www.alyac.co.kr

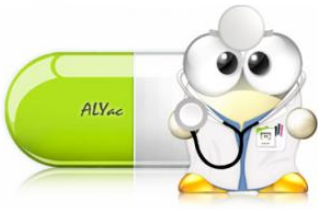
피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차



Part I 4월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

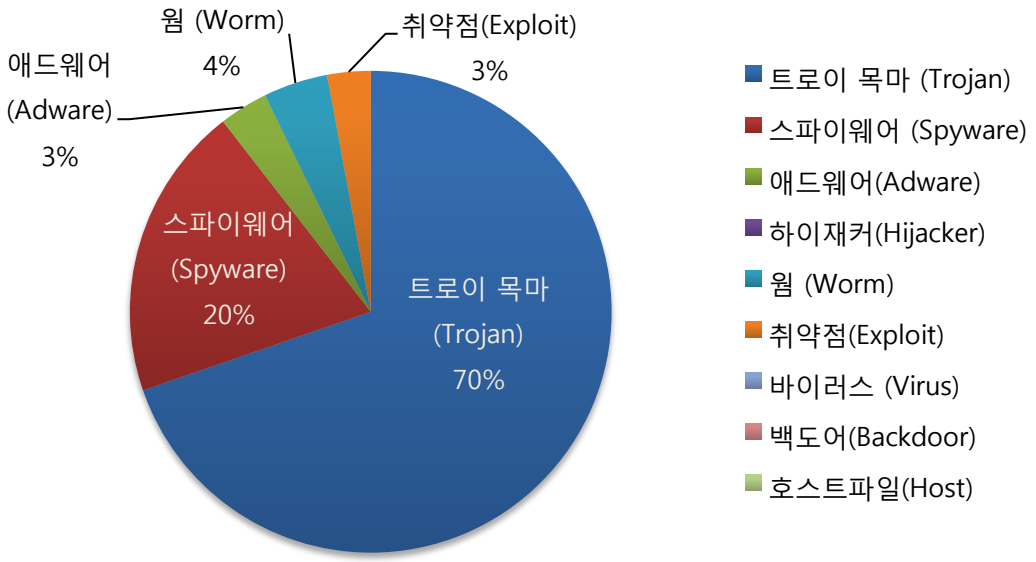
[2011년 4월 1일 ~ 2011년 4월 30일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	↑1	Variant.Fosniw.6	Trojan	54,129
2	↓1	S.SPY.Lineag-GLG	Spyware	44,723
3	-	V.TRJ.Clicker.Winsoft	Trojan	37,991
4	-	V.DWN.86016	Trojan	29,657
5	New	V.DWN.KorAdware.Gen	Trojan	26,328
6	↓1	V.DWN.Onlinegame.PA.Gen	Trojan	21,192
7	↓1	S.SPY.OnlineGames-H	Spyware	19,060
8	New	V.WOM.Conficker	Worm	13917
9	New	Trojan.Generic.5750564	Trojan	12,557
10	New	Variant.Buzy.1797	Trojan	12,359
11	New	Variant.Buzy.2702	Trojan	10,930
12	New	A.ADV.Admoke	Adware	10,609
13	New	Variant.Buzy.1775	Trojan	9,956
14	New	Variant.Buzy.1834	Trojan	9,777
15	New	Script.SWF.C13	Exploit	9,384

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

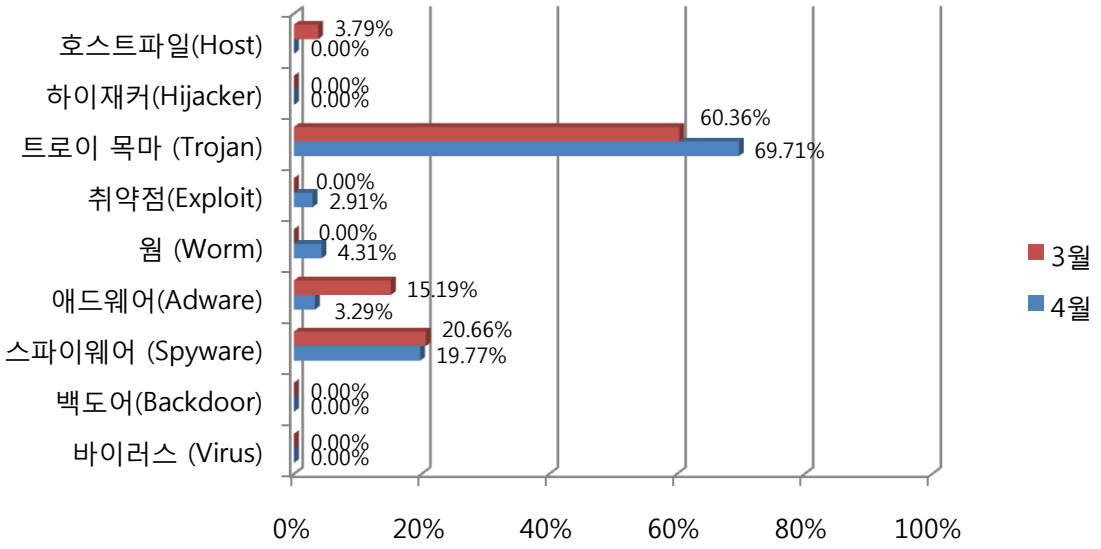
감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.
4월의 감염 악성코드 TOP 15는 Variant.Fosniw.6가 54,129건으로 TOP 15 중 1위를 차지하였으며, S.SPY.Lineag-GLG이 44,723건으로 2위, V.TRJ.Clicker.Winsoft가 37,991건으로 3위를 차지하였다.
이 외에도 4월에 새로 Top 15에 진입한 악성코드는 총 9종이다.
1위의 Variant.Fosniw.6는 3위 V.TRJ.Clicker.Winsoft의 변종파일이며 1,3위는 같은 악성코드로도 볼 수 있다. 이 두 악성코드는 서버와의 주기적인 통신을 통해 악성코드가 감염된 PC를 관리하는 것이 주 목적이다. 감염된 PC는 PC가 켜질 때마다 서버에 악성코드의 버전을 보내며 서버는 신종 악성코드가 있다면 새로운 악성코드를 다운로드 받을 수 있는 링크를 전달한다. 이처럼 서버와의 통신을 통해 새로운 악성파일을 다운로드 시켜, 감염 PC의 치료를 어렵도록 만드는 구조를 가지고 있다.
4월은 새로 진입한 악성코드가 매우 많았는데 그 중에서도 15위를 차지한 Script.SWF.C13은 다른 악성코드들에 비해 짧은 시간에 높은 순위를 차지하였다. 이유는 인터넷 게시판에 등록된 광고성 글에 악성 SWF파일을 삽입하여 불법 도박 사이트, 악성파일 유포 사이트로 연결시켰기 때문이다. 인터넷 사용자가 이 같은 피해를 막기 위해서는 항상 알약 실시간 감시를 켜두어야 한다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율은 트로이 목마(Trojan)가 70%로 가장 많은 비율을 차지하고, 스파이웨어(Spyware)가 20%, 웜(Worm)이 4%의 비율을 각각 차지하고 있다.

