www.alyac.co.kr

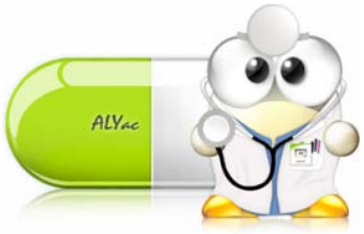
피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차



Part I 12월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

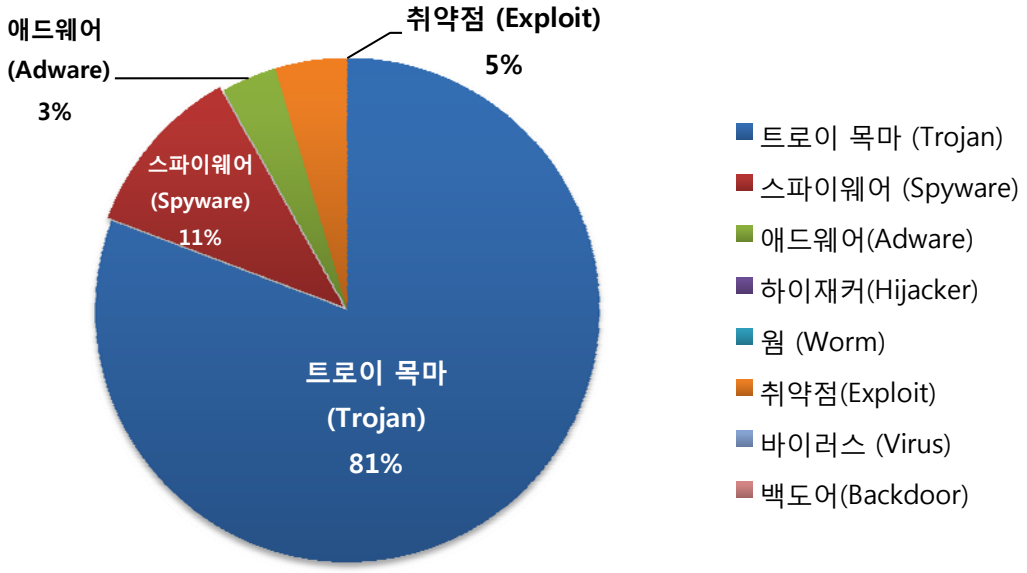
[2010년 12월 1일 ~ 2010년 12월 31일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	New	Trojan.Downloader.JNSD	Trojan	117,855
2	New	Trojan.Script.473910	Trojan	92,446
3	New	Variant.Downloader.73	Trojan	66,185
4	↓1	S.SPY.Lineag-GLG	Spyware	40,670
5	↓3	V.TRJ.Patched.imm	Trojan	35,080
6	↑2	Variant.Kazy.5867	Trojan	35,080
7	New	Exploit.CVE-2010-3962.C	Exploit	28,952
8	New	S.SPY.OnlineGames.imm	Spyware	28,683
9	↓1	Trojan.Generic.5181405	Trojan	28,650
10	New	V.TRJ.Clicker.Winsoft	Trojan	28,113
11	New	Trojan.Script.473934	Trojan	27,868
12	New	V.DWN.el.39xxxx	Trojan	25,807
13	↓11	Trojan.Generic.5190481	Trojan	23,628
14	New	A.ADV.Admoke	Adware	22,327
15	New	Variant.Kazy.6420	Trojan	20,109

