

작성자	허은정
분석 일자	2024.05.07~2024.05.10
작성 일자	2024.05.10
분석 대상	Windows7(SuNiNaTas).파일
문서 버전	3.0
작성자 E-mail	dmswjd4315@yonsei.ac.kr

0. 목차

1. 문제3

2. 분석 도구3

3. 환경3

4. Write-Up.....4

5. Flag..... 10

6. 별도 첨부 11

7. Reference 12

1. 문제

URL	http://suninatas.com/challenge/web29/web29.asp
문제 내용	<p>유준혁은 PC가 고장나서 형 유성준에게 PC를 고쳐달라고 했다. 그런데, 유성준은 동생의 PC를 고치면서 몇 가지 장난을 했다. 당신은 이 PC를 정상으로 돌려 놓아야 한다,</p> <ol style="list-style-type: none"> 0. 웹 서핑은 잘 되는데, 네이버에만 들어가면 사이버 경찰청 차단 화면으로 넘어간다. 원인을 찾으면 Key가 보인다. 1. 유성준이 설치해 놓은 키로거의 절대경로 및 파일명은?(모두 소문자) -ex) c:\windows\notepad.exe 2. 키로거가 다운로드 된 시간은? 3. 키로거를 통해서 알아내고자 했던 내용은 무엇인가? 내용을 찾음 -ex) 2016-05-27_22:00:00 (yyyy-mm-dd_hh:mm:ss) <p>인증 키 형식: lowercase(MD5(1번키+2번답+3번답+4번키))</p>
문제 파일	https://bully.kr/4Ql2hrT
문제 유형	disk forensics
난이도	1/3

2. 분석 도구

도구명	다운로드 링크	Version
VMware Player	https://www.vmware.com/	17.0
BrowsingHistoryView	https://www.nirsoft.net/utils/browsing_history_view.html	2.5.7.31


3. 환경

OS
Window 11 64-bit / VMWare windows 7



4. Write-Up

파일명	Windows7(SuNiNaTaS)
용량	3.41GB
SHA256	d7eb9a5aadcd38f6de10565109b5cd49a24d266c673ce9a2231352cb4b42a0a74
Timestamp	2024-05-09 13:47:09



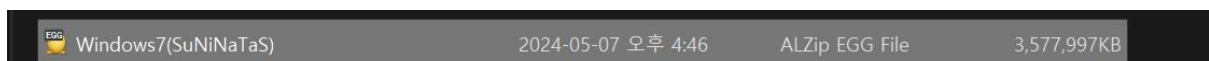
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text

00000000 45 47 47 41 00 01 3B 69 FA 56 00 00 00 00 22 82 E2 08 AC 93 90 85 0A 00 00 00 00 BC 25 00 00 00 00 00 00 47 75 65 73 74 41 70 70 73 43 61 63 68 65 2F 61 70 70 44 61 74 61 2F 30 62 34 37 37 39 61 32 37 31 39 32 35 36 33 30 35 61 39 39 63 62 35 37 35 30 30 62 37 35 34 2E 61 70 70 69 63 6F 6E 0B 95 86 2C 00 09 00 8D 8C E6 5E B5 D1 01 00 22 82 E2 08 13 0C B5 02 01 05 BC 25 00 00 68 25 00 00 88 41 1A D4 22 82 E2 08 6D 78 05 4C 1C 4C DB ED E2 6E 05 CA E2 4E 71 16 5F 74 29 5E BC 68 71

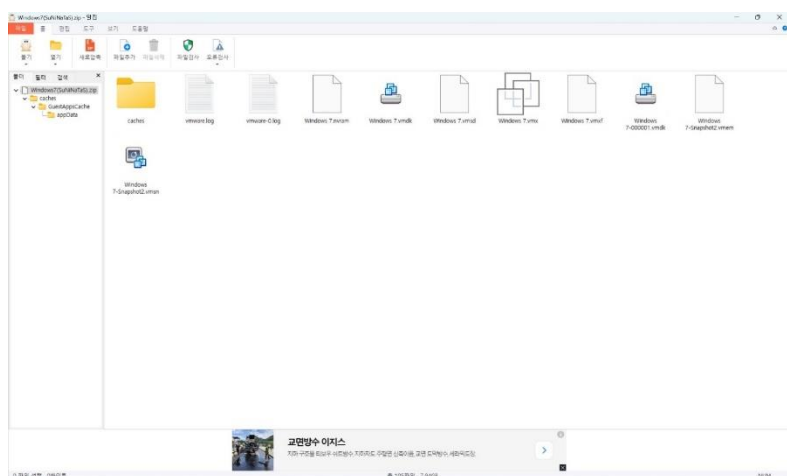
Decoded text

[사진 1] HxD를 이용하여 확인한 Windows7(SuNiNaTas) 파일

문제파일을 다운받았을 때 문제 파일 확장자를 알 수 없었다. 정확한 파일 확장자를 찾기 위해 HxD 를 이용하였고 이를 보니, EGG 파일이었다는 것을 알 수 있었다.



