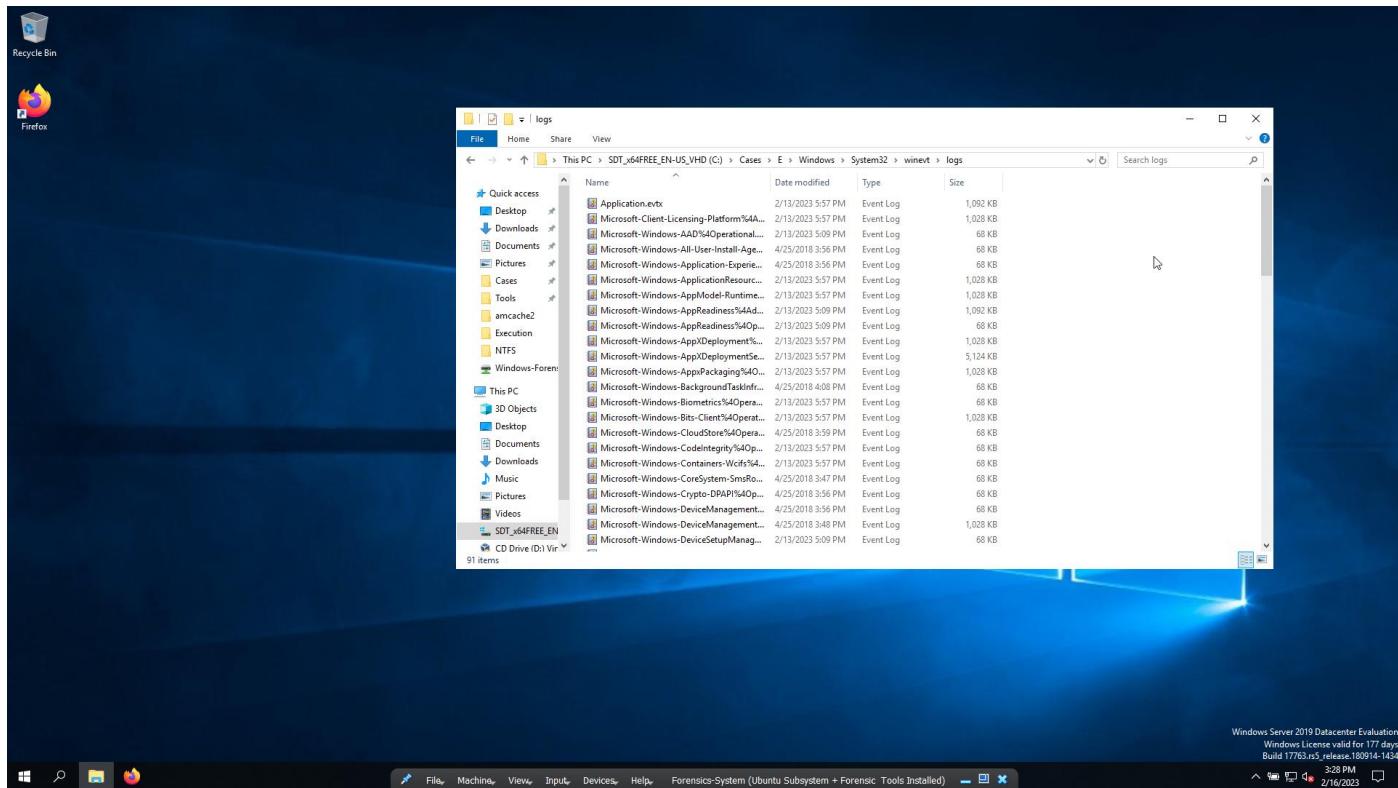


# Evidence of malicious activity:

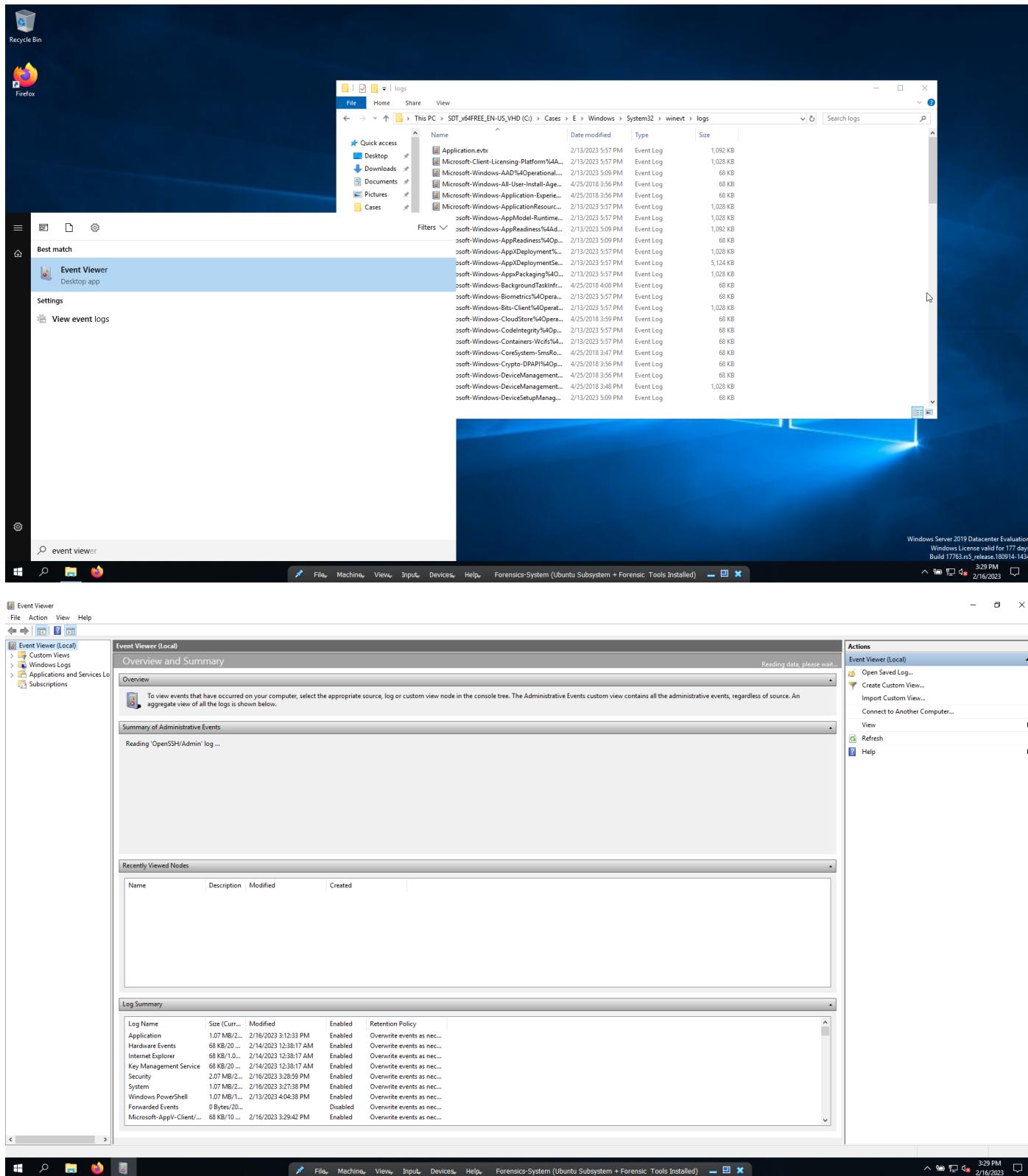
- Event Logs
- EventLogExplorer & EvtxECmd
- Windows Defender
- Service installs
- Security event log
- Authentication
- Powershell
- Malicious Powershell
- Sysmon & Malicious Sysmon

## Event Logs

- Location logs artifacts:
  - C:\Windows\System32\winevt\logs



- You can use the event log viewer that comes with windows:



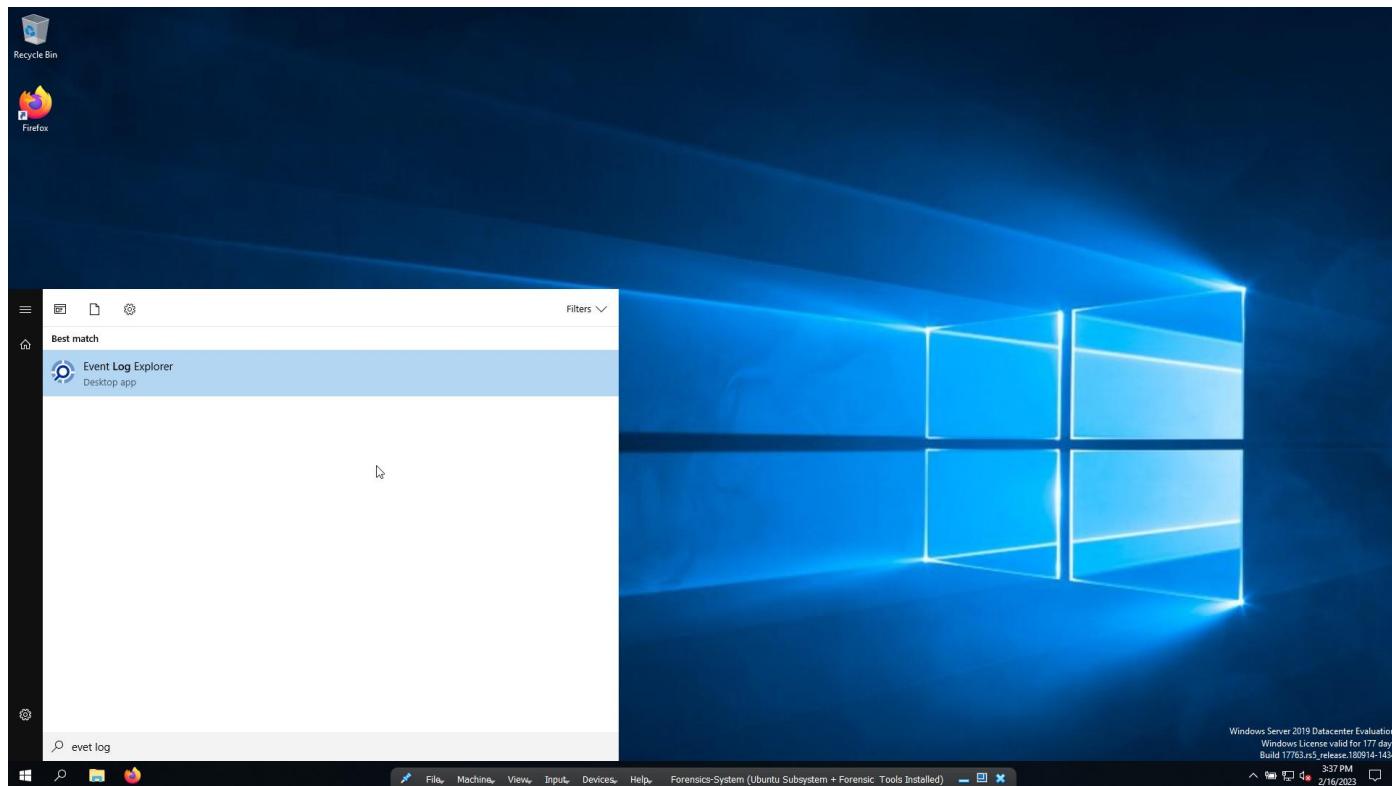
- Important logs are:
  - o Application – information about application in the operating system, service stopped, started, etc

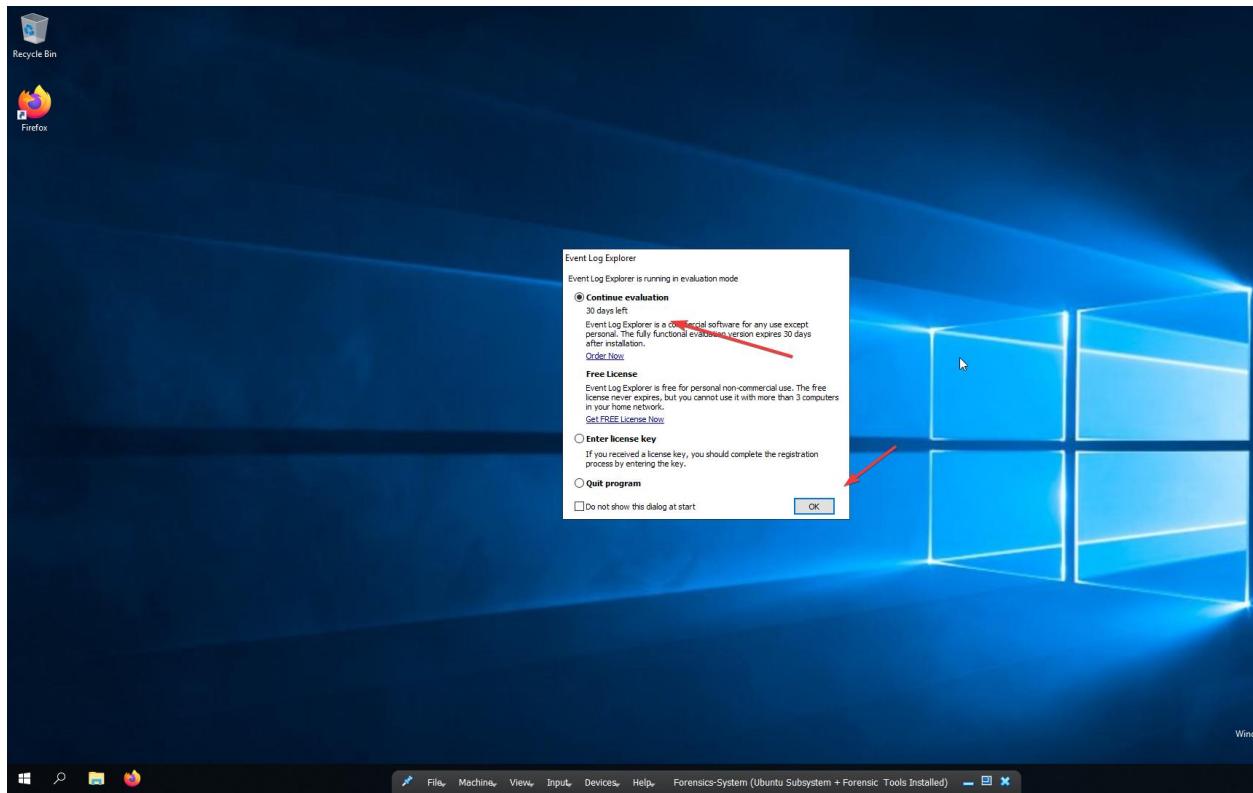
- Security – information about users, logins of users, when, how it logged
- You can start investigation event logs based on particular:
  - Timestamps
  - Applications
  - Users : Event ID example is 4624.
- More information on Event IDs :
 

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/>

## EventLogExplorer & EvtxECmd

- Tools used in forensic analysis of event logs:
  - Event Log Explorer





- Drag and drop the .evtx file.

Untitled.EWX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search

WBH-POHAJ6CQHQM (local)

Log Files Application (C:\Cases\Windows\System32\winet\logs\app)

Task templates

Type: Information

Date: 2/1

Filter: File Home Share View

UTC

Name Date modified Type Size

Name	Date modified	Type	Size
Application.evtx	2/19/2023 5:57 PM	Event Log	1,092 KB
Microsoft-Client-Licensing-Platform%4A...	2/19/2023 5:57 PM	Event Log	1,028 KB
Microsoft-Windows-AAD%Operational...	2/19/2023 5:09 PM	Event Log	68 KB
Microsoft-Windows-All-User-Install-Age...	4/25/2018 3:56 PM	Event Log	68 KB
Microsoft-Windows-Application-Experi...	4/25/2018 3:56 PM	Event Log	68 KB
Microsoft-Windows-ApplicationResource...	2/19/2023 5:57 PM	Event Log	1,028 KB
Microsoft-Windows-AppModel-Runtime...	2/19/2023 5:57 PM	Event Log	1,028 KB
Microsoft-Windows-AppReadiness%4Op...	2/19/2023 5:09 PM	Event Log	1,092 KB
Microsoft-Windows-AppReadiness%4Op...	2/19/2023 5:57 PM	Event Log	68 KB
Microsoft-Windows-AppDeploymentSe...	2/19/2023 5:57 PM	Event Log	1,028 KB
Microsoft-Windows-AppXDeploymentSe...	2/19/2023 5:57 PM	Event Log	5,124 KB
Microsoft-Windows-AppxPackaging%4O...	2/19/2023 5:57 PM	Event Log	1,028 KB
Microsoft-Windows-BackgroundTaskInfr...	4/25/2018 4:08 PM	Event Log	68 KB
Microsoft-Windows-Biometrics%4Opera...	2/19/2023 5:57 PM	Event Log	68 KB
Microsoft-Windows-Bits-Client%4Operat...	2/19/2023 5:57 PM	Event Log	1,028 KB
Microsoft-Windows-CloudStore%4Opera...	4/25/2018 3:59 PM	Event Log	68 KB
Microsoft-Windows-CodeIntegrity%4Op...	2/19/2023 5:57 PM	Event Log	68 KB
Microsoft-Windows-Containers-Wcrf%4...	2/19/2023 5:57 PM	Event Log	68 KB
Microsoft-Windows-CoreSystem-SmR0...	4/25/2018 3:47 PM	Event Log	68 KB
Microsoft-Windows-Crypto-DBAPI%4Op...	4/25/2018 3:56 PM	Event Log	68 KB
Microsoft-Windows-DeviceManagement...	4/25/2018 3:56 PM	Event Log	68 KB
Microsoft-Windows-DeviceManagement...	4/25/2018 3:48 PM	Event Log	1,028 KB
Microsoft-Windows-DeviceSetupManag...	2/19/2023 5:09 PM	Event Log	68 KB

Description

The User Profile Service has stopped.

1001 Windows Error Rep None N/A

MSEdgeWIN10

File Machine View Input Devices Help Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) 3:37 PM 2/16/2023

## ○ EvtxCmd

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

```
Administrator: C:\Windows\system32\cmd.exe
>-- WINE-90
>-- Log Files
>-- Task tem
C:\Tools\EZTools>EvtxECmd -d C:\Cases\E\Windows\System32\winevt\logs --csv c:\Cases\Analysis\EventLogs
EvtxECmd is not recognized as an internal or external command,
operable program or batch file.

C:\Tools\EZTools>EvtxECmd>EvtxECmd.exe E:\Windows\System32\winevt\logs --csv c:\Cases\Analysis\EventLogs
C:\Tools\EZTools>d EvtxECmd

C:\Tools\EZTools>EvtxECmd>EvtxECmd.exe -d C:\Cases\E\Windows\System32\winevt\logs --csv c:\Cases\Analysis\EventLogs
```

File Explorer

EvtxECmd

modified	Type	Size
023 3:54 PM	File folder	
022 11:21 AM	Application	4,991 KB

Details

Information 2/1 Downloads

Information 2/1 Music

Information 2/1 Pictures

Information 2/1 Videos

Information 2/1 SDT\_x64FREE\_EN

Information 2/1 CD Drive (D:\) Vir

Information 2/1 2 items

Information 2/13/2023 5:15:43 PM 1001 Windows Error Reg None N/A MSEdgeWIN10

Description

The User Profile Service has stopped.

File Explorer

EvtxECmd

modified	Type	Size
023 3:54 PM	File folder	
022 11:21 AM	Application	4,991 KB

Details

Information 2/1 Downloads

Information 2/1 Music

Information 2/1 Pictures

Information 2/1 Videos

Information 2/1 SDT\_x64FREE\_EN

Information 2/1 CD Drive (D:\) Vir

Information 2/1 2 items

Information 2/13/2023 5:15:43 PM 1001 Windows Error Reg None N/A MSEdgeWIN10

Description

The User Profile Service has stopped.

