

Event-Viewing

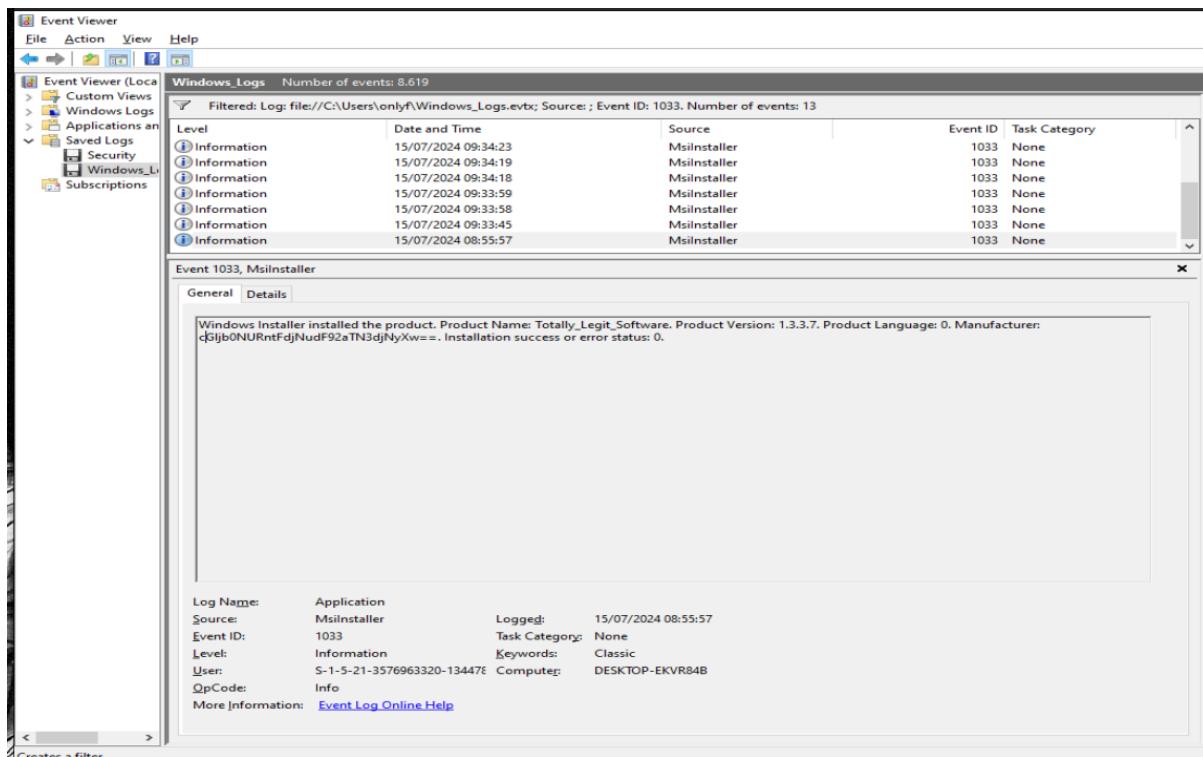
kami mendapatkan sebuah file .evtx yang bernama Windows_Logs.evtx dan kami membuka file tersebut untuk mencari event yang terkait yaitu

Deskripsi

Salah satu karyawan di perusahaan Anda memiliki komputer yang terinfeksi malware! Ternyata setiap kali mereka mencoba menghidupkan komputer, komputer tersebut langsung mati setelah mereka login. Cerita yang disampaikan oleh karyawan tersebut sebagai berikut:

1. Mereka menginstal perangkat lunak menggunakan installer yang diunduh secara online
2. Mereka menjalankan perangkat lunak yang diinstal, tetapi sepertinya tidak melakukan apa-apa
3. Sekarang setiap kali mereka menyalakan komputer dan masuk ke akun mereka, layar perintah hitam muncul dan tertutup dengan cepat, dan komputer langsung mati.
4. Cari bukti untuk setiap peristiwa ini dan ambil bendera (dibagi menjadi 3 bagian) dari log yang benar!

