirmable Information** - **SDB File**: ***Object*** -> ***Object Name*** (*"C:\Windows\AppPatch\Custom\{[GUID]}.sdb"*) - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs - **Process ID of the Process that Requested the Handle**: ***Process Information*** -> ***Process ID*** (matches the ID of the process created in event 4688) - **Process Details**: ***Access Request Information*** -> ***Access*** / ***Reason for Access*** (*"WriteData (or AddFile)" / "AppendData (or AddSubdirectory, or CreatePipeInstance")* - **Success or Failure**: ***Keywords*** (*"Audit Success"*) If an application is executed as a bypass, the following is recorded. ***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[Command Executed as Bypass]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **An ID of the Process of an Application Used for a Bypass That Executed the Application**: ***Process Information*** -> ***Creator Process ID*** Matches the process ID of an application used for a bypass - **Process Return Value**: ***Process Information*** -> ***Exit Status*** *"0x0"* if successful. If failed, a different value is entered according to the error. Depending on the application used for a bypass, such as one executed from a command prompt, the return value may not be "0x0" only by executing it as usual. For this reason, this information can be a reference for measuring whether the execution was *Although "an application executed as a bypass" is always started following "an application used for a bypass," it may be ended before or after the other application depending on how it is called.	Required
		Event Log - Sysmon	The following is recorded when an SDB file is installed. ***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C:\Windows\System32\sdbinst.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **Used SDB File**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId*** If an application is executed as a bypass, the following is recorded. ***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[Command Executed as Bypass]"* - **Confirmable Information** - **Process Start Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId*** - **Parent Process Name**: ***ParentImage*** *An application specified in SDB. **An application that is normally assumed not to be the parent of a process** becomes its parent process. - **Parent Process ID**: ***ParentProcessId*** *Matches the process ID of an application specified in SDB that was executed first. *If the process is for script files for batch processing or others, the process becomes the parent process and a child process will be further executed. By tracking process IDs in order, it is possible to confirm the process tree of the executed applications.	Required

Communication	Log Generation Location	Log Type and Name	Acquired Information Details	Additional Settings
- (Continued from the previous entry)	Host (Windows) (Continued from the previous entry)	Application and Service Log \Microsoft\Windows \Application-Experience \Program-Telemetry	***Event ID*** : **500** (Compatibility fix applied) - **Confirmable Information** - **Program Applied**: ***Details*** Tab -> ***UserData\CompatibilityFixEvent\ExePath*** - **Program Fix**: ***Details*** Tab -> ***UserData\CompatibilityFixEvent\FixName***	-
		Execution History - Prefetch	**File name: C:\Windows\Prefetch\SDBINST.EXE-5CC2F88B.pf** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time*** - **Remarks** - In addition to the above, the last execution date and time of the application used for a bypass and executed application will change.	-
		Execution History - Registry	**Registry Entry: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{[GUID]}.sdb** - **Confirmable Information** - **Content of SDB**: ***DisplayName*** (The name of an application used for a bypass) - **Delete Command**: ***UninstallString*** (*"%windir%\system32\sdbinst.exe -u "C:\Windows\AppPatch\Custom\{[GUID]}.sdb"*) **Registry Entry: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom\ {[Name of Application Used for UAC Bypass]}** - **Confirmable Information** - **SDB Installation Time Stamp**: ***DatabaseInstallTimeStamp*** (A hexadecimal value) **Registry Entry:** HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB\{[GUID]} - **Confirmable Information** - **SDB File Path**: ***DatabasePath*** (*"C:\Windows\AppPatch\Custom\{[GUID]}.sdb"*) - **SDB Type**: ***DatabaseType*** - **Content of SDB**: ***DatabaseDescription*** (The name of an application used for a bypass) - **SDB Installation Time Stamp**: ***DatabaseInstallTimeStamp*** (A hexadecimal value. The same value as one under "Custom" stated the above.) - **Remarks** - The above registry value is deleted when the SDB file is uninstalled and will not always be left. - Some tools in which an SDB file is uninstalled to delete evidence have been confirmed.	-

Remarks

Additional Event Logs That Can Be Output	- In addition to the above, "the application used for a bypass" and "the application executed as a bypass" may be recorded.

3.9.1. MS14-068 Exploit

Basic Information

Tool	Tool Name	MS14-068 Exploit
	Category	Capturing the Domain Administrator Privilege and Account Credentials
	Tool Overview	Changes the privileges of the domain user to those of another user
	Example of Presumed Tool Use During an Attack	This tool is used to perform operations requiring privileges pretending as an administrator by using an acquired domain user account. (For this test, Exploit is used to get the account's TGT ticket and mimikatz is used to log in remotely.) - Source host: Exploit execution source - Destination host: Machine logged in remotely with the acquired ticket
Operating Condition	Authority	Standard user
	Targeted OS	Windows
	Domain	Required
	Communication Protocol	88/tcp, 445/tcp
	Service	Active Directory Domain Services
Information Acquired from Log	Standard Settings	- Source host: Execution history (Prefetch)
	Additional Settings	- Source host: Execution history (Sysmon / audit policy) - Destination host: The fact that higher privileges than the normal privileges are granted to other accounts (audit policy)
Evidence That Can Be Confirmed When Execution is Successful		- Destination host: In the Event ID: **4672** of the event log "Security", high level privileges are granted to a standard user.

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	Additional Settings
OS: Windows user ↓ OS: Windows Server administrator	Source host	Event Log - Security	When a ticket is generated, the following process is executed.	Required
			Event ID : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name (ms14-068.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"\device\harddiskvolume2\[File Name (ms14-068.exe)]"* - ***Application Information*** -> ***Process ID*** : *"[Process ID Recorded in Event **4688**]"* - ***Network Information*** -> ***Direction*** : *"Outbound"* - ***Network Information*** -> ***Destination Address*** : *"[Domain Controller IP Address]"* - ***Network Information*** -> ***Destination Port*** / ***Protocol*** : *"88"* / *"6"* (TCP) - **Confirmable Information** - **Source Port**: ***Source Port*** *Used for association with logs on the Domain Controller side	
			When a ticket is used, the following process is executed.	
			Event ID : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name (mimikatz.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	
			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) - ***Process Information*** -> ***Process Name*** : *"[File Name (ms14-068.exe)]"* - **Confirmable Information** - **Target File**: ***Object*** -> ***Object Name*** - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs - **Process Details**: ***Access Request Information*** -> ***Access*** (*"WriteData (or AddFile)"* / *"AppendData (or AddSubdirectory, or CreatePipeInstance)"*) - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"System"* - ***Network Information*** -> ***Direction*** : *"Outbound"* - ***Network Information*** -> ***Destination Address*** : *"[Domain Controller IP Address]"* - ***Network Information*** -> ***Destination Port*** / ***Protocol*** : *"445"* / *"6"* (TCP) - **Confirmable Information** - **Source Port**: ***Source Port*** *Used for association with logs on the Domain Controller side	
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"[\device\harddiskvolume2\windows\system32\lsass.exe"* - ***Network Information*** -> ***Direction*** : *"Outbound"* - ***Network Information*** -> ***Destination Address*** : *"[Domain Controller IP Address]"* - ***Network Information*** -> ***Destination Port*** / ***Protocol*** : *"88"* / *"6"* (TCP) - **Confirmable Information** - **Source Port**: ***Source Port*** *Used for association with logs on the Domain Controller side	
			In the case of mimikatz.exe, when an acquired ticket is used, the use of privileges (failure) occurs. (It does not occur when mimikatz.exe is executed with administrator privileges.)	
			Event ID : **4673** (A privileged service was called) - ***Process Information*** -> ***Process Name*** : *"[File Name (mimikatz.exe)]"* - ***Process Information*** -> ***Process ID*** : *"[Process ID of the Tool]"* - ***Service Request Information*** -> ***Privileges*** : *"SeTcbPrivilege"* - ***Keyword*** : *"Audit Failure"* - **Confirmable Information** - **Account That Attempted the Above Operation**: **Account Name**	

Communication	Log Generation Location	Log Type and Name	Acquired Information Details	Additional Settings
OS: Windows user ↓ OS: Windows Server administrator (Continued from the previous entry)	Source host (Continued from the previous entry)	Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (ms14-068.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
			Event ID : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (mimikatz.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	
		Execution History - Prefetch	**File name:** `C:\Windows\Prefetch\[File Name (MS14-068.EXE)]-[RANDOM].pf` `C:\Windows\Prefetch\[File Name (MIMIKATZ.EXE)]-[RANDOM].pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-
	Destination host	Event Log - Security	When a ticket is generated, the following communication and authentication occur.	Required
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : `"[\device\harddiskvolume2\windows\system32\lsass.exe"` - ***Application Information*** -> ***Process ID*** : *"[Process ID Recorded in Event **4688**]"* - ***Network Information*** -> ***Direction*** : *"Outbound"* - ***Network Information*** -> ***Destination Address*** : *"[Domain Controller IP Address]"* - ***Network Information*** -> ***Destination Port*** / ***Protocol*** : *"88"* / *"6"* (TCP) - **Confirmable Information** - **Source Port**: ***Source Port*** *Used for association with logs on the Domain Controller side	
			Event ID : **4768** (A Kerberos authentication ticket (TGT) was requested) - ***Service Information*** -> ***Service Name*** : *"krbtgt"* - ***Additional Information*** -> ***Ticket Options*** : *"0x50800000"* - **Confirmable Information** - **Executing Account**: ***Account Information*** -> ***Account Name*** - **Source Host**: ***Network Information*** -> ***Client Address*** - **Source Port**: ***Network Information*** -> ***Client Port***	
			Event ID : **4769** (A Kerberos service ticket was requested) - ***Service Information*** -> ***Service Name*** : *"krbtgt"* - ***Additional Information*** -> ***Ticket Option*** : *"0x50800000"* - **Confirmable Information** - **Executing Account**: ***Account Information*** -> ***Account Name*** / ***Account Domain*** - **Source Host**: ***Network Information*** -> ***Client Address*** - **Source Port**: ***Network Information*** -> ***Client Port***	
			When an acquired ticket is used, the following communication occurs.	
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"System"* - ***Application Information*** -> ***Process ID*** : *"[Process ID Recorded in Event **4688**]"* - ***Network Information*** -> ***Direction*** : *"Outbound"* - ***Network Information*** -> ***Destination Address*** : *"[Domain Controller IP Address]"* - ***Network Information*** -> ***Destination Port*** / ***Protocol*** : *"445"* / *"6"* (TCP) - **Confirmable Information** - **Source Port**: ***Source Port*** *Used for association with logs on the Domain Controller side	
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : `"[\device\harddiskvolume2\windows\system32\lsass.exe"` - ***Application Information*** -> ***Process ID*** : *"[Process ID Recorded in Event **4688**]"* - ***Network Information*** -> ***Direction*** : *"Outbound"* - ***Network Information*** -> ***Destination Address*** : *"[Domain Controller IP Address]"* - ***Network Information*** -> ***Destination Port*** / ***Protocol*** : *"88"* / *"6"* (TCP) - **Confirmable Information** - **Source Port**: ***Source Port*** *Used for association with logs on the Domain Controller side	
			Event ID : **4769** (A Kerberos service ticket was requested) - **Confirmable Information** - **Client IP Address**: ***Network Information*** -> ***Client Address*** - **Ticket Request Type** (Two different pairs of ticket requests are output.) - ***Service Information*** : *"[Host Name]$"* , ***Ticket Option*** : *"0x40810000"* - ***Service Information*** : *"krbtgt"* , ***Ticket Option*** : *"0x60810010"*	
			Event ID : **4672** (Special privileges assigned to new logon) - **Confirmable Information** - **Account with Escalated Privileges**: ***Subject*** -> ***Account Name*** / ***Account Domain*** - **Available Special Privileges**: ***Special Privileges*** (*"SeSecurityPrivilege"* / *"SeRestorePrivilege"* / *"SeTakeOwnershipPrivilege"* / "SeDebugPrivilege" / *"SeSystemEnvironmentPrivilege"* / *"SeLoadDriverPrivilege"* / *"SeImpersonatePrivilege"* / *"SeEnableDelegationPrivilege"*)	
			Event ID : **4624** (An account was successfully logged on) - ***Logon Type*** : *"3"* - **Confirmable Information** - **Used Security ID**: ***New Logon*** -> ***Security ID*** *If the security ID used and the account does not correspond, this value is the security ID of the captured account. - **Account**: ***Account Name*** / ***Account Domain*** - **Host which Requested Logon**: ***Network Information*** -> ***Source Network Address***	

Remarks

Additional Event Logs That Can Be Output	Logs of commands executed with escalated privileges may be recorded at the destination host.