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

```
Administrator: C:\Windows\system32\cmd.exe
>-- WINE-90
>-- Log Files
>-- Task tem
Processing C:\Cases\E\Windows\System32\winevt\logs\Windows_PowerShell.evtx...
Chunk count: 5 Iterating records...

Event log details
Flags: 0x0
Chunk count: 5
Stored/Calculated CRC: 424A608A/424A608A
Earliest timestamp: 2018-04-25 15:48:38.0449765
Latest timestamp: 2023-02-13 17:29:07.2388400
Total event log records found: 231

Records included: 231 Errors: 0 Events dropped: 0

Metrics (including dropped events)
Event ID Count
104 6
100 27
103 20
500 170
500 8

Processed 91 files in 25.0357 seconds
```

File Explorer

EvtxECmd

modified	Type	Size
023 3:54 PM	File folder	
022 11:21 AM	Application	4,991 KB

Details

Information 2/1 Downloads

Information 2/1 Music

Information 2/1 Pictures

Information 2/1 Videos

Information 2/1 SDT\_x64FREE\_EN

Information 2/1 CD Drive (D:\) Vir

Information 2/1 2 items

Information 2/13/2023 5:15:43 PM 1001 Windows Error Reg None N/A MSEdgeWIN10

Description

The User Profile Service has stopped.

File Explorer

EvtxECmd

modified	Type	Size
023 3:54 PM	File folder	
022 11:21 AM	Application	4,991 KB

Details

Information 2/1 Downloads

Information 2/1 Music

Information 2/1 Pictures

Information 2/1 Videos

Information 2/1 SDT\_x64FREE\_EN

Information 2/1 CD Drive (D:\) Vir

Information 2/1 2 items

Information 2/13/2023 5:15:43 PM 1001 Windows Error Reg None N/A MSEdgeWIN10

Description

The User Profile Service has stopped.

Untitled.EXL - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Administrator C:\Windows\system32\cmd.exe

Processing C:\Cases\E\Windows\System32\winevt\logs\Windows PowerShell

Chunk count: 9, Iterating records...

Event log details

Flags: None

Chunk count: 5

Stored/Calculated CRC: 42446B8A/42446B8A

File timestamp: 2018-04-25 15:48:30.0449765

Last timestamp: 2023-02-13 17:29:07.2388400

Total event log records found: 231

Records included: 231 Errors: 0 Events dropped: 0

Metrics (including dropped events)

Event ID	Count
104	6
400	27
403	20
408	10
500	8

Processed 91 files in 25.0357 seconds

C:\Tools\EZTools\EvtxECmd>

File Home Share View

Name Date modified Type Size

20230216154311\_EvtxECmd\_Output.csv 2/16/2023 3:43 PM CSV File 27,657 KB

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- Cases
- Tools
- amcache2
- Execution
- NTFS
- Windows-Forensics
- This PC
- ID Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- SDT\_x64FREE\_EN
- CD Drive (D:\) Vir
- 1 item

2/13/2023 5:15:43 PM 1001 | Windows Error Rep None N/A MSEDEWIN10

Description

The User Profile Service has stopped.

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

20230216154311\_EvtxECmd\_Output.csv

Drag a column header here to group by that column

Line	Tag	Record Number	Event Record Id	Time Created	Event Id	Level	Provider	Channel	Process Id	Computer	User Id
1		1	1	2018-04-25 15...	4625	Info	Microsoft-Windows-EventSystem	Application		=	MSEDEWIN10
2		2	2	2018-04-25 15...	1531	Info	Microsoft-Windows-User Profiles Service	Application		1320	IEUSER-QHG143JP S-1-5-18
3		3	3	2018-04-25 15...	100	Info	WLMS	Application			IEUSER-QHG143JP
4		4	4	2018-04-25 15...	5615	Info	Microsoft-Windows-WMI	Application		2220	IEUSER-QHG143JP S-1-5-18
5		5	5	2018-04-25 15...	916	Info	ESENT	Application			IEUSER-QHG143JP
6		6	6	2018-04-25 15...	1016	Info	Microsoft-Windows-Security-SPP	Application			MSEDEWIN10
7		7	7	2018-04-25 15...	1034	Info	Microsoft-Windows-Security-SPP	Application			MSEDEWIN10
8		8	8	2018-04-25 15...	1003	Info	Microsoft-Windows-Security-SPP	Application			MSEDEWIN10
9		9	9	2018-04-25 15...	1005	Info	Microsoft-Windows-Search	Application			MSEDEWIN10
10		10	10	2018-04-25 15...	1003	Info	Microsoft-Windows-Search	Application			MSEDEWIN10
11		11	11	2018-04-25 15...	1531	Info	Microsoft-Windows-User Profiles Service	Application	1696	MSEDEWIN10	S-1-5-18
12		12	12	2018-04-25 15...	100	Info	WLMS	Application			MSEDEWIN10
13		13	13	2018-04-25 15...	916	Info	ESENT	Application			MSEDEWIN10
14		14	14	2018-04-25 15...	5615	Info	Microsoft-Windows-WMI	Application	2840	MSEDEWIN10	S-1-5-18
15		15	15	2018-04-25 15...	5617	Info	Microsoft-Windows-WMI	Application	2840	MSEDEWIN10	S-1-5-18
16		16	16	2018-04-25 15...	5	Info	Microsoft-Windows-Search-ProfileNotify	Application			MSEDEWIN10
17		17	17	2018-04-25 15...	1534	Warning	Microsoft-Windows-User Profiles Service	Application	1696	MSEDEWIN10	S-1-5-18
18		18	18	2018-04-25 15...	6003	Info	Microsoft-Windows-Winlogon	Application			MSEDEWIN10
19		19	19	2018-04-25 15...	6003	Info	Microsoft-Windows-Winlogon	Application			MSEDEWIN10
20		20	20	2018-04-25 15...	6000	Info	Microsoft-Windows-Winlogon	Application			MSEDEWIN10
21		21	21	2018-04-25 15...	1534	Warning	Microsoft-Windows-User Profiles Service	Application	1696	MSEDEWIN10	S-1-5-18
22		22	22	2018-04-25 15...	4097	Info	Microsoft-Windows-CAPI2	Application	1404	MSEDEWIN10	
23		23	23	2018-04-25 15...	4112	Info	Microsoft-Windows-CAPI2	Application	1404	MSEDEWIN10	
24		24	24	2018-04-25 15...	916	Info	ESENT	Application			MSEDEWIN10
25		25	25	2018-04-25 15...	916	Info	ESENT	Application			MSEDEWIN10
26		26	26	2018-04-25 15...	916	Info	ESENT	Application			MSEDEWIN10
27		27	27	2018-04-25 15...	6000	Info	Microsoft-Windows-Winlogon	Application			MSEDEWIN10
28		28	28	2018-04-25 15...	6000	Info	Microsoft-Windows-Winlogon	Application			MSEDEWIN10
29		29	29	2018-04-25 15...	6003	Info	Microsoft-Windows-Winlogon	Application			MSEDEWIN10
30		30	30	2018-04-25 15...	9027	Info	Desktop Window Manager	Application			MSEDEWIN10
31		31	31	2018-04-25 15...	6003	Info	Microsoft-Windows-Winlogon	Application			MSEDEWIN10
32		32	32	2018-04-25 15...	5	Info	Microsoft-Windows-Search-ProfileNotify	Application			MSEDEWIN10
33		33	33	2018-04-25 15...	6000	Info	Microsoft-Windows-Winlogon	Application			MSEDEWIN10

C:\Cases\Analysis\EventLogs\20230216154311\_EvtxECmd\_Output.csv

Total lines: 34,860 | Visible lines: 34,860 | Open files: 1 | Search options

- Filter the data by Time Created this year.

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

20230216154311\_EvtbECmd\_Output.csv

Drag a column header here to group by that column

Line Tag Record Number Event Record Id Time Created Provider Channel Process Id Computer User Id

Values Date Filters

Specific Date Periods

Yesterday Today Tomorrow Last Week Last Year

Last Month This Month Next Month This Week Next Year

OK Cancel

Total lines 34,860 | Visible lines 34,860 | Open files: 1 | Search options

345 PM 2/16/2023

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

20230216154311\_EvtbECmd\_Output.csv

Drag a column header here to group by that column

Line Tag Record Number Event Record Id Time Created Event Id Level Provider Channel Process Id Computer User Id

283 283 283 2023-02-13 17.. 4625 Info Microsoft-Windows-EventSystem Application 0 MSEDEWIN10 S-1-5-18

284 284 284 2023-02-13 17.. 1531 Info Microsoft-Windows-User Profiles Service Application 1408 MSEDEWIN10 S-1-5-18

285 285 285 2023-02-13 17.. 5615 Info Microsoft-Windows-WMI Application 2516 MSEDEWIN10 S-1-5-18

286 286 286 2023-02-13 17.. 900 Info Microsoft-Windows-Security-SPP Application 0 MSEDEWIN10

287 287 287 2023-02-13 17.. 16394 Info Microsoft-Windows-Security-SPP Application 0 MSEDEWIN10

288 288 288 2023-02-13 17.. 916 Info ESENT Application 0 MSEDEWIN10

289 289 289 2023-02-13 17.. 1066 Info Microsoft-Windows-Security-SPP Application 0 MSEDEWIN10

290 290 290 2023-02-13 17.. 8226 Info Microsoft-Windows-Security-SPP Application 0 MSEDEWIN10

291 291 291 2023-02-13 17.. 1034 Info Microsoft-Windows-Security-SPP Application 0 MSEDEWIN10

292 292 292 2023-02-13 17.. 1003 Info Microsoft-Windows-Security-SPP Application 0 MSEDEWIN10

293 293 293 2023-02-13 17.. 902 LogAlways Microsoft-Windows-Security-SPP Application 0 MSEDEWIN10

294 294 294 2023-02-13 17.. 100 WLMs Application 0 MSEDEWIN10

295 295 295 2023-02-13 17.. 5617 Info Microsoft-Windows-WMI Application 2516 MSEDEWIN10 S-1-5-18

296 296 296 2023-02-13 17.. 6003 Info Microsoft-Windows-Winlogon Application 0 MSEDEWIN10

297 297 297 2023-02-13 17.. 916 Info ESENT Application 0 MSEDEWIN10

298 298 298 2023-02-13 17.. 4097 Info Microsoft-Windows-CAPI2 Application 2484 MSEDEWIN10

299 299 299 2023-02-13 17.. 4112 Info Microsoft-Windows-CAPI2 Application 2484 MSEDEWIN10

300 300 300 2023-02-13 17.. 6003 Info Microsoft-Windows-Winlogon Application 0 MSEDEWIN10

301 301 301 2023-02-13 17.. 6000 Info Microsoft-Windows-Winlogon Application 0 MSEDEWIN10

302 302 302 2023-02-13 17.. 8230 Info Microsoft-Windows-Security-SPP Application 0 MSEDEWIN10

303 303 303 2023-02-13 17.. 0 Info sshd Application 0 MSEDEWIN10 S-1-5-21-1058341133-209241773

304 304 304 2023-02-13 17.. 0 Info sshd Application 0 MSEDEWIN10 S-1-5-21-1058341133-209241773

305 305 305 2023-02-13 17.. 8230 Info Microsoft-Windows-Security-SPP Application 0 MSEDEWIN10

306 306 306 2023-02-13 17.. 916 Info ESENT Application 0 MSEDEWIN10

307 307 307 2023-02-13 17.. 0 Info OpenSSH Application 0 MSEDEWIN10 S-1-5-21-1058341133-209241773

308 308 308 2023-02-13 17.. 4097 Info Microsoft-Windows-CAPI2 Application 2484 MSEDEWIN10

309 309 309 2023-02-13 17.. 1003 Info Microsoft-Windows-Security-SPP Application 0 MSEDEWIN10

310 310 310 2023-02-13 17.. 1013 LogAlways Microsoft-Windows-Security-SPP Application 0 MSEDEWIN10

311 311 311 2023-02-14 03.. 1531 Info Microsoft-Windows-User Profiles Service Application 1224 MSEDEWIN10 S-1-5-18

312 312 312 2023-02-13 17.. 4625 Info Microsoft-Windows-EventSystem Application 0 MSEDEWIN10

313 313 313 2023-02-13 17.. 900 Info Microsoft-Windows-Security-SPP Application 0 MSEDEWIN10

314 314 314 2023-02-13 17.. 16394 Info Microsoft-Windows-Security-SPP Application 0 MSEDEWIN10

Time Created Is this year

Total lines 34,860 | Visible lines 21,880 | Open files: 1 | Search options

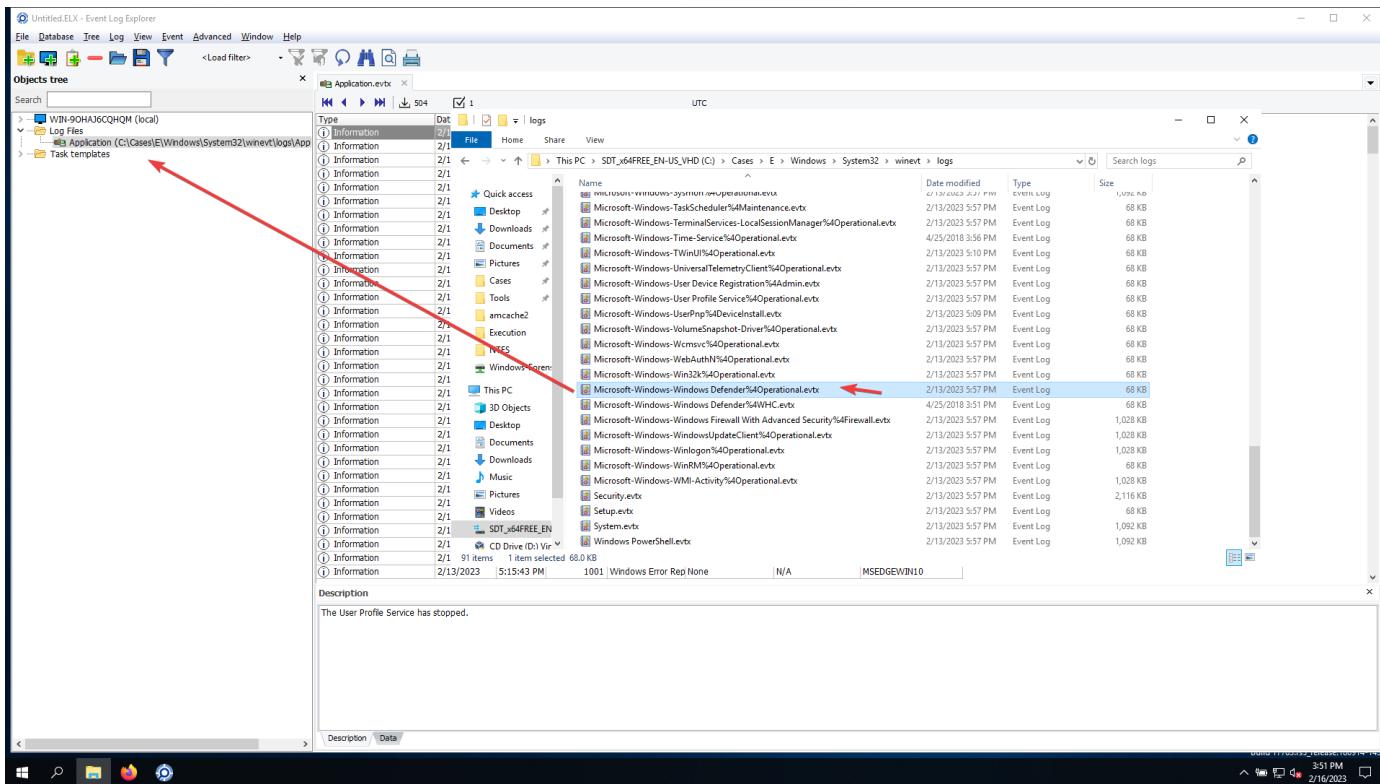
346 PM 2/16/2023

## Windows Defender

- Event IDs for Microsoft-Windows-Windows Defender:

- 5000: Defender enabled
- 5001: Defender disabled

- Load Microsoft-Windows-Windows Defender Operational :



The screenshot shows the Event Log Explorer interface with the following details:

- Title Bar:** Untitled.ELX - Event Log Explorer
- Menu Bar:** File, Database, Tree, Log, View, Event, Advanced, Window, Help
- Toolbar:** Includes icons for New, Open, Save, Print, Filter, and others.
- Objects Tree:** Shows a tree view of log files, with "Application.evtx" selected.
- Event List:** A table titled "Application.evtx" showing events from "Microsoft-Windows-Defender%Operational". The table includes columns: Type, Date, Time, Event, Source, Category, User, and Computer. The data shows multiple "Information" events occurring between 2/13/2023 and 4/25/2018, primarily from source "\SYSTEM" and user "MSEdgeVh110".
- Description Panel:** Displays a summary of a completed Microsoft Defender Antivirus scan, including Scan ID, Scan Type, Scan Parameters, User, and Scan Time.
- Bottom Status Bar:** Shows the date and time as 2/16/2023 3:51 PM.

- We can filter the data:

The screenshot shows the Event Log Explorer interface with the following details:

- Title Bar:** Untitled.ELX - Event Log Explorer
- Menu Bar:** File, Database, Tree, Log, View, Event, Advanced, Window, Help
- Toolbar:** Includes icons for New, Open, Save, Print, Filter, and others.
- Objects Tree:** Shows a tree view of log files, with "Application.evtx" selected.
- Event List:** A table titled "Application.evtx" showing events from "Microsoft-Windows-Defender%Operational". The table includes columns: Type, Date, Time, Event, Source, Category, User, and Computer. The data shows multiple "Information" events occurring between 2/13/2023 and 4/25/2018, primarily from source "\SYSTEM" and user "MSEdgeVh110".
- Description Panel:** Displays a summary of a completed Microsoft Defender Antivirus scan, including Scan ID, Scan Type, Scan Parameters, User, and Scan Time.
- Bottom Status Bar:** Shows the date and time as 2/16/2023 3:52 PM.

Screenshot of Event Log Explorer showing the filter dialog for Application.evtx.

The filter dialog is open with the following settings:

- Type:** Information
- Date:** 2/13/2023
- Time:** 5:22:43 PM
- Event:** 1001
- Source:** Microsoft-Windows None
- Category:** SYSTEM
- User:** MSEdgeWIN10
- Computer:** MSEdgeWIN10

**Filter:** 2/13/2023 5:21:35 PM

**Event ID(s):** 5000, 5001

**Description:**

Microsoft Defender Antivirus scan completed.  
Scan ID: E995F20A-C2BD-451F-AD14-417EF2B8A5CE2  
Scan Type: Antimalware  
Scan Parameters: Quick Scan  
User: NT AUTHORITY\NETWORK SERVICE  
Scan Time: 0:01:38

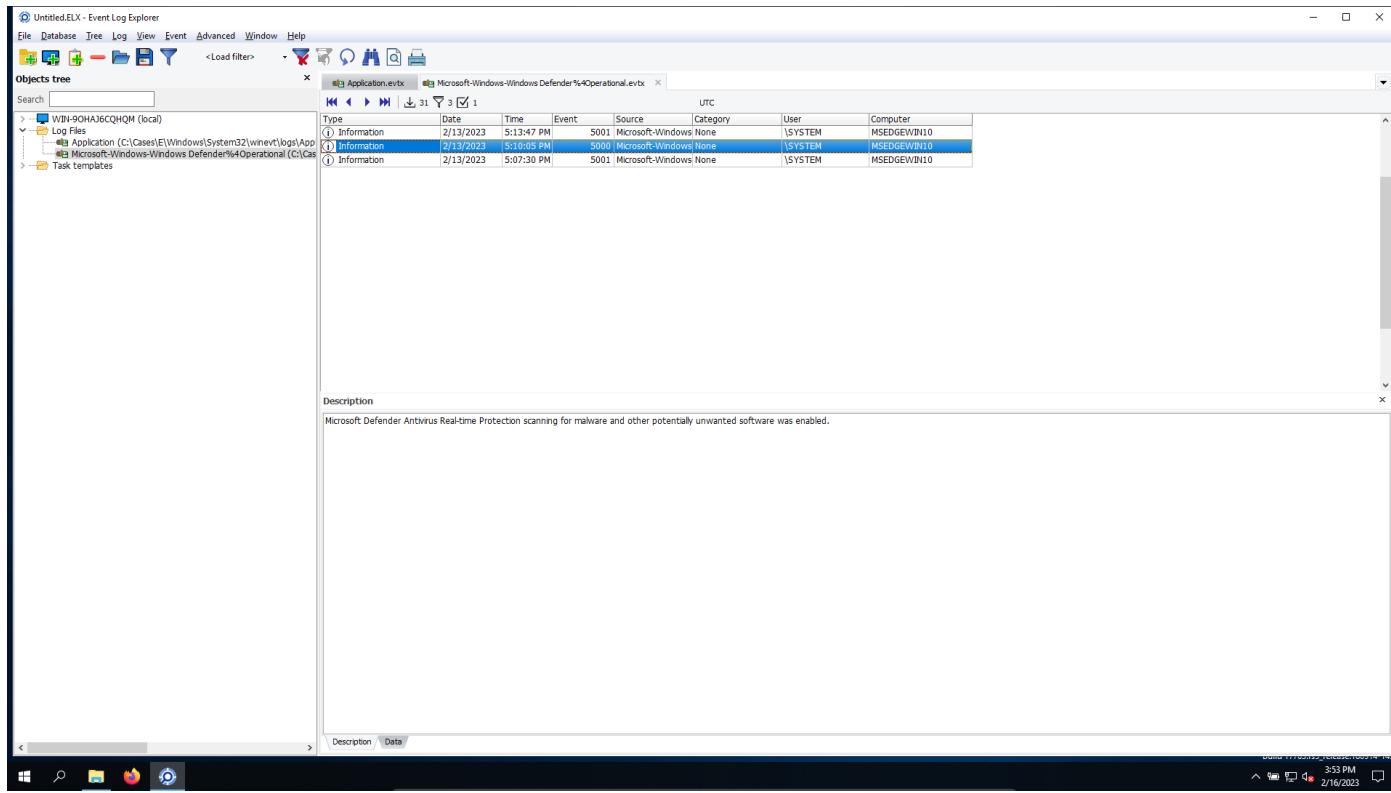
Screenshot of Event Log Explorer showing the filtered results for Application.evtx.