1033 -> untuk melihat installasi yang dilakukan oleh korban



kami menemukan sebuah text base64 `cGJjb0NURntFdjNudF92aTN3djNyXw==`

setelah kami melakukan decoding kami menemukan sebagian flag

```
cyberjunkie@shadow:~$ echo "cGJjb0NURntFdjNudF92aTN3djNyXw==" | base64 -d
picoCTF{Ev3nt_v13wv3r_cyberjunkie@shadow:~$
```

kami mencoba melakukan analisa lanjutan dengan event 4657 -> untuk melihat perubahan registry dari perangkat (setelah melakukan installasi, dan menjalankan perangkat lunak yang telah di installasi)

The screenshot shows the Windows Event Viewer interface. The main pane displays a table of events from the Windows Logs, filtered for event ID 4657. The table has columns for Level, Date and Time, Source, Event ID, and Task Category. All five entries show 'Information' level, various dates/times, 'Microsoft Windows security...' source, event ID 4657, and 'Registry' task category. Below this, a detailed view of one specific event (Event 4657) is expanded. The 'General' tab is selected, showing a summary of a registry value modification. The 'Details' tab is also visible. The summary includes fields like Subject (Security ID, Account Name, Account Domain, Logon ID), Object (Object Name, Object Value Name, Handle ID, Operation Type), Process Information (Process ID, Process Name), and Change Information (Old Value Type, Old Value). At the bottom of the details pane, there are fields for Log Name, Security, Source, Event ID, Task Category, Level, Keywords, User, Computer, and a link to 'More Information'.

dan kami kembali menemukan sebuah text base64 yang kemudian kami dekode, yang menghasilkan string

```
cyberjunkie@shadow:~$ echo "MXNfYV9wcjN0dHfdXMzZnVsXw==" | base64 -d
1s_a_pr3tty_us3ful_cyberjunkie@shadow:~$
```

selanjutnya target kami adalah event 1074 -> shutdown yang ada pada event log untuk melihat apakah ada base64 lainnya disana

The screenshot shows the Windows Event Viewer interface. At the top, it says "Windows Logs Number of events: 8,619" and "Filtered: Log: file:///C:/Users/onlyf/Windows_Logs.evt; Source: ; Event ID: 1074. Number of events: 4". Below this is a table with columns: Level, Date and Time, Source, Event ID, and Task Category. There are four entries, all from "User32" at different times on 15/07/2024. The Event ID column shows "1074" and the Task Category column shows "None".

Level	Date and Time	Source	Event ID	Task Category
Information	15/07/2024 10:02:35	User32	1074	None
Information	15/07/2024 10:01:05	User32	1074	None
Information	15/07/2024 09:59:18	User32	1074	None
Information	15/07/2024 09:46:14	User32	1074	None

Below the table, a specific event is expanded: "Event 1074, User32". It has tabs "General" and "Details". The General tab shows the following details:

The process C:\Windows\system32\shutdown.exe (DESKTOP-EKVR84B) has initiated the shutdown of computer DESKTOP-EKVR84B on behalf of user DESKTOP-EKVR84B\user for the following reason: No title for this reason could be found
Reason Code: 0x800000ff
Shutdown Type: shutdown
Comment: dDAwbF84MWJhM2ZIOX0=

The Details tab shows the following log information:

Log Name: System
Source: User32
Event ID: 1074
Level: Information
User: S-1-5-21-3576963320-13447E
OpCode: Info
Logged: 15/07/2024 10:01:05
Task Category: None
Keywords: Classic
Computer: DESKTOP-EKVR84B

kami menemukan bagian terakhir dari flag, yaitu dDAwbF84MWJhM2ZIOX0=
dan ketika dedecode

```
cyberjunkie@shadow:~$ echo "dDAwbF84MWJhM2ZIOX0=" | base64 -d  
t00l_81ba3fe9}cyberjunkie@shadow:~$
```

keutuhan flag secara keseluruhan

```
cyberjunkie@shadow:~$ echo "cGLjb0NURntFdjnudF92aTN3djNyXw==MXNFYV9wcjN0dH1fdXMzZnVsXw==dDAwbF84MWJhM2ZIOX0=" | base64 -d  
picoCTF{Ev3nt_vi3wv3r_1s_a_pr3tty_us3ful_t00l_81ba3fe9}cyberjunkie@shadow:~$
```

kami berhasil menemukannya

picoCTF{Ev3nt_vi3wv3r_1s_a_pr3tty_us3ful_t00l_81ba3fe9}