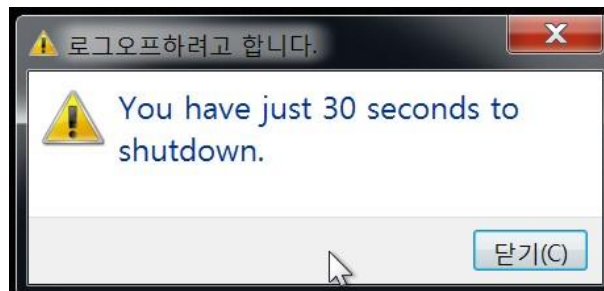
[사진 2] EGG 파일로 바꾼 파일



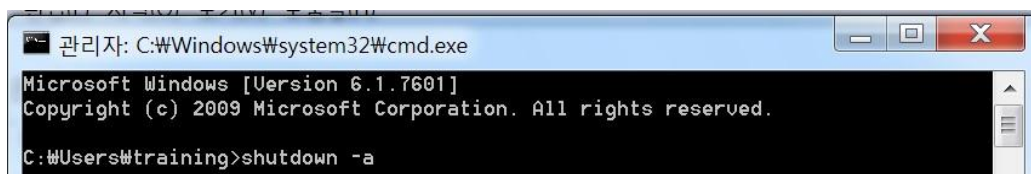
[사진 3] Windows 7(SuNiNaTas) 파일을 연 것

[WHS-2] .iso

[사진 2]처럼 확장자를 .egg 파일로 바꾼 다음 해당 파일을 열어보았다. 여기서 Windows 7.vmx 가 VMWare 로 열 수 있어 한 번 열어보았다.



[사진 4] VMWare 시작 화면



[사진 5] shutdown -a를 입력한 화면

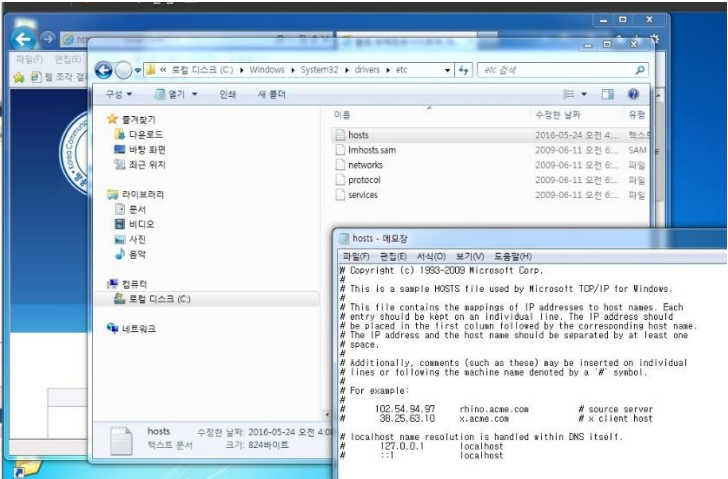
VMWare 로 열면 [사진 4]처럼 30 초 후 시스템을 종료한다는 메시지 창이 뜬다.

이 동작을 취소하기 위해 [사진 5]처럼 cmd 에 shutdown -a 를 입력하여 시스템 종료를 취소해준다.