3.9.2. Mimikatz (Golden Ticket)

Basic Information

Tool	Tool Name	Mimikatz (Golden Ticket)
	Category	Capturing the Domain Administrator Privilege and Account Credentials
	Tool Overview	Issues an unauthorized Kerberos ticket that is valid for an arbitrary period and grants access without additional authentication
	Example of Presumed Tool Use During an Attack	This tool is used to grant a host concealing a record of authentication requests access using the Golden Ticket. - Source host: Mimikatz execution source - Destination host: The host logon in by Mimikatz
Operating Condition	Authority	Standard user *The NTLM password hash for a krbtgt account on the domain must have already been acquired.
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	-
	Service	Active Directory Domain Service
Information Acquired from Log	Standard Settings	- Source host: Execution history (Prefetch)
	Additional Settings	- Source host: Execution history (Sysmon / audit policy) Access history (Sysmon - RawAccessRead, audit policy - Use of important privileges) - Destination host: Logon by an account with an illegal domain
Evidence That Can Be Confirmed When Execution is Successful		- Destination host: If the following log is in the event log, it is considered that unauthorised logon was attempted. - In the event IDs **4672**, **4624**, and **4634** in the event log "Security", a logon attempt by an account with an illegal domain is recorded.

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**	**Additional Settings**
OS: Windows user ↓ OS: Windows Server administrator	Source host	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name (mimikatz.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **4673** (A privileged service was called) - ***Process Information*** -> ***Process Name*** : *"[File Name (mimikatz.exe)]"* - ***Process Information*** -> ***Process ID*** : *"[Process ID of the Tool]"* - ***Service Request Information*** -> ***Privileges*** : *"SeTcbPrivilege"* - ***Keyword*** : *"Audit Failure"* - **Confirmable Information** - **Account That Attempted the Above Operation**: ***Account Name*** (Standard user)	
			- ***Event ID*** : **4663** (An attempt was made to access an object) **4656** (A handle to an object was requested) **4658** (The handle to an object was closed) - ***Process Information*** -> ***Process Name*** : *"[File Name (mimikatz.exe)]"* - **Confirmable Information** - **Target File**: ***Object*** -> ***Object Name*** - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs - **Process Details**: ***Access Request Information*** -> ***Access*** (*"WriteData (or AddFile)" / "AppendData (or AddSubdirectory or CreatePipeInstance)"*) - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (mimikatz.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
			Event ID : **9** (RawAccessRead detected) - ***Process*** : The ***ProcessId*** recorded in the event **1**. - ***Image*** : *"[File Name (mimikatz.exe)]"* - ***Device*** : *"*`\Device\HarddiskVolume2`*"*	
		Execution History - Prefetch	**File name:** **`C:\Windows\Prefetch\[Executable File(MIMIKATZ.EXE)]-[RANDOM].pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Executed Time and Date**: ***Last Execution Time***	-
	Destination host	Event Log - Security	***Event ID*** : **4769** (A Kerberos service ticket was requested) - **Confirmable Information** - **Client IP Address**: ***Network Information*** -> ***Client Address*** - **Ticket Request Type** (Two different pairs of ticket requests are output.) - ***Service Information*** : *"[Host Name]$"* , ***Ticket Options*** : *"0x40810000"* - ***Service Information*** : *"krbtgt"* , ***Ticket Options*** : *"0x60810010"*	Required
			Event ID : **4672** (Special privileges assigned to new logon) - **Confirmable Information** - **Account for which a Golden Ticket was Obtained**: ***Account*** (An existing account name) - **Domain**: ***Account Domain*** (An invalid value) - **Logon ID**: **Logon ID** *Used for association with other logs - **Available Privileges**: ***Special Privileges***	
			Event ID : **4624** (An account was successfully logged on) - ***Logon Type*** : *"3"* - ***New Logon*** -> ***Account Name*** / ***Account Domain*** : *"[* ***Account Name*** */* ***Account Domain*** *Recorded in Event* ***4672*** *]"* - ***New Logon*** -> ***Logon ID*** : *"[* ***Logon ID*** *Recorded in Event* ***4672*** *]"* - **Confirmable Information** - **Used Security ID**: ***New Logon*** -> ***Security ID*** - **Host That Used Authentication Information**: ***Network Information*** -> ***Source Network Address***	
			Event ID : **4634** (An account was logged off) - ***Logon Type*** : *"3"* - ***New Logon*** -> ***Account Name*** / ***Account Domain*** : *"[* ***Account Name*** */* ***Account Domain*** *Recorded in Event* ***4672*** *]"* - ***New Logon*** -> ***Logon ID*** : *"[* ***Logon ID*** *Recorded in Event* ***4672*** *]"*	

Remarks

Additional Event Logs That Can Be Output	At the host for which access was granted by using a Golden Ticket, logs related to the executed command may be recorded.

3.9.3. Mimikatz (Silver Ticket)

Basic Information

Tool	Tool Name	Mimikatz (Silver Ticket)
	Category	Capturing the Domain Administrator Privilege and Account Credentials
	Tool Overview	Issues an unauthorized Kerberos ticket that is valid for an arbitrary period and grants access without additional authentication
	Example of Presumed Tool Use During an Attack	This tool is used to grant a host concealing a record of authentication requests access using the Silver Ticket. - Source host: Mimikatz execution source - Destination host: The host logon in by Mimikatz
Operating Condition	Authority	Standard user *The NTLM password hash for a service account on the domain must have already been acquired.
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	-
	Service	Active Directory Domain Services
Information Acquired from Log	Standard Settings	- Source host: Execution history (Prefetch)
	Additional Settings	- Source host: Execution history (Sysmon / audit policy) - Destination host: Logon by an account with an invalid domain
Evidence That Can Be Confirmed When Execution is Successful		- Destination host: If the following log is in the event log, it is considered that unauthorised logon was attempted. - In the event IDs **4672**, **4624**, and **4634** in the event log "Security", a logon attempt by an account with an illegal domain is recorded.

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**	**Additional Settings**
OS: Windows user ↓ OS: Windows Server service account	Source host	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name (mimikatz.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **4673** (A privileged service was called) - ***Process Information*** -> ***Process Name*** : *"[File Name (mimikatz.exe)]"* - ***Process Information*** -> ***Process ID*** : *"[Process ID of the Tool]"* - ***Service Request Information*** -> ***Privileges*** : *"SeTcbPrivilege"* - ***Keyword*** : *"Audit Failure"* - **Confirmable Information** - **Account That Attempted the Above Operation**: ***Account Name*** (Standard user)	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (mimikatz.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
			Event ID : **9** (RawAccessRead detected) - ***Process*** : The ***ProcessId*** recorded in the event **1** - ***Image*** : *"[File Name (mimikatz.exe)]"* - ***Device*** : *"`\Device\HarddiskVolume2`"*	
		Execution History - Prefetch	File name: **`C:\Windows\Prefetch\[Executable File(MIMIKATZ.EXE)]-[RANDOM].pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Executed Time and Date**: ***Last Execution Time***	-
	Destination host	Event Log - Security	- Unlike a Golden Ticket, communication with the Domain Controller does not occur when a ticket is generated. - The following is a log recorded when an incoming connection is received using a ticket.	Required
			Event ID : **4672** (Special privileges assigned to new logon) - ***Special Privileges*** : *"SeSecurityPrivilege"* / *"SeBackupPrivilege"* / *"SeRestorePrivilege"* / *"SeTakeOwnershipPrivilege"* / *"SeSystemEnvironmentPrivilege"* / *"SeLoadDriverPrivilege"* / *"SeImpersonatePrivilege"* / *"SeEnableDelegationPrivilege"* - **Confirmable Information** - **Captured Account Name**: ***Account*** (An existing account name) - **Domain**: ***Account Domain*** (An invalid value) - **Logon ID**: ***Logon ID*** *Used for association with other logs - **Available Privileges**: ***Special Privileges***	
			Event ID : **4624** (An account was successfully logged on) - ***Logon Type*** : *"3"* - ***New Logon*** -> ***Account Name*** / ***Account Domain*** : *"[**Account Name** / **Account Domain** Recorded in Event **4672**]"* - ***New Logon*** -> ***Logon ID*** : *"[**Logon ID** Recorded in Event **4672**]"* - **Confirmable Information** - **Used Security ID**: ***New Logon*** -> ***Security ID*** - **Host That Used Authentication Information**: - ***Network Information*** -> ***Source Network Address***	
			Event ID : **4634** (An account was logged off) - ***Logon Type*** : *"3"* - ***New Logon*** -> ***Account Name*** / ***Account Domain*** : *"[**Account Name** / **Account Domain** Recorded in Event **4672**]"* - ***New Logon*** -> ***Logon ID*** : *"[**Logon ID** Recorded in Event **4672**]"*	

Remarks

Additional Event Logs That Can Be Output	At the host for which access was granted by using a Silver Ticket, logs related to the executed command may be recorded.

3.10.1. ntdsutil

Basic Information

Tool	Tool Name	ntdsutil
	Category	Obtaining Active Directory database
	Tool Overview	A command to maintain Active Directory databases
	Example of Presumed Tool Use During an Attack	This tool is used to extract NTDS.DIT, a database for NTDS, and other tools are used to analyze passwords (executed in Active Directory).
Operating Condition	Authority	Administrator
	Targeted OS	Windows Server
	Domain	Required
	Communication Protocol	-
	Service	Active Directory Domain Services
Information Acquired from Log	Standard Settings	- The fact that the service has started and that a driver was installed on a storage device - History of shadow copy creation
	Additional Settings	- Execution history (Sysmon / audit policy)
Evidence That Can Be Confirmed When Execution is Successful		If the following is confirmed, it is possible that information was breached. - If ntdsutil.exe was executed and the following log is recorded in the event log: - The Event ID **8222** is recorded in the event log "Security". - A request for a handle for *"[System Drive]\SNAP_[Date and Time]_VOLUME[Drive Letter]$"* was successful *Additionally, if a log indicating that files under C:\Windows\NTDS, which cannot be normally read, were copied (Event ID: **4663**) is recorded, it is possible that a shadow copy was used.

