[Terrorist] Write-Up

작성자	허은정	
분석 일자	2024-05-10	
작성 일자	2024-05-10	
분석 대상 USB_Image(SuNiNaTaS).파일		
문서 버전	2.0	
작성자 E-mail	dmswjd4315@yonsei.ac.kr	





0. 목차

1.	문제	3
	는석 도구	
	환경	
	Write-Up	
	Flag	
	별도 첨부	
7.	Reference	3



1. 문제

URL	http://suninatas.com/challenge/web32/web32.asp		
	경찰청으로부터 연쇄 테러 용의자로부터 압수한 USB 이미지 분석을 의뢰 받		
	았다. 최초 분석을 신입 직원에게 맡겼으나 Hex Editor로 여기 저기 둘러 보다		
	실수로 특정 부분이 손상되고 이미지가 인식되지 않는다. 당신은 포렌식 전문		
	가의 자존심을 걸고 이미지를 살려 내고 다음 테러를 예방하는데 기여를 해야		
문제	한다.		
내용	1. 다음 테러 계획이 들어있는 문서의 수정 일시는? (UTC+9)		
	2. 다음 테러 장소는?		
	인증키 형식 : lowercase(MD5(YYYY-MM-DD_HH:MM:SS_장소)		
	예) lowercase(MD5(2016-03-28_13:00:00_Pink Lake)		
문제			
파일	USB_Image(SuNiN aTaS)		
문제	, , , , , , , , , , , , , , , , , , ,		
유형	Disk Forensics		
난이도	2/5		

2. 분석 도구

도구명	다운로드 링크	Version
HxD	https://mh-nexus.de/en/downloads.php?product=HxD20	2.5.0
FTK Imager	https://www.exterro.com/	4.7.1.2

3. 환경

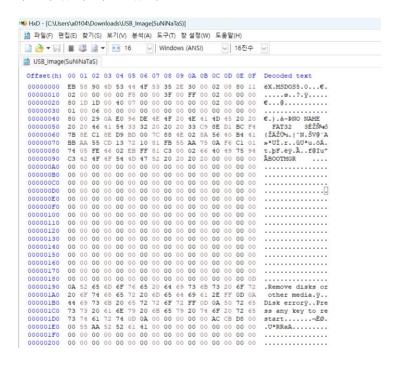
OS	
Window 11 64-bit	



4. Write-Up

파일명	USB_Image(SuNiNaTaS)	
용량	931MB	
SHA256	3512ca3524bb9bf7ca7dba819e43db08de89cb795f706cb4a6f3f2adb7ad59dc	
Timestamp	2024-05-10 09:22:25	

문제에 Download 파일이 있어 다운받았다.



[사진 1] 문제 파일을 HxD로 열어본 내용

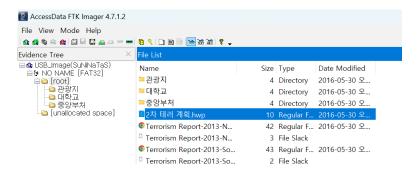
문제에서 보면 특정 부분이 손상되어 있다고 하여 [사진1]처럼 HxD로 열어보았다. HxD로 본 결과, FAT32(EB 58 90)이라는 것을 알 수 있었다. FTA32의 경우 0x1fe ~ 0x01ff에는 부트레코드의 시그니처 55AA가 있어야 하는데, [사진1]을 보면 시그니처의 위치가 이상하다는 것을 알 수 있다.



```
USB_Image(SuNiNaTaS)_1
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
          €.).à-ÞNO NAME
FAT32 3ÉŽÑ4ô
{ŽÁŽŮ4.|^N.ŠV@^A
 00000060
         00000070
                                                          ȻUÍ.r..ûUªu.öÁ.
                                                          t.þF.ëÿ.Ã..f@Iu"
 00000090
00000090
000000A0
000000B0
000000C0
000000D0
 000000F0
          00000100
          00000110
00000110
00000120
00000130
00000140
00000150
                                          00 00
00 00
00 00
00 00
00 00
                                                  00
                              00 00 00
                                       00
                                          00 00
                                                  00 00
                                                         move disks or ot
her media.ŷ.Dis
k errorŷ.Press
any key to resta
rt....¬ĒØ.U*
RRaA.
 00000180
          00 00 00 00 00 00 00
                              00 00 00 00 00 0D 0A 52 65
          00000190
                                    73 20 6F 72 20
                                                  6F
 000001A0
 00000180
000001B0
000001C0
000001D0
000001E0
000001F0
```

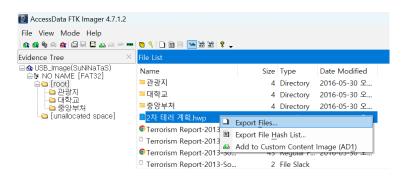
[사진 2] 부트레코드의 시그니처를 옮긴 사진

이를 해결하기 위해 00을 추가하여 Ox1fe ~ Ox01ff에 부트레코드의 시그니처를 옮겨 놓았다.



[사진 3] FTK Imager로 열어본 USB_Image

[사진3]을 보면 root 안에 2차 테러 계획.hwp가 있다는 것을 알 수 있습니다.



[사진 4] 해당 hwp 파일 Export

[사진 4]와 같이 해당 hwp파일을 Export 한 후 해당 파일을 열어 보았다.



WhiteHat School

2차 테러 계획

일 자	2016 - 07 - 15
시 간	09:00:00
<u>자소</u>	Rose Park

[사진 5] 해당 hwp파일 내용



[사진 6] 해당 hwp파일의 속성

[사진 5]를 통해 장소는 Rose Park라는 것을 알 수 있었다. [사진 6]을 통해서는 수정된 날짜가 2016-05-30_11:44:02라는 것을 알 수 있었다





MD5 해시 생성기 온라인

2016-05-30_11:44:02_Rose Park		생성하다
입력 문자열	2016-05-30_11:44:02_Rose Park	
MD5 해시(32비트)	8ce84f2f0568e3c70665167d44e53c2a	
MD5 해시(16비트)	0568e3c70665167d	
SHA1 해시	5cbf6a2fdd938534fc33904d87bd034cf43fb4d3	
Base64	MjAxNi0wNS0zMF8xMTo0NDowMl9Sb3NlIFBhcms=	

[사진 7] MD5 해시 생성한 결과(http://md5.ko.nrtool.com/)

해당 정보를 통해 인증키를 도출해보면 lowercase(MD5(2016-05-30_11:44:02_Rose Park))이다. 이를 통해 Auth Key = 8ce84f2f0568e3c70665167d44e53c2a 라는 것을 알 수 있다.



WhiteHat School

5. Flag

8ce84f2f0568e3c70665167d44e53c2a

6. 별도 첨부

7. Reference

- https://blog.forensicresearch.kr/13