

Event-Viewing

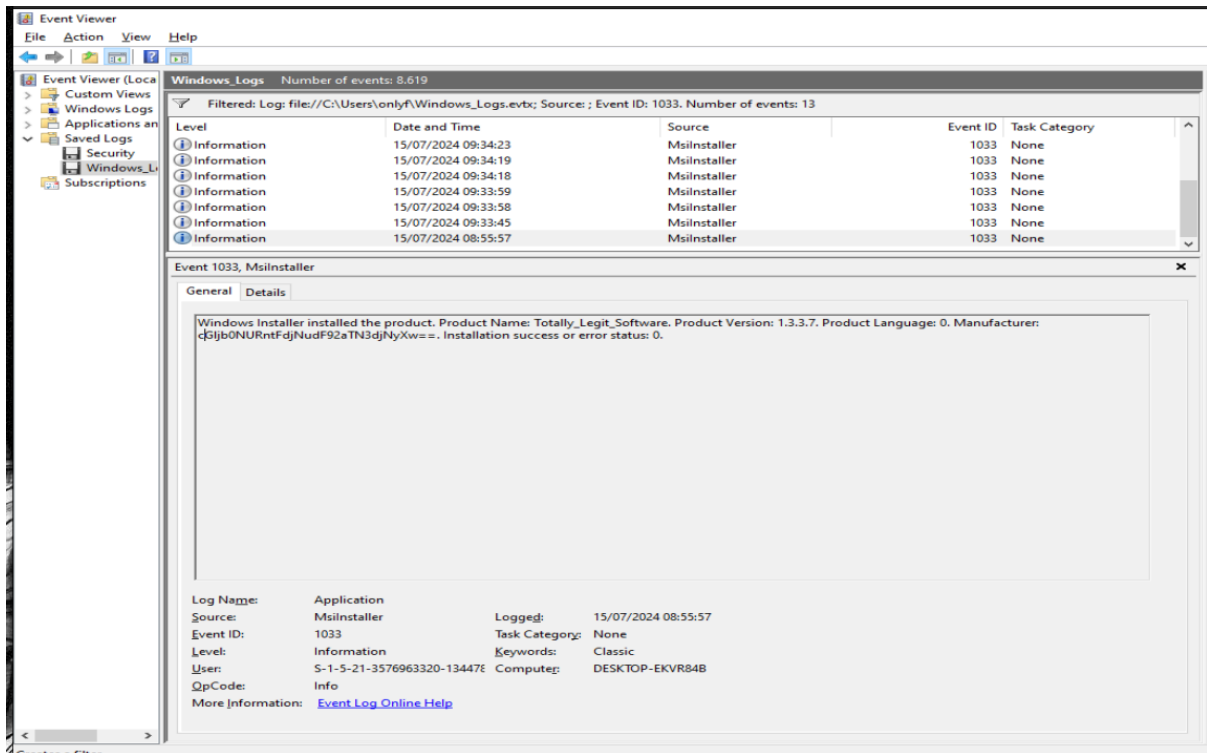
kami mendapatkan sebuah file .evtx yang bernama Windows_Logs.evtx dan kami membuka file tersebut untuk mencari event yang terkait yaitu

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 instalasi yang dilakukan oleh korban

