Event Log Analysis
Event Log 101

• What is Event Log?
  • Windows version of “syslog”.

• Where are these artifacts located in?
  • %SystemRoot%\System32\winevt\Logs
  • %SystemRoot% is “C:\Windows” typically.
Event Log 101

• There are three standard logs and lots of custom logs.

  **Standard logs**
  • Security
  • System
  • Application

  **Custom logs (Applications and Services Logs)**
  • RDP
  • PowerShell
  • Windows Firewall
  • ...
Event Log 101

- Each log contains following items.
  - Source
  - Event ID
  - Level
    - Information / Warning / Error
  - User
    - The target user of a event's message.
  - Date and Time
  - Computer
    - The target host of a event's message.
  - Description
    - The details are described in this un-normalized field!

- The event ID number is unique within each log, such as System, Security, Application, and other custom logs. However, the same ID number may be used if the log is different.
Event Log 101

• Audit policy
  • For security log, all logs are not enabled by default. “Audit policy” manages this.
  • You can confirm/edit the current audit policy with these applications / commands.
    • localpol.msc (online)
    • gedit.msc (online)
    • auditpol (online)
    • Regripper auditpol plugin (offline)
    • Volatility 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
Event Log 101

• There are lots of tools to view and/or parse event logs.
  • Event Viewer (default)
  • PowerShell (default)
  • Event Log Explorer (commercial) [1]
  • python-evtx [2]
  • EvtXtract [3]
  • Evtx Parser [4]
  • Libevtx [5]
  • Log Parser [6]
Event Log 101

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

**Kerberos**
  • The default authentication protocol for Windows domain networks.
  • But, if a session starts with IP address instead of host name, the NTLM authentication is used.

**NTLM**
  • A traditional authentication protocol.
Event Log 101

• Kerberos Authentication Mechanism
  1. A user on client requests a Ticket-granting Tickets (TGT)
  2. The Authentication Service (AS) sends a TGT, which is encrypted with password hash of the user.
  3. The client decrypt the TGT and send it to Ticket Granting Service (TGS) for a Service Ticket.
  4. The TGS sends the Service Ticket to the client.
  5. The client send the Service Ticket to the server.
  6. Then a service session start.
Event Log 101

• NTLM Authentication Mechanism
  1. A client requests access to a server.
  2. The server responds with a challenge message to the client.
  3. Clients send a response message to the server.
  4. The server sends challenge and response messages to the Domain Controller (DC).
  5. The DC confirms the user's authentication. If successful, the DC sends the server a confirmation.
  6. The server responds to the client to start a service.
Event Log 101

- Challenge Response Authentication Basic

Client Side:
- Entering password by User
  - Password
- Calculating hash
  - Password Hash
- [1] Authentication Request
  - Challenge
  - [3] Calculate "Response"
  - Password Hash
  - Challenge
  - [4] Calculate "Response"
  - Password Hash

Server Side:
- Getting User's password hash from account DB
  - Challenge
  - [5] Comparing "Responses"
  - Response
  - Response
  - Response

Copyright Internet Initiative Japan Inc.
Event Log 101

• The most important logs for incident response are...
  • Credential validation (Authentication, Account Logon)
    • 4768: requested a TGT
    • 4769: requested a Service Ticket
    • 4776: NTLM authentication
    \[Kerberos\text{ related}\]
  • Logon (Authorization?)
    • 4624: Logon
    • 4625: Logoff
    • 4634: Logon Failed (not default)

• These all events are logged in the standard "Security" log.
Event Log 101

• 4768: requested a TGT
  • This event logged on the Domain Controller. And both of success and failure requests are logged.

- 4768: requested a TGT
- This event logged on the Domain Controller. And both of success and failure requests are logged.
Event Log 101

• 4769: requested a Service Ticket
  • This event is logged on the Domain Controller. Both succeeded and failed requests are logged.
Event Log 101

• 4624: Logon
  • This event documents successful logon attempt to various components on the local computer.
  • This event also indicates "logon type".

```
4624: Logon
This event documents successful logon attempt to various components on the local computer.
This event also indicates "logon type".
```
Event Log 101

• 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)

Event Log 101

• What is “logon type”?
  • Interactive (2)
    • For Local logon with a user credential.
    • For example, if you sit in front of your PC, press Ctrl+Alt+Del keys, and type your user name and password; the log will be produced when the logon is attempted.
  
