




[Memoryyyyy Dumpppppppp] Write-Up

| | |
|------------|--|
| 작성자 | 김경민 |
| 분석 일자 | 2024.05.17 |
| 작성 일자 | 2024.05.18 |
| 분석 대상 | xczprob2 |
| 문서 버전 | 2.0 |
| 작성자 E-mail | rlarudals877@gmail.com |

목차

- 1. 문제3
- 2. 분석 도구3
- 3. 환경3
- 4. Write-Up.....4
- 5. Flag.....9
- 6. 별도 첨부 10
- 7. Reference 11

1. 문제

| | |
|-------|--|
| URL | http://xcz.kr/START/prob/prob24.php |
| 문제 내용 | <p>어느날 나는 커피집에서 노트북을 놓고 잠시 자리를 비웠다. 그리고 다시 와서 작업을 하다가 작업프로그램이 갑자기 꺼졌고, 작업파일들이 모두 다 삭제되었다.</p> <p>원인을 찾기위해 나는 서둘러 메모리 덤프를 만들었다. 이 메모리 덤프파일을 분석하여 다음 정보를 알아내자.</p> <p>키 형식: (Process Name_PID_Port_Process Execute Time(Day of the week-Month-Day-Hour:Min:Sec-Years) ex (explorer.exe_1234_7777_Mon-Jan-01-12:00:00-2012)</p> |
| 문제 파일 |  xczprob2.zip |
| 문제 유형 | 메모리 포렌식 |
| 난이도 | 2 / 5 |

2. 분석 도구

| 도구명 | 다운로드 링크 | Version |
|------------|---|---------|
| volatility | https://github.com/volatilityfoundation/volatility.git | 2.6 |
| | | |
| | | |

3. 환경

| OS |
|--------------|
| Ubuntu 22.04 |

4. Write-Up

| | |
|-----------|--|
| 파일명 | xczprob2 |
| 용량 | 40,657KB |
| SHA256 | 402D939F267CBF4CDF671CBEDF48EF0FF954EE198B62C8D6BC2AA241EB04CAD5 |
| Timestamp | 2023-09-27 10:47:39 |

1. vol.py -f imageinfo 명령어가 먹히질 않아서 관련 프로그램 설치해 주었다.

```
sudo apt update

sudo apt install -y python2

sudo apt install -y python2-dev

curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py

sudo python2 get-pip.py

git clone https://github.com/volatilityfoundation/volatility.git

cd volatility

sudo python2 setup.py install

sudo pip2 install distorm3 openpyxl ujson yara-python

python2 vol.py -f imageinfo
```

위 명령을 순서대로 입력하면 된다. 참고로 volatility 는 python2 에서 오류 없이 잘 설치된다.

2. 문제 파일도 다운로드를 받아 주었으나 파일이 열리지 않았다. 확장자가 .001 인 것이
원인이었다. 따라서 hex에서 푸터 시그니처를 37 7A BC AF 27 1C 로 변경하고 .zip 으로 저장해
다시 열었더니 성공적이었다.

[WHS-2] .iso

3. 그럼 다시 위의 파일을 imageinfo 명령어를 이용해서 운영체제 정보를 확인해보았다. 그 결과 winxp 를 사용한다는 것을 알 수 있었다.


```
kkm@kkm-VirtualBox:~/다운로드/xczprob2$ vol.py -f xczprob2 imageinfo
Volatility Foundation Volatility Framework 2.6.1

INFO      : volatility.debug      : Determining profile based on KDBG search...
Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
AS Layer1 : IA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (/home/kkm/다운로드/xczprob2/xczprob2)
PAE type : PAE
DTB : 0xbfa000L
KDBG : 0x80547b60L
Number of Processors : 1
Image Type (Service Pack) : 3
KPCR for CPU 0 : 0xffdf000L
KUSER_SHARED_DATA : 0xffdf000L
Image date and time : 2012-11-02 09:08:09 UTC+0000
Image local date and time : 2012-11-02 18:08:09 +0900
kkm@kkm-VirtualBox:~/다운로드/xczprob2$
```

[사진 1] xczprob2 파일 분석 결과 및 해당 명령어

[WHS-2] .iso

4. 그 다음에는 프로세스 리스트를 출력해서 확인해 보았다. (현재 실행 중인 프로세스 목록을 보면 시스템에서 실행 중인 프로그램과 서비스를 알 수 있는데 이 때 악성코드나 비정상적인 프로세스를 식별할 수 있으므로 프로세스 리스트를 출력하는 것이다.) 그 결과 눈에 띄는 프로세스들이 보였다.



```
kkm@kkm-VirtualBox: ~/다운로드/xczprob2
-11-02 09:04:44 UTC+0000
0xff36b990 uphclean.exe      1800    720     2     38     0     0 2012
-11-02 09:04:44 UTC+0000
0xff364470 wuauclt.exe      1996   1088     7    132     0     0 2012
-11-02 09:04:47 UTC+0000
0xff329438 alg.exe           340    720     6    101     0     0 2012
-11-02 09:04:49 UTC+0000
0xff30c220 explorer.exe      1044    984    14    414     0     0 2012
-11-02 09:05:16 UTC+0000
0xff2b9c10 rundll32.exe     1776   1044     4     79     0     0 2012
-11-02 09:05:28 UTC+0000
0xff2fb558 UnlockerAssista  1956   1044     1     28     0     0 2012
-11-02 09:05:29 UTC+0000
0xff2fd650 Mmm.exe          1736   1044     2     51     0     0 2012
-11-02 09:05:29 UTC+0000
0xff2cd4a0 ctfmon.exe        256    1044     1    115     0     0 2012
-11-02 09:05:30 UTC+0000
0xff423a88 conime.exe       252    1724     1     39     0     0 2012
-11-02 09:05:54 UTC+0000
0xff2b6180 nc.exe           1124   1724     3     64     0     0 2012
-11-02 09:06:48 UTC+0000
0xff3586b8 cmd.exe           164    1124     1     39     0     0 2012
-11-02 09:06:49 UTC+0000
0xff2dbb58 cmd.exe          1524   1044     1     33     0     0 2012

kkm@kkm-VirtualBox:~/다운로드/xczprob2$ vol.py -f xczprob2 --profile=WinXPSP2x86
pslist
Volatility Foundation Volatility Framework 2.6.1
```