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	Additional Settings
-	Active Directory Domain Controller	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\ntdsutil.exe"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Process ID**: ***Process Information*** -> ***New Process ID*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **4673** (A privileged service was called) - ***Process*** -> ***Process Name*** : *"C:\Windows\explorer.exe"* - **Confirmable Information** - **Privileges Used**: ***Service Request Information*** -> ***Privileges*** (*"SeTcbPrivilege"*)	
			Event ID : **8222** (Shadow copy has been created) - **Confirmable Information** - **Shadow Copy Name**: ***Shadow Device Name*** *This log is recorded without a need to configure additional settings.	
			Event ID : **4656** (A handle to an object was requested) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\VSSVC.exe"* - **Confirmable Information** - **Mount Point**: ***Object*** -> ***Object Name*** (*"C\SNAP_[Date and Time]_VOLUME[C]$"*) - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	
			- **Remarks** - If a log indicating that files under C:\Windows\NTDS, which cannot be normally read (event **4663**) was successful, it is considered that access was successful. Note that outputting the event **4663** requires the audit of object access.	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C:\Windows\System32\ntdsutil.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Event Log - System	***Event ID*** : **7036** - ***Detailed*** Tab -> It is possible that a start of a service with ***EventData\param1*** set to one of the following may be recorded: - *"Volume Shadow Copy"* - *"Microsoft Software Shadow Copy Provider"* - *"Windows Modules Installer"* *If a service has already been executed, a log will not be output.	-
			Event ID : **20001** - ***Details*** Tab -> ***System\Provider\Name*** is set to *"Microsoft-Windows-UserPnp"* . - **Confirmable Information** - **Process ID**: ***System\Execution\ProcessID*** *Matches the process ID of drvinst.exe output in the Sysmon log. - **Snapshot Name**: ***UserData\InstallDeviceID\DeviceInstanceID*** *If a similar snapshot was mounted before, an event log may not be output.	
		Execution History - Registry	Registry Entry: HKEY_LOCAL_MACHINE\CurrentControlSet\Enum\STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot[Snapshot Number] - If drvinst.exe has been executed, a new key is created.	-

Remarks

Additional Event Logs That Can Be Output	It is possible that the fact that a driver was installed is left in volsnap.inf as a difference. (*If a similar snapshot was mounted before, an event log may not be recorded.)

3.10.2. vssadmin

Basic Information

Tool	Tool Name	vssadmin
	Category	Obtaining Active Directory database
	Tool Overview	Creates Volume Shadow Copy and extracts NTDS.DIT
	Example of Presumed Tool Use During an Attack	This tool is used to extract NTDS.DIT, a database for NTDS, so that the password can be analysed using other tools.
Operating Condition	Authority	Administrator
	Targeted OS	Windows Server
	Domain	Required
	Communication Protocol	-
	Service	Active Directory Domain Services
Information Acquired from Log	Standard Settings	- The fact that the service has started and that a driver was installed on a storage device - History of shadow copy creation
	Additional Settings	- Execution history (Sysmon / audit policy)
Evidence That Can Be Confirmed When Execution is Successful		If the following log is in the event log, it is considered that a shadow copy was created. - The Event ID **8222** is recorded in the event log "Security". *Additionally, if a log indicating that files under `C:\Windows\NTDS`, which cannot be normally read, were copied (Event ID: **4663**) is recorded, it is possible that a shadow copy was used.

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	Additional Settings
-	Active Directory Domain Controller	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\vssadmin.exe"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Process ID**: ***Process Information*** -> ***New Process ID*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **8222** (A shadow copy was created) - **Confirmable Information** - **Shadow Copy Name**: ***Shadow Device Name***	-
			- **Remarks** - If a log indicating that files under `C:\Windows\NTDS`, which cannot be normally read (event **4663**) was successful, it is considered that access was successful. The content of an output log depends on the software used for copying. Note that outputting the event **4663** requires the audit of object access.	
		Event Log - System	***Event ID*** : **7036** - ***Detailed*** Tab -> ***System\Provider\Name*** : *"Service Control Manager"* - ***Details*** Tab -> ***EventData\param1*** : *"Volume Shadow Copy"* - **Confirmable Information** - **Executing the Service**: ***Details*** Tab -> ***EventData\param2*** (*"Being executed"*) *If the Volume Shadow Copy service is already running, a log will not be output.	-
			Event ID : **20001** - ***Detailed*** Tab -> ***System\Provider\Name*** : *"Microsoft-Windows-UserPnp"* - **Confirmable Information** - **Process ID**: ***System\Execution\ProcessID*** *Matches the process ID of drvinst.exe output in the Sysmon log. - **Snapshot Name**: ***UserData\InstallDeviceID\DeviceInstanceID*** *If a similar snapshot was mounted before, an event log may not be output.	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C:\Windows\System32\vssadmin.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *Drives that are targeted for creating a shadow copy are recorded. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Registry	**Registry Entry:** `HKEY_LOCAL_MACHINE\CurrentControlSet\Enum \STORAGE\VolumeSnapshot\HarddiskVolumeSnapshot[Snapshot Number]` - If drvinst.exe has been executed, a new key is created.	-

Remarks

Additional Event Logs That Can Be Output	The fact that a driver was installed may be left in volsnap.inf as a difference. (*If a similar snapshot was mounted before, an event log may not be recorded.)

3.11.1. net user

Basic Information

Tool	Tool Name	net Command (net user)
	Category	Adding or Deleting a User/Adding or Deleting a Group
	Tool Overview	Adds a user account in a client or the domain
	Example of Presumed Tool Use During an Attack	This tool is used to create accounts or additional sessions in the machine the attacker has infected or to communicate with other hosts.
Operating Condition	Authority	Administrator
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	- *With domain administrator, accounts can also be created on the Domain Controller.
	Service	-
Information Acquired from	Standard Settings	- The fact that a user has been added is recorded in a log.
	Additional Settings	- A user name and password specified by the "net user" command are recorded (Sysmon).
Evidence That Can Be Confirmed When Execution is Successful		If the following log is in the event log, it is considered that a user was added. - The Event ID **4720** is recorded in the event log "Security".

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	Additional Settings
-	Host (Windows)	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\net.exe"* *"C:\Windows\System32\net1.exe"* *After net.exe is executed, net1.exe is executed as a child process. - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** *It is type 1 or 2 because administrator rights are required. - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **4656** (SAM - A handle to an object was requested) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\lsass.exe"* - ***Object*** -> ***Object Type*** : *"SAM_DOMAIN"* - **Confirmable Information** - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs - **Requested Process**: ***Access Request Information*** -> ***Access*** (*"ReadPasswordParameters"* / *"CreateUser"* / *"LookupIDs"*) - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	
			Event ID : **4720** (A user account was created) - ***New Account*** -> ***Account Name*** : A user name specified by the "**net user**" command - **Confirmable Information** - **User Group**: ***Attribute*** -> ***Primary Group ID*** *Depending on the details of the process executed, a different event (such as **4722**, **4724**, **4726**, **4737**, and **4738**) is recorded.	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C\Windows\System32\net.exe"* *"C:\Windows\System32\net1.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *The fact that **a user was added (user /add)** and **the user name and password (if passed to the argument)** are recorded in the argument. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required

Remarks

Additional Event Logs That Can Be Output	If addition to a group or others were performed, the relevant access history is recorded.

3.12.1. net use

Basic Information

Tool	Tool Name	net Command (net use)
	Category	File Sharing
	Tool Overview	Connects to shared folders that are publicly available on the network
	Example of Presumed Tool Use During an Attack	This tool is used to send in tools to be used during attacks via shared folders and to acquire information from a file server. - Source host: net command execution source - Destination host: the machine accessed by the net command
Operating Condition	Authority	Standard user
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	445/tcp
	Service	Destination host: Server, Source host: Workstation
Information Acquired from Log	Standard Settings	-
	Additional Settings	- Source host: Execution history (Sysmon / audit policy) - Destination host: Although a record of using Windows Filtering Platform remains, audit policy of read data is required to confirm the specific access path. *If a write is made to a shared point, it is recorded in the audit policy of write data.
Evidence That Can Be Confirmed When Execution is Successful		- Source host: If the following log is in the event log, it is possible that file sharing occurred. - The Event ID **4689** (A process has exited) of net.exe was recorded in the event log "Security" with the execution result (return value) of "0x0".

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	Additional Settings
OS: Windows user ↓ OS: Windows user	Source host	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\net.exe"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Network Information*** -> ***Direction*** : *"Outbound"* - ***Network Information*** -> ***Destination Address*** : *"[Host Specified as a Shared Folder]"* - ***Network Information*** -> ***Destination Port / Protocol*** : *"445"* / *"6"* (TCP) - **Confirmable Information** - **Source Port**: ***Network Information*** -> ***Source Port***	
		Execution History - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C\Windows\System32\net.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *The **destination host** and **share path** are recorded. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
	Destination host	Event Log - Security	***Event ID*** : **5156** (The Windows Filtering Platform has allowed a connection) - ***Network Information*** -> ***Direction*** : *"Inbound"* - ***Network Information*** -> ***Source Address*** : *"[IP Address of the File Server]"* - ***Network Information*** -> ***Source Port*** / ***Protocol*** : *"445"* / *"6"* (TCP) - **Confirmable Information** - **Source Host**: ***Network Information*** -> ***Destination Address*** - **Source Port**: ***Network Information*** -> ***Destination Port*** *Matches the source port of the source host	Required
	Active Directory Domain Controller	Event Log - Security	***Event ID*** : **4624** (An account was successfully logged on) - ***Logon Type*** : *"3"* - ***Network Information*** -> ***Source Network Address*** : *"[**Destination Address** in Event 5156]"* - ***Network Information*** -> ***Source Port*** : *"[**Destination Port** Recorded in Event 5156]"* - **Confirmable Information** - **Used User**: ***New Logon*** -> ***Account Name*** / ***Account Domain***	Required

Remarks

Additional Event Logs That Can Be Output	- If read data is enabled in the audit policy, the connected share path is recorded in the event **5140** (file sharing). - If write access is made to a share point, it is recorded in audit of object access.

3.12.2. net share

Basic Information

Tool	Tool Name	net Command (net share)
	Category	File Sharing
	Tool Overview	Shares particular folders so that they are available via network
	Example of Presumed Tool Use During an Attack	This tool is used to create a share path on the host the attacker has infected to read and write files.
Operating Condition	Authority	Administrator
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	- *Although a shared path is used via network, adding a shared folder with "net share" is completed on the machine.
	Service	Server
Information Acquired from	Standard Settings	- Information on a share path may be left on the registry. *The value will be cleared when shared folder is disabled.
	Additional Settings	- Execution history (Sysmon / audit policy) *The shared path and used share name are recorded.
Evidence That Can Be Confirmed When Execution is Successful		If the following log is in the event log, it can be deemed that a shared folder was created. - The event ID: **5142** is recorded in the event log "Security".

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	Additional Settings
-	Host (Windows)	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\net.exe"* *"C:\Windows\System32\net1.exe"* *After net.exe is executed, net1.exe is executed as a child process. - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** *It is type 1 or 2 because administrator rights are required. - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **5142** (A network share object was added) - **Confirmable Information** - **Share Name**: ***Shared Information*** -> ***Share Name*** - **Folder Used for Sharing**: ***Share Path***	
		Event Log - Sysmon	***Event IDs*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C:\Windows\System32\net.exe"* *"C:\Windows\System32\net1.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *The **share name** and **folder used for sharing** are recorded in the argument. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Access History - Registry	**Registry Entry: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares\Security\[Share Name]$`** *The entry is created when shared folder is enabled (when it is disabled, the value is cleared). Since the value is cleared when sharing is disabled, it is difficult to detect an attack unless there is a system for always monitoring the registry.	-

Remarks

Additional Event Logs That Can Be Output	-

3.12.3. icacls

Basic Information

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

Tool	Tool Name	icacls
	Category	File Sharing
	Tool Overview	Changes the file access rights
	Example of Presumed Tool Use During an Attack	- This tool is used to change the rights to read a file that cannot be read by the used account. - It is also used to capture rights so that the content of a file created by the attacker will not be viewable.
Operating Condition	Authority	Standard user * When the Access Control List (ACL) has been changed, appropriate rights for the relevant files are required.
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	-
	Service	-
Information Acquired from Log	Standard Settings	Execution history (Prefetch)
	Additional Settings	Execution history (Sysmon / audit policy)
Evidence That Can Be Confirmed When Execution is Successful		If the following log is in the event log, it is considered that file access rights were changed. - The Event IDs: **4688** and **4689** on icacls.exe are recorded in the event log "Security", and the ***Exit Status*** in the event ID: **4689** is set to *"0x0"*. *Since it is not possible to determine the target files from the Event IDs **4688** and **4689**, it is necessary to additionally check the command line of icacls.exe from the event ID **1** of sysmon.