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

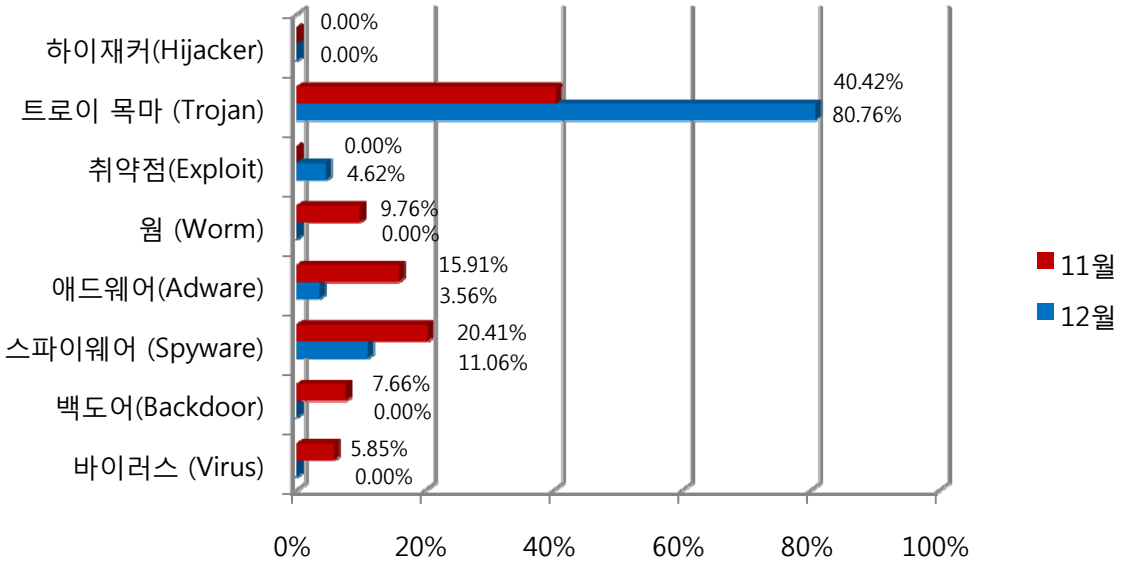
감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.
12월의 감염 악성코드 TOP 15는 Trojan.Downloader.JNSD가 117,855건으로 TOP 15 중 1위를 차지하였으며, Trojan.Script.473910이 92,446건으로 2위, Variant.Downloader.73가 66,185건으로 3위를 차지하였다. 이외에도 12월에 새로 Top 15에 진입한 악성코드는 10종이다.
12월에는 MS Internet Explorer의 보안 취약점(CVE-2010-0806)를 이용한 악성코드 유포 사례가 가장 많이 보고되었다. 또한 IT 관리자의 대응이 어려운 주말 기간 동안 주로 언론사 및 보안이 취약한 인터넷 사이트에 악성 스크립트를 삽입해 유포하는 경우가 많았다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율은 이번달에도 트로이 목마(Trojan)가 81%로 가장 많은 비율을 차지하였고, 전달에 비해 트로이목마 (Trojan) 비율이 2배 이상 증가하였다. (41% 비율↑)
12월에는 보안이 취약한 홈페이지를 통한 악성코드 유포 때문에 Trojan의 비율이 크게 증가하였다. 또한 악성코드 설치를 위하여 PC의 보안 취약점을 이용하기 때문에 취약점(Exploit)의 비율 또한 함께 증가하였다.