The results table shows the following events:

Type	Date	Time	Event	Source	Category	User	Computer
Information	2/13/2023	5:13:47 PM	5001	Microsoft-Windows None	SYSTEM	MSEdgeWIN10	
Information	2/13/2023	5:10:05 PM	5000	Microsoft-Windows None	SYSTEM	MSEdgeWIN10	
Information	2/13/2023	5:07:30 PM	5001	Microsoft-Windows None	SYSTEM	MSEdgeWIN10	

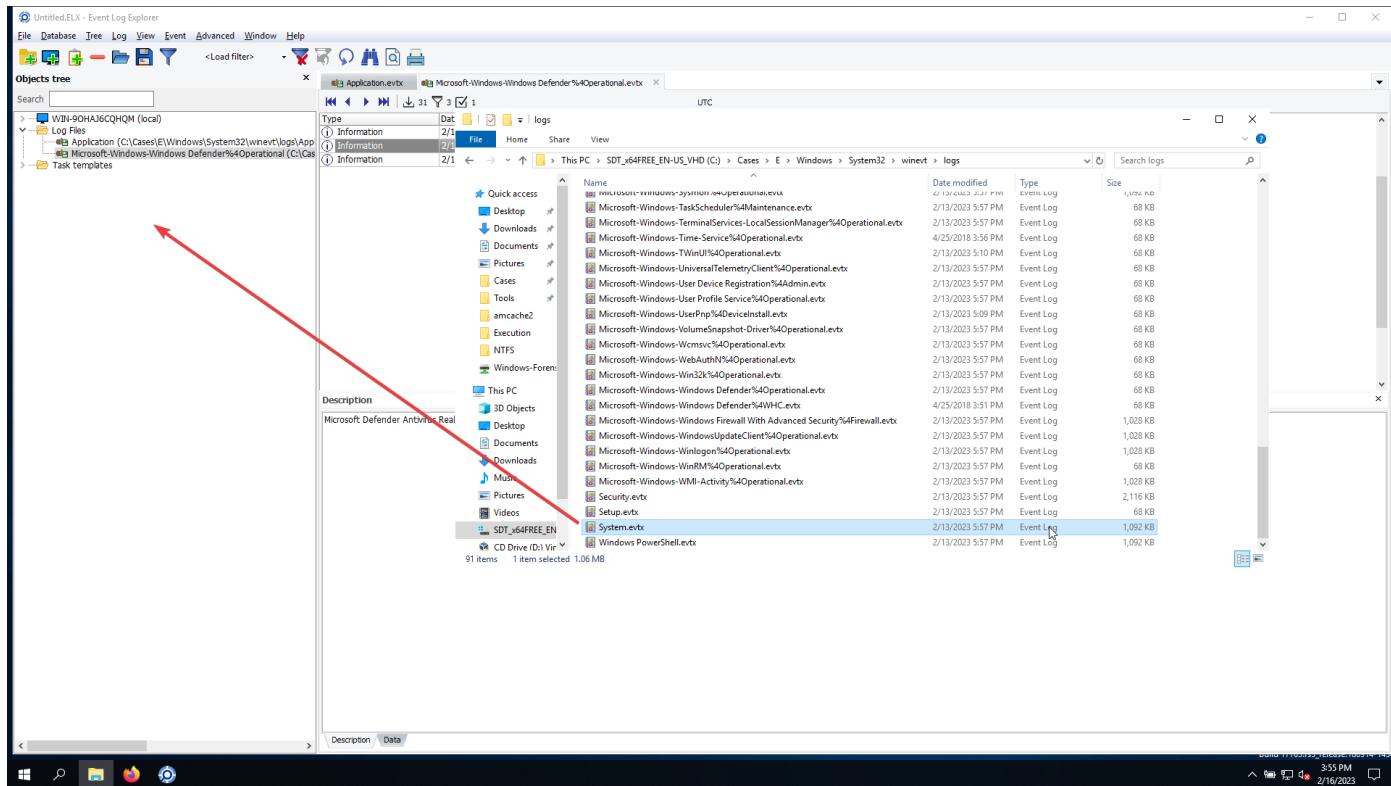
**Description:**

Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was disabled.



## Service installs

- Event IDs for System:
  - o 7045: A new service was installed.
  
- Load System log:



Type	Date	Time	Event	Source	Category	User	Computer
Information	2/13/2023	5:56:59 PM	50106	Microsoft-Windows Service State Event	NT AUTHORITY\LOC	MSEDGWV\N10	
Information	2/13/2023	5:56:59 PM	51057	Microsoft-Windows Service State Event	NT AUTHORITY\LOC	MSEDGWV\N10	
Information	2/13/2023	5:56:59 PM	51047	Microsoft-Windows Service State Event	NT AUTHORITY\LOC	MSEDGWV\N10	
Information	2/13/2023	5:56:59 PM	50105	Microsoft-Windows Service State Event	NT AUTHORITY\LOC	MSEDGWV\N10	
Information	2/13/2023	5:56:59 PM	50104	Microsoft-Windows Service State Event	NT AUTHORITY\LOC	MSEDGWV\N10	
Information	2/13/2023	5:56:59 PM	6006	EventLog	None	N/A	MSEDGWV\N10
Information	2/13/2023	5:56:58 PM	7002	Microsoft-Windows (1102)	SYSTEM	MSEDGWV\N10	
Information	2/13/2023	5:56:52 PM	1024	User22.....	None	\$-1-S-2-1-105834112	MSEDGWV\N10
Information	2/13/2023	5:56:48 PM	1	Microsoft-Windows (5)	SYSTEM	MSEDGWV\N10	
Information	2/13/2023	5:30:47 AM	7040	Service Control Msc None	SYSTEM	MSEDGWV\N10	
Information	2/13/2023	5:28:30 PM	7045	Service Control Msc None	\$-1-S-2-1-105834112	MSEDGWV\N10	
Information	2/13/2023	5:27:34 PM	7040	Service Control Msc None	SYSTEM	MSEDGWV\N10	
Information	2/13/2023	5:26:44 PM	44	Microsoft-Windows Windows Update Age	SYSTEM	MSEDGWV\N10	
Information	2/13/2023	5:25:13 PM	6	Microsoft-Windows None	SYSTEM	MSEDGWV\N10	
Information	2/13/2023	5:25:13 PM	7045	Service Control Msc None	\$-1-S-2-1-105834112	MSEDGWV\N10	
Information	2/13/2023	5:25:13 PM	7045	Service Control Msc None	\$-1-S-2-1-105834112	MSEDGWV\N10	
Information	2/13/2023	5:22:50 PM	19	Microsoft-Windows Windows Update Age	SYSTEM	MSEDGWV\N10	
Information	2/13/2023	5:22:48 PM	16	Microsoft-Windows None	\$-1-S-2-1-105834112	MSEDGWV\N10	
Information	2/13/2023	5:22:45 PM	43	Microsoft-Windows Windows Update Age	SYSTEM	MSEDGWV\N10	
Information	2/13/2023	5:22:44 PM	16	Microsoft-Windows None	SYSTEM	MSEDGWV\N10	
Information	2/13/2023	5:22:39 PM	19	Microsoft-Windows Windows Update Age	SYSTEM	MSEDGWV\N10	
Information	2/13/2023	5:22:39 PM	44	Microsoft-Windows Windows Update Age	SYSTEM	MSEDGWV\N10	
Information	2/13/2023	5:22:37 PM	16	Microsoft-Windows None	\$-1-S-2-1-105834112	MSEDGWV\N10	
Information	2/13/2023	5:22:37 PM	43	Microsoft-Windows Windows Update Age	SYSTEM	MSEDGWV\N10	
Information	2/13/2023	5:22:37 PM	19	Microsoft-Windows Windows Update Age	SYSTEM	MSEDGWV\N10	
Information	2/13/2023	5:22:35 PM	16	Microsoft-Windows None	\$-1-S-2-1-105834112	MSEDGWV\N10	
Information	2/13/2023	5:22:34 PM	43	Microsoft-Windows Windows Update Age	SYSTEM	MSEDGWV\N10	
Information	2/13/2023	5:22:34 PM	19	Microsoft-Windows Windows Update Age	SYSTEM	MSEDGWV\N10	
Information	2/13/2023	5:22:33 PM	16	Microsoft-Windows None	SYSTEM	MSEDGWV\N10	
Information	2/13/2023	5:22:33 PM	16	Microsoft-Windows None	SYSTEM	MSEDGWV\N10	
Information	2/13/2023	5:22:24 PM	16	Microsoft-Windows None	\$-1-S-2-1-105834112	MSEDGWV\N10	
Information	2/13/2023	5:22:24 PM	43	Microsoft-Windows Windows Update Age	SYSTEM	MSEDGWV\N10	

- Query based on event id 7045.

Untitled.EX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search [ ]

Log Files Application (C:\Cases\Windows\System32\winevt\logs\Application.evtx) Microsoft-Windows-Windows Defender%Operational (C:\Logs\System.evtx)

Type Date Time Event Source Category User Computer

Type	Date	Time	Event	Source	Category	User	Computer
(i) Information	2/13/2023	5:28:30 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	2/13/2023	5:25:13 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	2/13/2023	5:13:31 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	2/13/2023	5:08:56 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	4/25/2018	3:59:52 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	4/25/2018	3:52:24 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	4/25/2018	3:52:24 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	4/25/2018	3:52:23 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	4/25/2018	3:52:20 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	4/25/2018	3:48:17 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	4/25/2018	3:46:42 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	IUSER-QHG43JP	

Description

A service was installed in the system.

Service Name: AtomicTestService\_CMD  
 Service File Name: C:\AtomicRedTeam\atomic\T1543.003\bin\AtomicService.exe  
 Service Type: user mode service  
 Service Start Type: demand start  
 Service Account: LocalSystem

Description Data

- Installed by user 1000.

Untitled.EX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search [ ]

Log Files Application (C:\Cases\Windows\System32\winevt\logs\Application.evtx) Microsoft-Windows-Windows Defender%Operational (C:\Logs\System.evtx)

Type Date Time Event Source Category User Computer

Type	Date	Time	Event	Source	Category	User	Computer
(i) Information	2/13/2023	5:28:30 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	2/13/2023	5:25:13 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	2/13/2023	5:13:31 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	2/13/2023	5:08:56 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	4/25/2018	3:59:52 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	4/25/2018	3:52:24 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	4/25/2018	3:52:24 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	4/25/2018	3:52:23 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	4/25/2018	3:52:20 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	4/25/2018	3:48:17 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	MSEdgeWin10	
(i) Information	4/25/2018	3:46:42 PM	7045	Service Control Mar None	[S-1-5-21-1058341133-2092417715-4019509128-1000]	IUSER-QHG43JP	

Description

A service was installed in the system.

Service Name: AtomicTestService\_CMD  
 Service File Name: C:\AtomicRedTeam\atomic\T1543.003\bin\AtomicService.exe  
 Service Type: user mode service  
 Service Start Type: demand start  
 Service Account: LocalSystem

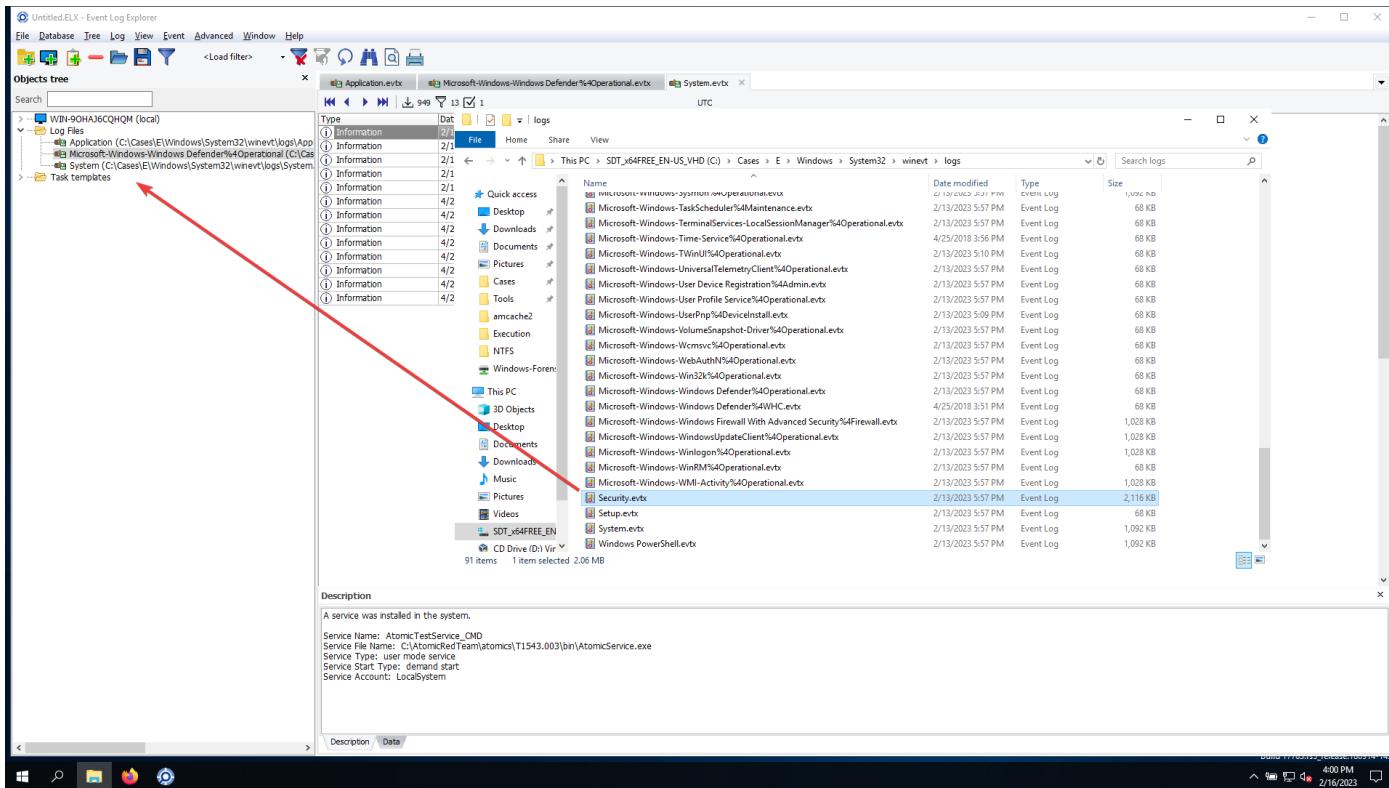
Description Data

Security event log

- Event IDs for Security:

- 4624: An account was successfully logged on.

- Load Security log:



- Query based on event id 4624.

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	2/13/2023	5:56:38 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:56:53 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:56:51 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:56:49 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:56:47 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:26:35 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:26:34 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:26:31 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:20:56 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:20:54 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:18:29 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:17:38 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:17:31 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:13:51 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:13:52 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:13:52 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:13:52 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:13:52 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:13:52 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:13:29 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:13:29 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:13:28 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:13:14 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:13:14 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:13:06 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:12:56 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:11:52 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:11:48 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:11:46 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:11:39 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:11:38 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:11:35 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	

Description  
An account was successfully logged on.  
Subject:  
Security ID: S-1-5-18  
Account Name: MSEDGEWIN10\$  
Account Domain: WORKGROUP  
Logon ID: 0x3e7  
Logon Information:  
Logon Type: 5  
Restricted Admin Mode: :  
Virtual Account: No

- You can see that there is A Logon Type information, you can find more information about it at :
   
<https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624>
- Important logon types:
  - o 2: Interactive – with peripherals access and a monitor
  - o 3: Network – logging through the network, remote
  - o 10: RemoteInteractive – logging to a computer remotely using Remote Desktop.
- Search for the same eventid but adding the user in text description:

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search [ ]

Log Files

- Application (C:\Cases\Windows\System32\winevt\logs\Application)
- Microsoft-Windows-Windows Defender%4Operational (C:\Cases\Windows\System32\winevt\logs\System)
- System (C:\Cases\Windows\System32\winevt\logs\System)
- Security (C:\Cases\Windows\System32\winevt\logs\Security)

Task templates

2147 481 ✓ 1 UTC

Type Date Time Event Source Category User Computer

Audit Success	2/13/2023	5:09:48 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:09:48 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10

2/ Filter

Apply filter to:  Active event log view (File: C:\Cases\Windows\System32\winevt\logs\Security.evtx)  Event log view(s) on your choice

Source:  ...  Exclude

Category:  ...  Exclude

User:  ...  Exclude

Computer:  ...  Exclude

Description

An account was successfully logged on.

Event ID(s):

Subject:

- Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000
- Account Name: MSEDGEWIN10\$
- Account Domain: WORKGROUP
- Logon ID: 0x3e7

Logon Information:

- Logon Type: 2
- Restricted Admin Mode: -
- Virtual Account: No
- Elevated Token: No

Impersonation Level: Impersonation

New Logon:

- Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000
- Account Name: MSEDGEWIN10\$
- Account Domain: WORKGROUP
- Logon ID: 0x21869
- Linked Logon ID: 0x2184c
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

- Process ID: 0x4d0
- Process Name: C:\Windows\System32\svchost.exe

Network Information:

- Workstation Name: MSEDGEWIN10
- Source Network Address: 127.0.0.1
- Source Port: 0

Detailed Authentication Information:

- Logon Process: User32
- Authentication Package: Negotiate
- Transsted Services: -
- Package Name (NTLM only): -

Description Data

OK Cancel

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search [ ]

Log Files

- Application (C:\Cases\Windows\System32\winevt\logs\Application)
- Microsoft-Windows-Windows Defender%4Operational (C:\Cases\Windows\System32\winevt\logs\System)
- System (C:\Cases\Windows\System32\winevt\logs\System)
- Security (C:\Cases\Windows\System32\winevt\logs\Security)

Task templates

2147 15 ✓ 1 UTC

Type Date Time Event Source Category User Computer

Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:09:51 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:09:51 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:05:04 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:05:04 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:03:25 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:03:25 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10
Audit Success	4/25/2018	4:00:22 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10
Audit Success	4/25/2018	4:00:16 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10
Audit Success	4/25/2018	3:59:36 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10
Audit Success	4/25/2018	3:59:09 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10

Description

An account was successfully logged on.