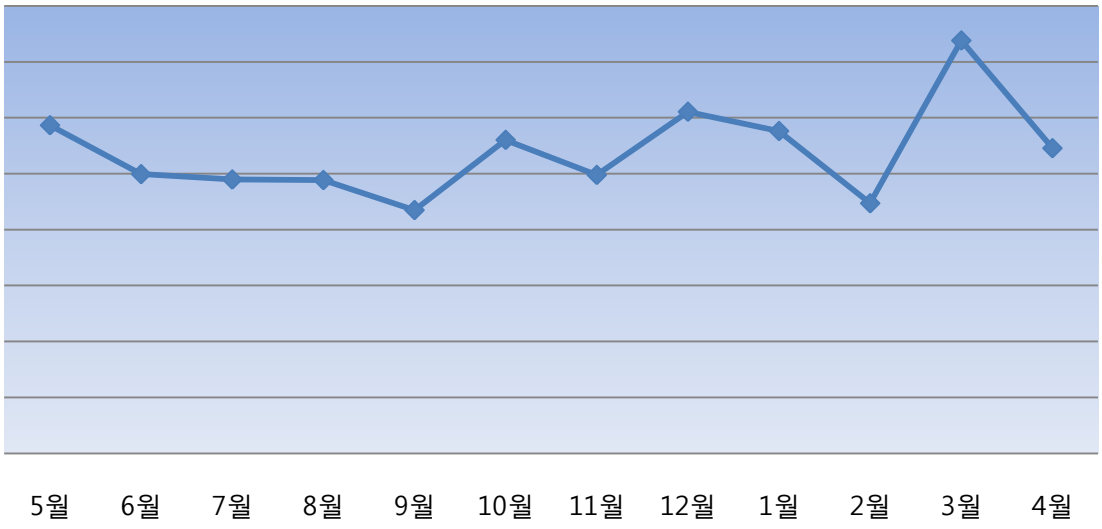
(3) 카테고리별 악성코드 비율 전월 비교



악성코드 유형별 비율을 전월과 비교한 그래프이다. 4월의 특이사항은 트로이목마(Trojan)가 전 월에 비해 약 9% 증가하였고 애드웨어(Adware)는 약 12%, 스파이웨어(Spyware)는 약 1%씩 감소하였다. TOP15의 상위권을 대부분 트로이목마(Trojan)가 차지해 전 월에 비해 트로이목마(Trojan)가 증가한 것으로 판단된다.

(4) 월별 피해 신고 추이

[2010년 05월 ~ 2011년 04월]

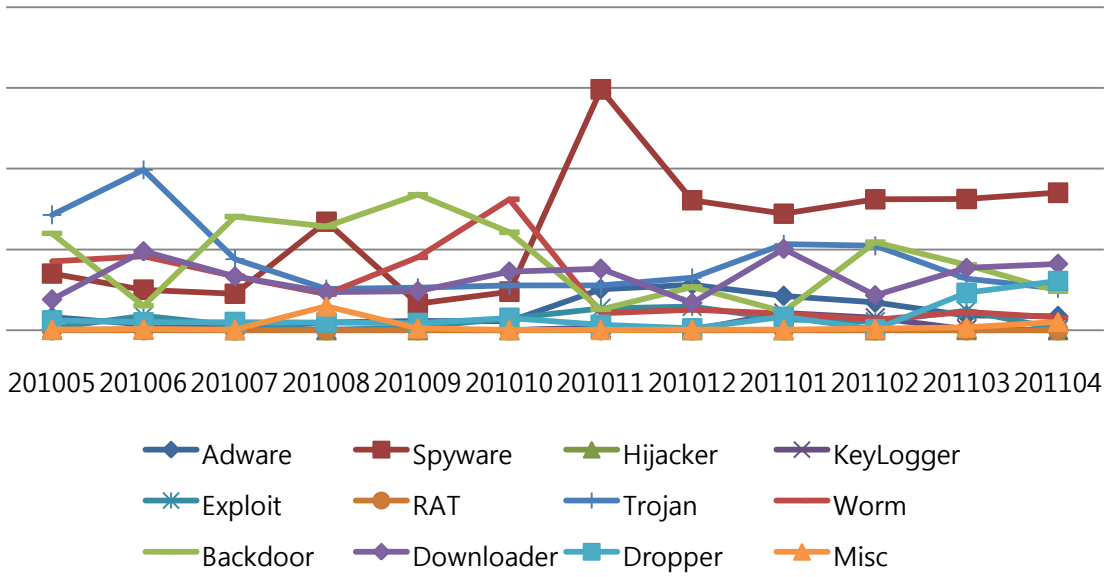


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월 별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월 별 신고 건수를 나타내는 그래프이다. 4월의 피해 신고추이는 전월에 비해 감소하였다. 3월에 3.4 디도스 대란으로 사용자의 문의 및 피해 신고가 급증 하였다가 사태가 마무리되면서 정상치 범위로 감소하였다.

(5) 월별 악성코드 DB 등록 추이

[2010년 05월 ~ 2011년 04월]



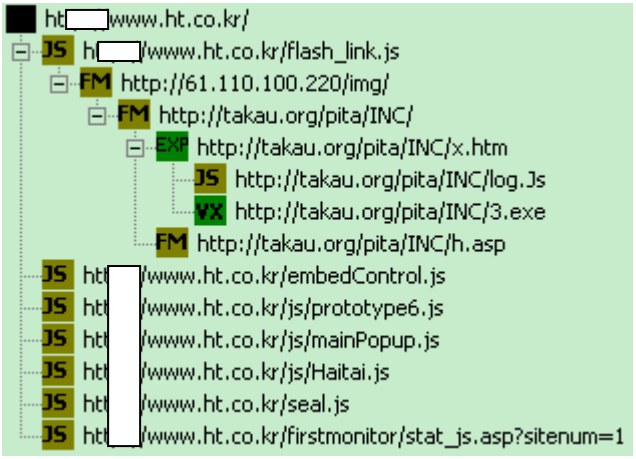
DB 등록추이는 변종이 많이 발생되는 순위라고도 할 수 있다. 4월은 전 월과 비교하여 별 다른 특이사항 없이 비슷한 수준을 유지하였다.

Part I 4월의 악성코드 통계

2. 악성코드 이슈 분석 – "Trojan.Dropper.OnlineGames.mi"

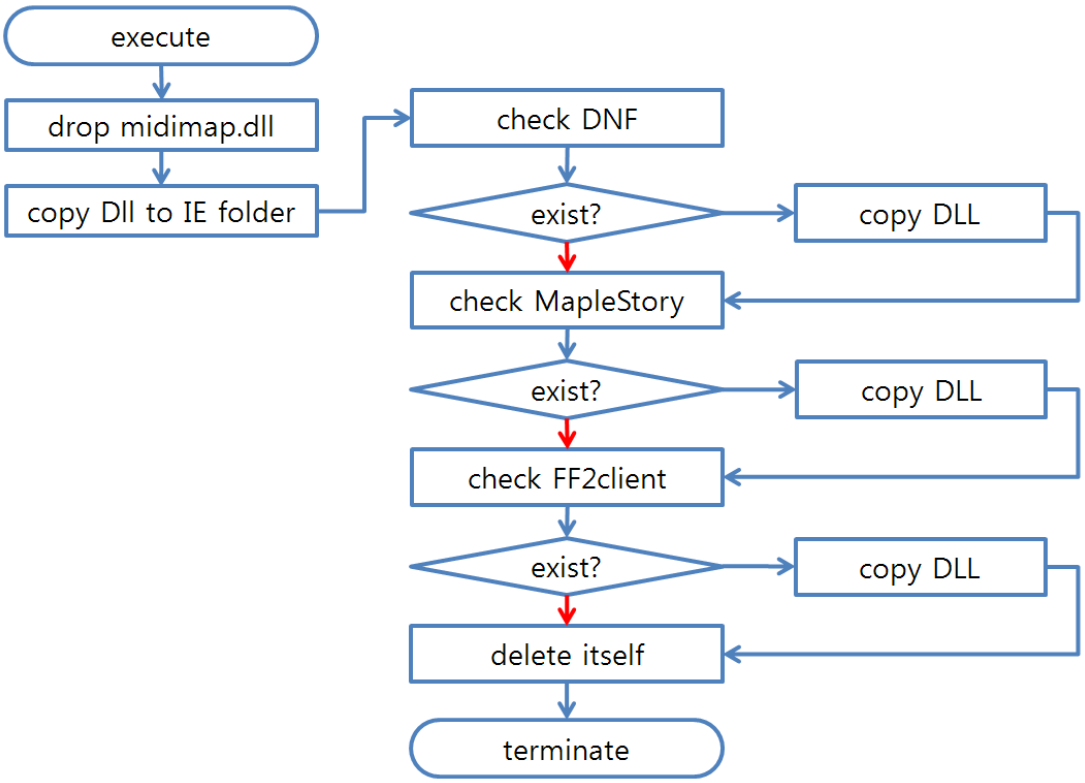
(1) 개요

이번 악성코드는 한 식품회사의 웹사이트에서 유포되었던 것으로, 주요 실행 프로세스인 '3.exe' 파일의 동작과 특징을 알아보고자 한다.