Points to be Confirmed

Communication	Log Generation Location	Log Type and Name	Acquired Information Details	Additional Settings
-	Host (Windows)	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\icacls.exe"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
		Execution History - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C:\Windows\System32\icacls.exe"* - **Confirmable Information** - **Process Start/End Date and Time (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *The **target file** and **set rights** are recorded in the argument. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	**File name: C:\Windows\Prefetch\ICACLS.EXE-CCAC2A58.pf** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Executed Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	-

3.13.1. sdelete

Basic Information

Tool	Tool Name	sdelete
	Category	Deleting Evidence
	Tool Overview	Deletes a file after overwriting it several times
	Example of Presumed Tool Use During an Attack	This tool is used to delete a file created in the course of an attack to make it impossible to be recovered.
Operating Condition	Authority	Standard user
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	-
	Service	-
Information Acquired from Log	Standard Settings	- Execution history (Prefetch) - A statement to the effect that a license agreement on the use of sdelete was consented is recorded in the registry. *If the tool was used in the past, it cannot be confirmed from the information obtained under the standard setting.
	Additional Settings	- Execution history (Sysmon / audit policy) - A record of deleting and overwriting the file to be deleted during the audit of object access
Evidence That Can Be Confirmed When Execution is Successful		- A file with its name similar to the following was repeatedly deleted. - Example: sdeleAAAAAAAAAAAAAAAAAAAA.AAA, sdeleZZZZZZZZZZZZZZZZZZZZ.ZZZ when the target to be deleted is sdelete.txt

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	Additional Settings
-	Host (Windows)	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name (sdelete.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status*** ***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) - ***Process Information*** -> ***Process Name*** : *"[File Name (sdelete.exe)]"* - **Confirmable Information** - **File to be Deleted**: ***Object*** -> ***Object Name*** *In the course of deleting a file by overwriting it, sdelete creates a file with its name consisting of a combination of the name of the file to be deleted and some letters, and repeats the delete operation. (Example: sdeleAAAAAAAAAAAAAAAAAAAA.AAA when the target to be deleted is sdelete.txt) - **Process Details**: ***Access Request Information*** -> ***Access*** *For the same object, "*DELETE*" or "*WriteData or AddFile*" is repeated. - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	Required
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (sdelete.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *In addition to the executable file, the number of overwriting operations and other options passed to sdelete.exe can be found. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	**File name: `C:\Windows\Prefetch\[File Name (SDELETE.EXE)]-[RANDOM].pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-
		Execution History - Registry	**Registry Entry: `HKEY_USERS\[SID]\Software\Sysinternals\Sdelete`** - When the tool is used for the first time, the effect that the license agreement was consented is recorded in ***EulaAccepted*** . - If sdelete was used on the machine in the past, it is not possible to determine its use by the attacker.	-

Remarks

Additional Event Logs That Can Be Output	-

3.13.2. timestomp

Basic Information

Tool	Tool Name	timestomp
	Category	Deleting Evidence
	Tool Overview	Changes the file timestamp
	Example of Presumed Tool Use During an Attack	For a file whose timestamp has changed as a result of the use by the attacker, this tool is used to conceal the access to the file by restoring the timestamp.
Operating Condition	Authority	Standard user
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	-
	Service	-
Information Acquired from Log	Standard Settings	- Execution history (Prefetch)
	Additional Settings	- Execution history (Sysmon / audit policy) - Auditing of change of file creation date and time
Evidence That Can Be Confirmed When Execution is Successful		If the following log is in the event log, it is considered that the timestamp was changed. - The Event ID: **4663** is recorded in the event log "Security", and the *"WriteAttributes"* ***keyword*** for the target file is set to *"Audit 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**	**Additional Settings**
-	Host (Windows)	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name (timestomp.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **4656** (A handle to an object was requested) - ***Process Information*** -> ***Process Name*** : *"[File Name (timestomp.exe)]"* - **Confirmable Information** - **Targeted File**: ***Object*** -> ***Object Name*** - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs - **Process Details**: ***Access Request Information*** -> ***Access*** (*"SYNCHRONIZE"* , *"ReadAttributes"* , *"WriteAttributes"*) - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	
			Event ID : **4663** (An attempt was made to access an object) - ***Process Information*** -> ***Process Name*** : *"[File Name (timestomp.exe)]"* - **Confirmable Information** - **Targeted File**: ***Object*** -> ***Object Name*** - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs - **Process Details**: ***Access Request Information*** -> ***Access*** (*"WriteAttributes"*) - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	
			Event ID : **4658** (The handle to an object was closed) - ***Process Information*** -> ***Process Name*** : *"[File Name (timestomp.exe)]"* - **Confirmable Information** - **Handle ID**: ***Object*** -> ***Handle ID*** *The same as the ***handle ID*** recorded in events **4663** and **4656** to be output first	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (timestomp.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *The **target file**, **properties to be changed**, and **new timestamp** are recorded in the argument in the command line. - **User Name**: ***User***	Required
			Event ID : **2** (File creation time changed) - ***Image*** : *"[File Name (timestomp.exe)]"* - **Confirmable Information** - **Date and Time (UTC) the Change Occurred**: ***UtcTime*** - **New File Name**: ***TargetFilename*** - **New Timestamp (UTC)**: ***CreationUtcTime*** - **Previous Timestamp (UTC)**: ***PreviousCreationUtcTime*** *The Event ID: 2 shows a change in the file creation date and time, but it is output regardless of the type (creation, change, or access) of the changed timestamp. If an item other than the creation date and time is changed, the same time (original date and time) is recorded in the timestamp before and after the change. *Timestamps other than for the creation date and time will not be recorded.	
			Event ID : **9** (RawAccessRead detected - Direct disk read detected) - ***Image*** : *"[File Name (timestomp.exe)]"* - **Confirmable Information** - **Name of the Device that has the Target File**: ***Device*** (`"\Device\HarddiskVolume2"`)	
		Execution History - Prefetch	**File name:** `C:\Windows\Prefetch\[File Name (TIMESTOMP.EXE)]-[RANDOM].pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-

Remarks

Additional Event Logs That Can Be Output	-

3.14.1. wevtutil

Basic Information

Tool	Tool Name	wevtutil
	Category	Deleting Event Log
	Tool Overview	Deletes Windows event logs
	Example of Presumed Tool Use During an Attack	This tool is used to delete the evidence of an attack. - Source host: wevtutil command execution source - Destination host: The machine accessed by the wevtutil command
Operating Condition	Authority	Administrator
	Targeted OS	Windows
	Domain	Not required
	Communication Protocol	135/tcp
	Service	Event Log
Information Acquired from	Standard Settings	- The fact that an event log was cleared remains in each cleared log of the host.
	Additional Settings	- The account used for clearing logs and the host that executed the clear command can be confirmed.
Evidence That Can Be Confirmed When Execution is Successful		- Source host: If the following log is in the event log, it is considered that logs were cleared. - The Event ID: **104** is recorded in each target event log.

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**	**Additional Settings**
OS: Windows user ↓ OS: Windows administrator	Source host	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\wevtutil.exe"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **4648** (A logon was attempted using explicit credentials) - ***Process Information*** -> ***Process Name*** : *"C:\Windows\System32\wevtutil.exe"* - ***Process Information*** -> ***Process ID*** : The same as the process ID recorded in the event **4688** - **Confirmable Information** - **Local Account**: ***Subject*** -> ***Account Name*** / ***Account Domain*** - **Account Used at Destination Host**: ***Account for which a Credential was Used*** -> ***Account Name*** / ***Account Domain*** - **Destination Host**: ***Target Server*** -> ***Target Server Name***	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"C:\Windows\System32\wevtutil.exe"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
	Destination host	Event Log - Each Target Log	***Event ID*** : **104** (The System log file was cleared) - **Confirmable Information** - **User**: ***Detailed*** Tab -> ***UserData\SubjectUserName / SubjectDomainName*** - **Target Log Name**: ***Detailed*** Tab -> ***UserData\Channel***	-
		Event Log - Security	***Event ID*** : **4672** (Special privileges assigned to new logon) - **Confirmable Information** - **Account with Escalated Privileges**: ***Subject*** -> ***Account Name*** / ***Account Domain*** - **Available Privileges**: ***Special Privileges*** (*"SeSecurityPrivilege"* / *"SeRestorePrivilege"* / *"SeTakeOwnershipPrivilege"* / "SeDebugPrivilege" / *"SeSystemEnvironmentPrivilege"* / *"SeLoadDriverPrivilege"* / *"SeImpersonatePrivilege"* / *"SeEnableDelegationPrivilege")*	Required
			Event ID : **4624** (An account was successfully logged on) - ***Logon Type*** : *"3"* - **Confirmable Information** - **Used Security ID**: ***New Logon*** -> ***Security ID*** - **Account**: ***Account Name*** / ***Account Domain*** - **Host which Requested Logon**: ***Network Information*** -> ***Source Network Address***	

Remarks

Additional Event Logs That Can Be Output	-

3.15.1. csvde

Basic Information

Tool	Tool Name	csvde
	Category	Acquisition of Account Information
	Tool Overview	Outputs account information on the Active Directory in the CSV format
	Example of Presumed Tool Use During an Attack	This tool is used to extract information on an existing account and select users and clients available as attack targets. - Source host: csvde command execution source - Destination host: The machine in which information is collected by the csvde command
Operating Condition	Authority	Standard user
	Targeted OS	Windows
	Domain Participation	Not required *By entering correct authentication information, it is possible to obtain information remotely from a client that does not participate in the domain.
	Communication Protocol	389/tcp
	Service	Active Directory Domain Services
Information Acquired from Log	Standard Settings	Source host: Execution history (Prefetch)
	Additional Settings	- Source host: The fact that a csv file was created by csvde.exe. The fact that *`"C:\Users\[User Name]\AppData\Local\Temp\csv[Random Number].tmp"`* was created as a temporary file when creating a csv file. - Destination host: Inbound to 389/tcp and login with Kerberos Authentication are recorded.
Evidence That Can Be Confirmed When Execution is Successful		- Source host: csvde.exe was executed and a file specified by the "-f" option was created. - `"C:\Users\[User Name]\AppData\Local\Temp\csv[Random Number].tmp"` was created and deleted.

