



Mission Name

ForensicsTest

History Background

In the previous mission, ETHAN is arrested by Claire and Tarain. Claire and Ethan are going to work together to catch the SHAX hackers and both must be tested on their skills.

Technical High-Level Overview

Player must put in practice his knowledge about Virus and AntiVirus. For testing Claire, player will receive Windows Defender events. The goal of this mission is to catch threat virus name that was spread on Phaldra's computer.

Short Mission Description

You're going to be tested to ensure that virus knowledge is up to date. Please catch the threat name of the virus on Phaldra's computer.

Mission Description

Player must put in practice his knowledge about Virus and AntiVirus. You're going to be tested to ensure that virus knowledge is up to date. Please catch the threat name of the virus on Phaldra's computer.

Location

SYLVARCON | EBAND DEPARTMENT - RECON HQ



Tools

- Event Log Explorer
- Evtx_dump

Questions

Which executable launched the alert on Windows Defender?

- Phaldra_test.exe

What is the event id related to the detection of the malware?

- 1117

Which is the name of Phaldra's computer?

- DESKTOP-15P11BS

Hints

1. Use any application which allows you to open EVTX files
2. Use Event Log Explorer application
3. Search for the word "Ransomware"

Write Up

Linux Method - no root necessary

- apt install libevtx-utils
- apt install python3-evtx
- <https://github.com/williballenthin/python-evtx>
- Git clone https://github.com/williballenthin/python-evtx.git

Once installed, we search the script to search for the event id 1116 or 1117, and you will get name of the virus on Phaldra's computer: Ransom:Win32/Stop.A!MTB

```
(root💀kali㉿kali)-[~/home/recon/tools/python-evtx/scripts]
└─# pwd
/home/recon/tools/python-evtx/scripts

[root💀kali㉿kali]-[~/home/recon/tools/python-evtx/scripts]
└─# █
```

Figure 1

```
[root💀kali㉿kali]-[~/home/recon/tools/python-evtx/scripts] # evtx_dump.py /home/challenges/03_ForensicsTest/Microsoft-Windows\Defender%4Operational.evtx | more █
```

Figure 2

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Defender" /><EventID Qualifiers="">1117</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>0</Task>
<Opcode>0</Opcode>
<Keywords>0x8000000000000000</Keywords>
<TimeCreated SystemTime="2049-12-08 13:07:05.914835"></TimeCreated>
<EventRecordID>35</EventRecordID>
<Correlation ActivityID="{af2a426e-5086-4971-bd46-c8e09fd1f557}" RelatedActivityID=""></Correlation>
<Execution ProcessID="2164" ThreadID="4568"></Execution>
<Channel>Microsoft-Windows-Defender/Operational</Channel>
<Computer>DESKTOP-15P11BS</Computer>
<Security UserID="S-1-5-18"></Security>
<System>
<EventData><Data Name="Product Name">Windows Defender Antivirus</Data>
<Data Name="Product Version">4.18.2011.6</Data>
<Data Name="Detection ID">06E41BF0-2E10-419B-9A2C-485E31394D53</Data>
<Data Name="Detection Time">2049-12-08T13:06:28.581Z</Data>
<Data Name="Unused"></Data>
<Data Name="Unused2"></Data>
<Data Name="Threat ID">2147767775</Data>
<Data Name="Threat Name">Ransom:Win32/Stop.A!MTB</Data>
<Data Name="Severity ID">5</Data>
<Data Name="Severity Name">Severe</Data>
<Data Name="Category ID">50</Data>
```

Figure 3

Windows Method

First of all, player should locate which tool can analyse, for example: Event Log Explorer

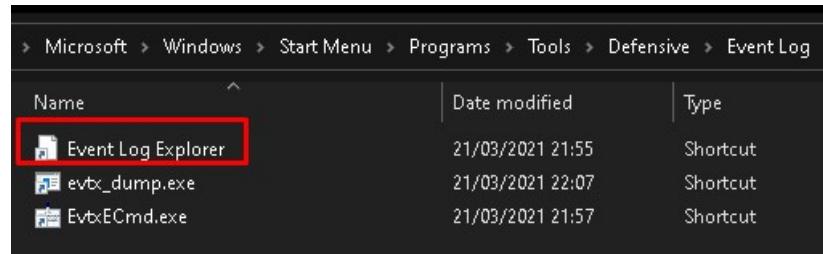


Figure 4

Later, player must analyse events to locate virus name on Phaldras Computer, opening EVTX file in this way:

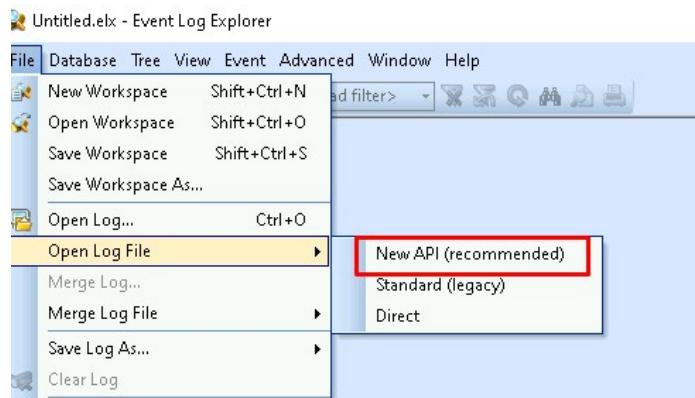


Figure 5

Once opened, search for the event id 1116 or 1117, and you will get name of the virus on Phaldras computer: Ransom:Win32/Stop.A!MTB

Type	Date	Time	Event	Source
Information	08/12/2049	14:08:39	1001	Microsoft-Window
Error	08/12/2049	14:08:07	2001	Microsoft-Window
Information	08/12/2049	14:08:01	1000	Microsoft-Window
Information	08/12/2049	14:07:05	1117	Microsoft-Window
Warning	08/12/2049	14:06:34	1116	Microsoft-Window
Error	08/12/2049	14:04:32	2001	Microsoft-Window
Error	08/12/2049	13:58:12	2001	Microsoft-Window
Information	08/12/2049	13:58:03	5007	Microsoft-Window
Information	08/12/2049	13:58:03	5007	Microsoft-Window
Information	08/12/2049	13:57:56	5007	Microsoft-Window

Description Name: Ransom:Win32/Stop.A!MTB
ID: 2147767775
Severity: Severe
Category: Ransomware
Path: file_{C:\Users\phaldr\\Desktop\phaldratest\phaldratest.exe}
Detection Origin: Local machine
Detection Type: Concrete
Detection Source: Real-Time Protection

Figure 6

Flag Information

flag{Ransom:Win32/Stop.A!MTB}