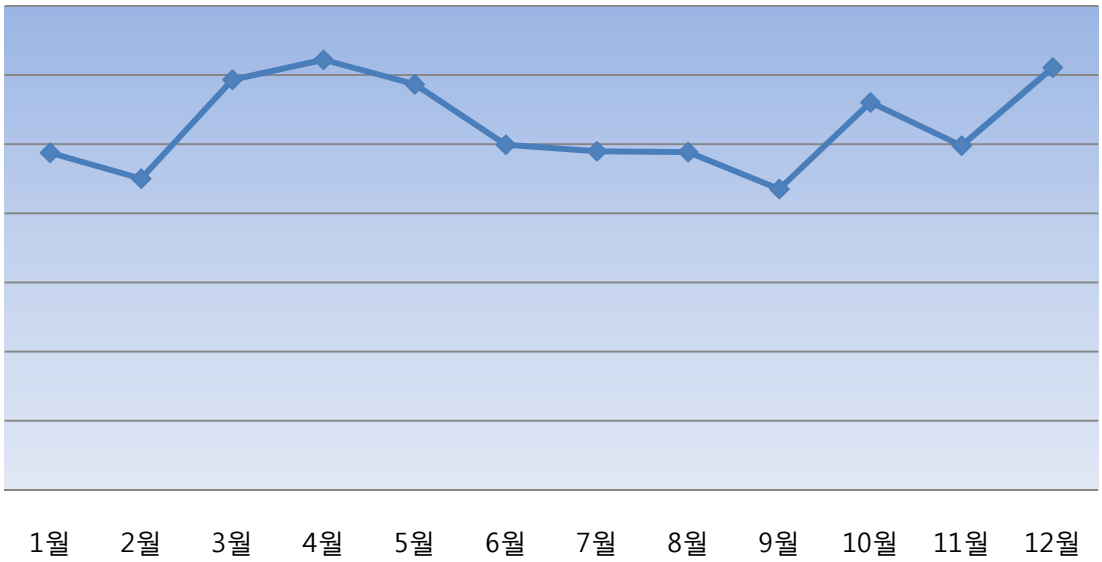
(3) 카테고리별 악성코드 비율 전월 비교



카테고리별 악성코드 비율을 전월과 비교하면, 트로이 목마(Trojan)와 취약점(Exploit)가 전달에 비해 크게 증가였으며, 대부분의 다른 악성코드는 비율이 감소했음을 알 수 있다. (바이러스, 취약점 등의 경우 Top15를 기준으로 했을 때 차지하는 비율이 없다는 것이다.)

(4) 월별 피해 신고 추이

[2010년 1월 ~ 2010년 12월]

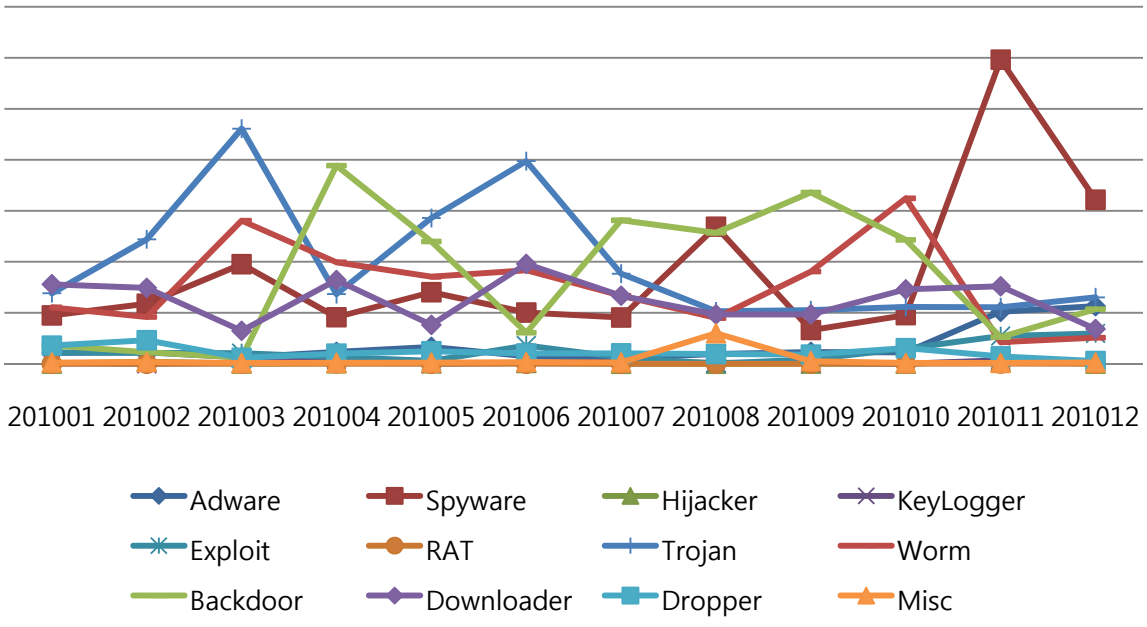


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프이다. 12월의 경우 전달(11월)보다 신고 건수가 다시 증가하였다.