  • Network (3)
    • This is the most generic logon type. This type of logon is used for SSO (Single-Sign-On). You don’t need to input any additional credentials if you have already had a rights to use services (E.g. connecting to a file server with SMB).

  • Batch (4)
    • For Task Scheduler and AT.

  • Service (5)
    • For Windows Services.
Event Log 101

• What is “logon type”?
  • Unlock (7)
    • For unlocking the screen lock.
  • RemoteInteractive (10)
    • For RDP.
  • CachedInteractive (11)
    • If the machine cannot communicate with the domain controllers and if you have logged on to the machine in the past, this type is logged when you log on in that situation.
      • E.g. If you take your laptop out with you, and log on to the laptop with a domain account offline.
  • CachedRemoteInteractive (12)
    • A similar situation to 11, but logged for RDP.
  • CachedUnlock (13)
    • A similar situation to 11, but logged for unlocking screen.
Event Log 101

• There are three "account types" for account/user names logged in Events.
  • User accounts
    • It's just user account. Generally this type of accounts are bind to each person or roll.
  • Computer accounts
    • This account type indicates each host. A name of this account type is terminated with character "$". For example, "DESKTOP-SHCTJ7L$" is a name of a computer account.
  • Service accounts
    • Each service account is created to be owner of a certain service. For example, IUSR is the owner of IIS, and krbtgt is the owner of a service that is a part of Key Distribution Center.
Remote Logon Events
Remote Logon Events

• There are a lot of remote logon methods that are used by attackers for Windows.
  • RDP
  • Task Scheduler/AT
  • Powershell Remoting
  • WinRS
  • WMIC
  • PsExec
  • Wmiexec
  • ...
RDP
RDP (1)

• Why this event is important?
  • Attackers sometimes use RDP to logon to remote computers while users are away from clients, or to penetrate servers. So, 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.
    • 4778: A session was reconnected to a Window Station. (Not default)
    • 4779: A session was disconnected from a Window Station. (Not default)

  • Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx
    • 1149: User authentication succeeded
    • 21: Remote Desktop Services: Session logon succeeded
    • 24: Remote Desktop Services: Session has been disconnected
    • 25: Remote Desktop Services: Session reconnection succeeded
RDP (2)

• How can we detect this event?
  • Logon with RDP
    • 4624 (Security.evtx)
      • Description
        • An account was successfully logged on.
      • How can we recognize RDP logon with this ID?
        • Filter with these logon types in this ID.
          • Logon type 10 (RemoteInteractive) or type 12 (CachedRemoteInteractive)
      • Why?
        • RemoteInteractive (10) and CachedRemoteInteractive (12) indicate RDP used clearly because these logon types are dedicated for RDP usage.
RDP (3)

• How can we detect this event?
  • Logon with RDP
    • 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.
          • But when “Restricted Admin mode” is used, this ID is not logged for the admin accounts.
        • This event ID logs SPNs (Service Principal Name) that indicates service names which a user wants to use. And SPN for RDP is “TERMSERV” or any SPNs are NOT included for RDP and several cases (E.g. local logon).
RDP (4)

• Let’s assume these conditions are given.
  • client-win10-1 (192.168.52.40)
    • Administrator’s PC
    • He uses toyoda, ninja-rdp, ninja-master accounts.
  • client-win10-2 (192.168.52.44)
    • Honda’s PC
    • He is a general employee and he don’t have any admin rights.
    • He uses only this PC and “honda” account.

• The owner of the “client-win10-1” often use RDP to logon to remote hosts. But not vise versa.

• Since event ID 4624 is recorded on the target host, which is the destination host when it was logged on from a remote host, let's check "client-win10-1" first to see if there are any logons from a remote host is recorded.
RDP (5)

• Open the below log with Event Log Explorer.
  • Training_Materials\EventLogAnalysis\RDP\Win10-1_Security.evtx
    • Original log file name: Security.evtx

• Notice:
  • You should drag the log file and drop it to the Event Log Explorer.
  • If you double-click the log file, Event Viewer, which is the Windows' default log viewer, starts instead. The viewer is not capable of complex filtering.
RDP (6)

• Click the “Filter Events” button.
(1) Click “Load” button.