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	Additional Settings
OS: Windows user ↓ OS: Windows Server domain user	Source host	Event Log - Security	***Event ID***: **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name***: *"[File Name (csvde.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID: **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name***: *"[File Name (csvde.exe)]"* - ***Network Information*** -> ***Direction***: *"Outbound"* - ***Network Information*** -> ***Destination Address***: *"[Domain Controller IP Address]"* - ***Network Information*** -> ***Destination Port*** / ***Protocol***: *"389"* / *"6"* (TCP) - **Confirmable Information** - **Source Port**: ***Source Port*** *Used for association with logs on the Domain Controller side	
			Event ID: **4663** (An attempt was made to access an object) **4656** (A handle to an object was requested) **4658** (The handle to an object was closed) - ***Process Information*** -> ***Process Name***: *"[File Name (csvde.exe)]"* - **Confirmable Information** - **Target File**: ***Object*** -> ***Object Name***: (*`"C:\Users\[User Name]\AppData\Local\Temp\csv[Random Number].tmp"`*) - **Handle ID (Used for Association with Other Logs)**: ***Object*** -> ***Handle ID*** - **Process Details**: ***Access Request Information*** -> ***Access*** (*"SYNCHRONIZE"* / *"WriteData (or AddFile)"* / *"AppendData (or AddSubdirectory, or CreatePipeInstance)"* / *"WriteEA"* / *"WriteAttributes"*) - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	
			Event ID: **4663** (An attempt was made to access an object) **4656** (A handle to an object was requested) **4658** (The handle to an object was closed) - ***Process Information*** -> ***Process Name***: *"[File Name (csvde.exe)]"* - ***Object*** -> ***Object Name***: *"[File specified with the "-f" option when executing csvde.exe]"* - **Confirmable Information** - **Handle ID (Used for Association with Other Logs)**: ***Object*** -> ***Handle ID*** - **Process Details**: ***Access Request Information*** -> ***Access*** (*"WriteData or AddFile"* / *"AppendData, AddSubdirectory, or CreatePipeInstance"*) - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	
			Event ID: **4663** (An attempt was made to access an object) **4656** (A handle to an object was requested) **4658** (The handle to an object was closed) - ***Process Information*** -> ***Process Name***: *"[File Name (csvde.exe)]"* - ***Object*** -> ***Object Name*** (*`"C:\Users\[User Name]\AppData\Local\Temp\csv[Random Number].tmp"`*) - **Confirmable Information** - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs - **Process Details**: ***Access Request Information*** -> ***Access*** (*"DELETE"*) - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	
		Event Log - Sysmon	***Event ID***: **1** (Process Create) **5** (Process Terminated) - ***Image***: *"[File Name (csvde.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *If a user or file name is specified, an argument is recorded. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	**File name: `C:\Windows\Prefetch\[File Name(CSVDE.EXE)]-[RANDOM].pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Executed Time and Date**: ***Last Execution Time***	-

Communication	Log Generation Location	Log Type and Name	Acquired Information Details	Additional Settings
OS: Windows user ↓ OS: Windows Server domain user (Continued from the previous entry)	Destination host	Event Log - Security	***Event ID*** : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"\device\harddiskvolume2\windows\system32\lsass.exe"* - ***Network Information*** -> ***Direction*** : *"Inbound"* - ***Network Information*** -> ***Source Port*** / ***Protocol*** : *"389" / "6"* (TCP) - ***Network Information*** -> ***Destination Port*** : *"[**Source Port** recorded in the client which executed csvde.exe]"* - **Confirmable Information** - **Source Host**: ***Destination Port***	Required
			Event ID : **4624** (An account was successfully logged on) **4634** (An account was logged off) - ***Logon Type*** : *"3"* - ***Network Information*** -> ***Source Network Address*** : *"[**Destination Address** in **Event 5156**]"* - ***Network Information*** -> ***Source Port*** : *"[**Destination Port** Recorded in Event **5156**]"* - **Confirmable Information** - **Used User**: ***New Logon*** -> ***Account Name / Account Domain*** - **New Logon ID**: ***New Logon*** -> ***Logon ID*** *Used for association with other logs	

Remarks

Additional Event Logs That Can Be Output	-

3.15.2. ldifde

Basic Information

Tool	Tool Name	ldifde
	Category	Acquisition of Account Information
	Tool Overview	Outputs account information on the Active Directory in the LDIF format
	Example of Presumed Tool Use During an Attack	This tool is used to extract information on an existing account and select users and clients available as attack targets. - Source host: ldifde command execution source - Destination host: The machine in which information is collected by the ldifde command
Operating Condition	Authority	Standard user
	Targeted OS	Windows
	Domain Participation	Not required *By entering correct authentication information, it is possible to obtain information remotely from a client that does not participate in the domain.
	Communication Protocol	389/tcp
	Service	Active Directory Domain Services
Information Acquired from Log	Standard Settings	- Source host: Execution history (Prefetch)
	Additional Settings	- Source host: The fact that a LDIF file was created by ldifde.exe. - Destination host: Inbound to 389/tcp and login with Kerberos Authentication are recorded.
Evidence That Can Be Confirmed When Execution is Successful		- Source host: ldifde.exe was executed and a file specified by the "-f" option was created.

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	Additional Settings
OS: Windows user ↓ OS: Windows Server domain user	Source host	Event Log - Security	*Event ID* : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name (ldifde.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	-
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"[File Name (ldifde.exe)]"* - ***Network Information*** -> ***Direction*** : *"Outbound"* - ***Network Information*** -> ***Destination Address*** : *"[Domain Controller IP Address]"* - ***Network Information*** -> ***Destination Port*** / ***Protocol*** : *"389"* / *"6"* (TCP) - **Confirmable Information** - **Source Port**: ***Source Port*** *Used for association with logs on the Domain Controller side	
			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) - ***Process Information*** -> ***Process Name*** : *"[File Name (ldifde.exe)]"* - ***Object*** -> ***Object Name*** : *"[File specified with the "-f" option when executing ldifde.exe]"* - **Confirmable Information** - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs - **Process Details**: ***Access Request Information*** -> ***Access*** (*"WriteData or AddFile"* / *"AppendData, AddSubdirectory, or CreatePipeInstance"*) - **Success or Failure**: ***Keywords*** (*"Audit Success"*)	
		Event Log - Sysmon	*Event ID* : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (ldifde.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *If a user or file name is specified, an argument is recorded. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	**File name:** `C:\Windows\Prefetch\[File Name (LDIFDE.EXE)]-[RANDOM].pf` - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Execution Time and Date**: ***Last Execution Time***	-
	Destination host	Event Log - Security	*Event ID* : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"`\device\harddiskvolume2\windows\system32\lsass.exe`"* - ***Network Information*** -> ***Direction*** : *"Inbound"* - ***Network Information*** -> ***Source Port*** / ***Protocol*** : *"389"* / *"6"* (TCP) - ***Network Information*** -> ***Destination Port*** : *"[**Source Port** recorded in the client which executed ldifde.exe]"* - **Confirmable Information** - **Source Host**: ***Destination Port*** - **Success or Failure**: ***Keyword***	Required
			Event ID : **4624** (An account was successfully logged on) - ***Logon Type*** : *"3"* - ***Network Information*** -> ***Source Network Address*** : *"[**Destination Address** in **Event 5156**]"* - ***Network Information*** -> ***Source Port*** : *"[**Destination Port** Recorded in Event **5156**]"* - **Confirmable Information** - **Used User**: ***New Logon*** -> ***Account Name*** / ***Account Domain*** - **New Logon ID**: ***New Logon*** -> ***Logon ID*** *Used for association with other logs	
			Event ID : **4634** (An account was logged off) - ***Subject*** -> ***Account Name*** / ***Account Domain*** / ***Logon ID*** : *"[The same as the one recorded in Event **4624**]"*	

Remarks

Additional Event Logs That Can Be Output	-

3.15.3. dsquery

Basic Information

Tool	Tool Name	dsquery
	Category	Acquisition of Account Information
	Tool Overview	Obtains information, such as users and groups, from a directory service
	Example of Presumed Tool Use During an Attack	This tool is used to extract information on an existing account and select users and clients available as attack targets. - Source host: dsquery command execution source - Destination host: The machine in which information is collected by the dsquery command
Operating Condition	Authority	Standard user * Depending on the Access Control List (ACL) setting, some information cannot be obtained with standard user privileges.
	Targeted OS	Windows
	Domain Participation	Not required * This investigation is conducted on the Domain Controller. By entering correct authentication information, it is possible to obtain information remotely from a client that does not participate in the domain.
	Communication Protocol	389/tcp
	Service	Active Directory Domain Services
Information Acquired from Log	Standard Settings	- Source host: Execution history (Prefetch)
	Additional Settings	- Source host: Execution history (Sysmon / audit policy) - Destination host: Inbound to 389/tcp and login with Kerberos Authentication are recorded.
Evidence That Can Be Confirmed When Execution is Successful		The successful execution of the tool cannot be determined from event logs, execution history, and so on. *If the extracted account information is saved, it can be considered that the tool execution was successful.

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	Additional Settings
OS: Windows user ↓ OS: Windows Server user	Source host	Event Log - Security	***Event ID*** : **4688** (A new process has been created) **4689** (A process has exited) - ***Process Information*** -> ***Process Name*** : *"[File Name (dsquery.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date**: Log Date - **Name of User Who Executed the Process**: ***Subject*** -> ***Account Name*** - **Domain of User Who Executed the Process**: ***Subject*** -> ***Account Domain*** - **Presence of Privilege Escalation at Process Execution**: ***Process Information*** -> ***Token Escalation Type*** - **Process Return Value**: ***Process Information*** -> ***Exit Status***	Required
			Event ID : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"[File Name (dsquery.exe)]"* - ***Network Information*** -> ***Direction*** : *"Outbound"* - ***Network Information*** -> ***Destination Address*** : *"[Domain Controller IP Address]"* - ***Network Information*** -> ***Destination Port*** / ***Protocol*** : *"389"* / *"6"* (TCP) - **Confirmable Information** - **Source Port**: ***Source Port*** *Used for association with logs on the Domain Controller side	
			Event ID : **4663** (An attempt was made to access an object) **4656** (A handle to an object was requested) **4658** (The handle to an object was closed) - ***Process Information*** -> ***Process Name*** : *"[File Name (dsquery.exe)]"* - ***Object*** -> ***Object Name*** : *"C:\Users\[User Name]\AppData\Local\Microsoft\Windows\SchCache\[Domain Name].sch"* - **Confirmable Information** - **Handle ID**: ***Object*** -> ***Handle ID*** *Used for association with other logs - **Process Details**: ***Access Request Information*** -> ***Access*** (*"WriteData or AddFile"* / *"AppendData, AddSubdirectory, or CreatePipeInstance"*) - **Success or Failure**: ***Keywords*** (*"Audit Success"*) *The Event IDs **4656**, **4663**, and **4658** may not be output if a valid sch file already exists.	
		Event Log - Sysmon	***Event ID*** : **1** (Process Create) **5** (Process Terminated) - ***Image*** : *"[File Name (dsquery.exe)]"* - **Confirmable Information** - **Process Start/End Time and Date (UTC)**: ***UtcTime*** - **Process Command Line**: ***CommandLine*** *If a user or file name is specified, an argument is recorded. - **User Name**: ***User*** - **Process ID**: ***ProcessId***	Required
		Execution History - Prefetch	**File name: `C:\Windows\Prefetch\[File Name (DSQUERY.EXE)]-[RANDOM].pf`** - **Confirmable Information** (the following can be confirmed using this tool: WinPrefetchView) - **Last Executed Time and Date**: ***Last Execution Time***	-
	Destination host	Event Log - Security	***Event ID*** : **5156** (The Windows Filtering Platform has allowed a connection) - ***Application Information*** -> ***Application Name*** : *"\device\harddiskvolume2\windows\system32\lsass.exe"* - ***Network Information*** -> ***Direction*** : *"Inbound"* - ***Network Information*** -> ***Source Port*** / ***Protocol*** : *"389"* / *"6"* (TCP) - ***Network Information*** -> ***Destination Port*** : *"[**Source Port** recorded in the client that executed dsquery.exe]"* - **Confirmable Information** - **Source Host**: ***Destination Port***	Required
			Event ID : **4624** (An account was successfully logged on) **4634** (An account was logged off) - ***Logon Type*** : *"3"* - ***Network Information*** -> ***Source Network Address*** : *"[**Destination Address** in **Event 5156**]"* - ***Network Information*** -> ***Source Port*** : *"[**Destination Port** Recorded in Event **5156**]"* - **Confirmable Information** - **Used User**: ***New Logon*** -> ***Account Name*** / ***Account Domain*** - **New Logon ID**: ***New Logon*** -> ***Logon ID*** *Used for association with other logs	

Remarks

Additional Event Logs That Can Be Output	-

3.16. Evidence That Can Be Observed for Successful Tool Execution

The following table describes criteria to observe the execution of a tool and command, and the success of the attack.
Note that logs are described in each sheet in more detail.