최초 해당 홈페이지를 접속하게되면 JS 파일을 통해 iframe 형식으로 61.110.100.220./img/index.html 로 접속하며, 이것은 다시 redirection 되며 취약점 CVE-2010-0806 을 이용한 'x.htm'파일을 통해 최종적으로 '3.exe'을 사용자 PC 에 설치하게 된다.

'3.exe' 파일은 온라인게임 계정을 탈취하는 데에 목적이 있으며 다음과 같은 행동을 한다.



(2) 악성코드 분석

파일명	3.exe
탐지명	Trojan.Dropper.OnlineGames.mi
주요 행동	midimap.dll 파일을 temp 폴더에 생성하고 특정 폴더에 복사한다.

① midimap.dll 파일 생성

실행 시 중복 실행 방지를 위해 mutex를 생성하고, temp폴더에 midimap.dll 파일을 생성한다. midimap 파일은 실제 악성행위를 하는 파일로 온라인 게임의 계정 탈취를 목적으로 한다. 생성시 모든 API는 직접 호출을 사용하지 않고 로드 하고자 하는 DLL 명을 역순으로 재 조합하여 원하는 함수의 주소를 얻어온다.

```
if ( Call_Function_("23lenreK", (int)"FindResourceA", (int)&dword_404A94) )
{
  v1 = Call_Function_("23lenreK", (int)"LoadResource", (int)dword_404A5C);
  if ( v1 )
  {
    if ( Call_Function_("23lenreK", (int)"LockResource", (int)&dword_404A58) )
    {
      Call_Function_("23lenreK", (int)"SizeofResource", (int)dword_404A5C);
      if ( Call_Function_("23lenreK", (int)"CreateFileA", (int)dword_404A98) != -1 )
                                        // midimap.dll
        v2 = Call_Function_("23lenreK", (int)"WriteFile", (int)dword_404A6C);
      Call_Function_("23lenreK", (int)"CloseHandle", (int)&dword_404A58);
    }
    Call_Function_("23lenreK", (int)"FreeResource", (int)&dword_404A58);
  }
}
return v2;
```

midimap.dll 파일의 생성

② IE registry 수정

다음과 같이 IE registry에 'TabProcGrowth' key를 생성하고 값을 '0'으로 설정한다.

HKEY_CURRENT_USER₩Software₩Microsoft₩Internet Explorer₩Main₩TabProcGrowth

TabProcGrowth REG_DWORD 0x00000000 (0)

이는 Tab Process Growth, 말 그대로 프로세스 증가 여부를 설정한다. '0' 이면 프로세스는 탭을 설정해도 자식 프로세스가 만들어지지 않는다. 이렇게 하는 이유는 다음에 보충해서 설명하겠다.

#ref> http://www.sysnet.pe.kr/Default.aspx?mode=2&sub=0&detail=1&wid=686

③ 타겟 프로세스 종료와 타겟 프로그램의 path 검색

```
.text:00401F78 E8 47 FB FF FF                call    _Find_Process_and_tskill_ ;
.text:00401F78                                                       ; DnF.exe
.text:00401F78                                                       ; PMClient.exe
.text:00401F78                                                       ; IEXPLORE.EXE
```

위의 그림과 같이 'DnF.exe', 'PMClient.exe', 'IEXPLORE.EXE' 프로세스의 PID를 확인해서 tskill.exe 명령을 통해 종료시킨다.

```
v6 = 't';
v5 = 0;
v7 = 's';
v8 = 'k';
v9 = 'i';
v10 = 'l';
v11 = 'l';
v12 = '.';
v13 = 'e';
v14 = 'x';
v15 = 'e';
v16 = ' ';
v17 = '%';
v18 = 'd';
wsprintfA(&v2, &v6, a1);
Call_Function_("231enreK", (int)"WinExec", (int)&dword_4044B4);
```

Process를 종료하면 타겟이 되는 프로그램의 레지스트리 키 값에서 path를 찾는다.

'(HLM)₩SOFTWARE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩App Paths₩IEXPLORE.EXE'
'software₩DNF₩path'
'SOFTWARE₩Wizet₩MapleStory₩ExecPath'
'software₩neowiz₩FIFAONLINE2₩InstallPath'

위의 레지스트리 값을 찾아보고 나타나지 않으면 다음과 같이 레지스트리 MUICahe에서 키 값을 찾는다.

경로 : software₩Microsoft₩windows₩ShellNoRoam₩MUICache₩
검색 : "DnF.exe", "Maplestory.exe", "FF2Client.exe"

해당 스트링이 존재하면 path를 버퍼에 저장하고 해당 경로에 DLL 파일을 복사한다.

```
check_game_path_and_copy_dll_("Dnf.exe");
if ( !Call__strcmpi_(Str1, algn_404E04) )
  check_MUICache_Path_of_game_("Dnf.exe");
Call_memst_(Str1, 0, 0x104u);
check_game_path_and_copy_dll_("MapleStory.exe");
if ( !Call__strcmpi_(Str1, algn_404E04) )
  check_MUICache_Path_of_game_("MapleStory.exe");
Call_memst_(Str1, 0, 0x104u);
check_game_path_and_copy_dll_("FF2Client.exe");
if ( !Call__strcmpi_(Str1, algn_404E04) )
{
  check_MUICache_Path_of_game_("FF2Client.exe");
```

이렇게 path를 모두 찾아 DLL 파일을 복사하면 자신을 삭제하고 루틴은 종료된다.

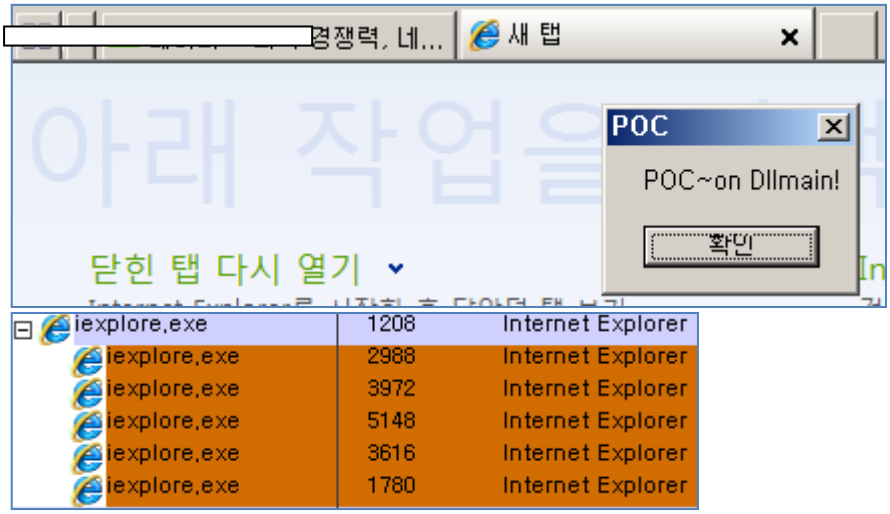
④ DLL 파일의 복사와 이유

결론부터 말하면 해당 path를 찾아 악성 DLL을 복사하는 이유는 "DLL Preloading" 기법을 이용하기 위해서다.