(2) Choose “Training_Materials\EventLogAnalysis\RDP\Sec4624_rdp.elc”, then click “Open” button.
Filter with Event ID 4624.

Filter with logon type 10 or 12.

Filter with Event ID 4624.

Filter with logon type 10 or 12.

Filter with Event ID 4624.
# RDP (9)

- How To Analyze
  - Logon with RDP

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Log Location</th>
<th>Logged Host</th>
<th>Where You Should Look</th>
<th>What You Get</th>
</tr>
</thead>
<tbody>
<tr>
<td>4624</td>
<td>Security.evtx</td>
<td>Destination (remote host)</td>
<td>Date, Time</td>
<td>Date/Time around RDP used</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Computer Name</td>
<td>Destination computer name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>New Logon\Security ID</td>
<td>Logon user’s SID</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>New Logon\Account Name</td>
<td>Logon user’s account name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>New Logon\Logon ID</td>
<td>An ID to combine with 4648 and others</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>New Logon\Logon GUID</td>
<td>An ID to combine with 4769</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Network Information\Source Network Address</td>
<td>Source IP address</td>
</tr>
<tr>
<td>Type</td>
<td>Date</td>
<td>Time</td>
<td>Event</td>
<td>Source</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
<td>--------</td>
<td>-------</td>
<td>--------------</td>
</tr>
<tr>
<td>Audit Success</td>
<td>2/8/2018</td>
<td>2:27:03 PM</td>
<td>4624</td>
<td>Microsoft-Windows-SecLogon</td>
</tr>
</tbody>
</table>

This message logged on client-win10-1 which is the destination of this RDP Session.

The destination host client-win10-1 (admin-PC)

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

ID 4624 is always logged on the destination host.
RDP (11)

• If the attackers do not use RestrictedAdmin mode when they logon to remote servers, event ID 4648 is logged on the both source and destination hosts because they need to input a credential to use RDP. Let’s check this.

• Open the below log with Event Log Explorer, and click “Filter Events” button.
  • Training_Materials\EventLogAnalysis\RDP\Win10-2_Security.evtx
  • Original log file name: Security.evtx

Notice: You should drag the log file and drop it to the Event Log Explorer.
(1) Click “Load” button.

(2) Choose “Training_Materials\EventLogAnalysis\RDP\Sec4648_rdp_src.elc”, then click “Open” button.
Filter with the event ID 4648.

Filter out localhost, computer accounts and SPNs.

Some kinds of rdp sessions are logged with a SPN for terminal server "TERMSRV". You should tweak the last condition to filter with that.
RDP (14)

• How To Analyze

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Log Location</th>
<th>Logged Host</th>
<th>Where You Should Look</th>
<th>What You Get</th>
</tr>
</thead>
<tbody>
<tr>
<td>4648</td>
<td>Security.evtx</td>
<td>Source</td>
<td>Date, Time</td>
<td>Date/Time around RDP used</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Computer Name</td>
<td>Source computer name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Subject\Security ID</td>
<td>SID of RDP used</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Subject\Account Name</td>
<td>User name of RDP used</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Target Server\Target Server Name</td>
<td>Destination computer name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Account Whose Credentials Were Used\Account Name</td>
<td>Logon user name of the remote host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Destination</td>
<td>Date, Time</td>
<td>Date/Time around RDP used</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Computer Name</td>
<td>Destination computer name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Account Whose Credentials Were Used\Account Name</td>
<td>Logon user name of the remote host</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Network Information\Source Network Address</td>
<td>Source IP address</td>
</tr>
</tbody>
</table>
The attackers have already had honda’s credential and ninja-rdp’s credential. And they moved laterally to “client-win10-1” with RDP.

This message logged on client-win10-2 which is the source of this RDP Session.
RDP (16)

• 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 192.168.52.40 is the system administrator’s PC, and Honda, who is a general employee, does not own that PC. And, he cannot know the credential of the “ninja-rdp” account, which is an administrative account.
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 lateral movement phase. So you should check this event.

• 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.
      • And 4624 with logon type 3 (Security.evtx) is logged at the same time if the task is registered from remote hosts. You can get the source address information by combining with date/time and the user name of these logs.