Category	Investigation Target	Success or Failure Decision
Command Execution	**PsExec**	If the following is confirmed, it is possible that PsExec was executed. - Source host: If the following log is in the event log - The Event ID **4689** (A process has exited) of psexec.exe was recorded in the event log "Security" with the execution result (return value) of "0x0". - Destination host: PSEXESVC.exe is installed.
	wmic	If the following logs that have the same log time are found at "source host" and "destination host", it is possible that a remote connection was made. - Source host: If the following log is in the event log: - The Event ID **4689** (A process has exited) of WMIC.exe was recorded in the event log "Security" with the execution result (return value) of "0x0". - Destination host: If the following log is in Sysmon: - It is recorded in the event log "Sysmon" that WmiPrvSE.exe was executed with the Event IDs **1** and **5**.
	PowerShell	If the following logs that have the same log time are found, it is possible that a remote command was executed. *This also applies to Prefetch. - Source host: If the following log is in the event log: - The Event ID **4689** (A process has exited) of PowerShell was recorded in the event log "Security" with the execution result (return value) of "0x0". - Destination host: If the following log is in the event log: - The Event ID **4689** (A process has exited) of wsmprovhost.exe was recorded in the event log "Security" with the execution result (return value) of "0x0".
	wmiexec.vbs	- Destination host: The "WMI_SHARE" share has been created and deleted.
	BeginX	- Source host: The fact that communication via a permitted port occurred unintentionally at the destination host is recorded. - Destination host: Unintended communication is permitted for Windows Firewall, and a tool that is listening at the relevant port exists.
	WinRM	- Source host: If the following log exists, it is possible that WinRM was executed. - A log indicating that cscript.exe accessed the destination host with Event IDs **1** and **5** of the event log "Sysmon" is recorded.
	WinRS	- The execution of WinRS is recorded in the event log "Application and Service\Microsoft\Windows\Windows Remote Management\Operational".
	at	- 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 value) of "0x0". - 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\Operational". - The Event IDs **200** (The operation that has been started) and **201** (The operation has been completed) are registered in the event log "\Microsoft\Windows\TaskScheduler\Operational", and the return value of the Event ID **201** is set to success.
	BITS	If the following log is in the event log, it is considered that a file was transferred. - The Event ID **60** is recorded in the event log "Application and Service Log\Microsoft\Windows\Bits-Client", and the status code is set to "0x0".
Password Hash Acquisition	**PWDump7**	The successful execution of the tool cannot be determined from event logs or execution history.
	PWDumpX	- Source host: If "[Path to Tool]\[Destination Address]-PWHashes.txt" has been created, it is considered that it was successfully executed.
	Quarks PwDump	- A temporary file ("SAM-[Random Number].dmp") was created and deleted.
	mimikatz (Password Hash Acquisition)	The successful execution of the tool cannot be determined from event logs or execution history.
	mimikatz (Ticket Acquisition)	- If a file that output a ticket is generated, it is considered that the process was successful.
	WCE	- The "C:\Users\[User Name]\AppData\Local\Temp\wceaux.dll" file was created and deleted.
	gsecdump	The successful execution of the tool cannot be determined from event logs or execution history.
	lslsass	The successful execution of the tool cannot be determined from event logs or execution history.
	Find-GPOPasswords.ps1	- A file in which a password was dumped (GPPDataReport-[Domain Name]-[Time and Date].csv) is output.
	Mail PassView	- If the extracted password is saved, it is considered that the execution was successful.
	WebBrowserPassView	- If the extracted password is saved, it is considered that the execution was successful.
	Remote Desktop PassView	- If the extracted password is saved, it is considered that the execution was successful.
Malicious Communication Relay (Packet Tunneling)	**Htran**	- Source host: If the following log is in the event log, it is possible that communication occurred. - It is recorded in the Event ID **5156** in the event log "Security" that a communication occurred with the tunnel host and tunnel destination host.
	Fake wpad	- Source host: Communication via 80/tcp and 8888/tcp was made with a host that is originally neither a proxy nor HTTP server. - Destination host: A host that is originally neither a proxy nor HTTP server was listening to 80/tcp and 8888/tcp. wpad.dat and proxy.log were created.
Remote Login	**RDP**	- Destination host: If the following logs are in the event log, it is considered that the connection was successful. - Event ID: **4624** is recorded in the event log "Security". - Event IDs **21** and **24** are recorded in the event log "Microsoft\Windows\TerminalServices-LocalSessionManager\Operational"
Pass-the-hash, Pass-the-ticket	**WCE**	- Source host: The fact that WCESERVICE was installed and executed is recorded. - Destination host: The fact that a logon was made from a remote host is recorded. - Both source host and destination host: The fact that communication using WMI occurred is recorded.
	mimikatz	- Destination host: If the following log is in the event log, it is considered that a remote login was made. - The Event ID 4624 is recorded in the event log "Security" regarding access from an unintended source host.
Escalation to SYSTEM Privileges	**MS14-058 Exploit**	- The Event ID: **4688** is recorded regarding a process executed with SYSTEM privileges, whose parent process cannot be the parent of the tool or that process.
	MS15-078 Exploit	- The Event ID: **4688** is recorded regarding a process executed with SYSTEM privileges, whose parent process cannot be the parent of the tool or that process.
Privilege Escalation	**SDB UAC Bypass**	- The fact that a process whose parent process name includes an application that is normally assumed not to be a parent process was executed is recorded.
Capturing the Domain Administrator and Account Credentials	**MS14-068 Exploit**	- Destination host: In the Event ID: 4672 of the event log "Security", high level privileges are granted to a standard user.
	Golden Ticket (mimikatz)	- Destination host: If the following log is in the event log, it is considered that unauthorised logon was attempted. - In the Event IDs 4672, 4624, and 4634 in the event log "Security", a logon attempt by an account with an illegal domain is recorded.
	Silver Ticket (mimikatz)	- Destination host: If the following log is in the event log, it is considered that unauthorised logon was attempted. - In the Event IDs 4672, 4624, and 4634 in the event log "Security", a logon attempt by an account with an illegal domain is recorded.

Category	Investigation Target	Success or Failure Decision
Capturing Active Directory Database (Creation of Domain Administrator or Addition of a User to Administrator Group)	**ntdsutil**	If the following is confirmed, it is possible that information was breached. - If ntdsutil.exe was executed and the following log is recorded in the event log: - The Event ID **8222** is recorded in the event log "Security". - A request for a handle for *`"[System Drive]\SNAP_[Date and Time]_VOLUME[Drive Letter]$"`* was successful *Additionally, if a log indicating that files under `C:\Windows\NTDS`, which cannot be normally read, were copied (Event ID: **4663**) is recorded, it is possible that a shadow copy was used.
	vssadmin	If the following log is in the event log, it is considered that a shadow copy was created. - The Event ID **8222** is recorded in the event log "Security". *Additionally, if a log indicating that files under `C:\Windows\NTDS`, which cannot be normally read, were copied (Event ID: **4663**) is recorded, it is possible that a shadow copy was used.
Adding or Deleting a Local User/Group	**net user**	- The Event ID 4720 is recorded in the event log "Security".
File Sharing	**net use**	- Source host: If the following log is in the event log, it is possible that file sharing occurred. - The Event ID 4689 (A process has exited) of net.exe was recorded in the event log "Security" with the execution result (return value) of "0x0".
	net share	- The Event ID: 5142 is recorded in the event log "Security".
	icacls	- The Event IDs: **4688** and **4689** on icacls.exe are recorded in the event log "Security", and the Exit Status in the Event ID: **4689** is set to "0x0". *Since it is not possible to determine the target files from the Event IDs **4688** and **4689**, it is necessary to additionally check the command line of icacls.exe from the Event ID **1** of sysmon.
Deleting Evidence	**sdelete**	- A file with its name similar to the following was repeatedly deleted. - Example: sdeleAAAAAAAAAAAAAAAAAAAA.AAA, sdeleZZZZZZZZZZZZZZZZZZZZ.ZZZ when the target to be deleted is sdelete.txt
	timestomp	- The Event ID: 4663 is recorded in the event log "Security", and the "WriteAttributes" keyword for the target file is set to "Audit Success".
Deleting Event Log	**wevtutil**	- The Event ID: **104** is recorded in each target event log.
Acquisition of Account Information	**csvde**	- Source host: csvde.exe was executed and a file specified by the "-f" option was created. - `"C:\Users\[User Name]\AppData\Local\Temp\csv[Random Number].tmp"` was created and deleted.
	ldifde	- Source host: ldifde.exe was executed and a file specified by the "-f" option was created.
	dsquery	- If the extracted account information is saved, it can be considered that the tool execution was successful.

4. Acquiring Additional Logs

This chapter describes the importance of acquiring detailed logs that cannot be obtained with the default settings as stated in the findings reported in Chapter 3, and matters that should be taken into consideration when acquiring additional detailed logs.

4.1. Importance of Acquiring Additional Logs

This research found that the tools installed by default in Windows leave execution traces of evidence in event logs, but most tools that are not installed in Windows do not leave execution traces of evidence anywhere. For example, Remote Desktop Protocol (RDP), a tool for remote login, and "at", a tool for scheduling tasks, leave evidence of execution in the event logs Microsoft\Windows\TerminalServices-LocalSessionManager\Operational and Microsoft\Windows \TaskScheduler\Operational, respectively, indicating that the tools have been executed.

Conversely, in an environment where the audit policy is enabled and Sysmon is installed for acquiring additional logs, evidence of execution of most tools can be acquired. For example, by configuring audit policy settings, when a temporary file is created, it can be recorded in the event log. As a result, if an attacker attempts to collect account information by using "csvde", the temporary file that is created, C:\Users\[User_Name]\AppData\Local\Temp\csv[Random_Number].tmp, is recorded in the event log. To investigate the execution of tools, these settings need to be configured in advance to acquire detailed logs.

Note that detailed logs can be acquired with audit software (such as asset management software) without enabling the audit policy and installing Sysmon. When such software monitors the following Windows OS operations, it can be recorded in a similar manner as in an environment where the audit policy is enabled and Sysmon is installed:

- Executing processes
- Writing files

4.2. Precautions When Changing the Additional Log Acquisition Settings

The increase in the amount of logs should be considered in advance when acquiring additional detailed logs. Because the amount of logs increases when the audit policy is enabled, log rotation accelerates, and older logs are maintained for a shorter period of time. Therefore, when enabling the audit policy, consider changing the maximum size of event logs at the same time. The maximum size of event logs can be changed with Event Viewer or the "wevtutil" command.

Note that changing the maximum size of event logs may exhaust storage capacity. JPCERT/CC recommends that storage capacity be evaluated before changing the maximum size of event logs.

5. How to Use This Report in Incident Investigation

This chapter describes how this research report can be used in the field of incident investigation through same examples using the results in Chapter 3 of this report.

5.1. Incident Investigation Using This Report

Chapter 3 was created on the assumption that it will be used when identifying tools that might be executed as part of incident investigations. Searching for keywords, such as an event ID and file name of a characteristic event log and a registry entry found during incident investigation, can find out possible tools that were executed.

An incident investigation often starts by checking any suspicious logs in the "Security" event log. Then, if "Event ID: 4663 (An attempt was made to access an object)" is found for example, it is assumed that there is evidence that the file `192.168.100.100-PWHashes.txt` was created temporarily (recorded when the audit policy is enabled). Searching Chapter 3 for the distinctive text `PWHashes.txt` finds it is a file created when PWDumpX is executed.