Subject:

- Security ID: S-1-5-18
- Account Name: MSEDGEWIN10\$
- Account Domain: WORKGROUP
- Logon ID: 0x3e7

Logon Information:

- Logon Type: 2
- Restricted Admin Mode: -
- Virtual Account: No
- Elevated Token: No

Impersonation Level: Impersonation

New Logon:

- Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000
- Account Name: MSEDGEWIN10\$
- Account Domain: WORKGROUP
- Logon ID: 0x21869
- Linked Logon ID: 0x2184c
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

- Process ID: 0x4d0
- Process Name: C:\Windows\System32\svchost.exe

Network Information:

- Workstation Name: MSEDGEWIN10
- Source Network Address: 127.0.0.1
- Source Port: 0

Detailed Authentication Information:

- Logon Process: User32
- Authentication Package: Negotiate
- Transsted Services: -
- Package Name (NTLM only): -

Description Data

Untitled.EKL - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search [ ]

WBN-90HAJ6CQHQM (local)

Log Files

- Application (C:\Cases\1\Windows\System32\winevt\Logs\Application)
- Microsoft-Windows-Defender%4Operational (C:\Cases\1\Windows\System32\winevt\Logs\Microsoft-Windows-Defender%4Operational)
- System (C:\Cases\1\Windows\System32\winevt\Logs\System)
- Security (C:\Cases\1\Windows\System32\winevt\Logs\Security)

Task templates

Application.evtx Microsoft-Windows-Defender%4Operational.evtx System.evtx Security.evtx

Type Date Time Event Source Category User Computer

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Login	N/A	MSEdgeV110	
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon	N/A	MSEdgeV110	
Audit Success	2/13/2023	5:09:51 PM	4624	Microsoft-Windows Logon	N/A	MSEdgeV110	
Audit Success	2/13/2023	5:09:51 PM	4624	Microsoft-Windows Logon	N/A	MSEdgeV110	
Audit Success	2/13/2023	5:05:04 PM	4624	Microsoft-Windows Logon	N/A	MSEdgeV110	
Audit Success	2/13/2023	5:05:04 PM	4624	Microsoft-Windows Logon	N/A	MSEdgeV110	
Audit Success	2/13/2023	5:03:35 PM	4624	Microsoft-Windows Logon	N/A	MSEdgeV110	
Audit Success	2/13/2023	5:03:35 PM	4624	Microsoft-Windows Logon	N/A	MSEdgeV110	
Audit Success	4/25/2018	4:00:22 PM	4624	Microsoft-Windows Logon	N/A	MSEdgeV110	
Audit Success	4/25/2018	4:00:16 PM	4624	Microsoft-Windows Logon	N/A	MSEdgeV110	
Audit Success	4/25/2018	3:59:36 PM	4624	Microsoft-Windows Logon	N/A	MSEdgeV110	
Audit Success	4/25/2018	3:59:09 PM	4624	Microsoft-Windows Logon	N/A	MSEdgeV110	

Description

An account was successfully logged on.

Subject:

- Security ID: S-1-5-18
- Account Name: MSEdgeV110\$
- Account Domain: WORKGROUP
- Logon ID: 0x3e?

Login Information:

- Logon Type: 2 ←
- Reference Admin Mode: No
- Virtual Account: No
- Elevated Token: No

Impersonation Level: Impersonation

New Logon:

- Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000
- Account Name: MSEdgeV110\$
- Account Domain: MSEdgeV110
- Logon ID: 0x21869
- Linked Logon ID: 0x2184c
- Network Account Name: MSEdgeV110
- Network Account Domain: MSEdgeV110
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

- Process ID: 0xd40
- Process Name: C:\Windows\System32\svchost.exe

Network Information:

- Connection Name: MSEdgeV110
- Source Network Address: 127.0.0.1
- Source Port: 0

Detailed Authentication Information:

- Logon Process: User32
- Authentication Package: Negotiate
- Transcript Services: -
- Package Name (NTLM only): -

Description Data

4:09 PM 2/16/2023

## Authentication

- When an Administrator is logging on , two access tokens are issued, one elevated that means high privilege and another that is not elevated and means low privilege. Logon ID being in relation with high or low privilege token.

The screenshot shows the Windows Event Log Explorer interface. The left pane displays the 'Objects tree' with several log files selected. The right pane shows a table of events with the following columns: Type, Date, Time, Event, Source, Category, User, and Computer. A specific event is highlighted in blue, corresponding to the logon ID 0x21869 mentioned in the text.

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:09:51 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:09:51 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:05:48 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:03:35 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:03:35 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	4/25/2018	4:00:22 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	4/25/2018	4:00:16 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	4/25/2018	3:59:36 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	
Audit Success	4/25/2018	3:59:09 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	

**Description:**  
An account was successfully logged on.  
**Subject:**  
Security ID: S-1-5-18  
Account Name: MSEDGEWIN10\$  
Account Domain: WORKGROUP  
Logon ID: 0x3e7  
**Logon Information:**  
Logon Type: 2  
Reference Admin Mode: No  
Virtual Account: No  
Elevated Token: No  
**Impersonation Level:** Impersonation  
**New Logon:**  
Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000  
Account Name: MSEDGEWIN10  
Logon ID: 0x21869  
Link Logon ID: 0x2189c  
Network Account Name: -  
Network Account Domain: -  
Logon GUID: {00000000-0000-0000-0000-000000000000}  
**Process Information:**  
Process ID: 0x4d0  
Process Name: C:\Windows\System32\svchost.exe  
**Network Information:**  
Workstation Name: MSEDGEWIN10  
Source Network Address: 127.0.0.1  
Source Port: 0  
**Detailed Authentication Information:**  
Logon Process: User32  
Authentication Package: Negotiate  
Transited Services: -  
Package Name (HTML only): -

- Search based on Logon ID in text description:

0x21869

The screenshot shows the Windows Event Log Explorer interface. The left pane displays the 'Objects tree' with several log files selected. The right pane shows a table of events with the following columns: Type, Date, Time, Event, Source, Category, User, and Computer. A specific event is highlighted in blue, corresponding to the logon ID 0x21869 mentioned in the text.

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	2/13/2023	5:56:58 PM	4647	Microsoft-Windows Logoff	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:21:01 PM	4797	Microsoft-Windows User Account Management	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:21:01 PM	4797	Microsoft-Windows User Account Management	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:21:01 PM	4797	Microsoft-Windows User Account Management	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:21:01 PM	4797	Microsoft-Windows User Account Management	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:21:01 PM	4797	Microsoft-Windows User Account Management	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:21:01 PM	4797	Microsoft-Windows User Account Management	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:21:01 PM	4797	Microsoft-Windows User Account Management	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:21:01 PM	4797	Microsoft-Windows User Account Management	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:21:01 PM	4797	Microsoft-Windows User Account Management	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:21:01 PM	4797	Microsoft-Windows User Account Management	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:21:01 PM	4797	Microsoft-Windows User Account Management	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:21:01 PM	4797	Microsoft-Windows User Account Management	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:21:01 PM	4797	Microsoft-Windows User Account Management	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:21:01 PM	4797	Microsoft-Windows User Account Management	N/A	MSEDGEWIN10	
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon	N/A	MSEDGEWIN10	

**Description:**  
An attempt was made to query the existence of a blank password for an account.  
**Subject:**  
Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000  
Account Name: IElUser  
Account Domain: MSEDGEWIN10  
Logon ID: 0x21869  
**Additional Information:**  
Caller Workstation: MSEDGEWIN10  
Target Account Name: DefaultAccount  
Target Account Domain: MSEDGEWIN10

- Go back to the previous search:

Untitled.EX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search [ ]

Log Files Application (C:\Cases\1\Windows\System32\winevt\Logs\Application) Microsoft-Windows-Defender%Operational (C:\Cases\1\Windows\System32\winevt\Logs\Microsoft-Windows-Defender%Operational) System (C:\Cases\1\Windows\System32\winevt\Logs\System) Security (C:\Cases\1\Windows\System32\winevt\Logs\Security) Task templates

Application.evtx Microsoft-Windows-Defender%Operational.evtx System.evtx Security.evtx

2147 15 ✓ 1 UTC

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:09:51 PM	4624	Microsoft-Windows Logon		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:09:51 PM	4624	Microsoft-Windows Logon		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:05:04 PM	4624	Microsoft-Windows Logon		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:05:04 PM	4624	Microsoft-Windows Logon		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:03:35 PM	4624	Microsoft-Windows Logon		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:03:35 PM	4624	Microsoft-Windows Logon		N/A	MSEDGEWIN10
Audit Success	4/25/2018	4:00:22 PM	4624	Microsoft-Windows Logon		N/A	MSEDGEWIN10
Audit Success	4/25/2018	4:00:16 PM	4624	Microsoft-Windows Logon		N/A	MSEDGEWIN10
Audit Success	4/25/2018	3:59:36 PM	4624	Microsoft-Windows Logon		N/A	MSEDGEWIN10
Audit Success	4/25/2018	3:59:09 PM	4624	Microsoft-Windows Logon		N/A	MSEDGEWIN10

Description

An account was successfully logged on.

Subject:

- Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000
- Account Name: IEdgeUser
- Account Domain: MSEDGEWIN10
- Logon ID: 0x2184c

Logon Information:

- Logon Type: 2
- Restrict Admin Mode: No
- Virtual Account: No
- Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:

- Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000
- Account Name: IEdgeUser
- Account Domain: MSEDGEWIN10
- Logon ID: 0x2184c
- Link Logon ID: 0x21869
- Network Account Name:
- Network Account Domain:
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

- Process ID: 0x4d0
- Process Name: C:\Windows\System32\svchost.exe

Network Information:

- Workstation Name: MSEDGEWIN10
- Source Network Address: 127.0.0.1
- Source Port: 0

Detailed Authentication Information:

- Logon Process: User32
- Authentication Package: Negotiate
- Transited Services: -
- Package Name (NTLM only): -

Description / Data

0x2184c

Untitled.EX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search [ ]

Log Files Application (C:\Cases\1\Windows\System32\winevt\Logs\Application) Microsoft-Windows-Defender%Operational (C:\Cases\1\Windows\System32\winevt\Logs\Microsoft-Windows-Defender%Operational) System (C:\Cases\1\Windows\System32\winevt\Logs\System) Security (C:\Cases\1\Windows\System32\winevt\Logs\Security) Task templates

Application.evtx Microsoft-Windows-Defender%Operational.evtx System.evtx Security.evtx

2147 12 ✓ 1 UTC

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	2/13/2023	5:28:16 PM	4732	Microsoft-Windows Security Group Management		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:28:16 PM	4724	Microsoft-Windows User Account Management		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:28:16 PM	4738	Microsoft-Windows User Account Management		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:28:16 PM	4798	Microsoft-Windows User Account Management		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:28:16 PM	4732	Microsoft-Windows Security Group Management		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:28:16 PM	4738	Microsoft-Windows User Account Management		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:28:16 PM	4722	Microsoft-Windows User Account Management		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:28:16 PM	4720	Microsoft-Windows User Account Management		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:28:16 PM	4728	Microsoft-Windows Security Group Management		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:11:34 PM	4672	Microsoft-Windows Special Logon		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon		N/A	MSEDGEWIN10
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon		N/A	MSEDGEWIN10

Description

A member was added to a security-enabled local group.

Subject:

- Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000
- Account Name: IEdgeUser
- Account Domain: MSEDGEWIN10
- Logon ID: 0x2184c

Member:

- Security ID: S-1-2-1-1058341133-2092417715-4019509128-1004
- Account Name: -

Group:

- Security ID: S-1-5-32-544
- Group Name: Administrators
- Group Domain: BuiltIn

Additional Information:

- Privileges: -

Description / Data

- Example of privileges needed in order to execute malicious activity .

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Load filter < Load filter >

Objects tree

Search [ ]

W:\H-90HAJ6CQHQM (local)

Log Files

- Application (C:\Cases\Windows\System32\winevt\logs\Application.evtx)
- Microsoft-Windows-Windows Defender%4Operational (C:\Cases\Windows\System32\winevt\logs\Microsoft-Windows-Defender%4Operational.evtx)
- System (C:\Cases\Windows\System32\winevt\logs\System.evtx)
- Security (C:\Cases\Windows\System32\winevt\logs\Security.evtx)

Task templates

2147 12 [ ] 1

UTC

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	2/13/2023	5:28:16 PM	4732	Microsoft-Windows Security Group Management	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:28:16 PM	4724	Microsoft-Windows User Account Management	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:28:16 PM	4738	Microsoft-Windows User Account Management	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:28:16 PM	4798	Microsoft-Windows User Account Management	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:28:16 PM	4732	Microsoft-Windows Security Group Management	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:28:16 PM	4724	Microsoft-Windows User Account Management	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:28:16 PM	4738	Microsoft-Windows User Account Management	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:28:16 PM	4728	Microsoft-Windows Security Group Management	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:11:34 PM	4672	Microsoft-Windows Special Logon	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon	N/A	MSEGEWIN10	

Description

Special privileges assigned to new logon.

Subject:

- Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000
- Account Name: IEUser
- Account Domain: MSEGEWIN10
- Logon ID: 0x2194

Privileges:

- SeSecurityPrivilege
- SeTakeOwnershipPrivilege
- SeLoadDriverPrivilege
- SeRestorePrivilege
- SeDebugPrivilege
- SeAuditPrivilege
- SeSystemEnvironmentPrivilege
- SeImpersonatePrivilege
- SeDelegateSessionUserImpersonatePrivilege

Data

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Load filter < Load filter >

Objects tree

Search [ ]

W:\H-90HAJ6CQHQM (local)

Log Files

- Application (C:\Cases\Windows\System32\winevt\logs\Application.evtx)
- Microsoft-Windows-Windows Defender%4Operational (C:\Cases\Windows\System32\winevt\logs\Microsoft-Windows-Defender%4Operational.evtx)
- System (C:\Cases\Windows\System32\winevt\logs\System.evtx)
- Security (C:\Cases\Windows\System32\winevt\logs\Security.evtx)

Task templates

2147 12 [ ] 1

UTC

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	2/13/2023	5:28:16 PM	4732	Microsoft-Windows Security Group Management	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:28:16 PM	4724	Microsoft-Windows User Account Management	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:28:16 PM	4738	Microsoft-Windows User Account Management	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:28:16 PM	4798	Microsoft-Windows User Account Management	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:28:16 PM	4732	Microsoft-Windows Security Group Management	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:28:16 PM	4724	Microsoft-Windows User Account Management	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:28:16 PM	4738	Microsoft-Windows User Account Management	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:28:16 PM	4728	Microsoft-Windows Security Group Management	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:28:16 PM	4720	Microsoft-Windows User Account Management	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:11:34 PM	4672	Microsoft-Windows Special Logon	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon	N/A	MSEGEWIN10	
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon	N/A	MSEGEWIN10	

Description

A user account was created.

Subject:

- Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000
- Account Name: art-test
- Account Domain: MSEGEWIN10
- Logon ID: 0x2194

New Account

- Security ID: S-1-5-21-1058341133-2092417715-4019509128-1004
- Account Name: art-test
- Account Domain: MSEGEWIN10

Attributes:

- SAM Account Name: art-test
- Display Name: <value not set>
- User Principal Name: <value not set>
- Home Directory: <value not set>
- Script Path: <value not set>
- Profile Path: <value not set>
- User Workstation: <value not set>
- Password Last Set: <never>
- Account Expires: <never>
- Primary Group ID: 513
- Allowed To Delegate To: -
- Old UAC Value: 0x0
- New UAC Value: 0x15
- User Account Control:

  - Account Disabled
  - 'Password Not Required' - Enabled
  - 'Normal Account' - Enabled
  - User Parameters: <value not set>
  - SID History:
  - Logon Hours: -

Additional Information:

- Privileges: -

Data

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search [ ]

Log Files

- Application (C:\Cases\E\Windows\System32\winevt\logs\Application)
- Microsoft-Windows-Defender%4Operational (C:\Cases\E\Windows\System32\winevt\logs\Microsoft-Windows-Defender%4Operational)
- System (C:\Cases\E\Windows\System32\winevt\logs\System)
- Security (C:\Cases\E\Windows\System32\winevt\logs\Security)

Task templates

Application.evtx Microsoft-Windows-Defender%4Operational.evtx System.evtx Security.evtx

2147 12 1 UTC

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	2/13/2023	5:28:16 PM	4732	Microsoft-Windows Security Group Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:28:16 PM	4724	Microsoft-Windows User Account Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:28:16 PM	4738	Microsoft-Windows User Account Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:28:16 PM	4798	Microsoft-Windows User Account Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:28:16 PM	4732	Microsoft-Windows Security Group Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:28:16 PM	4738	Microsoft-Windows User Account Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:28:16 PM	4722	Microsoft-Windows User Account Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:28:16 PM	4720	Microsoft-Windows User Account Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:28:16 PM	4728	Microsoft-Windows Security Group Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:11:34 PM	4672	Microsoft-Windows Special Logon	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon	N/A	MSEdgeWIN10	

Description

A user account was enabled.

Subject:

- Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000
- Account Name: IEUser
- Account Domain: MSEdgeWIN10
- Logon ID: 0x2184

Target Account:

- Security ID: S-1-5-21-1058341133-2092417715-4019509128-1004
- Account Name: art-test
- Account Domain: MSEdgeWIN10

Description

A member was added to a security-enabled local group.

Subject:

- Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000
- Account Name: IEUser
- Account Domain: MSEdgeWIN10
- Logon ID: 0x2184

Member:

- Security ID: S-1-5-32-545
- Account Name: Users

Group:

- Security ID: S-1-5-32-545
- Group Name: Users
- Group Domain: Builtin

Additional Information:

- Privileges: -

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search [ ]

Log Files

- Application (C:\Cases\E\Windows\System32\winevt\logs\Application)
- Microsoft-Windows-Defender%4Operational (C:\Cases\E\Windows\System32\winevt\logs\Microsoft-Windows-Defender%4Operational)
- System (C:\Cases\E\Windows\System32\winevt\logs\System)
- Security (C:\Cases\E\Windows\System32\winevt\logs\Security)

Task templates

Application.evtx Microsoft-Windows-Defender%4Operational.evtx System.evtx Security.evtx

2147 12 1 UTC

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	2/13/2023	5:28:16 PM	4732	Microsoft-Windows Security Group Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:28:16 PM	4724	Microsoft-Windows User Account Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:28:16 PM	4738	Microsoft-Windows User Account Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:28:16 PM	4798	Microsoft-Windows User Account Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:28:16 PM	4732	Microsoft-Windows Security Group Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:28:16 PM	4738	Microsoft-Windows User Account Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:28:16 PM	4722	Microsoft-Windows User Account Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:28:16 PM	4720	Microsoft-Windows User Account Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:28:16 PM	4728	Microsoft-Windows Security Group Management	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:11:34 PM	4672	Microsoft-Windows Special Logon	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon	N/A	MSEdgeWIN10	
Audit Success	2/13/2023	5:11:34 PM	4624	Microsoft-Windows Logon	N/A	MSEdgeWIN10	

Description

A member was added to a security-enabled local group.