• 4624 (Security.evtx)
  • How can we recognize Task Scheduler/AT with this ID?
    • We can filter with logon type 4 with this ID to get tasks triggered and those dates.
Task Scheduler/AT Events (3)

• Let’s assume this condition is given.
  • We have already known attackers moved laterally around 25th February 2018 from forensic analysis so far.
  • So we should look for registrations of tasks around that time at first.

• Open the below log with Event Log Explorer, and click “Filter Events” button.
  • Training_Materials\EventLogAnalysis\TaskSched\Win10-2_TaskSchedOpe.evtx
    • Original log name: Microsoft-Windows-TaskScheduler%4Operational.evtx

Notice:
You should **drag the log file and drop it to** the Event Log Explorer.
Filter with Event ID 106.
## Task Scheduler/AT Events (5)

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

*1 : Microsoft-Windows-TaskScheduler%4Operational.evtx
Task Scheduler/AT Events (6)

Now, you can check whether legitimate tasks or not.

Registered event dates

User’s name or SID

Task name
If the AT is used, task name is always "\At*". "*" means a number.
Task Scheduler/AT Events (7)

• We got date/time, task name and registered user name from 106.
  • But where did this user register this task from?
    • If the task is registered from the remote host, then you can find 4624 type 3 log.
    • If the task is registered locally, 4624 type 3 message is not logged at the same time.
Task Scheduler/AT Events (8)

• Let's find the ID 4624 with logon type 3 logs, which is logged at the same time with the ID 106 we confirmed before.
• Open the log below with Event Log Explorer, and click “Filter Events” button.
  • Training_Materials\EventLogAnalysis\TaskSched\Win10-2_Security.evtx
  • Original log name: Security.evtx

Notice:
You should drag the log file and drop it to the Event Log Explorer.
(1) Click “Load” button.

(2) Choose “Training_Materials\EventLogAnalysis\TaskSched\Sec4624_type3_Feb25_9PM.elc”, then click “Open” button.
Filter with the event ID 4624.

Filter with logon type 3

Filter with Feb/25/2018 9 PM to 10 PM
You can see the same time and the same user name between 106 and 4624.

ID 4624 is always logged on destination host.

We got the remote IP (source) address!
Task Scheduler/AT Events (12)

• We confirmed “ninja-master” registered the task named “task_name” from 192.168.52.40 at 9:06:55 PM on 25th Feb.

• What process is executed?

• And how many times were this command executed?

• You should see the below log again!
  • Artifacts\evt\remote_logon\TaskSched\Win10-2_TaskSchedOpe.evtx
Task Scheduler/AT Events (13)

• We should see the IDs below.
  • 107: Task triggered on scheduler
    • We can get execution times by counting this logs.
  • 110: Task triggered by user
    • We can get execution times by counting this logs.
  • 200: Action Started
    • We can see the execution file name.
Filter with Event ID 107, 110 and 200.

Filter with the task name "\task_name".
### Task Scheduler/AT Events (15)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Log Location</th>
<th>Logged Host</th>
<th>Where You Should Look</th>
<th>What You Get</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>*1</td>
<td>Destination (remote host)</td>
<td>Date, Time</td>
<td>Date/Time around Task Scheduler used</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Computer Name</td>
<td>Destination computer name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>action</td>
<td>Execution file name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>task</td>
<td>Task name</td>
</tr>
<tr>
<td>107</td>
<td>*1</td>
<td>Destination (remote host)</td>
<td>Date, Time</td>
<td>Date/Time around Task Scheduler used</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Computer Name</td>
<td>Destination computer name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This event ID</td>
<td>Task triggered on scheduler</td>
</tr>
<tr>
<td>110</td>
<td>*1</td>
<td>Destination (remote host)</td>
<td>Date, Time</td>
<td>Date/Time around Task Scheduler used</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Computer Name</td>
<td>Destination computer name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This event ID</td>
<td>Task triggered by user</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>user</td>
<td>User name which task triggered</td>
</tr>
</tbody>
</table>

*1 : Microsoft-Windows-TaskScheduler%4Operational.evtx
The task was executed three times.

