

Autoruns

Description

드림이의 컴퓨터에 누군가가 USB 저장장치를 연결했다가 해제한 후에,
컴퓨터를 재부팅할 때마다 계산기 프로그램이 실행되고 있어요. 도대체 어떻게 된 일일까요?

Windows 레지스트리를 분석해 플래그를 찾아보세요

Info

FLAG = DH{ MD5(File) }

FLAG는 자동 실행되고 있는 exe 파일을 MD5 해시로 계산한 값을 이용해 만듭니다.

예를 들어 대상 파일의 MD5 해시값이 00112233445566778899AABBCCDDEEFF 라
플래그는 DH{00112233445566778899AABBCCDDEEFF}입니다.

사용한 도구

FTK Imager, Registry Explorer

1. NTUSER.DAT 분석

경로: `C:\Windows\Users\victim\NTUSER.DAT` 추출

분석 내용: `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` 내부에 존재하는
MyProgram을 확인해보면 `C:\Users\victim\malware.exe`가 부팅될때마다 실행되는
걸 확인할 수 있다.

Key name	# values	# subkeys	Last write timestamp
ClickMe	0	1	2024-01-17 02:06:28
CloudExperienceHost	0	1	2024-04-04 12:23:57
CloudStore	2	2	2024-04-04 12:40:03
ContentDeliveryManager	15	6	2024-04-04 12:23:34
Cortana	2	0	2024-01-17 02:07:44
Diagnostics	0	1	2024-01-17 02:07:19
Explorer	13	42	2024-04-04 12:44:13
Ext	0	0	2024-01-17 02:07:33
Feeds	13	1	2024-04-04 12:11:32
FileAssociations	1	1	2024-01-17 02:07:32
History	0	1	2024-01-17 02:06:28
GameVirt	2	1	2024-04-04 12:06:00
Group Policy	0	2	2024-04-04 12:45:04
Holographic	1	2	2024-01-17 02:07:43
ime	0	1	2024-01-17 02:06:28
ImmersiveShell	1	1	2024-01-17 02:07:44
InstallService	0	1	2024-01-17 02:35:21
Internet Settings	13	10	2024-01-17 02:09:17
Indevices	9	2	2024-04-04 12:42:30
Lock Screen	1	0	2024-01-17 02:06:28
Mobility	0	0	2024-01-17 02:06:28
Notifications	0	1	2024-01-17 02:08:02
PenWorkspace	0	1	2024-01-17 02:06:28
Policies	0	0	2024-01-17 02:06:28
PrecisionTouchPad	11	1	2024-01-17 02:06:28
Privacy	4	0	2024-01-17 02:07:19
PushNotifications	1	3	2024-01-17 02:07:29
ADU	2	0	2024-01-17 02:06:28
Run	3	0	2024-04-04 12:31:59
Search	0	1	2024-04-04 12:26:16
Screenavers	0	4	2024-01-17 02:06:28
Search	17	2	2024-04-04 12:47:45
SearchSettings	1	0	2024-01-17 02:07:19
Security and Maintenance	0	2	2024-01-17 02:11:14
Settlysync	4	1	2024-01-17 02:09:14
Shell Extensions	0	1	2024-01-17 02:07:32
ControlPanel	0	1	2024-01-17 02:07:45

Value Name	Value Type	Data	Value Stack	Is Deleted	Data Record Realized
OneDrive	REG_SZ	"C:\Users\Victim\AppData\Local\Microsoft\OneDrive\OneDrive.exe"	00:00:00:00	<input type="checkbox"/>	<input type="checkbox"/>
MicrosoftEdgeAutolaunch	REG_SZ	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe"	BA-28-32-6A-	<input type="checkbox"/>	<input type="checkbox"/>
MyProgram	REG_SZ	"C:\Users\Victim\malware.exe"		<input type="checkbox"/>	<input type="checkbox"/>

Type viewer	Stack viewer	Binary viewer
Value name	OneDrive	
Value type	REG_SZ	
Value	"C:\Users\Victim\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background	
Raw value	22-00-43-00-3A-00-5C-00-55-00-73-00-63-00-72-00-73-00-5C-00-76-00-69-00-63-00-74-00-69-00-6D-00-5C-00-41-00-70-00-70-00-44-00-61-00-74-00-61-00-5C-00-4C-00-6F-00-63-00-61-00-6C-00-5C-00-4D-00-69-00-63-00-72-00-6F-00-73-00-6F-00-66-00-74-00-5C-00-4F-00-6E-00-65-00-44-00-72-00-69-00-76-00-65-00-5C-00-4F-00-6E-00-65-00-44-00-72-00-69-00-76-00-65-00-2E-00-65-00-78-00-65-00-22-00-20-00-3F-00-62-00-63-00-68-00-67-00-72-	

2. malware.exe의 hash값 추출

- FTK Imager에서 malware.exe의 hash 값 추출

File List			
Name	Size	Type	Date Modif...
Pictures	576 (1...	Direct...	2024-01-1...
PrintHood	296 (1...	Repars...	2024-01-1...
Recent	252 (1...	Repars...	2024-01-1...
Saved Games	152 (1...	Direct...	2024-01-1...
Searches	56 (1 ...	Direct...	2024-01-1...
SendTo	252 (1...	Repars...	2024-01-1...
Templates	264 (1...	Repars...	2024-01-1...
Videos	256 (1...	Direct...	2024-04-0...
시작 메뉴	268 (1...	Repars...	2024-01-1...
\$I30	8,192 (...	NTFS I...	2024-04-0...
\$TXF DATA	56 (1 ...	NTFS ...	2024-04-0...
malware.exe	26,624...	Regul...	2022-05-0...
NTUSER.DAT	1,310,...	Regul...	2024-04-0...
NTUSER.DAT.FileSl...	196,60...	File Sl...	
ntuser.dat.LOG1	253,95...	Regul...	2024-01-1...
ntuser.dat.LOG1.Fil...	81,920...	File Sl...	
ntuser.dat.LOG2	434,17...	Regul...	2024-01-1...
NTUSER.DAT{53b3...		\$I30 I...	
NTUSER.DAT{53b3...	65,536...	Regul...	2024-01-1...
NTUSER.DAT{53b3...	524,28...	Regul...	2024-01-1...

```
MD5,SHA1,FileNames
"302021d31f2d0bce01d7afc26bfe2ba2","8a1c6e08700b39c943ffe5521997d36ef60e7786","DiskImage.E01\WONAME [NTFS]\[root]\Users\victim\malware.exe"
```