DLL Preloading 기법은 어플리케이션이 DLL을 로드할 때 Working directory부터 이루어진다는 점을 착안한 것인데 midimap.dll을 타겟이 되는 프로그램의 Working directory에 복사하면 아무런 제제 없이 프로세스에 로드되게 된다. 이는 system32폴더에 있는 정상

파일인 midimap.dll이 대부분의 응용프로그램에서 로드 된다는 것을 이용한 것이다.

앞서 IE레지스트리의 키를 "TabProcGrowth(Tab Process Growth)"를 '0'으로 설정하는 것도 위의 이유와 관련이 있는데 실제 POC 파일을 가지고 확인해 보니, TabProcGrowth 키를 생성하지 않은 상태에서 Tab을 여러 개 만들어 IE 자식 프로세스가 다수 생성되면 POC 파일이 불 특정하게 로드가 되었다.

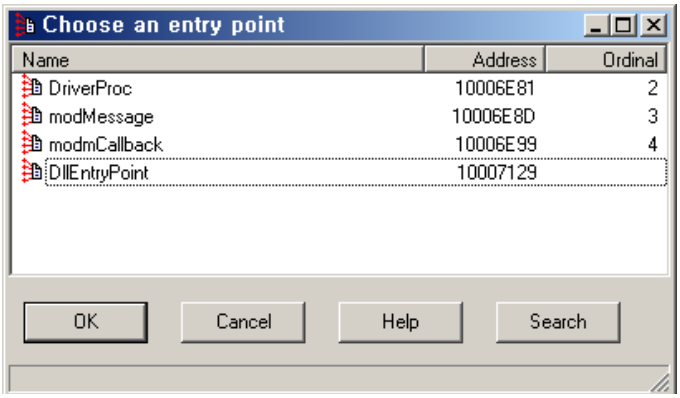


IE에서 악성 DLL이 로드되지 않으면 차후 javasrip.dll과 flash10d(*).ocx 파일의 수정이 되지 않아 사용자 정보탈취가 어렵게 된다.

⑤ midimap.dll(악성) 파일의 행위

파일명	midimap.dll
탐지명	Spyware.OnlineGames.mi
주요 행동	IE, DNF, Maplestory, FIFA2에 각각 로드되어 사용자 정보를 탈취한다.

midimap.dll 파일은 로드 시 바로 실행되기 위해 DllEntryPorint(winmain)에 바로 악성코드가 포함되어 있으며, 정상 midimap.dll의 API 함수 호출을 대비하여 다음과 같이 함수를 Export한다.



Export된 DriverProc, modMessage, modmCallback 함수는 호출 시 다음과 같이 system32의 midimap.dll을 로드하여 다시 해당 함수 주소 값을 호출하도록 되어있다.

```
GetSystemDirectoryA(&String1, 0x104u);
v10 = 0;
String2 = 'WW';
v3 = 'm';
v4 = 'i';
v5 = 'd';
v6 = 'i';
v7 = 'm';
v8 = 'a';
v9 = 'p';
lstrcatA(&String1, &String2);                   // system32\midimap
DLL_BaseAddress = (int)Call_LoadLibraryA(&String1);
```

악성 메인 코드를 살펴보면 다음과 같이 Thread 생성하여 작동한다.

```
loc_10006FAE:                           ; CODE XREF: DllMain(x,x,x)+63↑j
push    offset aIexplore_exe            ; "IEXPLORE.EXE"
call    _CreateThread_IE_               ; jscript.dll과 flash를 인라인 패치
mov     [esp+10Ch+var_10C], offset aDnf_exe ; "dnf.exe"
call    _CreateThread_DNF_
mov     [esp+10Ch+var_10C], offset aMaplestory_exe ; "MapleStory.exe"
call    _CreateThread_MapleStory_
mov     [esp+10Ch+var_10C], offset aFf2client_exe ; "FF2Client.exe"
call    _CreateThread_FF2_
```

각 스레드가 하는 행위는 간략하게 설명하자면 다음과 같다.

#IExplorer Thread

로드된 jscript.dll를 확인하여 c63f0c01 바이너리를 찾아서 5byte+"90 90 90"로 총 8byte 교체(후킹)한다.

실행 시 url을 확인하여 특정 사이트에 접속하면 id/pw를 탈취하도록 되어있다.

url -> df.nexon.com, pmang.com, nexon.com, itembay.com

메모리상에 "Flash"로 시작되는 모듈(ex: flash10b.ocx)도 확인하여 존재하면

0f3f3f3f3f3fff3f3f8b3fe83f3f3f3f8b3f853f0f3f3f3f3f3f6a 또는

0f3f3fb33f843f753f813f3f3f3f3f7d로 되어있는 바이너리를 찾아서 교체한다.

실행 시 "%s?a1=HG&a3=%s&a4=%s"이런 식으로 값을 저장하여 외부로 전송한다.

#DNF Thread

"Data", "pw" 스트링을 찾아 위와 같이 "%s?a1=HG&a3=%s&a4=%s" 형태로 외부에 전송

"user:%s pass:%s dis:%d level:%d money:%d" 스트링을 찾아

"%s?a1=%d&a3=%s&a4=%s&a10=%d&a11=%d&a9=%s" 형태로 외부에 전송

#MapleStory Thread

내부에서 "maple", 'id', "pw" 스트링을 찾아 위와 같이 "%s?a1=HG&a3=%s&a4=%s" 형태로 외부에 전송한다.

FF2Client Thread

npggNT.des (PMang GameGuard관련 프로그램)를 확인해서 inline patch한다.

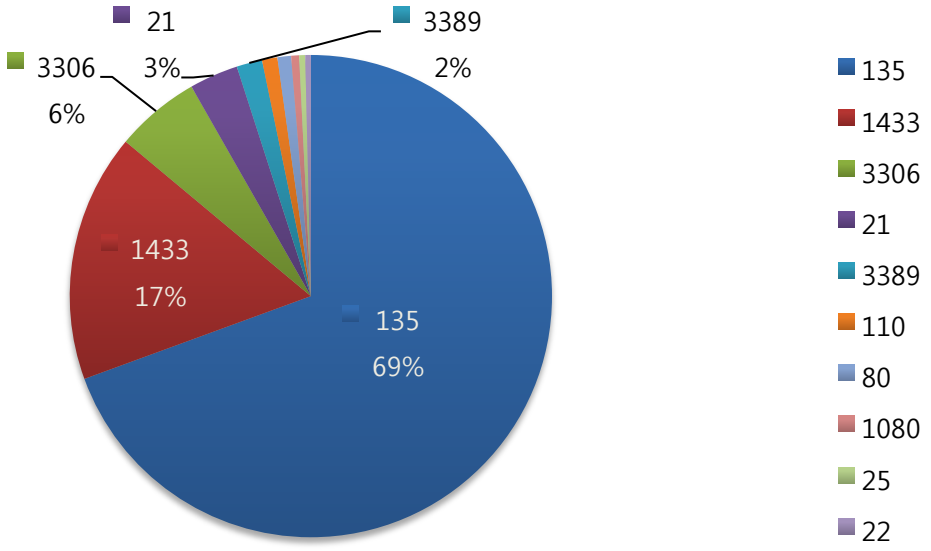
(3) 결론

DLL preloading 취약점과 IE TabProcGrowth 레지스트리 키를 확인해서 악성코드로부터의 피해를 최소화해야 한다.