(5) 월별 악성코드 DB 등록 추이

[2010년 1월 ~ 2010년 12월]



12월은 스파이웨어(Spyware) 계열의 악성코드 변종이 가장 많이 등록 되었지만 전달에 비해서는 크게 감소되었다. 다음으로 트로이목마 악성코드(Trojan)가 많이 등록되었다. 이번 달 스파이웨어(Spyware)는 MS Internet Explorer 취약점을 이용하는 악성코드의 DB 등록이 급증하였다.

Part I 12월의 악성코드 통계

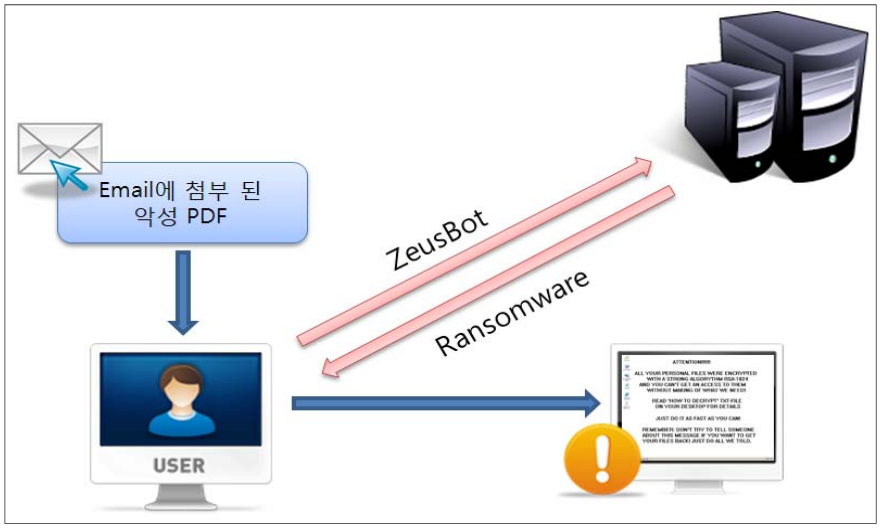
2. 악성코드 이슈 분석 – "PC 사용자에게 금품을 요구하는 랜섬웨어(Ransomware)"

이번에 분석 내용은 PC 사용자에게 금품을 요구하는 악성코드인 랜섬웨어(Ransomware)에 대해 알아본다. 우선 랜섬웨어(ransomware)의 정의는 "미국에서 발견된 스파이웨어 등의 신종 악성 프로그램." 컴퓨터 사용자의 문서를 볼모로 잡고 금품을 요구한다고 해서 '랜섬(ransom)'이란 수식어가 붙었다.

인터넷 사용자의 컴퓨터에 잠입해 내부 문서나 스프레이시트, 그림 파일 등을 제멋대로 암호화해 열지 못하도록 만들거나 첨부된 이메일 주소로 접촉해 돈을 보내 주면 해독용 열쇠 프로그램을 전송해 준다며 금품을 요구하는 프로그램을 뜻한다.

1) 유포 경로

현재까지 이메일을 통해 전파 된 것으로 확인되며, 첨부파일로 삽입 된 악성 PDF를 실행하면 Zbot이 실행 되어 특정 서버에서 랜섬웨어 파일을 다운로드 한다.



<랜섬웨어 악성코드 실행단계>

2) 파일 분석 – V.TRJ.Ransom.10752

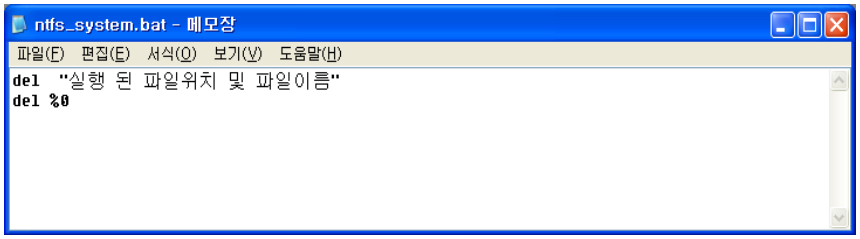
① 리소스 로드

파일이 가지고 있는 리소스 중 "cfg" 데이터를 복호화 하여, 차후 사용자에게 보여 줄 텍스트 파일(HOW TO DECRYPT FILES.txt)의 내용을 만든다.