Execution file 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 on February 25, 2018 at 21:06:55.
  • “cmd.exe” was executed three times in 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.
  • It logs every task trigger and launch requests.
## Task Scheduler/AT Events (19)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Log Location</th>
<th>Logged Host</th>
<th>Where You Should Look</th>
<th>What You Get</th>
</tr>
</thead>
<tbody>
<tr>
<td>4624</td>
<td>Security.evtx</td>
<td>Destination (remote host)</td>
<td>Date, Time</td>
<td>Date/Time around Task Scheduler used</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Computer Name</td>
<td>Destination computer name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>New Logon\Security ID</td>
<td>Logon user’s SID</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>New Logon\Account Name</td>
<td>Logon user’s account name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>New Logon\Logon ID</td>
<td>An ID to combine with 4648 and others</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>New Logon\Logon GUID</td>
<td>An ID to combine with 4769</td>
</tr>
</tbody>
</table>
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.

Task Scheduler/AT Events (22)

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

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

• For AT command, you should look this folder.
  • c:\windows\tasks
  • *.job
Task Scheduler/AT Events (23)

• You might also need to check these logs below.
  • Microsoft-Windows-TaskScheduler%4Operational.evtx
    • 100: Task started
    • 102: Task completed
    • 140: Task updated
    • 141: Task deleted
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**
    - To change the copied file name and the service name for remote computers
      (default: %SystemRoot%\PSEXESVC.exe and PSEXESVC)
  - **-s**
    - To be executed by SYSTEM account.
  - **-c**
    - To copy a program to remote computers
      - It is copied to Admin$ (%SystemRoot%)
  - **-u**
    - To use a specific credential to log on to remote computers.
      - Logon type 2 & logon type 3 is occurred.
PsExec Detection (3)

• 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 including this string by default.
PsExec Detection Method 1 (2)

• Open the below log with Event Log Explorer, and click “Filter Events” button.
  • Training_Materials\EventLogAnalysis\PsExec\win7_system_psexec_en.evtx

Notice:
You should drag the log file and drop it to the Event Log Explorer.
Filter with a part of default service and execution name.

PSEXE
PsExec Detection Method 1(4)

- How To Analyze

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Log Location</th>
<th>Logged Host</th>
<th>Where You Should Look</th>
<th>What You Get</th>
</tr>
</thead>
<tbody>
<tr>
<td>7045</td>
<td>System.evtx</td>
<td>Destination (remote host)</td>
<td>Date, Time</td>
<td>Date/Time around Task Scheduler used</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Computer Name</td>
<td>Destination computer name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User</td>
<td>Actual user name or SID for execution</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Service Name</td>
<td>Installed service name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Service File Name</td>
<td>Copied execution file name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Service Type</td>
<td>Whether user or kernel mode service</td>
</tr>
</tbody>
</table>
You can find 7045 (Service registration) and 7036 (Change service state). Note that 7036 could not be logged on Windows 8/10 hosts.

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

You can also get the SID or the user name of the actual user even if the -s option is used.
PsExec Detection Method 1 (6)

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

![Image showing log entries with relevant dates and times]
PsExec Detection Method 1 (7)

- Open the below log with Event Log Explorer, and click “Filter Events” button.
  - Artifacts\evtx\remote_logon\PSExc\win7_security_psexec_en.evtx

Notice:
You should drag the log file and drop it to the Event Log Explorer.
(1) Click “Load” button.

(2) Choose “Training_Materials\EventLogAnalysis\PsExec\Sec4624_remote_logon_type3.elc”, then click “Open” button.
PsExec

Filter with event ID 4624.