Further proceeding with the investigation while referring to Section 3.3.2 finds that "PWDumpX" is a command attackers execute to acquire a password hash. Additionally, the fact that the temporary file [*Destination_Address*]`-PWHashes.txt` was created implies that the attacker had completed the purpose of acquiring the password hash on the server with IP address 192.168.100.100.

Investigating the server with IP address 192.168.100.100 explains that the file `C:\Windows\System32\DumpSvc.exe` was created and executed, and the fact that the service "PWDumpX Service" was installed is recorded as "Event ID: 7045 (A service was installed in the system)." This allows for determining that the attacker acquired the password hash for the IP address 192.168.100.100.

Section 3.16 describes how to verify that each tool was executed. Referring to the section for planning an investigation strategy in advance of commencing an incident investigation is encouraged as it shows information recorded by each tool in a list.

6. Conclusion

As it is becoming apparent that many organizations have suffered damage due to targeted attacks, the importance of incident investigations to further examine such damage is increasing. This report summarizes and presents evidence suggesting the execution of tools and its corresponding relationship with tools, which are the key to a successful incident investigation.

Many tools do not leave evidence of having been executed with the default Windows settings, which may cause incident investigations to remain unsolved. To analyze what the attacker did in detail, an environment that allows for more logs to be collected than those obtained with the default settings needs to be prepared in advance.

Under the current circumstances where it is difficult to prevent infiltration of a network, it is important to always consider and improve the method for acquiring logs to analyze the amount of damage after an incident occurs in order to prevent the spread of damage and review post-incident security measures. In addition to reviewing and being prepared for responses that are not limited to the method for acquiring additional logs using Windows standard functionality as shown in this report, also use other methods that combine the use of audit software or similar. Moreover, JPCERT/CC recommends that this report be used to identify evidence of tool execution by attackers in the event of a suspicious incident. JPCERT/CC hopes that this report will be of help in early detection and accurate response to targeted attacks, which are becoming more sophisticated.

7. Appendix A

This appendix describes how to install Sysmon and how to enable the audit policy. Note that it has been confirmed that setting up the audit policy and installing Sysmon will increase the amount of event logs. Before enabling the setting and installing the tool, it is recommended to verify its impact.

7.1. How to Install Sysmon

1. Download Sysmon from the following site:

https://technet.microsoft.com/en-us/sysinternals/dn798348

2. Execute the command prompt as a user with administrator privileges and execute the following command:

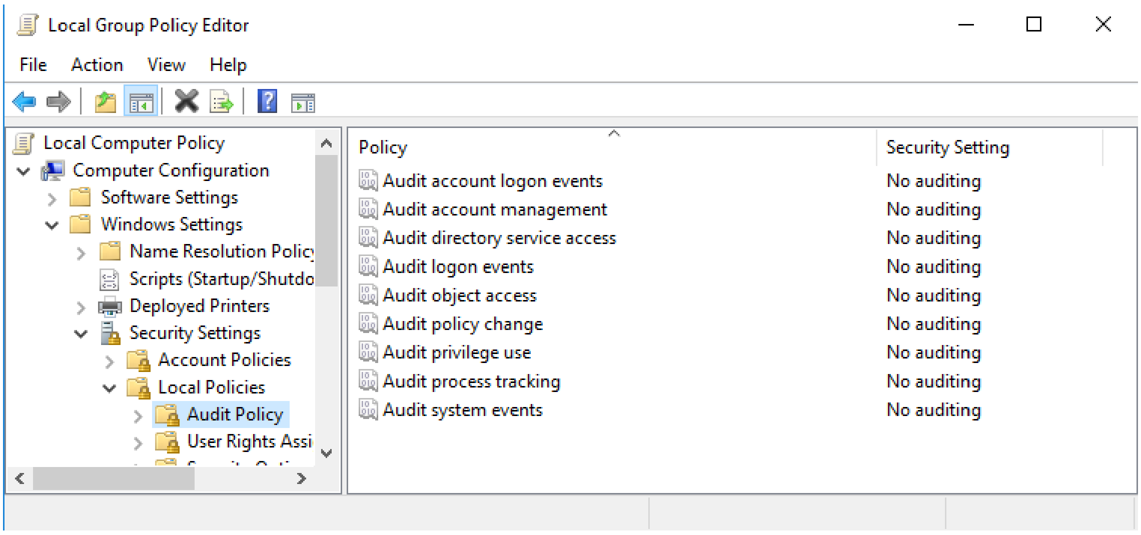
```
> Sysmon.exe -i
```

* Although adding the option "-n" enables network connection logs to be acquired, network connection should be dealt with in the audit policy.

7.2. How to Enable the Audit Policy

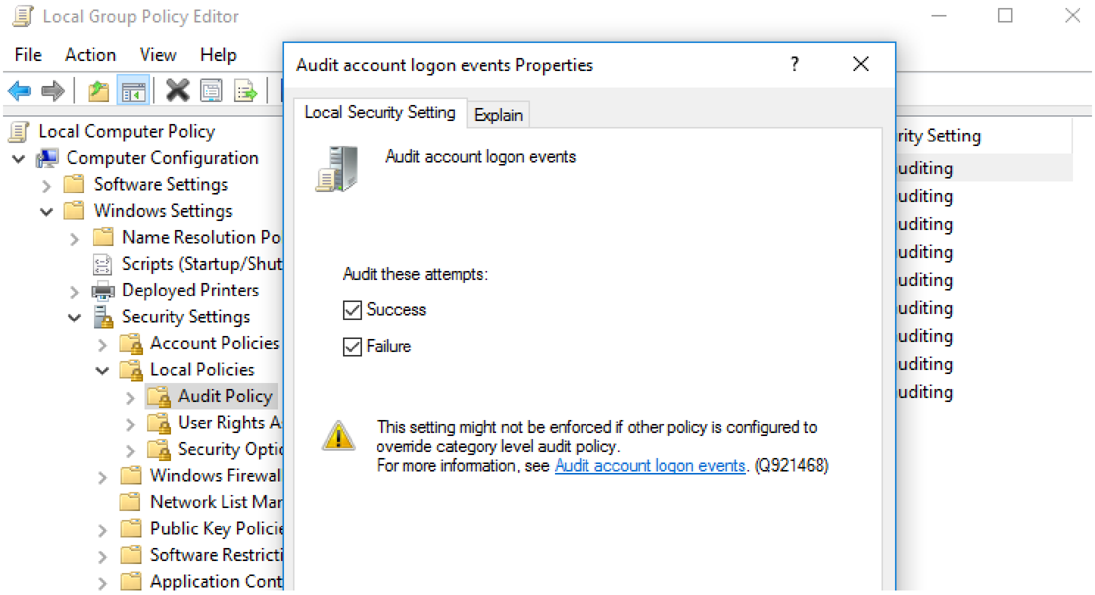
The following describes how to enable the audit policy on a local computer. Note that the following shows settings in Windows 10.

1. Open the Local Group Policy Editor. (Enter "gpedit.msc" into the [Search] box and execute it.)



Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

2. Select [Computer Configuration]→[Windows Settings]→[Security Settings]→[Local Policies]→[Audit Policy], and enable "Success" or "Failure" for each policy.



Audit account logon events

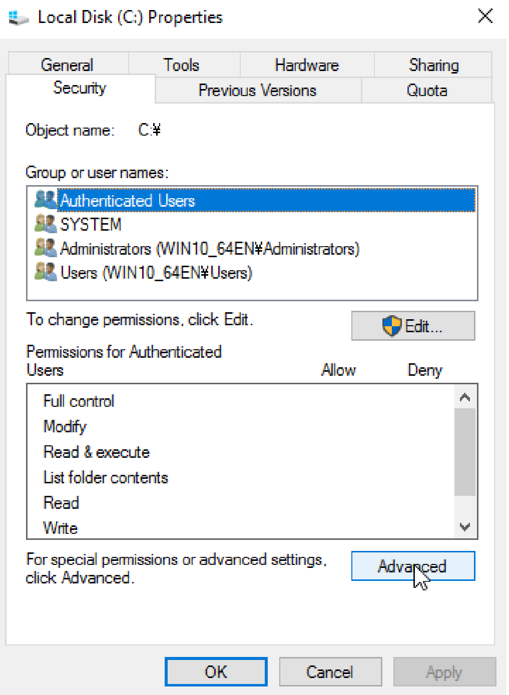
Audit these attempts:

☑ Success

☑ Failure

This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit account logon events. (Q921468)

3. Select [Local Disk (C:)]→[Properties]→[Security] tab→[Advanced].



Object name: C:¥

Group or user names:

Authenticated Users
SYSTEM
Administrators (WIN10_64EN¥Administrators)
Users (WIN10_64EN¥Users)

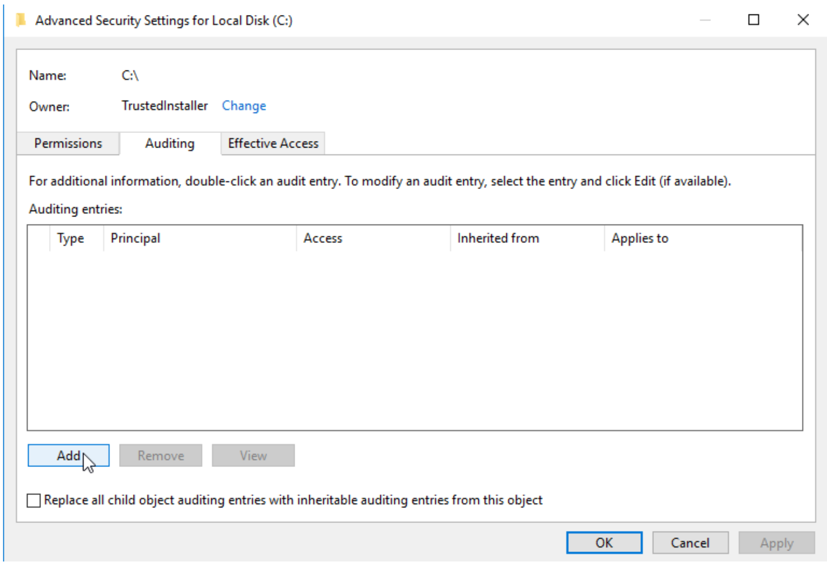
To change permissions, click Edit.

Permissions for Authenticated Users

Full control
Modify
Read & execute
List folder contents
Read
Write

For special permissions or advanced settings, click Advanced.