pFile	Raw Data	Value
00005C74	79 AD A8 B1 2A 58 19 A6 C0 70 B1 69 A4 0A 9B 7D	y . . . *X . . . p . i . . . }
00005C84	78 A8 A8 B1 2A 58 81 A5 C0 70 B8 60 84 2A BB 3C	x . . . *X . . . p . ` . * . <
00005C94	0D D9 CD DF 5E 31 76 C8 E1 51 90 49 84 2A BB 70	. . . . ^1v . . Q . I . * . p
00005CA4	73 EC C4 DD 0A 21 76 D3 B2 50 C1 0C D6 79 F4 13	s . . . . !v . . P . . . y . .
00005CB4	18 C1 88 D7 43 34 7C D5 E0 58 C1 01 CB 7E F4 51	. . . . C4 | . . X . . . ~ . Q
00005CC4	59 C9 C7 D2 5F 35 7C C8 B4 03 9D 49 D0 6F E3 09	Y . . . _5 | . . . . I . o . .
00005CD4	0A 81 88 D5 4B 2C 78 C4 A1 03 D4 1A 88 2A F8 18	. . . . K , x . . . . . * . .
00005CE4	0B D9 C1 D7 43 3B 78 D2 A5 03 9D 49 CF 7D F6 50	. . . . C ; x . . . . I . } . P
00005CF4	1F C4 C4 D4 59 74 39 D0 A9 14 D4 06 8D 2A F3 1C	. . . . Y t 9 . . . . . * . .
00005D04	0F C8 88 D3 4F 3D 77 86 A5 1E D2 1B DD 7A EF 18	. . . . O = w . . . . . z . .
00005D14	1D 8D CA C8 0A 39 39 D0 A5 02 C8 49 D7 7E E9 12	. . . . . 99 . . . . I . ~ . .
00005D24	17 CA 88 D2 53 28 71 C3 B2 50 E3 3A E5 27 AA 4D	. . . . S (q . . P . : . ' . M
00005D34	4B 99 86 91 7E 30 7C 86 AF 02 D8 0E CD 64 FA 11	K . . . ~ 0 | . . . . . d . .

② 뮤텍스(Mutex) 확인

Mutex("ilold") 확인 후 존재하면 ntfs_system.bat 파일을 생성하여 실행 된 파일을 삭제하고 프로그램을 종료한다. 동일한 Mutex가 없으면 스레드를 생성한다.