Subject:

- Security ID: S-1-5-21-1058341133-2092417715-4019509128-1000
- Account Name: IEUser
- Account Domain: MSEdgeWIN10
- Logon ID: 0x2184

Member:

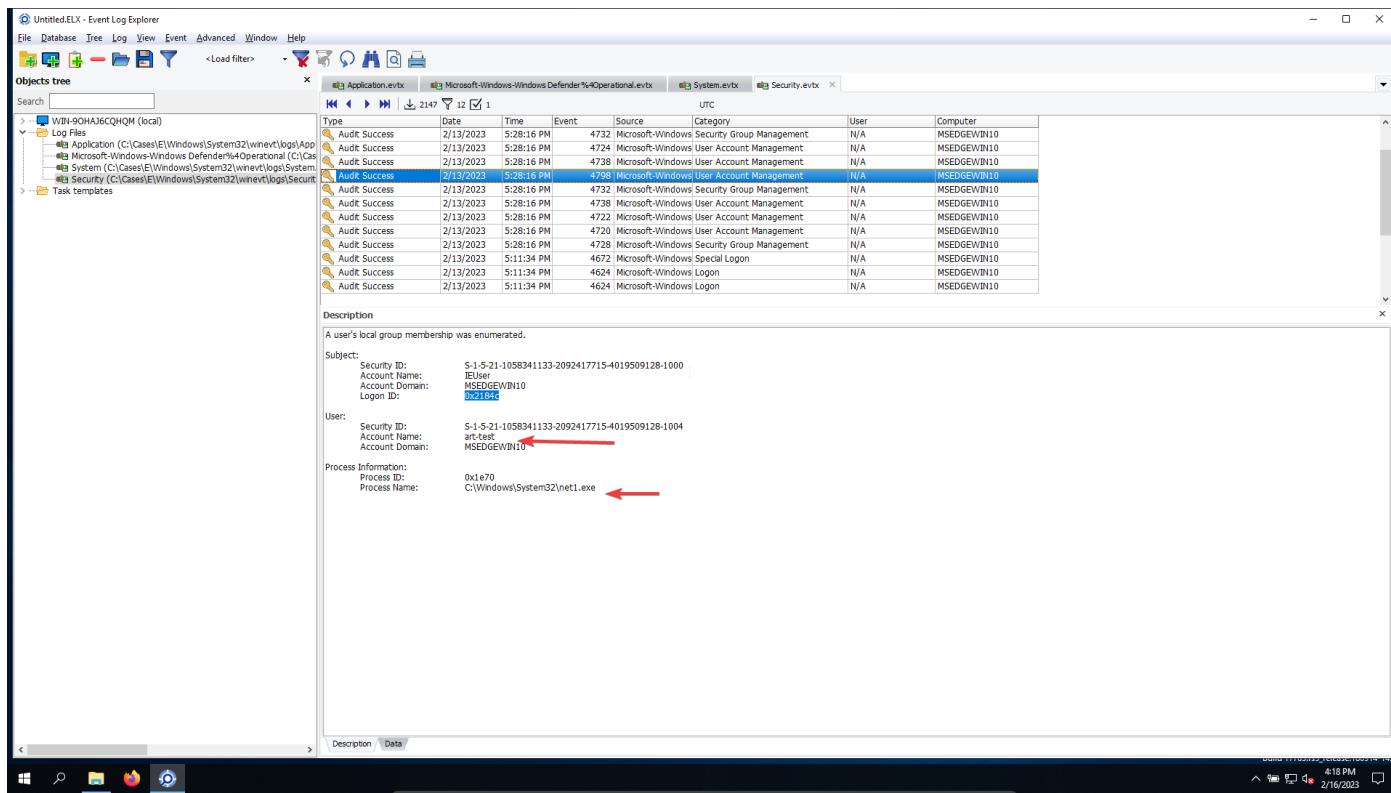
- Security ID: S-1-5-32-545
- Account Name: Users

Group:

- Security ID: S-1-5-32-545
- Group Name: Users
- Group Domain: Builtin

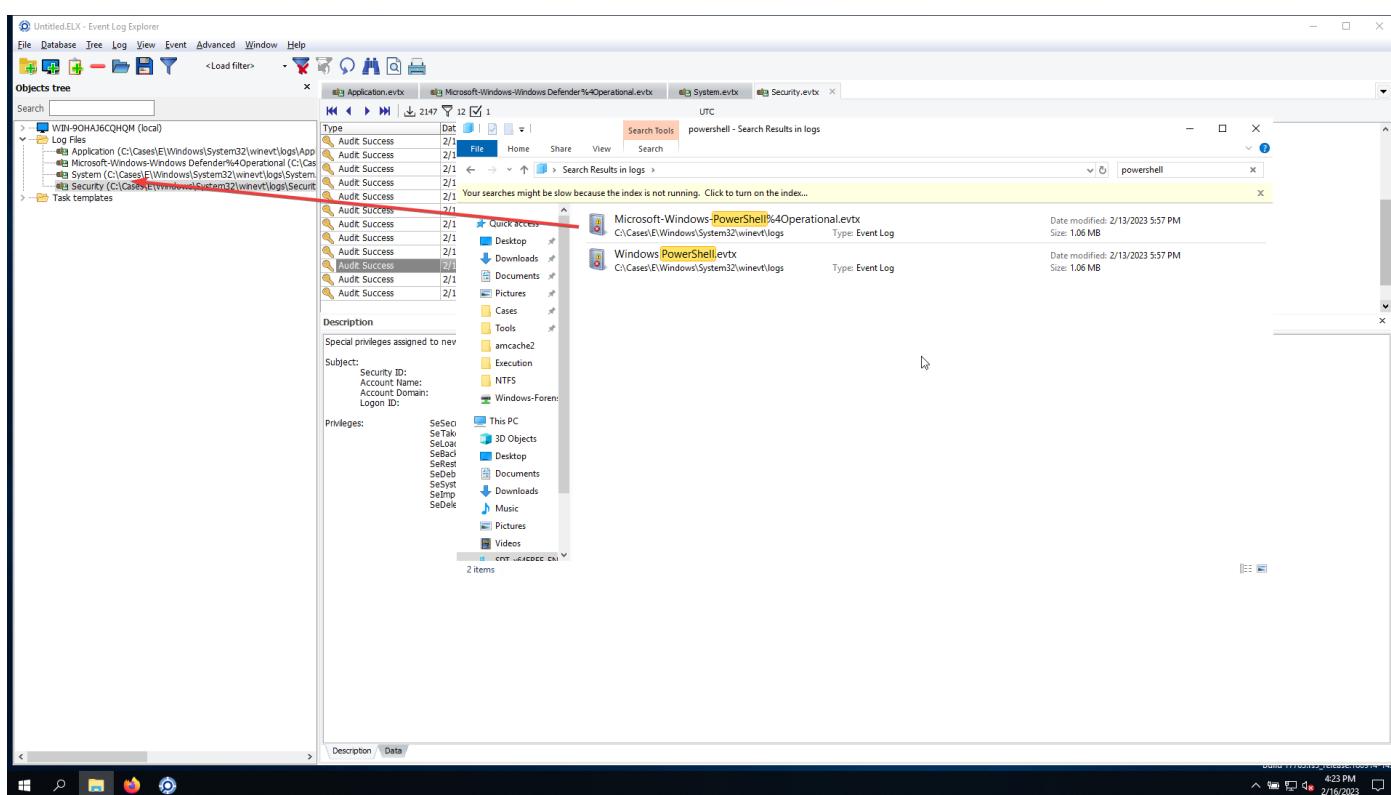
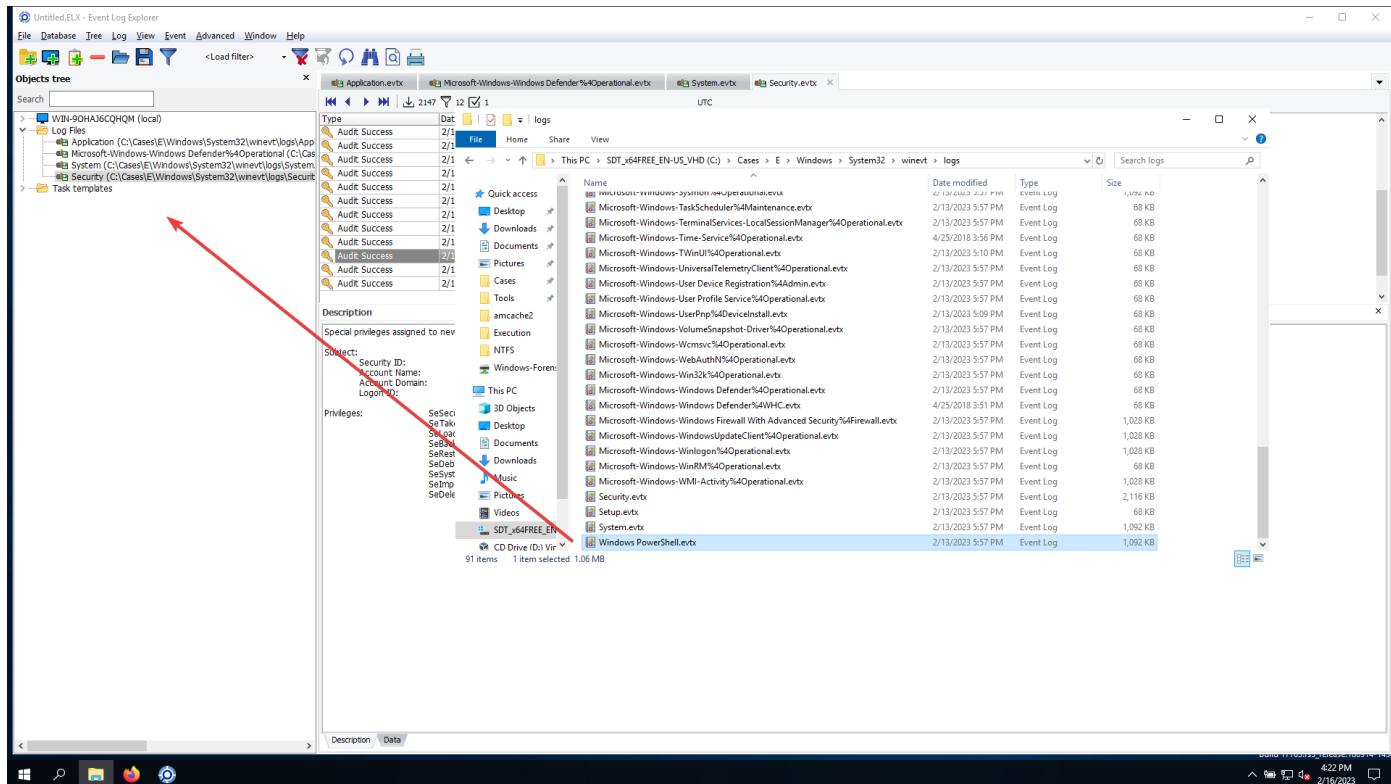
Additional Information:

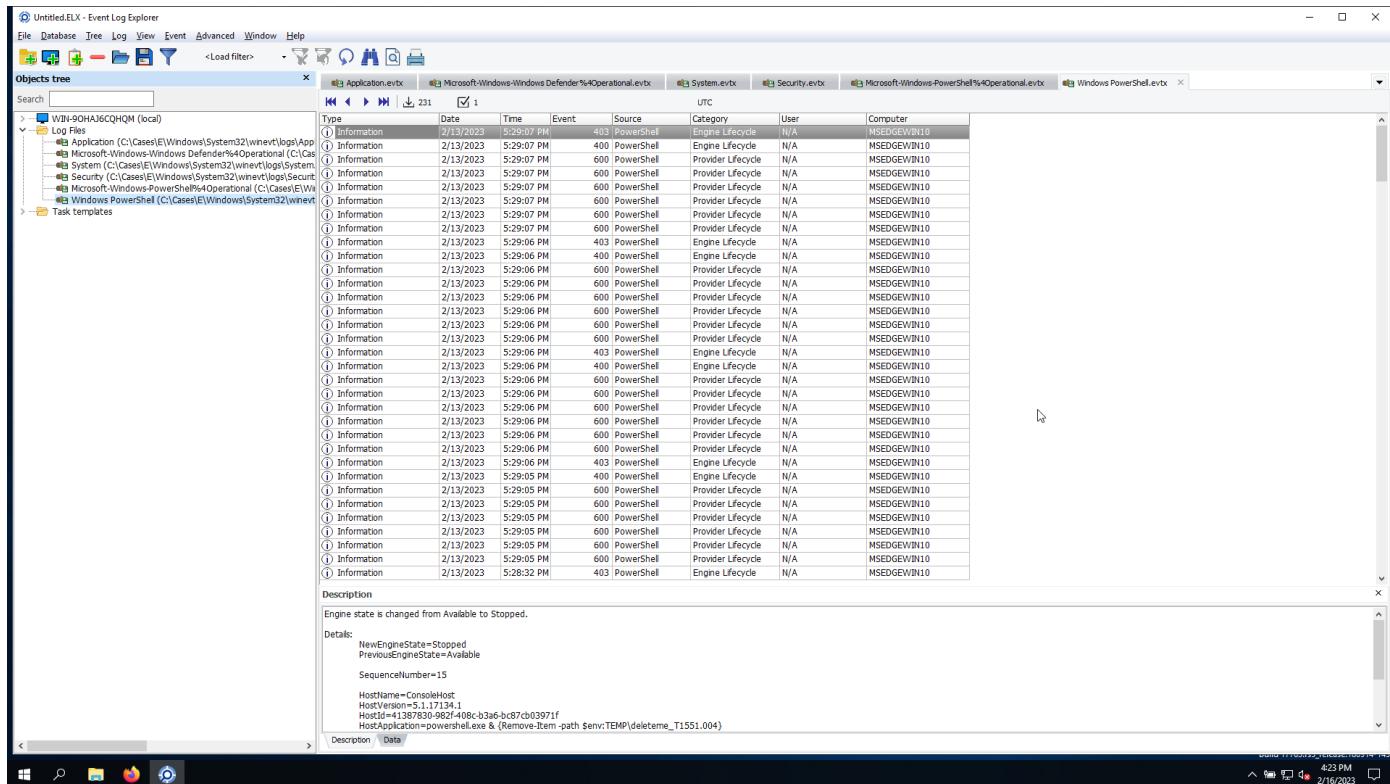
- Privileges: -



# Powershell

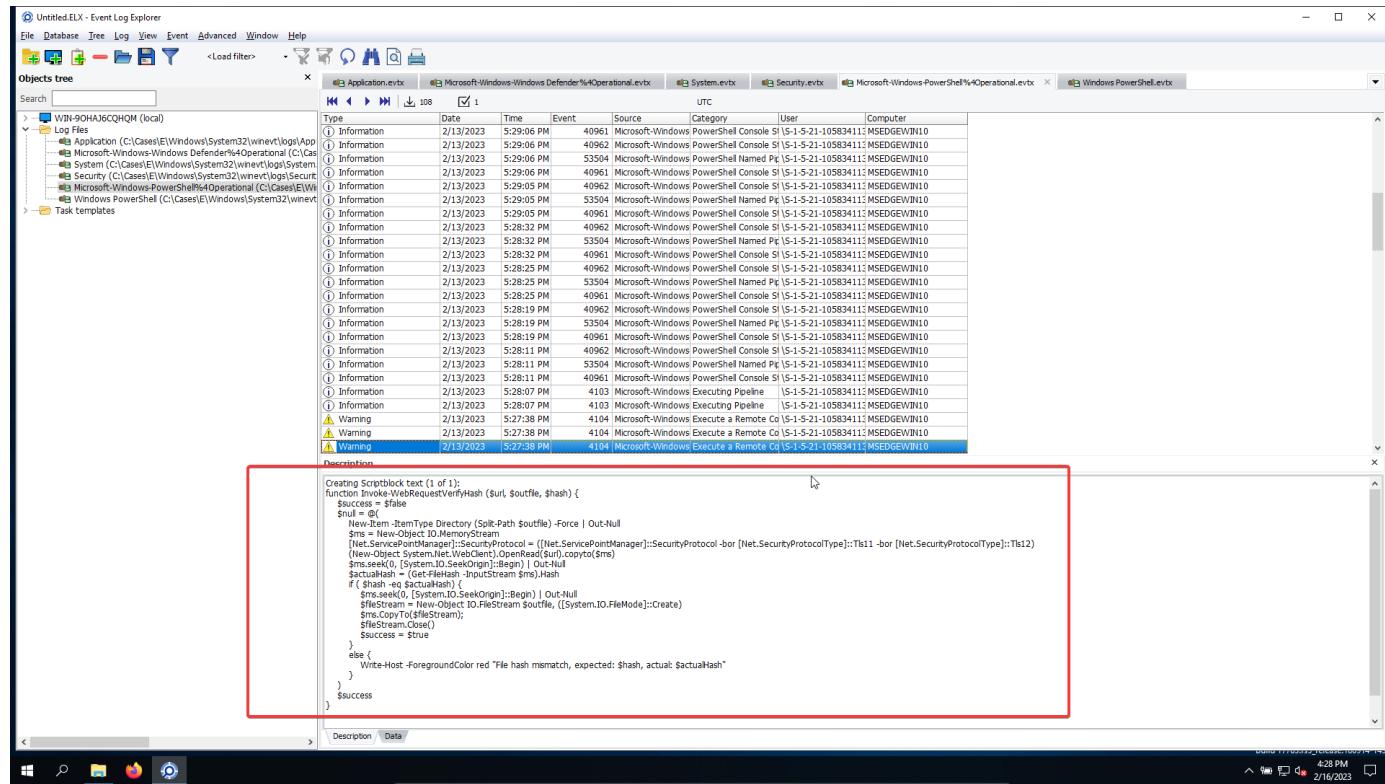
- Event IDs for Windows PowerShell:
    - 400: Engine state is changed from None to Available.
  - Load Windows PowerShell:



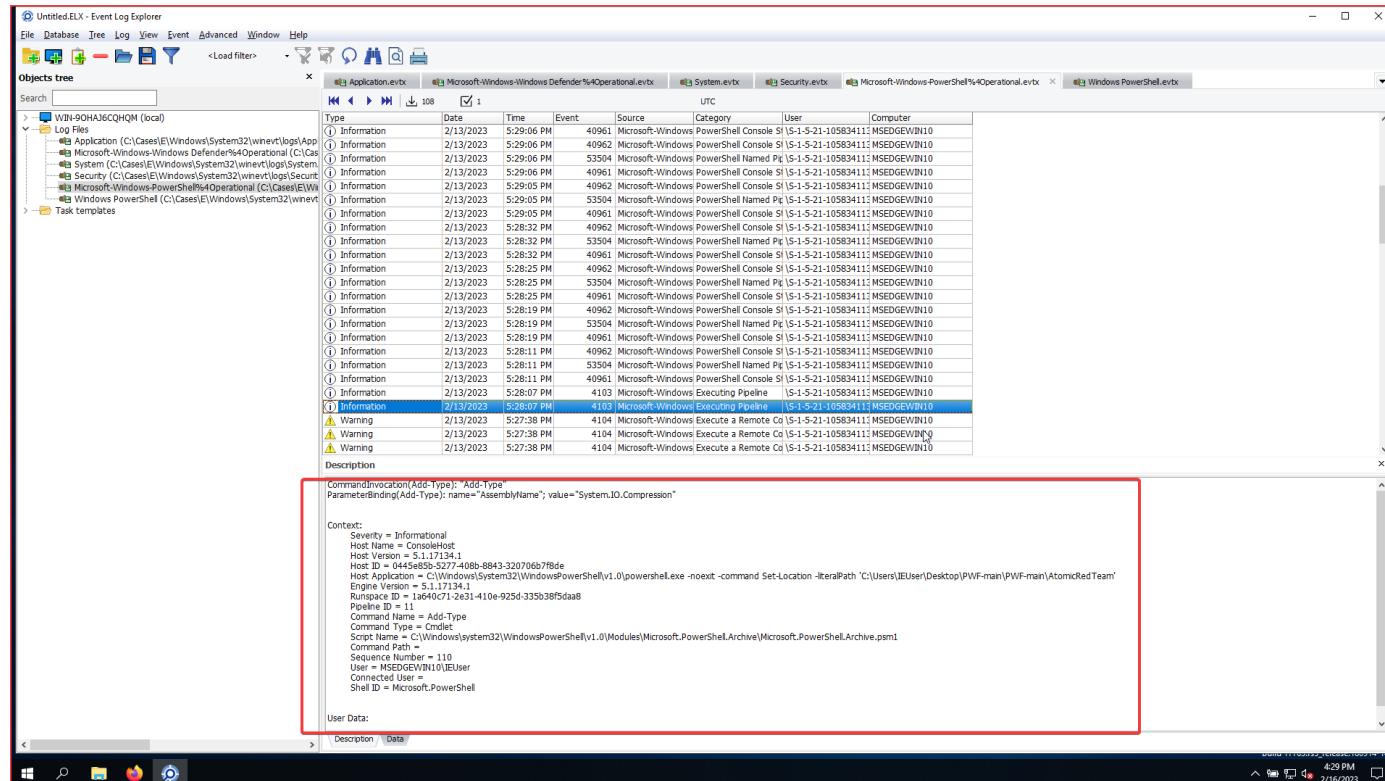


- You can see a lot of information in Windows Powershell , for example , powershell command executed, sequence number grows until 403, included. The Event goes 400,600 and ends with 403.

- In Windows Powershell Operational you can see code being executed:



- Important Event ids 4103,4104 for execution analysis, you can gather payloads, commands executed, modules called.