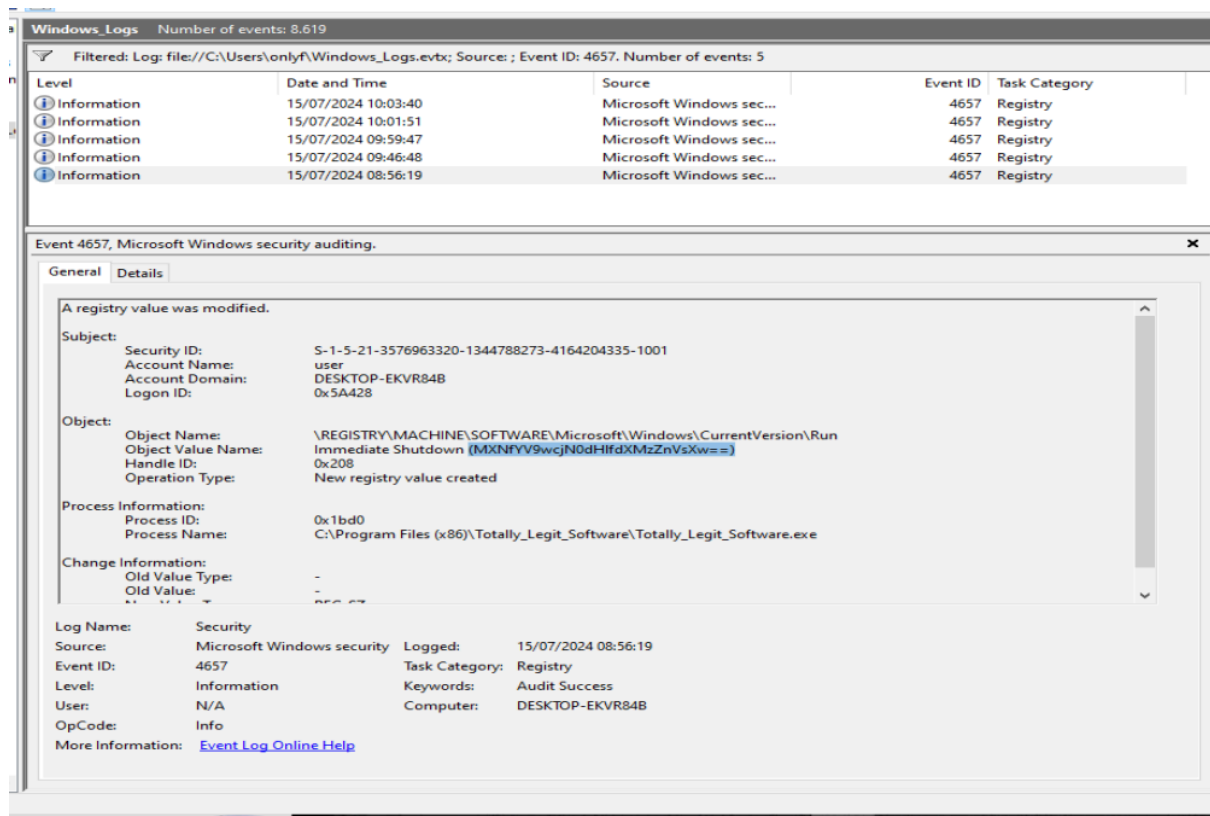


kami menemukan sebuah text base64 `cGljb0NURntFdjNudF92aTN3djNyXw==`

setelah kami melakukan decoding kami menemukan sebagian flag

```
cyberjunkie@shadow:~$ echo "cGljb0NURntFdjNudF92aTN3djNyXw==" | base64 -d
picoCTF{Ev3nt_vi3wv3r_
```

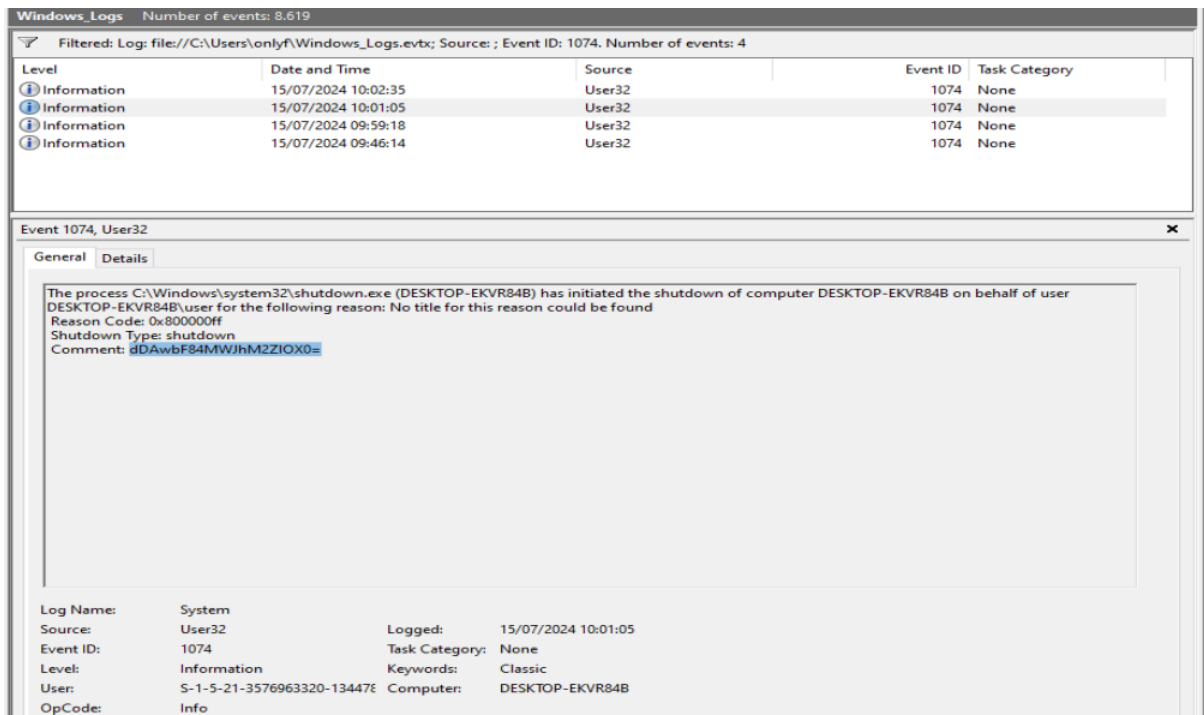
kami mencoba melakukan analisa lanjutan dengan event 4657 -> untuk melihat perubahan registry dari perangkat (setelah melakukan instalasi, dan menjalankan perangkat lunak yang telah di instalasi)



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

```
cyberjunkie@shadow:~$ echo "MXNfYV9wcjN0dHlfdXMzZnVsXw==" | 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



kami menemukan bagian terakhir dari flag, yaitu dDAwbF84MWJhM2ZlOX0=
dan ketika dedecode

```
cyberjunkie@shadow:~$ echo "dDAwbF84MWJhM2ZlOX0=" | base64 -d
t00l_81ba3fe9}cyberjunkie@shadow:~$
```

keutuhan flag secara keseluruhan

```
cyberjunkie@shadow:~$ echo "cGljb0NURntFdjNudF92aTN3djNyXw==MXNFYV9wcjN0dHlfdXMzZnVsXw==dDAwbF84MWJhM2ZlOX0=" | 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}