[사진 2] 프로세스 리스트 출력 결과 및 해당 명령어

5. 위의 표시한 프로세스들을 확인해 보자면 밑에 나와있다.

- uphclean.exe – 사용자 프로필 하이브 정리 서비스
- UnlockerAssista – 파일 또는 폴더의 락을 해제하는 unlocker 응용프로그램
- nc.exe – netcat(nc)은 TCP 나 UDP 프로토콜을 사용하는 네트워크 연결에서 데이터를 읽고 쓰는 유틸리티 프로그램/리눅스에 내장되어 있고 포트 스캔, 파일 전송 및 포트 수신이 가능
- conime.exe – 악성코드가 삽입된 웹사이트 이용시 윈도우의 취약점을 이용하여 설치되고, 해킹 목적으로 구성된 스파이웨어

[WHS-2] .iso

6. 또한 각 파일의 프로세스 관계 역시 살펴보자면 밑에와 같다. 이를 통해 nc.exe nc.exe 프로세스를 통해 conime.exe 프로그램이 심어져서 작업 파일들이 삭제됐다고 생각했다.

- nc.exe 1124 1724
 - cmd.exe 164 1124
 - cmd.exe 616 164
- conime.exe 252 1724

7. 그래서 nc.exe 를 통해 conime.exe 프로그램이 심어졌고, 이 프로그램의 실행을 통해 작업 프로그램이 종료되고 작업 파일이 삭제된 과정을 마치고 연결이 종료됐을 것이라고 생각해서 connscan 플러그인으로 확인했다. (connscan 은 메모리 덤프를 분석하는데 사용된다. 시스템 메모리에서 네트워크 연결 정보를 추출하고 분석한다.)

연결이 종료된 또는 현재 실행 중인 tcp 세션을 출력(윈도우 XP)해보면 -> PID 가 1124 인 nc.exe 프로세스가 연결을 종료한 것으로 보아 추측이 맞는 것 같다.

```
kkk@kkk-VirtualBox:~/다운로드/xczprob2$ vol.py -f xczprob2 --profile=WinXPSP2x86
connscan
Volatility Foundation Volatility Framework 2.6.1

pto.Hash)
Offset(P) Local Address Remote Address Pid
-----
0x05558b38 172.30.1.6:80 1.226.182.38:59495 1124
kkk@kkk-VirtualBox:~/다운로드/xczprob2$
```

[사진 3] 네트워크 연결 정보 추출 및 해당 명령어

[WHS-2] .iso

8. 그 다음에는 위의 네트워크 정보를 확인해보았다. 문제에서 요구한 키 형식이 (Process Name_PID_Port_Process Execute Time(Day of the week-Month-Day-Hour:Min:Sec-Years) 이므로 키는 nc.exe_1124_80_Fri-Nov-02-09:06:48-2012 인 것을 알 수 있다.

```
ERROR : volatility.debug : Please specify a location (-L) or filename (-F)
kkm@kkm-VirtualBox: ~/다운로드/xczprob2$ vol.py -f xczprob2 --profile=winXPSP2x86
sockets
```

| Offset(V) | PID | Port | Proto | Protocol | Address | Create Time |
|------------|------|------|-------|----------|------------|------------------------------|
| 0xff23ed08 | 1124 | 80 | 6 | TCP | 0.0.0.0 | 2012-11-02 09:06:48 UTC+0000 |
| 0xff344d80 | 732 | 500 | 17 | UDP | 0.0.0.0 | 2012-11-02 09:04:44 UTC+0000 |
| 0xff236e98 | 4 | 138 | 17 | UDP | 172.30.1.6 | 2012-11-02 09:04:38 UTC+0000 |
| 0xff3443b8 | 4 | 445 | 6 | TCP | 0.0.0.0 | 2012-11-02 09:04:28 UTC+0000 |
| 0xff234e98 | 948 | 135 | 6 | TCP | 0.0.0.0 | 2012-11-02 09:04:28 UTC+0000 |

nc.exe_1124_80_Fri-Nov-02-09:06:48-2012

Submit

Allow popup For share on facebook

[사진 4] 네트워크 정보 출력 및 해당 명령어 및 플래그 정답

5. Flag

nc.exe_1124_80_Fri-Nov-02-09:06:48-2012

6. 별도 첨부

7. Reference