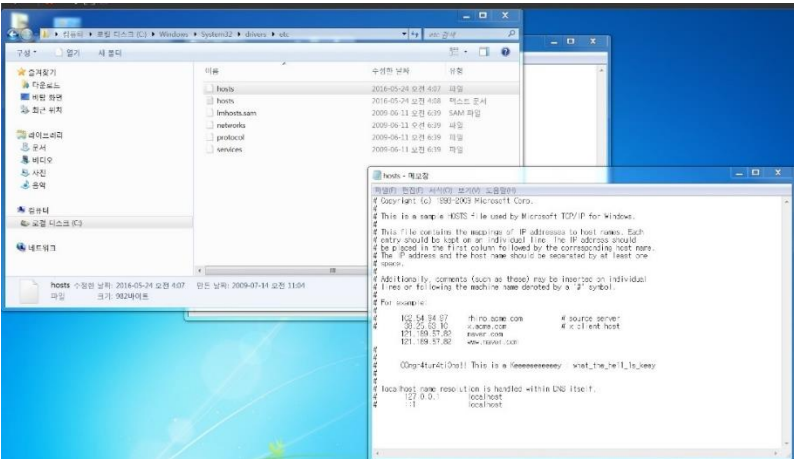
[사진 6] naver.com들어간 사진

1 번 문제를 봤듯이 [사진 6]을 보면 네이버에 접속만 하면 경찰청 차단페이지로 넘어간다는 것을 알 수 있다. 이를 통해, hosts 파일이 변조된 것이라고 생각을 하여 hosts 파일이 존재하는 곳인 C:\Windows\System32\drivers\etc 에 들어가 보았다.



[사진 7] host 텍스트 파일 확인

[사진 7]에 있는 hosts 텍스트 문서를 열어보면 key값과 naver 주소가 적혀져 있지 않다.

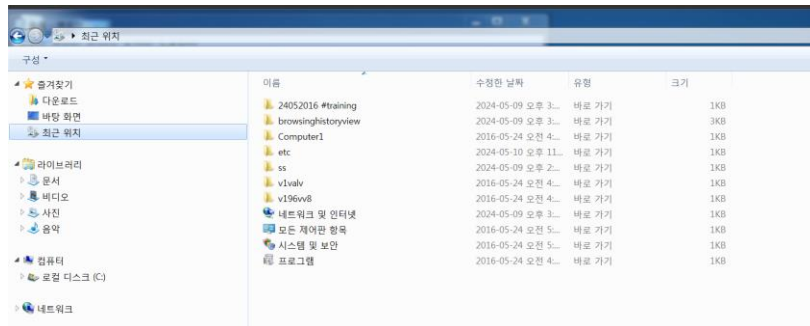


[사진 8] host 파일 확인

그래서 숨겨져 있는 파일들을 다 보이게 만들었다. 그 후 host파일을 메모장을 통해 열어본 결과 [사진 8]과 같이 나왔고 이를 통해 첫번째 키 값이 what_the_he11_1s_keey임을 알 수 있었다.

[WHS-2] .iso

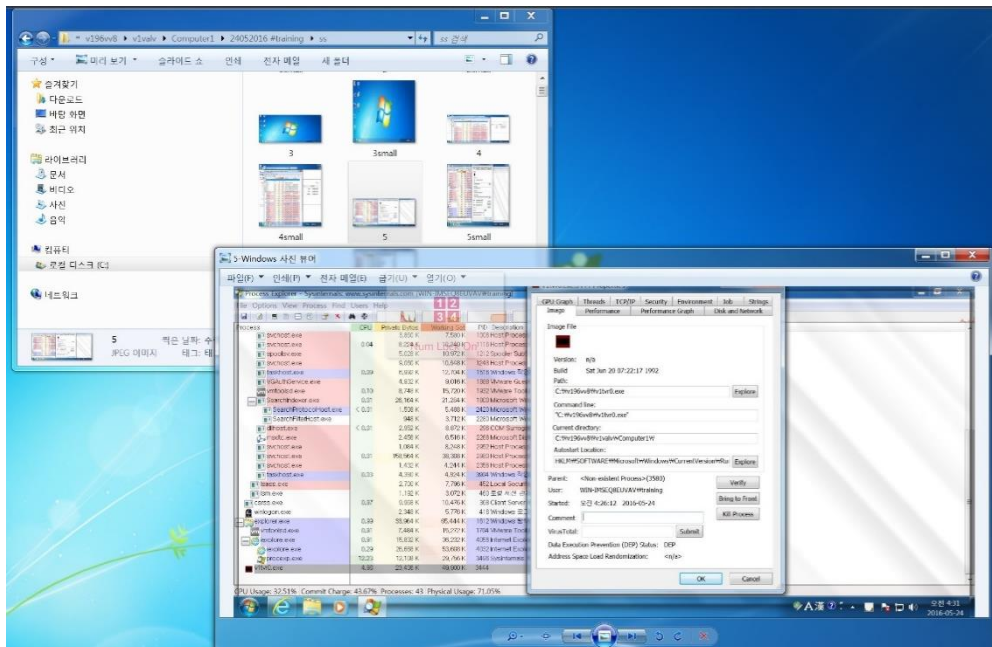
2.유성준이 설치해 놓은 키로거의 절대경로 및 파일명은?(모두 소문자)