Part I 4월의 악성코드 통계

3. 허니팟/트래픽 분석

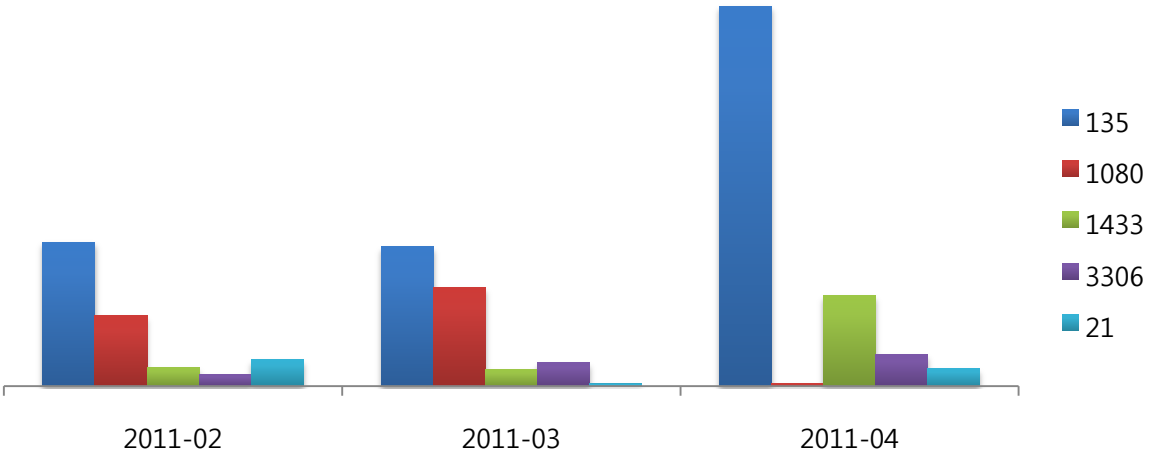
(1) 상위 Top 10 포트



이번 달에도 예전부터 사용되던 자동화된 코드로 취약점을 노리는 트래픽이 다수를 차지했다. 네트워크 관리자는 사용하지 않는 포트가 열려있는지 지속적으로 관심을 두고 확인해야 하며 일반 사용자는 자신이 사용하는 계정의 비밀번호를 주기적으로 교체하고 알약의 실시간 감시를 반드시 사용해야 한다.

(2) 상위 Top 5 포트 월별 추이

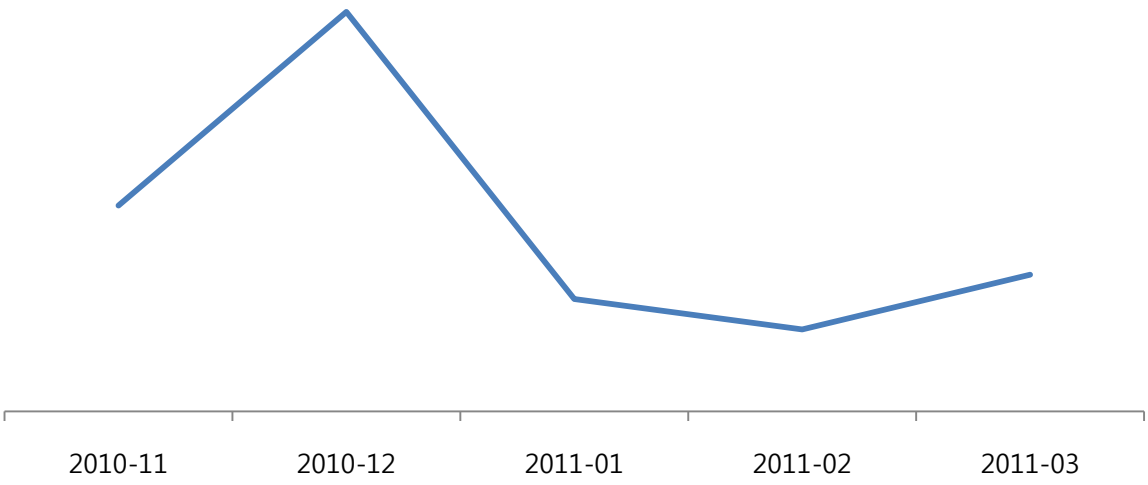
[2010년 02월 ~ 2011년 04월]



3개월간의 악성 트래픽 동향은 자동화된 공격으로 웹 서버의 계정을 탈취하려는 시도나 취약점을 이용해 악성코드를 감염시키려는 시도가 가장 많았으므로 자신이 운용하는 서버의 보안 패치나 계정 관리에 평소 늘 관심을 두어야 한다.

(3) 악성 트래픽 유입 추이

[2010년 11월 ~ 2011년 04월]

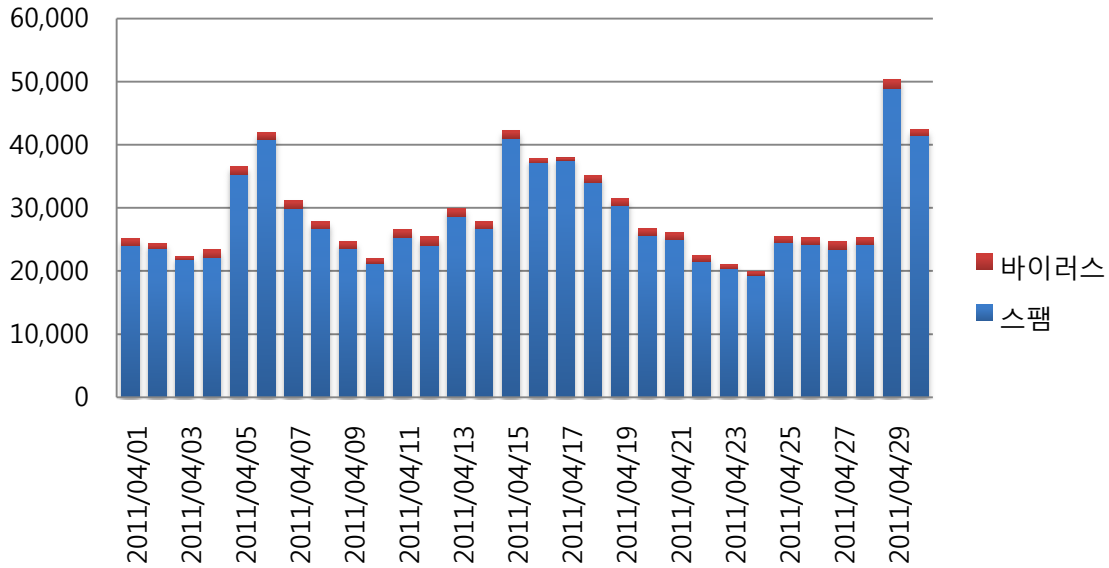


과거와 같이 알려진 취약점에 대한 자동화된 공격보다는 금전적인 목적을 갖거나, 이념이 상이한 국가의 중요 기관 네트워크를 마비시키기 위한 사이버전(戰)성격의 공격이 증가하고 있으므로 3.3 DDoS, 금융시스템 해킹과 같은 사건처럼 국가나 주요기업 등 특정 타겟에 대한 공격에 주의해야 한다. 특히 공격자가 대상 단체 구성원의 실수에 의해 생기는 보안 홀을 노려 공격하는 경우가 많으므로 우리의 보안의식이 매우 중요하다. 평소 기본적인 보안수칙들을 숙지하고 항상 실천해야 한다.