# Malicious Powershell

- Search in Windows PowerShell.evtx, by filtering with Event ID 400:

**Screenshot 1 (Top): Untitled.ELX - Event Log Explorer showing Windows PowerShell.evtx logs from 2/13/2023.**

The screenshot shows the Event Log Explorer interface with the Windows PowerShell.evtx log selected. The log contains numerous event entries with Event ID 400, all categorized as "Engine Lifecycle". The details pane shows the following information for one event:

```

Details:
NewEngineState=Stopped
PreviousEngineState=Available
SequenceNumber=15
Hostname=ConsolHost
HostVersion=5.1.17134.1
HostId=41387830-982f-408c-b3a6-bc87cb03971f
HostApplication=powershell.exe & (Remove-Item -path $env:TEMP\deleteme_T1551.004)
Engines=1
RunspaceId=4fc0cd02-4d57-40b1-8659-23c80f907f0
Pipelined=
CommandName=
 CommandType=
 ScriptName=
 CommandPath=
 CommandLine=

```

**Screenshot 2 (Bottom): Untitled.ELX - Event Log Explorer showing Windows PowerShell.evtx logs from 4/25/2018.**

The screenshot shows the Event Log Explorer interface with the Windows PowerShell.evtx log selected. The log contains numerous event entries with Event ID 400, all categorized as "Engine Lifecycle". The details pane shows the following information for one event:

```

Details:
NewEngineState=Available
PreviousEngineState=None
SequenceNumber=13
Hostname=ConsolHost
HostVersion=5.1.17134.1
HostId=0445e85b-5277-408b-8843-320706b7f8de
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noexit -Command Set-Location -LiteralPath 'C:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam'
Engines=1
RunspaceId=1640c71-2a31-410e-925d-335b38f5da8
Pipelined=
CommandName=
 CommandType=
 ScriptName=
 CommandPath=
 CommandLine=

```

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Load filter

Objects tree

Search [ ]

Log Files Application (C:\Cases\Windows\System32\winevt\Logs\App) Microsoft-Windows-Defender%Operational (C:\Cases\Windows\System32\winevt\Logs\Defender%Operational) System (C:\Cases\Windows\System32\winevt\Logs\System) Security (C:\Cases\Windows\System32\winevt\Logs\Security) Microsoft-Windows-PowerShell%Operational (C:\Cases\Windows\System32\winevt\Logs\PowerShell) Windows PowerShell (C:\Cases\Windows\System32\winevt\Logs\PowerShell)

Task templates

231 27 0 UTC

Type	Date	Time	Event	Source	Category	User	Computer
Information	2/13/2023	5:29:06 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:29:05 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:28:32 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:28:25 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:28:19 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:28:11 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:27:38 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:27:24 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:27:01 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:26:57 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:26:57 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:26:23 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:25:02 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:22:47 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	4/25/2018	4:00:30 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	4/25/2018	4:00:28 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	4/25/2018	4:00:23 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	4/25/2018	4:00:18 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	4/25/2018	3:59:57 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	4/25/2018	3:59:12 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	4/25/2018	3:59:01 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	4/25/2018	3:56:26 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	4/25/2018	3:56:05 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	4/25/2018	3:48:36 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	4/25/2018	3:48:30 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10

Description

Engine state is changed from None to Available.

Details:

```

NewEngineState=Available
PreviousEngineState=None
SequenceNumber=13
HostName=CompuHost
HostVersion=5.1.17134.1
HostId=2e0f04d4-695d-4f15-a1d2-9468d51cad29
HostApplication=powershell.exe & {Url = "https://github.com/edcanaryco/atomic-red-team/raw/master/atomics/T1566.001/bin/PhishingAttachment.xlm"
[Net.ServicePointManager].SecurityProtocol = [Net.SecurityProtocolType]::Tls12
Invoke-WebRequest -Uri $url -Method Post -Body $body -ContentType "application/x-ms-tnefmessage" -SessionVariable $env:TEMP\PhishingAttachment.xlm"
}
Invoke-WebRequest -Uri $url -Method Post -Body $body -ContentType "application/x-ms-tnefmessage" -SessionVariable $env:TEMP\PhishingAttachment.xlm"
}
EngineVersion=5.1.17134.1
RunspaceId=a5db5ea4-1105-4537-8070-eb405af2f257
PipelineCount=0
CommandName=
CommandType=
ScriptName=
CommandPath=
CommandLine=

```

Description Data

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Load filter

Objects tree

Search [ ]

Log Files Application (C:\Cases\Windows\System32\winevt\Logs\App) Microsoft-Windows-Defender%Operational (C:\Cases\Windows\System32\winevt\Logs\Defender%Operational) System (C:\Cases\Windows\System32\winevt\Logs\System) Security (C:\Cases\Windows\System32\winevt\Logs\Security) Microsoft-Windows-PowerShell%Operational (C:\Cases\Windows\System32\winevt\Logs\PowerShell) Windows PowerShell (C:\Cases\Windows\System32\winevt\Logs\PowerShell)

Task templates

231 16 0 UTC

Type	Date	Time	Event	Source	Category	User	Computer
Information	2/13/2023	5:29:07 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:29:06 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:29:05 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:28:32 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:28:25 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:28:19 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:28:11 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:27:38 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:27:24 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:27:01 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:26:57 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:26:57 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:26:23 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:25:02 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
Information	2/13/2023	5:22:47 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10

Description

Engine state is changed from None to Available.

Details:

```

NewEngineState=Available
PreviousEngineState=None
SequenceNumber=13
HostName=Windows PowerShell ISE Host
HostVersion=5.1.17134.1
HostId=2e0f04d4-695d-4f15-a1d2-9468d51cad29
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe C:\Users\IEUser\Desktop\PWF-main\PWF-main\Install-Sysmon.ps1
EngineVersion=5.1.17134.1
RunspaceId=beb8c83c-0f3c-4c16-a7d7-00a0177a344e
PipelineCount=0
CommandName=
CommandType=
ScriptName=
CommandPath=
CommandLine=

```

Description Data

- Execution:
  - o Executing powershell from the Sysmon folder:

The screenshot shows the Windows Event Log Explorer interface. The left pane displays a tree view of log files, with the 'Windows PowerShell' log file selected. The right pane shows a table of events with columns: Type, Date, Time, Event, Source, Category, User, and Computer. A specific event is highlighted in blue, and its details are shown in a red-bordered box below:

```

Description
Engine state is changed from None to Available.

Details:
NewEngineState=Available
PreviousEngineState=None
SequenceNumber=13

HostName=Windows PowerShell ISE Host
HostVersion=5.1.17134.1
HostId=d9949790-a065-4eb8-bf8f-c04929abf311
HostApplication=d:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe C:\Users\IEUser\Desktop\PWF-man\Install-Sysmon.ps1
EngineVersion=5.1.17134.1
RunspaceId=beb8c85c-0fc3-4c16-a7d7-00a0177a344e
PipelineId=
CommandName=
 CommandType=
 ScriptName=
 CommandPath=
 CommandLine=

```

- Executing powershell from the AtomicRedTeam folder:

The screenshot shows the Windows Event Log Explorer interface. The left pane displays a tree view of log files, with the 'Windows PowerShell' log file selected. The right pane shows a table of events with columns: Type, Date, Time, Event, Source, Category, User, and Computer. A specific event is highlighted in blue, and its details are shown in a red-bordered box below:

```

Description
Engine state is changed from None to Available.

Details:
NewEngineState=Available
PreviousEngineState=None
SequenceNumber=13

HostName=ConsoleHost
HostVersion=5.1.17134.1
HostId=d9949790-a065-4eb8-bf8f-c04929abf311
HostApplication=d:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noexit -command Set-Location -literalPath 'C:\Users\IEUser\Desktop\PWF-man\Install-Sysmon'
EngineVersion=5.1.17134.1
RunspaceId=674b5d07-8e27-4bfa-645e-f556576d
PipelineId=
CommandName=
 CommandType=
 ScriptName=
 CommandPath=
 CommandLine=

```

- Downloading suspicious file from github

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

<Load filter>

Objects tree

Search [ ]

WIN-POHAJ6CQHOM (local)

Log Files

- Application (C:\Case\Windows\System32\win32k\Logs\Application)
- Microsoft-Windows-Defender%4Operational (C:\Case\Windows\System32\Logs\Microsoft-Windows-Defender%4Operational)
- System (C:\Case\Windows\System32\win32k\Logs\System)
- Security (C:\Case\Windows\System32\win32k\Logs\Security)
- Microsoft-Windows-PowerShell%4Operational (C:\Case\Windows\System32\Logs\Microsoft-Windows-PowerShell%4Operational)
- Windows PowerShell (C:\Case\Windows\System32\win32k\Logs\Windows PowerShell)

Task templates

UTC

Type	Date	Time	Event	Source	Category	User	Computer
(I) Information	2/13/2023	5:29:07 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEVIN10
(I) Information	2/13/2023	5:29:06 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEVIN10
(I) Information	2/13/2023	5:29:06 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEVIN10
(I) Information	2/13/2023	5:29:05 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEVIN10
(I) Information	2/13/2023	5:28:32 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEVIN10
(I) Information	2/13/2023	5:28:25 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEVIN10
(I) Information	2/13/2023	5:28:19 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEVIN10
(I) Information	2/13/2023	5:28:11 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEVIN10
(I) Information	2/13/2023	5:27:38 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEVIN10
(I) Information	2/13/2023	5:27:24 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEVIN10
(I) Information	2/13/2023	5:27:01 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEVIN10
(I) Information	2/13/2023	5:26:57 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEVIN10
(I) Information	2/13/2023	5:26:57 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEVIN10
(I) Information	2/13/2023	5:26:23 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEVIN10
(I) Information	2/13/2023	5:25:02 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEVIN10
(I) Information	2/13/2023	5:22:47 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEVIN10

Description

Engine state is changed from None to Available.

Details:

NewEngineState=Available  
PreviousEngineState=None  
SequenceNumber=13  
HostVersion=5.1.17134.1  
HostId=2e9d6040-034f-4f15-add2-9468d51cad29  
HostApplication=powershell.exe & ([url = "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1566.001/bin/PhishingAttachment.vbs"]  
[Net.ServicePointManager::];SecurityProtocol = [Net.SecurityProtocolType]::Tls12  
Invoke-WebRequest -Uri \$url -Method Post -Body \$content -SessionVariable \$env:TEMP\PhishingAttachment.xml)  
EngineVersion=5.1.17134.1  
RunspaceId=\$ad585ea4-1105-4537-8070-be405af2257  
PooledId=  
CommandName=  
CommandType=  
ScriptName=  
CommandPath=  
CommandLine=

Description Data

4:37 PM 2/16/2023

- Fileless attack payload. Registry is being modified .

The screenshot shows the Microsoft Event Explorer interface. The left pane displays the 'Objects tree' with a selected node 'Windows PowerShell (C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe)'. The main pane shows a table of events from the 'Application.evtx' log. One specific event is highlighted with a red box, which corresponds to the detailed view shown in the bottom right pane. This event is an 'Information' type event (ID 400) from 'PowerShell' at 2/13/2023 5:28:19 PM. The 'Description' field contains the following text:

Engine state is changed from None to Available.

Details:

```
NewEngineState=Available  
PreviousEngineState=None  
SequenceNumber=13  
HostName=ConsoleHost  
HostVersion=5.1.17134.1  
HostProcessId=47016  
HostProcessName=powershell.exe & (# Encoded payload in next command is the following "Set-Content -path "$env:SystemRoot\Temp\art-marker.txt" -value "Hello from the Atomic Red Team"")  
reg add "HKKEY_CURRENT_USER\Software\Classes\AtomicRedTeam" /v ART /t REG_SZ /d "U2V0LUVJbnBnQXBhdGgIRbN6YU3bzGVtUm9dc9UZWIwL2FyC1tYX/ZxJudHh0AtdmFsdVUgkIbGxvIGZybz20gdGhIEF0b21pYyBSZVQgVGvhbSI=" /f  
{Text.Encoding}={ASCII.GetString([Convert]::FromBase64String((gp $HKCU\Software\Classes\AtomicRedTeam).ART))}  
SequenceNumber=13  
RunspaceId={82c282e-90d4-4c2-99a0-816cac933d1  
PipelineId=0  
CommandName=  
CommandType=  
ScriptName=  
CommandPath=  
CommandLine=
```

- Going to Cyberchef and decrypting the payload executed by powershell through the registry:

U2V0LUNvbNlbnQgLBhdGggIIRlbnY6U3IzdGVtUm9vdC9UZW1wL2  
 FydC1tYXJrZXIudHh0liAtdmFsdWUgIkhlbGxvIGZyb20gdGhIEF0b21pY  
 yBSZWQgVGvhbSI=

The screenshot shows the CyberChef interface with a 'From Base64' operation selected. The input field contains a long string of characters, and the output field shows the decoded PowerShell command:

```
Set-Content -path "$env:SystemRoot\Temp\art-marker.txt" -value "Hello from the Atomic Red Team"
```

## ○ Persistence mechanism for startup folder

The screenshot shows the Event Log Explorer interface with a log entry selected. The event details pane shows the following information:

**Description**

```
Engine state is changed from None to Available.
Details:
  NewEngineState=Available
  PreviousEngineState=None
  SequenceNumber=13
  HostName=ConsoleHost
  HostVersion=5.1.17134.1
  HostId=7493982159444b9f-d897920018
  HostAppContainer= & (Copy-Item C:\AtomicRedTeam\atomic\T1547.001\rc\batstartup.bat "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\batstartup.bat"
  Copy-Item C:\AtomicRedTeam\atomic\T1547.001\src\batstartup.bat "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\batstartup.bat"
  Start-Process "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup\batstartup.bat"
  Start-Process "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup\batstartup.bat"
  EngineVersion=5.1.17134.1
  RunspaceId=91ca872d-ad3e-44fc-a579-c87a023604a7
  PipelineId=
  CommandName=
  CommandType=
  ScriptName=
  CommandPath=
  CommandLine=
```

## ○ Process Injection via mavinject.

The screenshot shows the Windows Event Log Explorer interface. The main pane displays a table of log entries from the Application.evtx log. One entry is selected, highlighted with a blue border. The details pane below shows the following event information:

**Description**

Engine state is changed from None to Available.

**Details:**

```

NewEngineState=Available
PreviousEngineState=None
SequenceNumber=13

HostName=ConsoleHost
HostVersion=5.1.17134.1
HostId=142e43f8-0e33-4a3d-a88c-a14af5b03661
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe & ($myid = ([start-Process notepad -PassThru].id
mvinject $myid ($ExecutionContext|Select-Team|atomic\$T1055.001) |sc|x64\$T1055.001.dl)
EngineVersion=5.1.17134.1
EngineVersion=5defeaac7-31cb-467c-894f-ed4e08bb0b2a
PipelineId=
CommandName=
 CommandType=
 ScriptName=
 CommandPath=
 CommandLine=

```

## ○ Testing if the file exists:

The screenshot shows the Windows Event Log Explorer interface. The main pane displays a table of log entries from the Application.evtx log. One entry is selected, highlighted with a blue border. The details pane below shows the following event information:

**Description**

Engine state is changed from None to Available.

**Details:**

```

NewEngineState=Available
PreviousEngineState=None
SequenceNumber=13

HostName=ConsoleHost
HostVersion=5.1.17134.1
HostId=R235845-5032-41a7-b671-351d00e9fb47
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe & {if (Test-Path $env:TEMP\deleteme_T1551.004) {exit 0} else {exit 1}}
EngineVersion=5.1.17134.1
EngineVersion=5050cb04-643b-42d4-bd9-f8c52230c8a
PipelineId=
CommandName=
 CommandType=
 ScriptName=
 CommandPath=
 CommandLine=

```

## ○ Creating the file

Untitled.EXL - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search [ ]

Log Files

- Application (C:\Cases\1\Windows\System32\winevt\logs\app)
- Microsoft-Windows-Defender%4Operational (C:\Cases\1\Windows\System32\winevt\logs\defop)
- System (C:\Cases\1\Windows\System32\winevt\logs\system)
- Security (C:\Cases\1\Windows\System32\winevt\logs\security)
- Microsoft-Windows-PowerShell%4Operational (C:\Cases\1\Windows\System32\winevt\logs\powershell)
- Windows PowerShell (C:\Cases\1\Windows\System32\winevt\logs\powershell)

Task templates

Application.evtx Microsoft-Windows-Defender%4Operational.evtx System.evtx Security.evtx Microsoft-Windows-PowerShell%4Operational.evtx Windows PowerShell.evtx

UTC

Type	Date	Time	Event	Source	Category	User	Computer
(i) Information	2/13/2023	5:29:07 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:29:06 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:29:06 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:29:05 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:28:32 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:28:25 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:28:19 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:28:11 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:27:38 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:27:24 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:27:01 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:26:57 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:26:57 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:26:23 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:25:02 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:22:47 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10

Description

```
Engine state is changed from None to Available.

Details:
NewEngineState=Available
PreviousEngineState=None
SequenceNumber=13
Hostname=Console0
HostVersion=5.1.17134.1
HostId=925c076-ead2-4ee-acdf-34483d22f7f
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe & {if (Test-Path $env:TEMP\deleteme_T1551.004) {rm $env:TEMP\deleteme_T1551.004} else {exit 1}}
EngineVersion=5.1.17134.1
RunspaceId=d473199-c3c2-40d8-8ec1-b90cd47614ae
PipelineId=
CommandName=
CommandType=
ScriptName=
CommandPath=
CommandLine=
```

Description Data

4:46 PM 2/16/2023

## ○ File check

Untitled.EXL - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search [ ]

Log Files

- Application (C:\Cases\1\Windows\System32\winevt\logs\app)
- Microsoft-Windows-Defender%4Operational (C:\Cases\1\Windows\System32\winevt\logs\defop)
- System (C:\Cases\1\Windows\System32\winevt\logs\system)
- Security (C:\Cases\1\Windows\System32\winevt\logs\security)
- Microsoft-Windows-PowerShell%4Operational (C:\Cases\1\Windows\System32\winevt\logs\powershell)
- Windows PowerShell (C:\Cases\1\Windows\System32\winevt\logs\powershell)

Task templates

Application.evtx Microsoft-Windows-Defender%4Operational.evtx System.evtx Security.evtx Microsoft-Windows-PowerShell%4Operational.evtx Windows PowerShell.evtx

UTC

Type	Date	Time	Event	Source	Category	User	Computer
(i) Information	2/13/2023	5:29:06 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:29:06 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:29:05 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:28:32 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:28:25 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:28:11 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:27:38 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:27:24 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:27:01 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:26:57 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:26:23 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:25:02 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10
(i) Information	2/13/2023	5:22:47 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEV\N10

Description

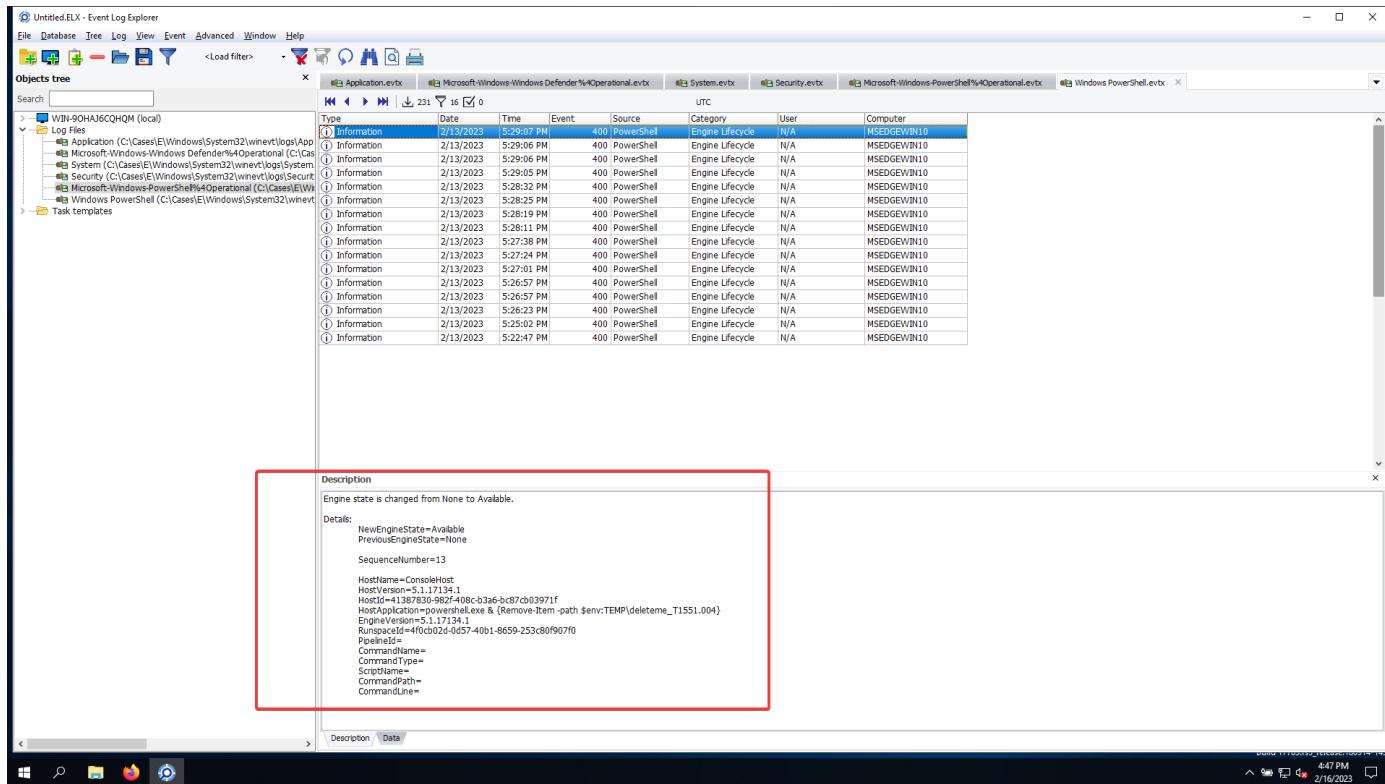
```
Engine state is changed from None to Available.

Details:
NewEngineState=Available
PreviousEngineState=None
SequenceNumber=13
Hostname=Console0
HostVersion=5.1.17134.1
HostId=925c076-ead2-4ee-acdf-34483d22f7f
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe & {if (Test-Path $env:TEMP\deleteme_T1551.004) {rm $env:TEMP\deleteme_T1551.004} else {exit 1}}
EngineVersion=5.1.17134.1
RunspaceId=d473199-c3c2-40d8-8ec1-b90cd47614ae
PipelineId=
CommandName=
CommandType=
ScriptName=
CommandPath=
CommandLine=
```