이름	수정된 날짜	유형	크기
24052016 #training	2024-05-09 오후 3...	배로 가기	1KB
browsinghistoryview	2024-05-09 오후 3...	배로 가기	3KB
Computer1	2016-05-24 오전 4...	배로 가기	1KB
etc	2024-05-10 오후 11...	배로 가기	1KB
ss	2024-05-09 오후 2...	배로 가기	1KB
v196w8	2016-05-24 오전 4...	배로 가기	1KB
v196w8	2016-05-24 오전 4...	배로 가기	1KB
네트워크 및 인터넷	2024-05-09 오후 3...	배로 가기	1KB
모든 제어판 항목	2016-05-24 오전 5...	배로 가기	1KB
시스템 및 보안	2016-05-24 오전 5...	배로 가기	1KB
프로그램	2016-05-24 오전 4...	배로 가기	1KB

[사진 9] 해당 운영체제의 최근 위치

최근 위치에서 폴더를 보던 중 수상한 파일인 v196w8을 발견하여 들어가보았다.



[사진 10] 키로거 이미지 파일

위와 같은 경로에서 이미지 파일을 찾을 수 있었고 [사진 8]에 경로가 나타나 있다. 해당 파일의 경로는 c:\wv196w8wv1tr0.exe 임을 알 수 있었다.

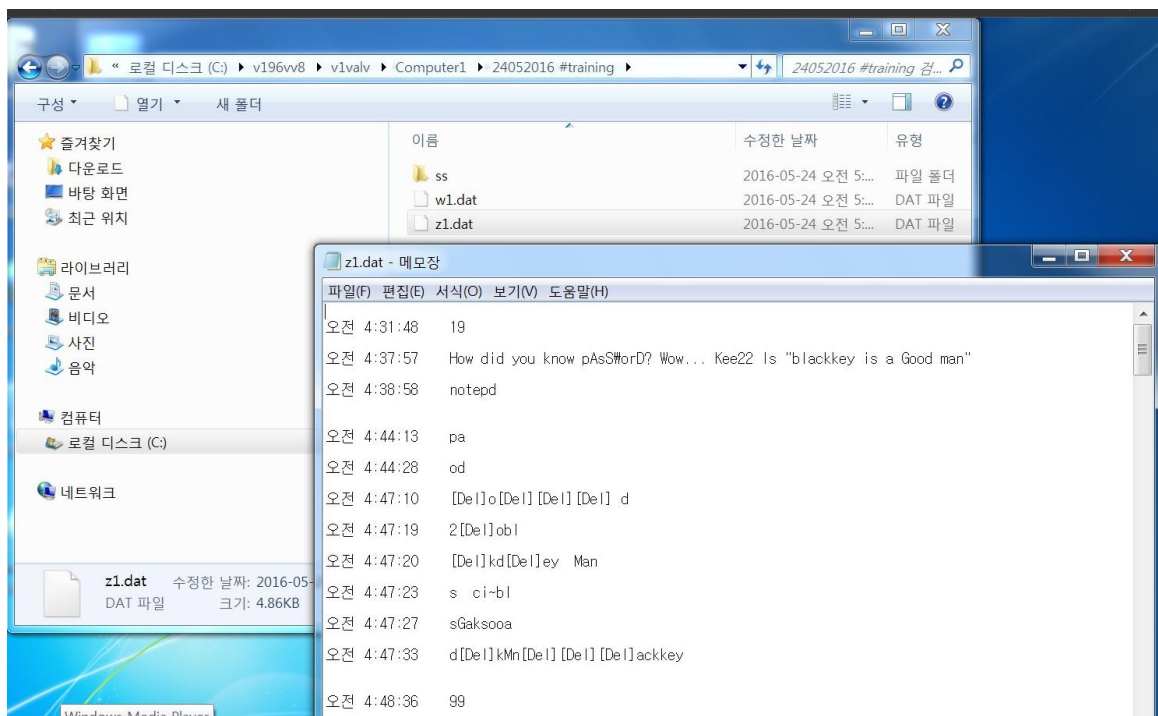
3.키로거가 다운로드 된 시간은?