Part I 4월의 악성코드 통계

4. 스팸 메일 분석

(1) 일별 스팸 및 바이러스 통계 현황

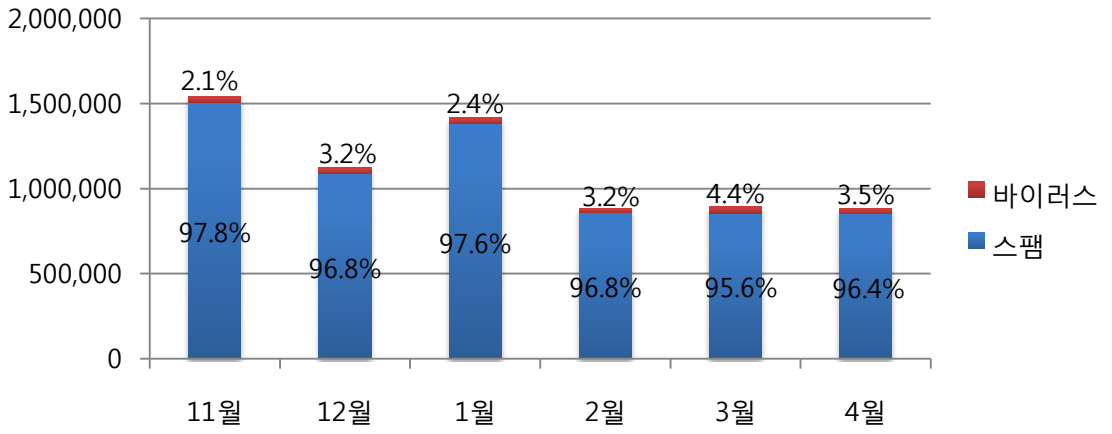


일 별 스팸 및 바이러스 통계 현황 그래프는 하루에 오는 바이러스 및 스팸메일의 개수를 나타내는 그래프이다. 4월 말부터 스팸 메일이 급증한 이유는 쇼핑몰의 주문 확인서로 위장한 스팸 메일 때문이며 이는 악성코드를 첨부해 유포하고 있다.

제목은 Successful ordre[임의숫자]이며 Order details.zip 파일이 첨부되어 발송되고 있다. 첨부된 파일은 윈도우 시스템에 존재하는 정상 svchost.exe를 강제로 실행한 후 해당 정상 파일의 메모리 영역에 자신의 코드 일부를 강제로 덮어 쓰게 한다. 메모리 영역 일부가 덮어 쓰여진 정상 svchost.exe의 프로세스는 특정 시스템으로 접속을 시도하여 접속이 성공하면 다른 파일을 다운로드 한다. 현재 다운로드 된 다른 파일은 pusk.exe로 실행하면 허위백신이 실행된다. 허위백신은 PC의 악성코드를 치료를 위해 비용을 지불 할 것을 요구한다. 주문하지도 않은 해외 쇼핑몰의 주문 확인 메일은 허위 백신을 설치하기 위한 목적으로 유포된 악성 스팸메일일 가능성이 매우 높으므로 피해를 예방하기 위해서는 의심스런 이메일을 열람하지 않으며, 이메일 안에 포함된 URL 링크나 첨부파일도 클릭하지 말아야 한다.

(2) 월별 통계 현황

[2010년 11월 ~ 2011년 04월]



월별 통계 현황은 악성코드 첨부 및 스팸메일이 전체메일에서 차지하는 비율을 나타내는 그래프이다. 4월의 스팸 메일은 96.4%, 바이러스 메일은 3.5%를 차지하였다. 3월에 비해서는 바이러스 메일 비율이 약 1% 증가 하였으며, 전체적인 메일 수신 량은 전 월과 비슷하였다.

(3) 스팸 메일 내의 악성코드 현황

[2011년 4월 1일 ~ 2011년 4월 30일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	12,342	39.86 %
2	W32/MyDoom-H	4,677	15.11 %
3	Mal/ZipMal-B	4,010	12.95 %
4	W32/Virut-T	2,013	6.50 %
5	W32/Bagz-D	1,348	4.35 %
6	W32/Lovgate-V	1,155	3.73 %
7	Mal/BredoZp-B	681	2.20 %
8	Troj/Invo-Zip	672	2.17 %
9	W32/Lovgate-F	375	1.21 %
10	W32/Bagle-CF	326	1.05 %

스팸메일 내의 악성코드 현황은 4월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프이다. 현재 W32/Mytob-C 이 39.86 %로 1위를 차지하였다. 2위는 15.11 %를 차지한 32/MyDoom-H, 3위는 12.95 %를 차지한 Mal/ZipMal-B이다.

Part Ⅱ 보안 이슈 돋보기

1. 4월의 보안 이슈

4월에는 고도의 보안시스템을 자랑하는 대형 금융기관들의 해킹피해가 연달아 발생하였습니다. 이번 사건들을 통하여 금융계 전체에 보안투자와 인적 보안관리의 중요성이 다시 인식되었으며 해킹 피해를 막기 위한 대책과 보안투자 계획들이 속속 발표되고 있습니다.

• 대형 시중은행에 데이터베이스 삭제 공격 발생

외부와 격리된 국내 은행의 내부망에 악성코드를 심은 뒤, 신용카드 사용내역 등 금융거래 정보가 기록된 은행 데이터베이스를 대량으로 삭제한 해킹사건이 발생하였습니다. 공격자는 몇 개월간의 치밀한 분석을 통해 시스템 내부 구조를 파악한 뒤, 서버 및 백업 시스템까지 모두 삭제하는 명령을 실행하여 복구에 상당한 기간이 소요되었습니다. 금전 취득의 목적을 가진 다른 해킹들과는 달리 금융거래를 교란, 사회 기간망을 뒤흔들었던 사건으로서 매우 심각한 보안사고로 인식되었습니다. 한편 검찰은 이번 공격을 북한의 소행으로 발표하였으며 이번 사건으로 인해 국가 차원의 금융보안대책들이 활발히 논의되고 있습니다.

• 금융기관 개인정보 유출 사고

또 다른 대형 금융기관에서는 조직적인 해커집단의 공격에 의해 수 십만 명의 고객 개인정보가 유출되는 사고가 발생하였습니다. 필리핀에 거점을 두고 수개월에 걸쳐 공격을 모의한 해커집단은 이번 공격으로 대량의 개인정보를 훔친 뒤 이를 공개하겠다며 피해 기관을 협박해 거액을 요구하였습니다. 모 시중은행의 데이터베이스 삭제 사건과는 공격 목적이 다르지만 대형금융기관이 연달아 해킹 당했다는 점에서 금융계 전체에 대한 준비와 대책이 필요해 보입니다.

• 아이폰 위치정보 무단 저장 논란

국내에도 많은 소비자를 확보하고 있는 애플사의 아이폰이 사용자 위치정보 무단 저장 논란에 휩싸였습니다. 전 세계 아이폰 사용자들의 거센 반발이 있었으며 실제로 아이폰 내에 저장된 특정 위치정보파일을 분석한 결과, 휴대폰 사용자의 동선이 그대로 드러났습니다. 애플사는 이에 대해 와이파이 접속을 원활히 하기 위한 기지국정보를 저장한것이라고 발표했으며 5월 초, 패치를 통해 위치정보를 수집하지 않거나 해당 파일을 삭제할 수 있도록 iOS를 수정 하면서 논란이 일단락 되었습니다.

<와이파이 로그파일에서 추출한 위치정보>

• 소니 PSN 해킹당해 수 천만 명 개인정보 유출

해커와의 법정공방을 벌이던 소니社가 초유의 개인정보 유출사고를 당했습니다.
소니 측은 4월 26일, 자사의 공식 블로그를 통해 "플레이스테이션 네트워크와 큐리오시티 온라인 고객 7700만명의 개인정보를 해커가 훔쳐갔을 수 있다"고 공식 발표했으며, 한국 방통위는 두 서비스에 (www.playstation.co.kr, www.qriocity.com) 가입되어있는 사용자들에게 "동일한 비밀번호를 사용한 타 사이트가 있다면 반드시 비밀번호는 변경할 것"을 권고 했습니다. 해당사이트의 국내 이용자는 국내 이용자는 23만명 이상일것으로 추정되고 있습니다.