Filter out:
- localhost
- computer accounts
- system account
- anonymous account

Filter with logon type 3.
PsExec Detection Method 1 (10)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Log Location</th>
<th>Logged Host</th>
<th>Where You Should Look</th>
<th>What You Get</th>
</tr>
</thead>
<tbody>
<tr>
<td>7045</td>
<td>System.evtx</td>
<td>Destination (remote host)</td>
<td>Date, Time</td>
<td>Date/Time around Task Scheduler used</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Computer Name</td>
<td>Destination computer name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User</td>
<td>Actual user name or SID for execution</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Service Name</td>
<td>Installed service name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Service File Name</td>
<td>Copied execution file name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Service Type</td>
<td>Whether user or kernel mode service</td>
</tr>
<tr>
<td>4624</td>
<td>Security.evtx</td>
<td>Destination (remote host)</td>
<td>Date, Time</td>
<td>Date/Time around Task Scheduler used</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Computer Name</td>
<td>Destination computer name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>New Logon\Security ID</td>
<td>Logon user’s SID</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>New Logon\Account Name</td>
<td>Logon user’s account name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>New Logon\Logon ID</td>
<td>An ID to combine with 4648 and others</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>New Logon\Logon GUID</td>
<td>An ID to combine with 4769</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Network Information\Source Network Address</td>
<td>Source IP address</td>
</tr>
</tbody>
</table>
You can get the actual account name and the source address.

<table>
<thead>
<tr>
<th>Type</th>
<th>Date</th>
<th>Time</th>
<th>Event</th>
<th>Source</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Success</td>
<td>2/20/2018</td>
<td>8:11:18 PM</td>
<td>\S-1-5-21-3671970501-3975728774-4289435121-3101</td>
<td>4624 Microsoft-Windows-SeLogon</td>
<td></td>
</tr>
<tr>
<td>Audit Success</td>
<td>2/20/2018</td>
<td>8:11:18 PM</td>
<td>\S-1-5-21-3671970501-3975728774-4289435121-3101</td>
<td>4624 Microsoft-Windows-SeLogon</td>
<td></td>
</tr>
<tr>
<td>Audit Success</td>
<td>2/20/2018</td>
<td>8:11:18 PM</td>
<td>\S-1-5-21-3671970501-3975728774-4289435121-3101</td>
<td>4624 Microsoft-Windows-SeLogon</td>
<td></td>
</tr>
<tr>
<td>Audit Success</td>
<td>2/20/2018</td>
<td>8:11:18 PM</td>
<td>\S-1-5-21-3671970501-3975728774-4289435121-3101</td>
<td>4624 Microsoft-Windows-SeLogon</td>
<td></td>
</tr>
<tr>
<td>Audit Success</td>
<td>2/20/2018</td>
<td>8:11:18 PM</td>
<td>\S-1-5-21-3671970501-3975728774-4289435121-3101</td>
<td>4624 Microsoft-Windows-SeLogon</td>
<td></td>
</tr>
<tr>
<td>Audit Success</td>
<td>2/20/2018</td>
<td>8:11:18 PM</td>
<td>\S-1-5-21-3671970501-3975728774-4289435121-3101</td>
<td>4624 Microsoft-Windows-SeLogon</td>
<td></td>
</tr>
</tbody>
</table>

New Logon:
- Security ID: \S-1-5-21-3671970501-3975728774-4289435121-3101
- Account Name: ninja-master
- Account Domain: NINJA MOTORS
- Logon ID: 0xc2e8a
- Linked Logon ID: (null)
- Network Account Name: -
- Network Account Domain: -
- Logon Server: -

Process Information:
- Process ID: 0x0
- Process Name: -

Network Information:
- Workstation Name: -
- Source Network Address: 192.168.52.40
- Source Port: 64216

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 execution name and the service name of PsExec with -r option, we can still detect PsExec execution because of the following characteristics.

  • The PsExec service execution file (default: PSEXESVC.exe) is copied to “%SystemRoot%” directory on the remote computer.
  
  • The service name is the same as the execution 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 execution file, not “SYSTEM”.

Copyright Internet Initiative Japan Inc.
PsExec Detection Method 2 (2)

• We use the same log as the previous exercise’s one. Click “Filter Events” button.
  • Training_Materials\EventLogAnalysis\PSEexec\win7_system_psexec_en.evtx
PsExec

(1) Click “Load” button.

(2) Choose “Training_Materials\EventLogAnalysis\PsExec\Sys7045_psexec.elc”, then click “Open” button.
PsExec

Filter with:
- containing .exe in the file name
- containing %SystemRoot% in the file name
- user mode service for service type
- LocalSystem as service account
- demand start as service start type

Filter with the event ID 7045.

Filter out the “SYSTEM” account.
This execution file is directly under the %SystemRoot% directory.

The file name is not the default PSEexec name, but...

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 20\textsuperscript{th} Feb.
  • The temporary service name is “WindowsWMIIService”.

To be continued...