4. On the [Auditing] tab, add an object to be audited.



Advanced Security Settings for Local Disk (C:)

Name: C:\

Owner: TrustedInstaller Change

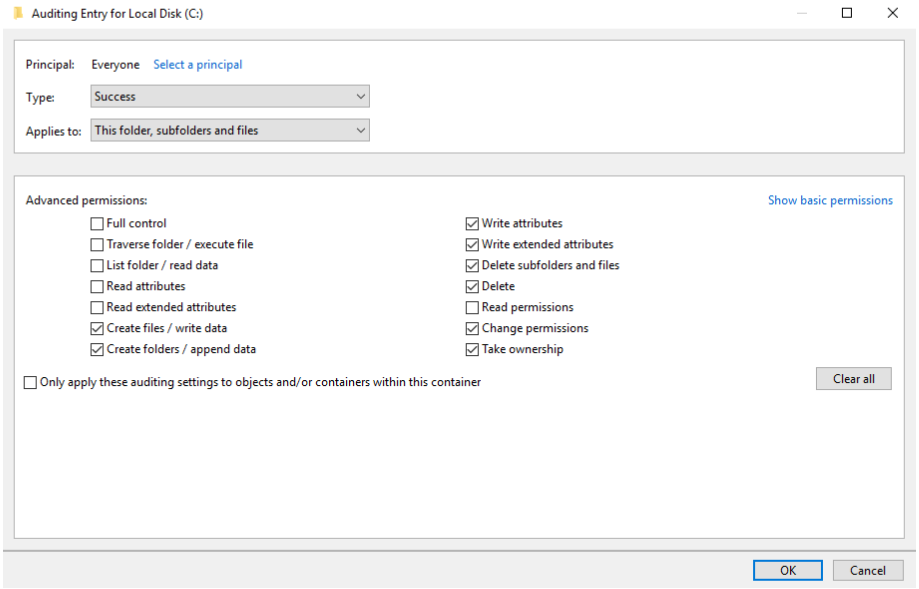
For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to

☐ Replace all child object auditing entries with inheritable auditing entries from this object

5. As shown below, select the user to be audited and access method to be audited.



Auditing Entry for Local Disk (C:)

Principal: Everyone Select a principal

Type: Success

Applies to: This folder, subfolders and files

Advanced permissions: Show basic permissions

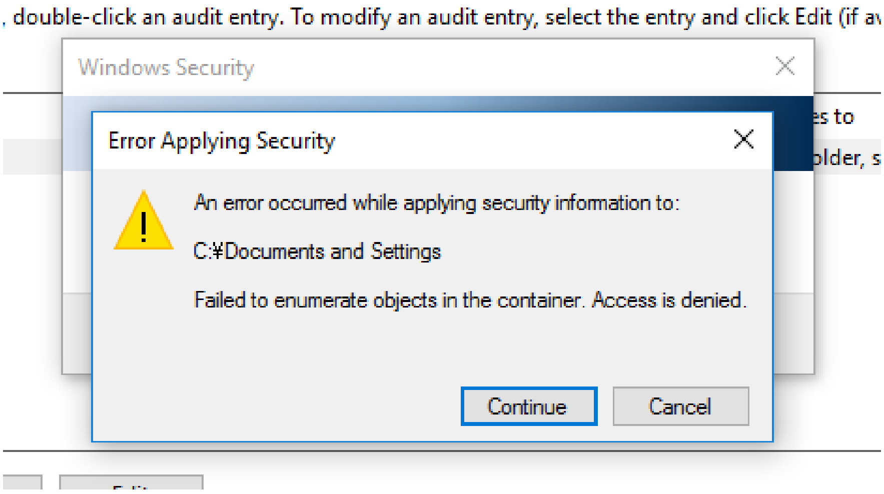
☐ Full control
☐ Traverse folder / execute file
☐ List folder / read data
☐ Read attributes
☐ Read extended attributes
☑ Create files / write data
☑ Create folders / append data
☑ Write attributes
☑ Write extended attributes
☑ Delete subfolders and files
☑ Delete
☐ Read permissions
☑ Change permissions
☑ Take ownership

☐ Only apply these auditing settings to objects and/or containers within this container

The "Permissions" set here are as follows. (Although recording file read enables a more detailed investigation, it is excluded as doing so will increase the amount of logs.)

- Create files / write data
- Create folders / append data
- Write attributes
- Write extended attributes
- Delete subfolders and files
- Delete
- Change permissions
- Take ownership

Although configuring the above settings displays many errors as shown below, select "Continue."



, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if av

An error occurred while applying security information to:

C:¥Documents and Settings

Failed to enumerate objects in the container. Access is denied.

8. Appendix B

This list describes logs recorded by default and other logs recorded by configuring additional settings, including audit policy settings and installation of Sysmon.
The list only contains selected logs that can be used for incident investigation out of all logs that can be acquired.

Target	Acquirable Log							
	Log		How to Obtain	Required Setting	Identifier	Event Name	Overview	Main Information That Can Be Acquired
Common to All	Windows Log	Security	Recorded by default Windows settings		104	The System log file was cleared	Clearing of logs	- The cleared log channel
					7036	The [Service Name] service entered the [Status] state	A change of the service state (the same ID for execution and stop)	- Service name - State
					7045	A service was installed in the system	Installation of a service	- Service name - Executable file name - Service type - Startup type - Service account
		System			20001	Device Installation	Installation of a device driver	- Device instance ID - Driver name - Success or failure
					8222	Shadow copy has been created	Creation of a shadow copy	- Account name, domain - UUID of a shadow copy - Computer name - Source of a shadow copy - Created shadow device name
		Security (audit policy)	Enable each audit. Auditing of a file system additionally requires SACL settings. Each log is saved in "Windows Log > Security".	Logon/Logoff > Auditing of Logon	4624	An account was successfully logged on	Account logon	- Security ID - Account name, domain - Logon ID Used for association with other event logs - Logon type The main logon types include 2 = Local Interactive, 3 = Network, and 10 = Remote Interactive - Process ID - Process name - Login source: Workstation name, source network address, source port - Authentication method: Authentication package
					4634	An account was logged off	Account logoff	- Security ID - Account name, domain - Logon ID - Logon type
					4648	A logon was attempted using explicit credentials	A specified logon attempt by a particular account	- Executing account information: Subject: - Security ID - Account name, domain - Logon ID - Account whose credentials were used - Account name, domain - Target server - Target server name - Process information - Process ID - Process name - Network information - Network address - Port
				Object access > Auditing of handle operations	4656	A handle to an object was requested	A handle request for reading or writing an object	- Account name, domain - Handle object: Object name - Handle ID Used for association with other event logs - Process ID - Process name
					4658	The handle to an object was closed	Ending the use of and releasing of a handle	- Account name, domain - Handle ID - Process ID - Process name
					4690	An attempt was made to duplicate a handle to an object	Duplication of an existing handle for use in other processes	- Account name, domain - Source handle ID - Source process ID - Source handle ID - Source process ID
				Object access	4660	An object was deleted	Deleting an object	- Account name, domain - Handle ID - Process ID - Process name
					4663	File System,"An attempt was made to access an object	Access made to an object	- Account name, domain - Logon ID - Object name - Handle ID - Process name - Process ID - Requested processing
				Object access > Auditing of SAM	4661	A handle to an object was requested	A handle request to SAM (Acquirable information is the same as that of the event 4656)	- Account name, domain - Handle object: Object name - Handle ID Used for association with other event logs - Process ID - Process name
				Use of special privileges	4672	Special privileges assigned to new logon	Assignment of special privileges to a particular logon instance	- Security ID - Executing account name, domain - Logon ID - Assigned special privileges
					4673	A privileged service was called	Execution of a process requiring particular privileges	- Security ID - Account name, domain - Service name - Process ID - Process name - Used privileges
				Detailed tracking > Auditing of process creation	4688	A new process has been created	Startup of a process	- Account name, domain - Process ID - Process name - Presence of privilege escalation: Token escalation type - Parent process ID: Creator process ID
				Detailed tracking > Auditing of process termination	4689	A process has exited	Process termination	- Account name, domain - Process ID - Process name - Return value: Exit status
				Account management > Auditing of user account management	4720	A user account was created	Account creation	- Executing account information: Subject: - Security ID - Account name, domain - Logon ID - Information on the account to be added: New account: - Security ID - Account name, domain - Other attribute information
					4726	A user account was deleted	Account deletion	- Executing account information: Subject: - Security ID - Account name, domain - Logon ID - Information on the account to be deleted: Target account: - Security ID - Account name, domain

Target	Acquirable Log							
	Log		How to Obtain	Required Setting	Identifier	Event Name	Overview	Main Information That Can Be Acquired
				Account management > Auditing of security group management	4728	A member was added to a security-enabled global group	Addition of a member to a group (used when a member has been added to a group on the domain)	- Executing account information: Subject - Security ID - Account name, domain - Logon ID - Target user: Member - Security ID - Account name - Target group: Group - Security ID - Group name - Group domain
					4729	A member was removed from a security-enabled global group	Removal of a member from a group (used when a member has been removed from a group on the domain)	- Executing account information: Subject - Security ID - Account name, domain - Logon ID - Target user: Member - Security ID - Account name - Target group: Group - Security ID - Group name - Group domain
Common to All (Continued from the previous entry)	Windows Log (Continued from the previous entry)	Security (audit policy) (Continued from the previous entry)	ditto	Account Logon > Auditing of the Kerberos authentication service	4768	A Kerberos authentication ticket (TGT) was requested	An authentication request for an account	- Account name, domain - Security ID - Source address, source port - Ticket option - Return value
				Account logon > Auditing of Kerberos service ticket operations	4769	A Kerberos service ticket was requested	An access authentication request for an account	- Account name, domain, logon ID - Service name, service ID - Client address, port - Ticket option
				Policy change > Auditing of a change in the MPSSVC rule level policy	4946	A change was made to the Windows Firewall exception list. A rule was added.	Addition of a Windows Firewall rule	- Profile - Target rule name
				Object access > Auditing of file sharing	5140	A network share object was accessed	Access to network share	- Security ID - Account name, domain - Logon ID - Source address, source port - Share name - Share path - Requested process
					5142	A network share object was added	Creation of a new network share	- Security ID - Account name, domain - Share name - Share path
					5144	A network share object was deleted	Deletion of a network share	- Security ID - Account name, domain - Share name - Share path
				Object access > Detailed auditing of file sharing	5145	A network share object was checked to see whether client can be granted desired access	Confirmation of whether a file share point can be used	- Security ID - Account name, domain - Logon ID - Source address, source port - Share name - Share path, relative target name
				Object access > Auditing of Filtering Platform connections	5154	The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections	Port listening by an application or service	- Process ID - Process name - Address, port - Protocol number
					5156	The Windows Filtering Platform has permitted a connection	Whether a connection is allowed by the Windows Filtering Platform (Windows Firewall) (if rejected, a different Event ID (5152) will be recorded)	- Process ID - Process name - Direction (outbound, inbound) - Source address, source port - Destination address, destination port - Protocol number
	Application and Service	Sysmon	Downloaded from the Microsoft website https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx	Application and service log > Microsoft > Windows > Sysmon > Operational	1	Process Create	Startup of a process	- Process start date and time: UtcTime - Process command line: CommandLine The option passed to the executable file is recorded. If an IP address or user name of another host is specified in the option, it is possible to read it from here. - User name: User - Process ID: ProcessId
					5	Process Terminated	Process termination	- Process end date and time: UtcTime - Process ID: ProcessId
					8	CreateRemoteThread detected	Creating a new thread from another process	- Thread creation date and time: UtcTime - Caller process ID: SourceProcessId - Caller process name: SourceImage - Callee process ID: TargetProcessId - Callee process name: TargetImage
at		Microsoft > Windows > TaskScheduler > Operational	Recorded by default Windows settings		106	Task registered	Registration of a new task	- Executing account name, domain - Created task name
					200	Action started	Execution of a task	- Task name - Executed operation
					129	Created Task Process	Process executing in a task	- Task name - Process ID - Executed process
					201	Action completed	Termination of a process executed in a task	- Task name - Terminated process - Return value
					102	Task completed	Termination of a task	- Executing account name, domain - Task name
WinRM / WinRS		Microsoft > Windows > Windows Remote Management > Operational			6	Creating WSMan Session	Creation of a new session	− Destination host name
					169	User authentication: authenticated successfully	User authentication: authenticated successfully	- User name, domain
RDP		Microsoft > Windows > TerminalServices > LocalSessionManager > Operational			21	Remote Desktop Services: Session logon succeeded	New logon via RDP	- Session connection start date and time - Executing account name, domain - Source network address
					24	Remote Desktop Services: Session has been disconnected	Disconnection of an RDP session	- Session connection start date and time - Executing account name, domain - Source network address

Index

JPCERT/CC will not be liable for any loss or damage that may arise from any information contained in this document.