• 7월부터 개인정보 제3자 동의 안해도 된다.

지금까지는 '개인정보 제3자 제공 동의'가 필요하지 않은 서비스에서도 약관을 의무적으로 동의하게 하거나 동의하지 않으면 아예 가입이 되지 않는 서비스가 많았습니다.
4월 5일, 개정 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'이 공포되어 7월부터 시행됩니다. 법 개정에 따라 앞으로는 불필요한 '개인정보 제3자 제공' 약관에 동의하지 않아도 웹사이트등의 서비스에 가입할 수 있게 되었습니다.

Part Ⅱ 4 월의 이슈 돋보기

2. 4월의 취약점 이슈

• Microsoft 4월 정기 보안 업데이트

Internet Explorer 취약점으로 인한 원격코드 실행 문제, SMB 클라이언트 및 서버의 취약점으로 인한 원격코드 실행 문제, Microsoft Excel, PowerPoint, Office 취약점으로 인한 원격코드 실행 문제, MHTML 취약점으로 인한 정보유출 문제 등을 해결한 Microsoft 4월 정기 보안 업데이트를 발표하였습니다.

<해당 제품>

- **Windows XP**
- **Windows Vista**
- **Windows 7**
- **Windows Server 2003**
- **Windows Server 2008**
- **Microsoft Office (MS11-029, MS11-021, MS11-022, MS11-023)**

<취약점 목록>

Internet Explorer 누적 보안 업데이트(2497640)

이 보안 업데이트는 Internet Explorer에 대해 비공개적으로 보고된 취약점 4건과 공개된 취약점 1건을 해결합니다. 이 보안 업데이트의 심각도는 Windows 클라이언트의 Internet Explorer 6, Internet Explorer 7 및 Internet Explorer 8에 대해서는 긴급이며, Windows 서버의 Internet Explorer 6, Internet Explorer 7 및 Internet Explorer 8에 대해서는 보통입니다. Internet Explorer 9은 이 취약점의 영향을 받지 않습니다.

가장 위험한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 이러한 취약점 중 하나를 성공적으로 악용한 공격자는 로컬 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

SMB 클라이언트의 취약점으로 인한 원격 코드 실행 문제점(2511455)

이 보안 업데이트는 Microsoft Windows의 공개된 취약점 1건과 비공개적으로 보고된 취약점 1건을 해결합니다. 이 취약점으로 인해 공격자가 특수하게 조작된 SMB 응답을 클라이언트가 시작한 SMB 요청에 보낼 경우 원격 코드 실행이 발생할 수 있습니다. 이 취약점을 악용하려면 공격자는 사용자가 특수하게 조작된 SMB 서버에 SMB 연결을 시작하도록 유도해야 합니다.

SMB 서버의 취약점으로 인한 원격 코드 실행 문제점(2508429)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 취약점으로 인해 공격자가 특수하게 조작된 SMB 패킷을 만들어 영향을 받는 시스템에 보

내는 경우 원격 코드 실행이 허용될 수 있습니다. 방화벽 구성 모범 사례와 표준 기본 방화벽 구성을 이용하면 기업 경계 외부에서 이 취약점을 악용하려는 공격으로부터 네트워크를 보호할 수 있습니다.

ActiveX 킬(Kill) 비트 누적 보안 업데이트(2508272)

이 보안 업데이트는 Microsoft 소프트웨어에 대해 비공개적으로 보고된 취약점 2건과 공개된 취약점 1건을 해결합니다. 이러한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특정 ActiveX 컨트롤을 인스턴스화하는 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다. 또한 이 업데이트에는 3개의 타사 ActiveX 컨트롤에 대한 킬(Kill) 비트도 포함되어 있습니다.

.NET Framework의 취약점으로 인한 원격 코드 실행 문제점(2484015)

이 보안 업데이트는 Microsoft .NET Framework의 공개된 취약점을 해결합니다. 사용자가 XBAP(XAML 브라우저 응용 프로그램)을 실행할 수 있는 웹 브라우저를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 이 취약점으로 인해 클라이언트 시스템에서 원격 코드가 실행될 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다. 서버에서 ASP.NET 페이지 처리를 허용하고 공격자가 해당 서버에 특수하게 조작한 ASP.NET 페이지를 성공적으로 업로드하여 실행할 경우 이 취약점으로 인해 IIS를 실행하는 서버 시스템에서 원격 코드 실행이 허용될 수 있습니다. 이러한 경우는 웹 호스팅 시나리오에서 발생할 수 있습니다. 이 취약점은 CAS(코드 액세스 보안) 제한을 우회하기 위해 Windows .NET 응용 프로그램에서 사용될 수도 있습니다.

GDI+의 취약점으로 인한 원격 코드 실행 문제점(2489979)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows GDI+의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 영향을 받는 소프트웨어를 사용하여 특수하게 조작된 이미지를 보거나 특수하게 조작된 콘텐츠가 포함된 웹사이트를 탐색할 경우 원격 코드 실행이 허용될 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

DNS 확인 취약점으로 인한 원격 코드 실행 문제점(2509553)

이 보안 업데이트는 비공개적으로 보고된 Windows DNS 확인의 취약점을 해결합니다. 이 취약점을 악용한 공격자가 네트워크에 액세스하고 특수하게 조작된 LLMNR 브로드캐스트 쿼리를 대상 시스템에 보내는 사용자 지정 프로그램을 만들 경우 원격 코드 실행이 허용될 수 있습니다. 최선의 방화벽 구성 방법과 표준 기본 방화벽 구성을 이용하면 기업 경계 외부에서 들어오는 공격으로부터 네트워크를 보호할 수 있습니다. 인터넷과 연결되는 시스템의 경우, 필요한 포트만 최소한으로 열어 두는 것이 안전합니다. 이런 경우 LLMNR 포트를 인터넷에서 차단해야 합니다.

JScript 및 VBScript 스크립팅 엔진의 취약점으로 인한 원격 코드 실행 취약점(2514666)
이 보안 업데이트는 비공개적으로 보고된 JScript 및 VBScript 스크립팅 엔진의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 웹 사이트를 방문할 경우 원격 코드 실행이 허용될 수 있습니다. 공격자는 강제로 사용자가 웹 사이트를 방문하도록 할 수 없습니다. 대신 공격자는 사용자가 전자 메일 메시지 또는 메신저 메시지의 링크를 클릭하여 공격자의 웹 사이트를 방문하도록 유도하는 것이 일반적입니다.

OpenType CFF(Compact Font Format) 드라이버의 취약점으로 인한 원격 코드 실행 문제점(2507618)
이 보안 업데이트는 비공개적으로 보고된 OpenType CFF(Compact Font Format) 드라이버의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 CFF 글꼴로 렌더링된 콘텐츠를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 특수하게 조작된 콘텐츠를 보도록 만들 수는 없습니다. 대신 공격자는 사용자가 전자 메일 메시지 또는 메신저 메시지의 링크를 클릭하여 공격자의 웹 사이트를 방문하도록 유도하는 것이 일반적입니다.

Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점(2489279)
이 보안 업데이트는 Microsoft Office에서 발견되어 비공개적으로 보고된 취약점 9건을 해결합니다. 사용자가 특수하게 조작된 Excel 파일을 열면 이러한 취약점으로 인해 원격 코드 실행이 허용될 수 있습니다. 이러한 취약점 중 하나를 성공적으로 악용한 공격자는 로그온한 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점(2489283)
이 보안 업데이트는 Microsoft PowerPoint에서 발견되어 비공개적으로 보고된 3건의 취약점을 해결합니다. 이러한 취약점으로 인해 사용자가 특수하게 조작된 PowerPoint 파일을 열 경우 원격 코드 실행이 발생할 수 있습니다. 이러한 취약점 중 하나를 성공적으로 악용한 공격자는 로컬 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다. Microsoft 기술 자료 문서 2501584에서 사용할 수 있는 PowerPoint 2010, "PowerPoint 2010의 제한된 보기에서 편집을 사용하지 않도록 설정"에 대한 Microsoft Fix it 자동화 솔루션은 CVE-2011-0655 및 CVE-2011-0656에 설명된 취약점을 악용하는 공격 경로를 차단합니다.

Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점(2489293)
이 보안 업데이트는 Microsoft Office의 공개된 취약점 1건과 비공개적으로 보고된 취약점 1건을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 Office 파일을 열거나 특수하게 조작된 라이브러리 파일과 동일한 네트워크 디렉터리에 있는 합법적인

Office 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 이러한 취약점 중 하나를 성공적으로 악용한 공격자는 로그온한 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Windows 팩스 표지 편집기의 취약점으로 인한 원격 코드 실행 문제점(2527308)

이 보안 업데이트는 Microsoft Windows에서 발견되어 공개적으로 보고된 취약점 2건을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 팩스 표지 파일(.cov)을 Windows 팩스 표지 편집기를 사용하여 열 경우 원격 코드 실행이 허용될 수 있습니다. 이러한 취약점 중 하나를 성공적으로 악용한 공격자는 로그온한 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

MFC(Microsoft Foundation Class) 라이브러리의 취약점으로 인한 원격 코드 실행 문제점(2500212)

이 보안 업데이트는 MFC(Microsoft Foundation Class) 라이브러리를 사용하여 만든 특정 응용 프로그램의 일반에 공개된 취약점을 해결합니다. 이 취약점으로 인해 사용자가 영향을 받는 응용 프로그램과 연결된 합법적인 파일 및 특수하게 조작된 라이브러리 파일과 동일한 네트워크 폴더에 있는 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 공격에 성공하려면, 사용자가 신뢰할 수 없는 원격 파일 시스템 위치 또는 WebDAV 공유를 방문하거나 이러한 위치에서 영향을 받는 응용 프로그램이 로드되는 문서를 열어야 합니다.

MHTML의 취약점으로 인한 정보 유출 문제점(2503658)

이 보안 업데이트는 일반에 공개된 Microsoft Windows MHTML 프로토콜 처리기의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 웹 사이트를 방문할 경우 정보 유출이 발생할 수 있습니다. 웹 기반의 공격 시나리오에서 웹 사이트는 이 취약점을 악용하는 데 사용되는 특수하게 조작된 링크를 포함하고 있을 수 있습니다. 공격자는 사용자가 웹 사이트를 방문하고 특수하게 조작된 링크를 열도록 유도해야 합니다.

워드패드 텍스트 변환기의 취약점으로 인한 원격 코드 실행 문제점(2485663)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 보안 업데이트의 심각도는 지원 대상인 모든 Windows XP 및 Windows Server 2003 에디션에 대해 중요입니다. 지원 대상인 모든 Windows Vista, Windows Server 2008, Windows 7 및 Windows Server 2008 R2 에디션은 이 취약점의 영향을 받지 않습니다.

이러한 취약점으로 인해 사용자가 WordPad를 사용하여 특수하게 조작된 파일을 열 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.

Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점(2506223)

이 보안 업데이트는 Microsoft Windows에서 발견되어 비공개적으로 보고된 취약점 30건을 해결합니다. 이 취약점으로 인해 공격자가 시스템에 로컬로 특수하게 조작한 응용 프로그램을 실행할 경우 권한 상승이 허용될 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그온 자격 증명을 가지고 로컬로 로그온할 수 있어야 합니다. 익명의 사용자에 의해서나 원격으로는 이 취약점을 악용할 수 없습니다.

<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-apr.mspx

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

• Adobe Flash Player 신규 취약점 업데이트 권고

CVE Number : CVE-2011-0611

Adobe Flash Player에 영향을 주는 취약점을 해결한 보안 업데이트가 발표되었습니다. 공격자는 스팸 메일, 메신저의 링크 등을 통해 특수하게 조작된 Flash파일이 삽입된 엑셀 및 MS워드 파일을 사용자가 열어보도록 유도하여 악성코드를 유포할 수 있으므로 주의가 필요하며 낮은 버전의 Flash Player 사용하고 있다면 최신버전으로 업데이트 해야 합니다.

<해당 제품>

- Adobe Flash Player 10.2.153.1 및 이전 버전
- 크롬 웹브라우저에서 사용하는 Adobe Flash Player 10.2.154.25 및 이전 버전
- 안드로이드 환경에서 동작하는 Adobe Flash Player 10.2.156.12 및 이전 버전
- Adobe AIR 2.6.19120 및 이전 버전

<해결책>

Adobe Flash Player Download Center에서 Adobe Flash Player 최신 버전을 설치하거나 자동 업데이트를 이용하여 최신버전으로 업그레이드 하시기 바랍니다.

http://get.adobe.com/kr/flashplayer

http://get.adobe.com/kr/air/

<참고 사이트>

http://www.adobe.com/support/security/bulletins/apsb11-07.html

• Adobe Flash Reader/Acrobat 신규 취약점 보안업데이트 권고

CVE Number : CVE-2011-0611, CVE-2011-0610

Adobe Acrobat/Reader에 영향을 주는 취약점을 해결한 보안 업데이트가 발표되었습니다. 신규 취약점이 발견되었습니다. 본 취약점을 이용하여 악성코드를 유포할 수 있으므로 주의가 필요하며 낮은 버전의 Flash Player 사용하고 있다면 최신버전으로 업데이트 해야 합니다.

<해당 제품>

- 윈도우 환경에서 동작하는 Adobe Reader 10.0.1 및 이전 버전
- AcrobatX 10.0.2 및 이전 버전

<해결책>

Adobe Download Center에서 Adobe Flash Player 최신 버전을 설치하거나 자동 업데이트를 이용하여 최신버전으로 업그레이드 하시기 바랍니다.

http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Windows

http://www.adobe.com/support/downloads/product.jsp?product=1&platform=Windows

<참고 사이트>

http://www.adobe.com/support/security/bulletins/apsb11-08.html

• ipTIME유무선 공유기 취약점 보안 업데이트 권고

EFM-Networks社의 제품인 ipTIME유무선 공유기 전 제품에 영향을 주는 취약점을 해결한 보안업데이트가 발표되었습니다.

해당 취약점은 관리자 패스워드가 설정되지 않은 취약한 환경에서 발생하며, 공격자는 장비에 대한 명령 실행 및 백도어 설치가 가능하므로 낮은 버전의 펌웨어를 사용하고 있다면 최신버전으로 업데이트 해야 합니다.

<해당 제품>

- ipTIME 2WAM을 제외한 펌웨어 7.52 및 이전버전 전 제품

<해결책>

제조사 홈페이지에서 [고객지원] – [다운로드] – [펌웨어]를 클릭하여 각 제품의 펌웨어를 7.62 버전으로 업데이트

http://iptime.co.kr/~iptime/bbs/view.php?id=notice&no=522

<참고 사이트>

http://iptime.co.kr/~iptime/

Contact us…

㈜이스트소프트 알약보안대응팀

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr

http://www.bizhard.com/Center/News/Event_Read.aspx?nid=13