URL	Title	Visit Time	Visit Count	Visited From	Visit Type	Visit Duration	Web Browser	User Profile	Browser Profile	URL Length	Typed Count	History File
http://shell.windows.c...		2024-05-09 오후 3:22:25	1		Internet Explorer	training				56		C:\Users\Wt...
http://shell.windows.c...		2024-05-09 오후 3:14:12	1		Internet Explorer	training				56		C:\Users\Wt...
http://192.168.163.1/fi...		2016-05-24 오전 5:00:55	8		Internet Explorer	training				50		C:\Users\Wt...
http://192.168.163.1/fi... Benryz WebShare		2016-05-24 오전 5:28:58	28		Internet Explorer	training				42		C:\Users\Wt...
http://192.168.163.1/fi... Benryz WebShare		2016-05-24 오전 5:28:32	24		Internet Explorer	training				42		C:\Users\Wt...
http://192.168.163.1/fi...		2016-05-24 오전 4:31:19	3		Internet Explorer	training				62		C:\Users\Wt...
http://192.168.163.1/fi...		2016-05-24 오전 4:31:17	2		Internet Explorer	training				75		C:\Users\Wt...
http://192.168.163.1/fi... Benryz WebShare		2016-05-24 오전 4:31:19	21		Internet Explorer	training				51		C:\Users\Wt...
http://192.168.163.1/fi...		2016-05-24 오전 4:25:06	1		Internet Explorer	training				71		C:\Users\Wt...
http://192.168.163.1/fi...		2016-05-24 오전 5:06:56	2		Internet Explorer	training				81		C:\Users\Wt...
http://192.168.163.1/fi... Benryz WebShare		2016-05-24 오전 5:06:58	13		Internet Explorer	training				54		C:\Users\Wt...
http://192.168.163.1/fi...		2016-05-24 오전 5:04:11	1		Internet Explorer	training				51		C:\Users\Wt...
http://192.168.163.1/fi...		2016-05-24 오전 5:04:14	1		Internet Explorer	training				54		C:\Users\Wt...
http://192.168.163.1/fi... Benryz WebShare		2016-05-24 오전 5:04:14	10		Internet Explorer	training				39		C:\Users\Wt...
http://192.168.163.1/fi... Benryz WebShare		2016-05-24 오전 5:06:56	Ad		Internet Explorer	training				77		C:\Users\Wt...

[사진 11] BrowsingHistoryView로 본 키로거 다운 시간

키로거 다운 시간을 쉽게 알 수 있는 프로그램인 BrowsingHistoryView를 이용하여 확인한 결과 2016-05-24_04:25:06에 받은 것을 알 수 있었다.

4.키로거를 통해서 알아내고자 했던 내용은 무엇인가? 내용을 찾으면 Key가 보인다.



[사진 12] z1.dat 파일 내용

키로거가 설치된 경로로 가보면 w1.dat파일과 z1.dat 파일이 존재한다. 이때 z1.dat파일을 열어보면 key값인 blackkey is a Good man임을 알 수 있었다.

MD5 해시 생성기 온라인

입력 문자열	what_the_he11_1s_keeyc:\v196vv8\v1tvr0.exe2016-05-24_04:25:06blackkey is a Good man
MD5 해시(32비트)	970f891e3667fce147b222cc9a8699d4
MD5 해시(16비트)	3667fce147b222cc
SHA1 해시	afb184a69ff6f2d6b3bf0d053b6b779acdc97c1
Base64	d2hhdF90aGVfaGUxMV8xc19rZWV5YzpcdjE5NnZ2OFx2MXR2cjAuZXhlMjAxNi0wNS0yNF8wNDoyNTowNmJsYWNRa2V5IGlzIGEgR29vZCBtYW4=

[사진 13] MD5 해시 생성한 결과(<http://md5.ko.nrtool.com/>)

위에서 찾은 키값 및 정답을 이용하여 인증 키를 도출해보면

lowercase(MD5(what_the_he11_1s_keey + c:\v196vv8\v1tvr0.exe + 2016-05-24_04:25:06 + blackkey is a Good man))입니다. 이를 통해 Auth Key = 970f891e3667fce147b222cc9a8699d4 임을 알 수 있다.

5. Flag

970f891e3667fce147b222cc9a8699d4

6. 별도 첨부

7. Reference