Description Data

4:47 PM 2/16/2023

## ○ Delete the file

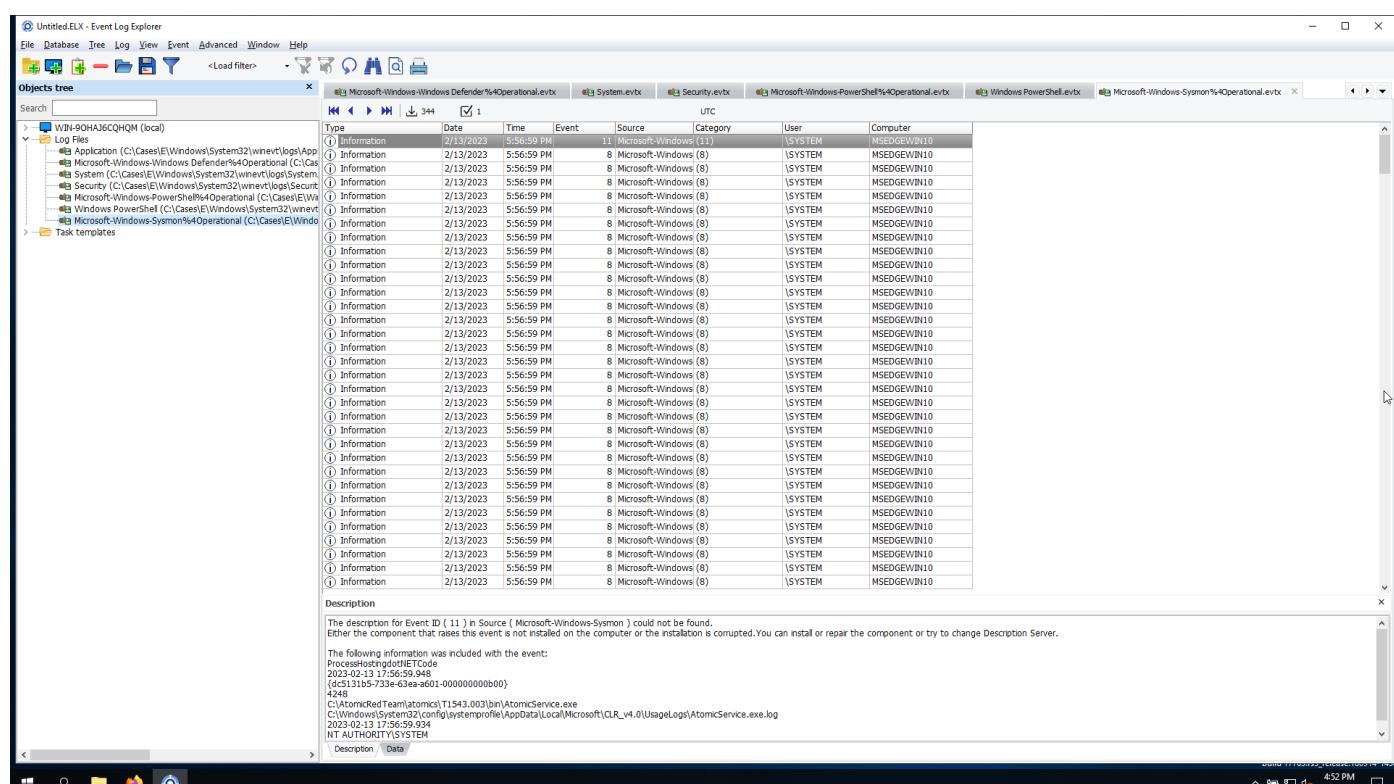
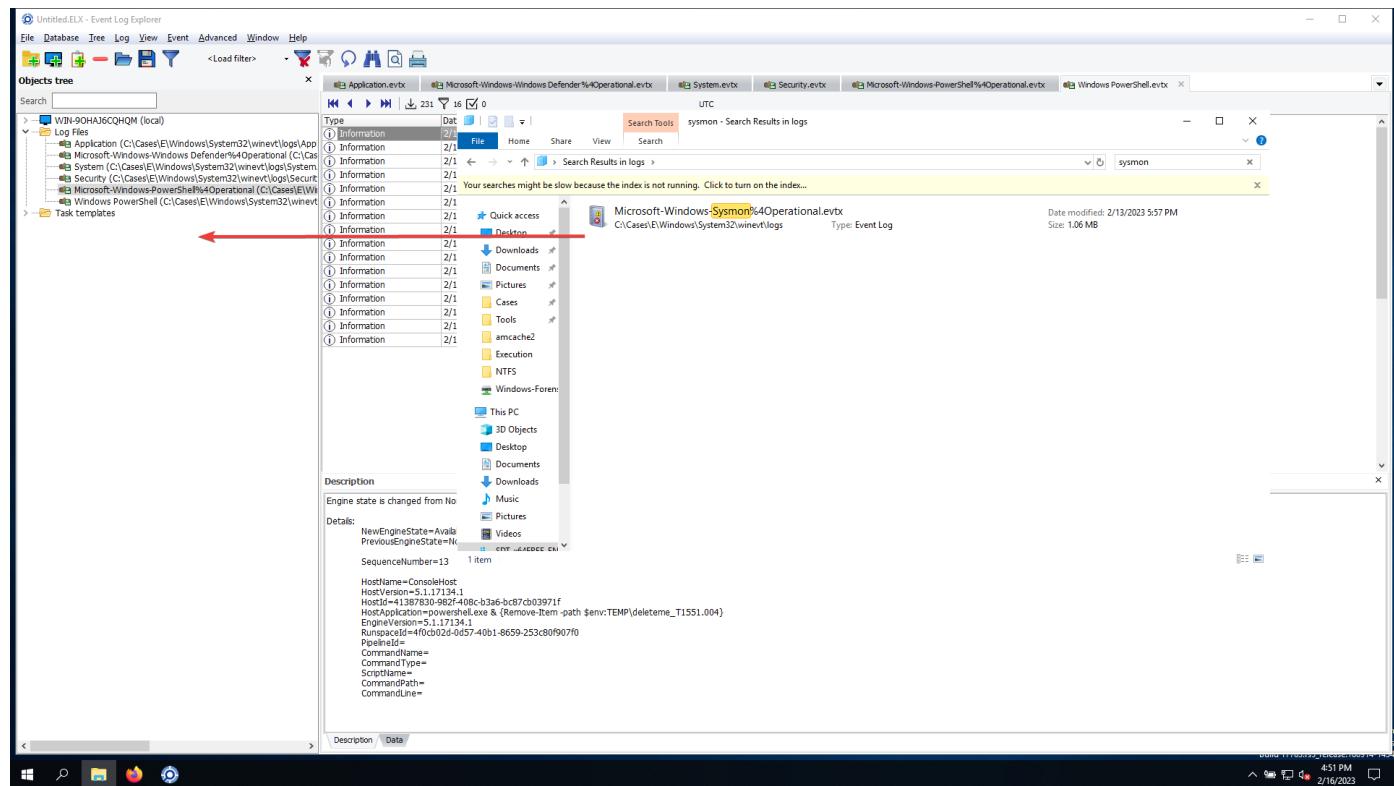


- Summary of deleteme file : If the file didn't existed, create it, if it existed, remove it.

## Sysmon & Malicious Sysmon

- Event IDs for Microsoft-Windows-Sysmon:
  - 1: Process creation
  - 3: Network creation
  - 11: File creation
  - 12,13: Registry events
  - 22: DNS query

- Load the Sysmon evtx:



Untitled.EXL - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Log Files

WBN-90HAJ6CQHQM (local)

Application (C:\Cases\1\Windows\System32\winevt\Logs\Appl...  
Microsoft-Windows-Defender%4Operational (C:\Cases\1\...  
System (C:\Cases\1\Windows\System32\winevt\Logs\System...  
Security (C:\Cases\1\Windows\System32\winevt\Logs\Secur...  
Microsoft-Windows-PowerShell%4Operational (C:\Cases\1\...  
Windows PowerShell (C:\Cases\1\Windows\System32\winevt\...  
Microsoft-Windows-Symon%4Operational (C:\Cases\1\Wind...  
Task templates

Search [ ] 344  1 UTC

Type	Date	Time	Event	Source	Category	User	Computer
(i) Information	2/13/2023	5:56:59 PM	8	Microsoft-Windows (8)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:56:58 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:56:58 PM	13	Microsoft-Windows (13)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:56:58 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:56:57 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:56:57 PM	22	Microsoft-Windows (22)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:56:53 PM	5	Microsoft-Windows (5)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:56:52 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:56:52 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:56:50 PM	22	Microsoft-Windows (22)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:56:49 PM	22	Microsoft-Windows (22)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:29:07 PM	11	Microsoft-Windows (11)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:29:06 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:29:06 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:29:06 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:29:06 PM	11	Microsoft-Windows (11)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:29:06 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:29:06 PM	11	Microsoft-Windows (11)	\SYSTEM	MSEDGEWIN10	
Description	The description for Event ID ( 1 ) in Source ( Microsoft-Windows-Symon ) 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:							
2023-02-13 17:56:52,351 {dc5131b5-79d4-63ea-a501-000000000000} 2536 C:\Windows\System32\LogonUI.exe 10.0.17134.1 (WinBuild.160101.0800) Windows User Interface Host Microsoft® Windows® Operating System Microsoft Corporation LogonUI.exe "LogonUI.exe" /flags0x0 /state0x0x3e8055 /state10.0.17134.0 C:\Windows\System32 NT AUTHORITY\SYSTEM {dc5131b5-79d4-63ea-a501-000000000000} 0x3e7 1 System MDS+3AD3281A9534FDD0A90D7E5BEE8B46,SHA256=536ABG6D36A44A42C4126380B470A5D20B789291585AE4EF94190C08C1C233,IMPHASH=B9B0B64B08B38276711093CA94348D39 {00000000-0000-0000-0000-000000000000} 540 - - -							
Description	Data						

process

user context

parent process

System

- Search mavinject process with eventid 1, process injection order of execution:

Untitled.EXL - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Log Files

WBN-90HAJ6CQHQM (local)

Application (C:\Cases\1\Windows\System32\winevt\Logs\Appl...  
Microsoft-Windows-Defender%4Operational (C:\Cases\1\...  
System (C:\Cases\1\Windows\System32\winevt\Logs\System...  
Security (C:\Cases\1\Windows\System32\winevt\Logs\Secur...  
Microsoft-Windows-PowerShell%4Operational (C:\Cases\1\...  
Windows PowerShell (C:\Cases\1\Windows\System32\winevt\...  
Microsoft-Windows-Symon%4Operational (C:\Cases\1\Wind...  
Task templates

Search [ ] 344  1 UTC

Type	Date	Time	Event	Source	Category	User	Computer
(i) Information	2/13/2023	5:28:32 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:28:32 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
(i) Information	2/13/2023	5:28:32 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	

Description

The description for Event ID ( 1 ) in Source ( Microsoft-Windows-Symon ) 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:

```

2023-02-13 17:28:32,361
{dc5131b5-7340-63ea-a901-000000000000}
3536
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
10.0.17134.1 (WinBuild.160101.0800)
Windows PowerShell
Microsoft® Windows® Operating System
Microsoft Corporation
PowerShell.exe
"powershell.exe" & ($cmdp = (Start-Process notepad -PassThru).Id
$cmdp | New-Item -InvertRunNn C:\AtomicRedTeam\atomics\T1055.001\src\x64\T1055.001.dll)
C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10\IEUser
{dc5131b5-5f4d-63ea-4c18-000000000000}
0x2194c
1
High
MDS+95000560239032BC68B4C2FDFFDE913,SHA256=D3F8FADEB29D2B7BD596C4504A6DAE5C034E789B6A3DEF8E013BDA7D14466677,IMPHASH=741776AACFC5B71FF59832DCDACE0F
{dc5131b5-72f8-63ea-6601-000000000000}
7080
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noexit -command Set-Location -IteralPath 'C:\Users\IEUser\Desktop\PWF-man\PWF-main\AtomicRedTeam'
MSEDGEWIN10\IEUser

```

Description Data

Untitled.EKL - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search [ ]

Log Files

- Application (C:\Cases\Windows\System32\winevt\logs\App)
- Microsoft-Windows-Defender%4Operational (C:\Cases\Windows\System32\winevt\logs\Defender)
- System (C:\Cases\Windows\System32\winevt\logs\System)
- Security (C:\Cases\Windows\System32\winevt\logs\Security)
- Windows PowerShell (C:\Cases\Windows\System32\winevt\PowerShell)
- Microsoft-Windows-Sysmon%4Operational (C:\Cases\Windows\System32\winevt\Logs\sysmon)

Task templates

Type Date Time Event Source Category User Computer

Information 2/13/2023 5:28:32 PM 1 Microsoft-Windows (1) \SYSTEM MSEdgeWIN10

Information 2/13/2023 5:28:32 PM 1 Microsoft-Windows (1) \SYSTEM MSEdgeWIN10

Information 2/13/2023 5:28:32 PM 1 Microsoft-Windows (1) \SYSTEM MSEdgeWIN10

Description

The description for Event ID ( 1 ) in Source ( Microsoft-Windows-Syman ) 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:

```

2023-02-13 17:28:32,647
{dc5131b5-7340-43ea-a010-000000000000}
3164
C:\Windows\System32\notepad.exe
10.0.17134.1 (VnBuild.160101.0800)
NotePad
Microsoft Windows® Operating System
Microsoft Corporation
NOTEPAD.EXE
"C:\Windows\system32\notepad.exe"
C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10\IEUser
{dc5131b5-d45b-63ea-4c18-020000000000}
0x2184c
1
High
MD5-BB9A068BF3DD9024C7F389D7B2B58D2,SHA256-899346F9F283A4FD5A03015A3F58CDE589C0B6A5C4D642CC74E9B22C1348D7,IMPHASH-Af8224EB74E94301B59B88492740A75
{dc5131b5-7340-43ea-a901-000000000000}
5356
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
"powershell.exe" & ($mynd = (Start-Process notepad -PassThru).Id
$aviedd $mynd /INJECTRUNNING C:\AtomicRedTeam\atomics\T1055.001\src\x64\T1055.001.dll)
MSEdgeWIN10\IEUser
0x2184c
1
High
MD5-9C001A0631D5E4010F4CB1CF1C9E592,SHA256-2028CCA5B2F0C81D1AD0C62503C8A51DA0304688802A05F07E260903D91D1748,IMPHASH-4AC1FF363262ABCE50D8C51CE1CEDA
{dc5131b5-7340-43ea-a901-000000000000}
5356
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
"powershell.exe" & ($mynd = (Start-Process notepad -PassThru).Id
$aviedd $mynd /INJECTRUNNING C:\AtomicRedTeam\atomics\T1055.001\src\x64\T1055.001.dll)
MSEdgeWIN10\IEUser

```

Untitled.EKL - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search [ ]

Log Files

- Application (C:\Cases\Windows\System32\winevt\logs\App)
- Microsoft-Windows-Defender%4Operational (C:\Cases\Windows\System32\winevt\logs\Defender)
- System (C:\Cases\Windows\System32\winevt\logs\System)
- Security (C:\Cases\Windows\System32\winevt\logs\Security)
- Windows PowerShell (C:\Cases\Windows\System32\winevt\PowerShell)
- Microsoft-Windows-Sysmon%4Operational (C:\Cases\Windows\System32\winevt\Logs\sysmon)

Task templates

Type Date Time Event Source Category User Computer

Information 2/13/2023 5:28:32 PM 1 Microsoft-Windows (1) \SYSTEM MSEdgeWIN10

Information 2/13/2023 5:28:32 PM 1 Microsoft-Windows (1) \SYSTEM MSEdgeWIN10

Information 2/13/2023 5:28:32 PM 1 Microsoft-Windows (1) \SYSTEM MSEdgeWIN10

Description

The description for Event ID ( 1 ) in Source ( Microsoft-Windows-Syman ) 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:

```

2023-02-13 17:28:32,660
{dc5131b5-7340-43ea-ac01-000000000000}
6032
C:\Windows\System32\javiewc.exe
10.0.17134.1 (VnBuild.160101.0800)
Microsoft Java Virtual Machine
Microsoft Java Virtualization Injector
Microsoft Windows® Operating System
Microsoft Corporation
javiewc64.exe
C:\Windows\System32\javiewc.exe" 3164 /INJECTRUNNING C:\AtomicRedTeam\atomics\T1055.001\src\x64\T1055.001.dll
C:\Users\IEUser\AppData\Local\Temp\MSEDGEWIN10\IEUser
{dc5131b5-d45b-63ea-4c18-020000000000}
0x2184c
1
High
MD5-9C001A0631D5E4010F4CB1CF1C9E592,SHA256-2028CCA5B2F0C81D1AD0C62503C8A51DA0304688802A05F07E260903D91D1748,IMPHASH-4AC1FF363262ABCE50D8C51CE1CEDA
{dc5131b5-7340-43ea-a901-000000000000}
5356
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
"powershell.exe" & ($mynd = (Start-Process notepad -PassThru).Id
$aviedd $mynd /INJECTRUNNING C:\AtomicRedTeam\atomics\T1055.001\src\x64\T1055.001.dll)
MSEdgeWIN10\IEUser

```

- Search everything based on parent process id: 7080, beggining of the attack:

Untitled.EKL - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search [ ]

Log Files

Type Date Time Event Source Category User Computer

Information 2/13/2023 5:26:54 PM 11 Microsoft-Windows (11) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:54 PM 11 Microsoft-Windows (11) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:54 PM 11 Microsoft-Windows (11) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:54 PM 11 Microsoft-Windows (11) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:54 PM 11 Microsoft-Windows (11) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:54 PM 11 Microsoft-Windows (11) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:49 PM 22 Microsoft-Windows (22) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:48 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:48 PM 22 Microsoft-Windows (22) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:49 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:47 PM 22 Microsoft-Windows (22) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:23 PM 11 Microsoft-Windows (11) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:23 PM 1 Microsoft-Windows (1) \SYSTEM MSEDGEWIN10

Description

The description for Event ID ( 1 ) in Source ( Microsoft-Windows-Syman ) 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:

2023-02-13 17:26:23.148  
(dc5131b5-72df-43ea-6601-000000000000)  
[0x0] C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  
1.0.17134.1 (WinBuild.160101.0800)  
Windows PowerShell  
Microsoft Windows® Operating System  
Microsoft Corporation  
PowerShell.exe  
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noexit -command Set-Location -LiteralPath 'C:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam'  
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  
MSEDGEWIN10\IEUser  
(dc5131b5-6f6-43ea-4c18-020000000000)  
0x2184C  
1  
High  
MD5=9500560239032BC68B4C2FDCDEF913,SHA256=D3F8FADEB290287B0596C4504A60AE5C04E78986A3DEFBE013BDA7D14466677,IMPHASH=741776AACFC5B71FF59832DCDACE0F  
(dc5131b5-647-43ea-5b00-000000000000)  
3356  
C:\Windows\explorer.exe  
C:\Windows\Explorer.EXE  
MSEDGEWIN10\IEUser

Untitled.EKL - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search [ ]

Log Files

Type Date Time Event Source Category User Computer

Information 2/13/2023 5:26:54 PM 11 Microsoft-Windows (11) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:54 PM 11 Microsoft-Windows (11) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:54 PM 11 Microsoft-Windows (11) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:54 PM 11 Microsoft-Windows (11) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:54 PM 11 Microsoft-Windows (11) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:54 PM 11 Microsoft-Windows (11) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:49 PM 22 Microsoft-Windows (22) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:49 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:49 PM 22 Microsoft-Windows (22) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:49 PM 3 Microsoft-Windows (3) \SYSTEM MSEDGEWIN10

Information 2/13/2023 5:26:23 PM 11 Microsoft-Windows (11) \SYSTEM MSEDGEWIN10

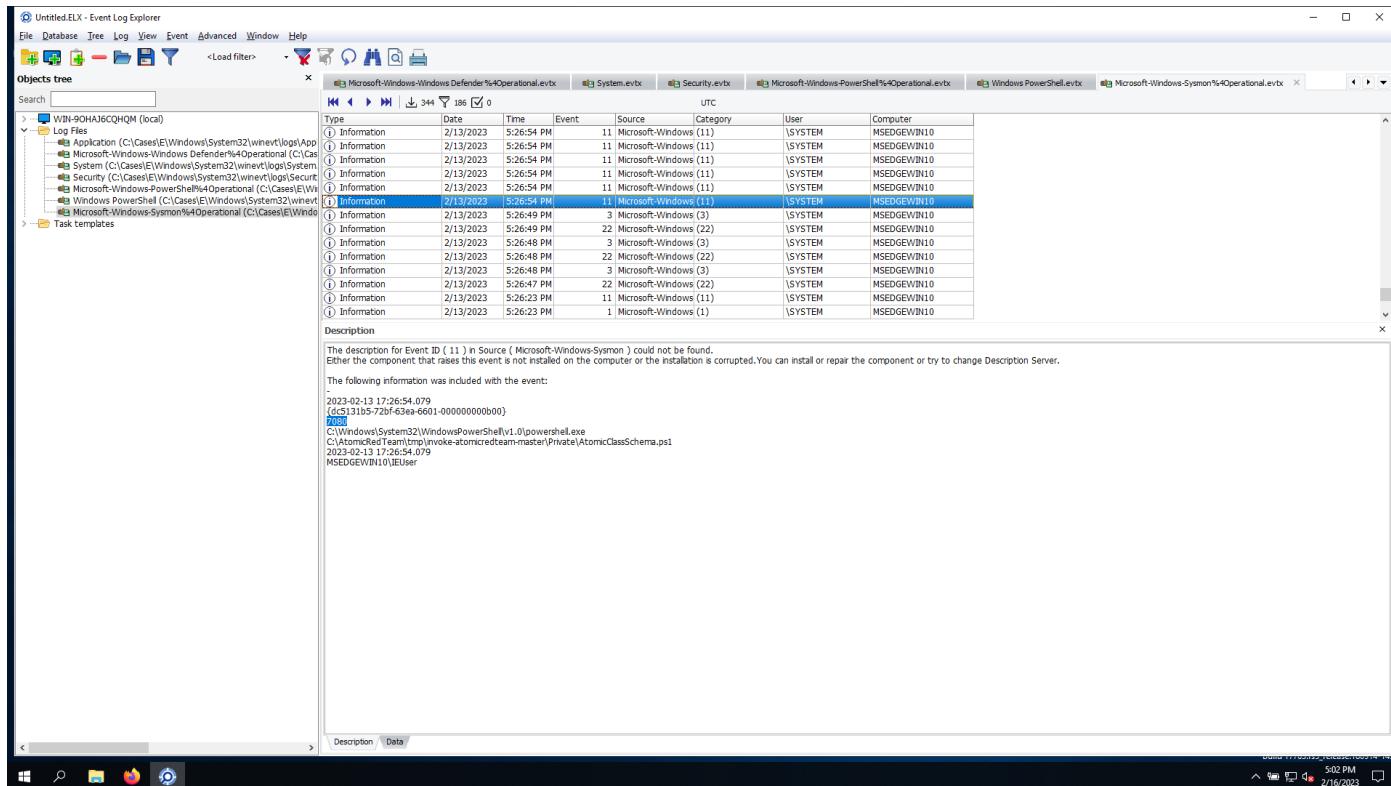
Information 2/13/2023 5:26:23 PM 1 Microsoft-Windows (1) \SYSTEM MSEDGEWIN10

Description

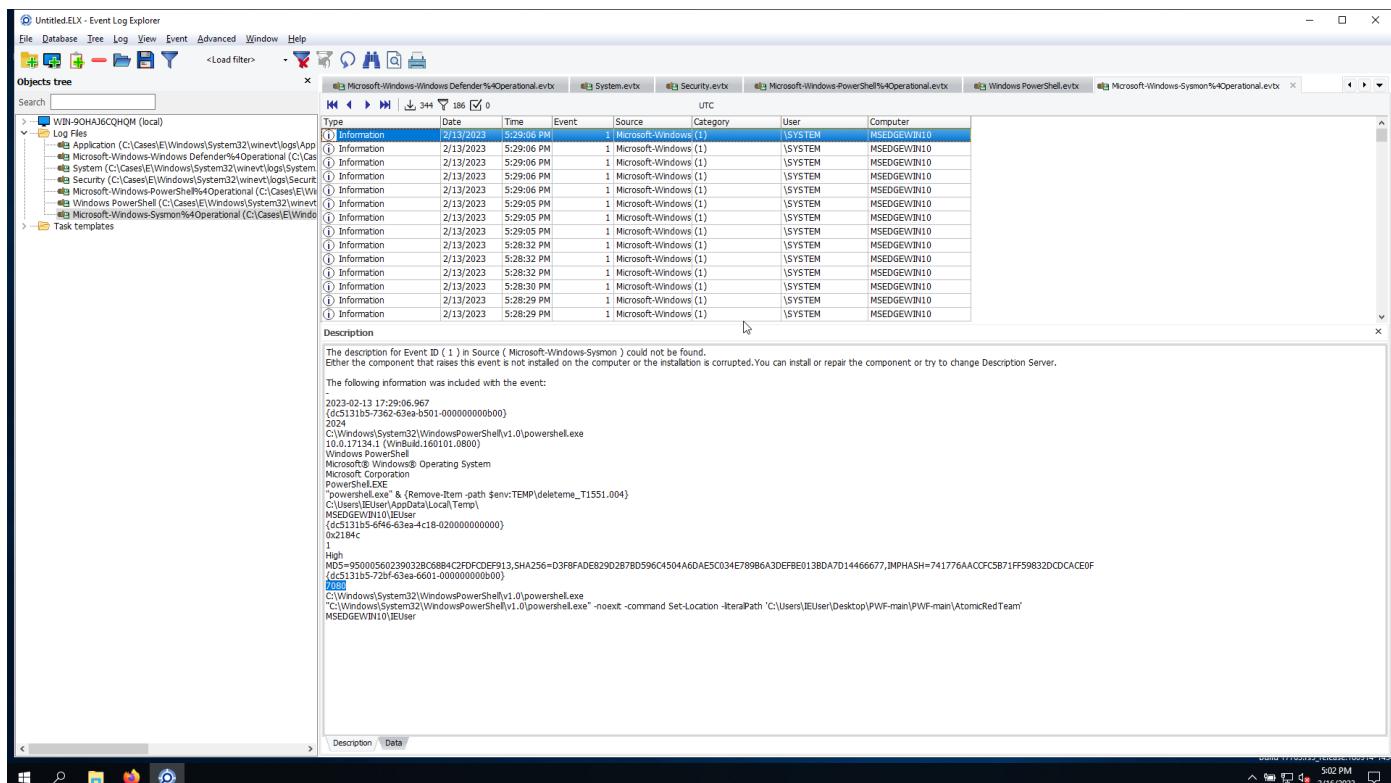
The description for Event ID ( 22 ) in Source ( Microsoft-Windows-Syman ) could not be found.  
Either the component that raises this event is not installed on the computer or the installation is corrupted. You can install or repair the component or try to change Description Server.

The following information was included with the event:

2023-02-13 17:26:37.598  
(dc5131b5-72df-43ea-6601-000000000000)  
[0x0] raw.githubusercontent.com  
0::ffff:185.199.109.132::ffff:185.199.110.133::ffff:185.199.108.133::ffff:185.199.111.133;  
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  
MSEDGEWIN10\IEUser



- End of the attack:



The screenshot shows the Unfiled.EXL Event Log Explorer application window. The left sidebar displays a tree view of log files, with 'WDB-90HAJ6CQHQ (local)' selected. The main pane shows a table of events from the 'Microsoft-Windows-Sytem%Operational.evtx' log. The table has columns for Type, Date, Time, Event, Source, Category, User, and Computer. Most events are of type 'Information' and occurred at 5:29:06 PM on 2/13/2023. The first event is highlighted in blue. A tooltip for this event states: 'The description for Event ID (1) in Source ( Microsoft-Windows-Sytem ) could not be found. Either the component that raises the 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.' Below the table, a detailed description of the event is provided, mentioning 'whoom.exe' and its connection to 'AtomicRedTeam'. The bottom status bar shows the date as 2/16/2022 and the time as 5:03 PM.

Type	Date	Time	Event	Source	Category	User	Computer
Information	2/13/2023	5:29:06 PM	1	Microsoft-Windows(1)	[SYSTEM]	MSEGEVW\N10	
Information	2/13/2023	5:29:06 PM	1	Microsoft-Windows(1)	[SYSTEM]	MSEGEVW\N10	
Information	2/13/2023	5:29:06 PM	1	Microsoft-Windows(1)	[SYSTEM]	MSEGEVW\N10	
Information	2/13/2023	5:29:06 PM	1	Microsoft-Windows(1)	[SYSTEM]	MSEGEVW\N10	
Information	2/13/2023	5:29:06 PM	1	Microsoft-Windows(1)	[SYSTEM]	MSEGEVW\N10	
Information	2/13/2023	5:29:06 PM	1	Microsoft-Windows(1)	[SYSTEM]	MSEGEVW\N10	
Information	2/13/2023	5:29:06 PM	1	Microsoft-Windows(1)	[SYSTEM]	MSEGEVW\N10	
Information	2/13/2023	5:29:06 PM	1	Microsoft-Windows(1)	[SYSTEM]	MSEGEVW\N10	
Information	2/13/2023	5:29:05 PM	1	Microsoft-Windows(1)	[SYSTEM]	MSEGEVW\N10	
Information	2/13/2023	5:28:32 PM	1	Microsoft-Windows(1)	[SYSTEM]	MSEGEVW\N10	
Information	2/13/2023	5:28:32 PM	1	Microsoft-Windows(1)	[SYSTEM]	MSEGEVW\N10	
Information	2/13/2023	5:28:32 PM	1	Microsoft-Windows(1)	[SYSTEM]	MSEGEVW\N10	
Information	2/13/2023	5:28:30 PM	1	Microsoft-Windows(1)	[SYSTEM]	MSEGEVW\N10	
Information	2/13/2023	5:28:29 PM	1	Microsoft-Windows(1)	[SYSTEM]	MSEGEVW\N10	
Information	2/13/2023	5:28:29 PM	1	Microsoft-Windows(1)	[SYSTEM]	MSEGEVW\N10	

Description

The description for Event ID (1) in Source ( Microsoft-Windows-Sytem ) could not be found. Either the component that raises the 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:

- 2023-02-13 17:29:06.662  
(c5131b5-7362-63ea-0401-000000000000)  
29  
C:\Windows\System32\whoom.exe  
10.0.17134.1 (WinBuild.160101.0800)  
Whoom - displays logged on user information  
Microsoft Windows® Operating System  
Microsoft Windows®  
whoom.exe  
"C:\Windows\system32\whoom.exe"  
C:\Windows\Desktop\{PWF-main}\PWF-main\AtomicRedTeam  
MSEGEVW\N10\IEUser  
(c5131b5-6f46-63ea-4c18-020000000000)  
0x2184c  
1  
High  
MD5=A1B8E1AD24DE09417CA7459F5C1701,SHA256=59D6065C2D02D1466F88AE087197F122C7D7EFF84A12C8D874C42F4EFEB5D,IMPHASH=7FF07588766F747CE57DFAC70743F888  
(c5131b5-72b6-63ea-6601-000000000000)  
7680  
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noexit -command Set-Location -literalPath 'C:\Users\IEUser\Desktop\{PWF-main}\PWF-main\AtomicRedTeam'  
MSEGEVW\N10\IEUser

The screenshot shows the Windows Event Log Explorer interface. The left pane displays the 'Objects tree' with a selected node 'WBN-90HAJ6CQHQM (local)'. The right pane lists events from the 'Microsoft-Windows-Symanet%#Operational.evtx' log. A specific event, ID 1, is highlighted in blue. The event details are as follows:

Type	Date	Time	Event	Source	Category	User	Computer
Information	2/13/2023	5:29:06 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:29:06 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:29:06 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:29:05 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:29:05 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:29:05 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:28:32 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:28:32 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:28:32 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:28:30 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:28:29 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:28:29 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:28:27 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:28:27 PM	1	Microsoft-Windows (1)	\SYSTEM	MSEDGEWIN10	

**Description**

```

The description for Event ID ( 1 ) in Source ( Microsoft-Windows-Symanet ) 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:
-
2023-02-13 17:28:27.749
{dc5131b5-733b-63ea-9c01-0000000000b0}
8112
C:\Windows\System32\cmd.exe
10.0.17134.1 (WinBuild.160101.0800)
Windows Command Processor
Microsoft Windows® Operating System
Microsoft Corporation
Cmd.Exe
"cmd.exe" /c tasks /create /tn "T1053_005_OnLogon" /sc onlogon /tr "cmd.exe /c calc.exe" & schtasks /create /tn "T1053_005_OnStartup" /sc onstart /ru system /tr "cmd.exe /c calc.exe"
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noexit -command Set-Location -iteraPath 'C:\Users\[EUser\Desktop]\PWF-man\PWF-man\AtomicRedTeam'
MSEDGEWIN10\[EUser]
0x2194c
]
High
MD5=4E2ACF4FB4396495A84268C94A6A245F,SHA256=9A7CS8B98D70631AA1473FB57B4260B367D72429A5455B433A05EE251F3236,DMPHASH=8542FB14699D84D7E8DA92F66145C7F
{dc5131b5-72d1-63ea-6601-0000000000b0}
7080
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noexit -command Set-Location -iteraPath 'C:\Users\[EUser\Desktop]\PWF-man\PWF-man\AtomicRedTeam'
MSEDGEWIN10\[EUser]

```

- Search everything based on parent process id: 7080 and event id 3- Network Connections, 22- DNS names :

The screenshot shows the Windows Event Log Explorer interface. The left pane displays the 'Objects tree' with a selected node 'WBN-90HAJ6CQHQM (local)'. The right pane lists events from the 'Microsoft-Windows-Symanet%#Operational.evtx' log. A specific event, ID 22, is highlighted in blue. The event details are as follows:

Type	Date	Time	Event	Source	Category	User	Computer
Information	2/13/2023	5:27:30 PM	3	Microsoft-Windows (3)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:27:30 PM	3	Microsoft-Windows (3)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:27:29 PM	3	Microsoft-Windows (3)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:27:29 PM	3	Microsoft-Windows (3)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:27:28 PM	22	Microsoft-Windows (22)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:26:58 PM	3	Microsoft-Windows (3)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:26:58 PM	3	Microsoft-Windows (3)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:26:58 PM	22	Microsoft-Windows (22)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:26:49 PM	3	Microsoft-Windows (3)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:26:49 PM	22	Microsoft-Windows (22)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:26:48 PM	3	Microsoft-Windows (3)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:26:48 PM	22	Microsoft-Windows (22)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:26:48 PM	3	Microsoft-Windows (3)	\SYSTEM	MSEDGEWIN10	
Information	2/13/2023	5:26:47 PM	22	Microsoft-Windows (22)	\SYSTEM	MSEDGEWIN10	

**Description**

```

The description for Event ID ( 22 ) in Source ( Microsoft-Windows-Symanet ) 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:
-
2023-02-13 17:26:37.998
{dc5131b5-72d1-63ea-6601-0000000000b0}
7080
raw.githubusercontent.com
0
::ffff:185.199.109.133::ffff:185.199.110.133::ffff:185.199.108.133::ffff:185.199.111.133;
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
MSEDGEWIN10\[EUser]

```

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search [ ]

WBN-90HAJ6CQHQM (local)

Log Files

- Application (C:\Cases\Windows\System32\winevt\Logs\Appln.evtx)
- System (C:\Cases\Windows\System32\winevt\Logs\System.evtx)
- Security (C:\Cases\Windows\System32\winevt\Logs\Security.evtx)
- Microsoft-Windows-PowerShell%4Operational (C:\Cases\Windows\System32\winevt\PowerShell.evtx)
- Microsoft-Windows-Sysmon%4Operational (C:\Cases\Windows\System32\winevt\Sysmon.evtx)

Task templates

344 22 0

UTC

Type	Date	Time	Event	Source	Category	User	Computer
(i) Information	2/13/2023	5:27:30 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:27:30 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:27:29 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:27:29 PM	22	Microsoft-Windows (22)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:26:58 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:26:58 PM	22	Microsoft-Windows (22)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:26:48 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:26:48 PM	22	Microsoft-Windows (22)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:26:48 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:26:47 PM	22	Microsoft-Windows (22)	SYSTEM	MSEDGEV\N10	

Description

The description for Event ID ( 3 ) in Source ( Microsoft-Windows-Syman ) 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:

```
2023-02-13 17:26:37.702  
(dc5131b5-72f6-63ea-6601-000000000000)  
7980  
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  
tcp  
true  
false  
10.0.2.15  
MSEDGEV\N10  
5/0281  
  
false  
185.199.109.133  
cdn-185-199-109-133.github.com  
443  
https
```

5:04 PM 2/16/2023

Untitled.ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

Objects tree

Search [ ]

WBN-90HAJ6CQHQM (local)

Log Files

- Application (C:\Cases\Windows\System32\winevt\Logs\Appln.evtx)
- Microsoft-Windows-Windows Defender%4Operational (C:\Cases\Windows\System32\winevt\Logs\Defender.evtx)
- System (C:\Cases\Windows\System32\winevt\Logs\System.evtx)
- Security (C:\Cases\Windows\System32\winevt\Logs\Security.evtx)
- Microsoft-Windows-PowerShell%4Operational (C:\Cases\Windows\System32\winevt\PowerShell.evtx)
- Microsoft-Windows-Sysmon%4Operational (C:\Cases\Windows\System32\winevt\Sysmon.evtx)

Task templates

344 22 0

UTC

Type	Date	Time	Event	Source	Category	User	Computer
(i) Information	2/13/2023	5:27:37 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:27:36 PM	22	Microsoft-Windows (22)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:27:36 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:27:34 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:27:33 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:27:32 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:27:31 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:27:31 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:27:30 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:27:30 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:27:29 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:27:29 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:27:28 PM	22	Microsoft-Windows (22)	SYSTEM	MSEDGEV\N10	
(i) Information	2/13/2023	5:26:58 PM	3	Microsoft-Windows (3)	SYSTEM	MSEDGEV\N10	

Description

The description for Event ID ( 22 ) in Source ( Microsoft-Windows-Syman ) 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:

```
2023-02-13 17:27:26.232  
(dc5131b5-72f6-63ea-6601-000000000000)  
7980  
www.powershellgallery.com  
0  
type: 5 powershellgallerytrafficmanager.trafficmanager.net:type: 5 psg-prod-centralus.cloudapp.net::ffff:40.122.208.145;  
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  
MSEDGEV\N10\IEUser
```

5:05 PM 2/16/2023