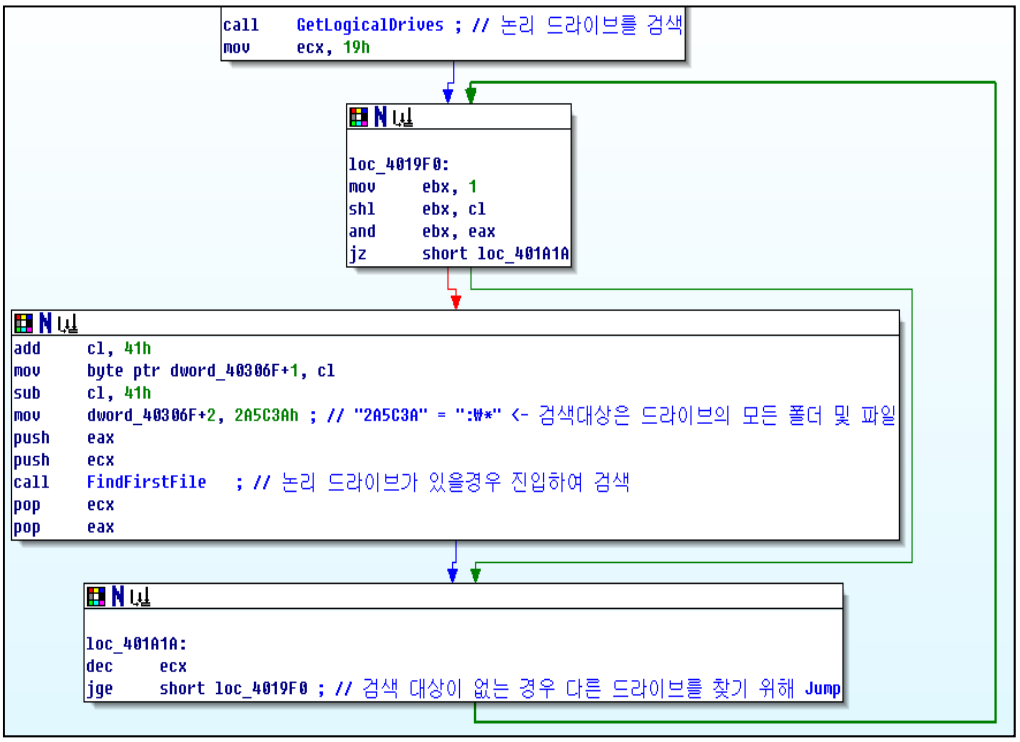
<Nftf_system.bat 파일의 내용>

③ 드라이브 찾기

감염된 시스템에서 논리 드라이브로 이루어진 D드라이브를 찾는다.

D드라이브에서 폴더와 파일을 검색하여 자신이 찾는 확장자가 없는 경우 또는 D드라이브가 없는 경우에 C드라이브로 타겟을 변경하여 검색한다.

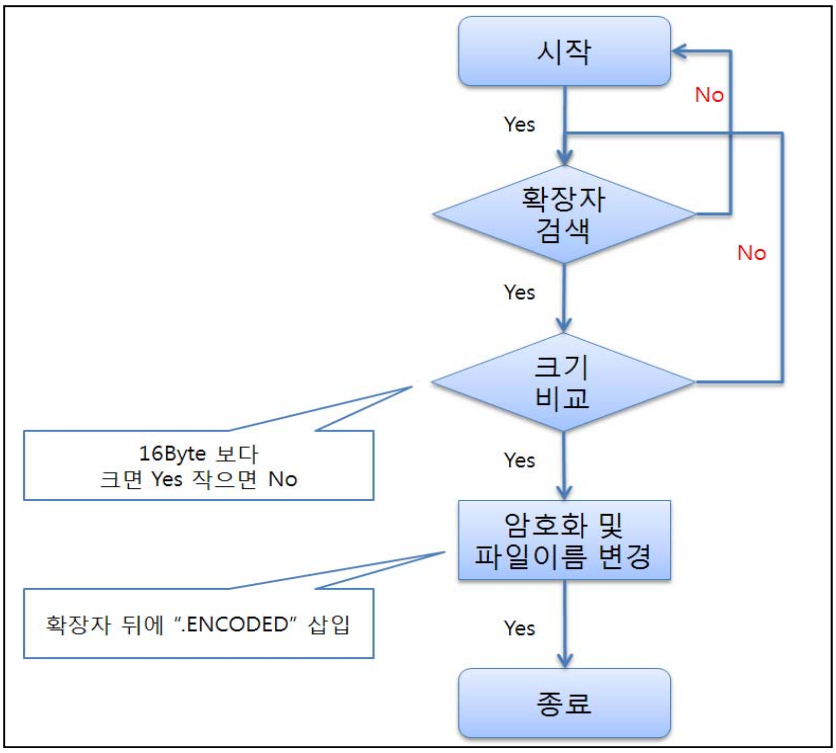
(악성코드는 일반적으로 C:₩를 먼저 스캔하는 경우가 많은데 해당 악성코드는 사용자들이 문서 및 백업파일을 D드라이브에 저장하는 습관을 잘 알고 있다.)



④ 확장자 검색

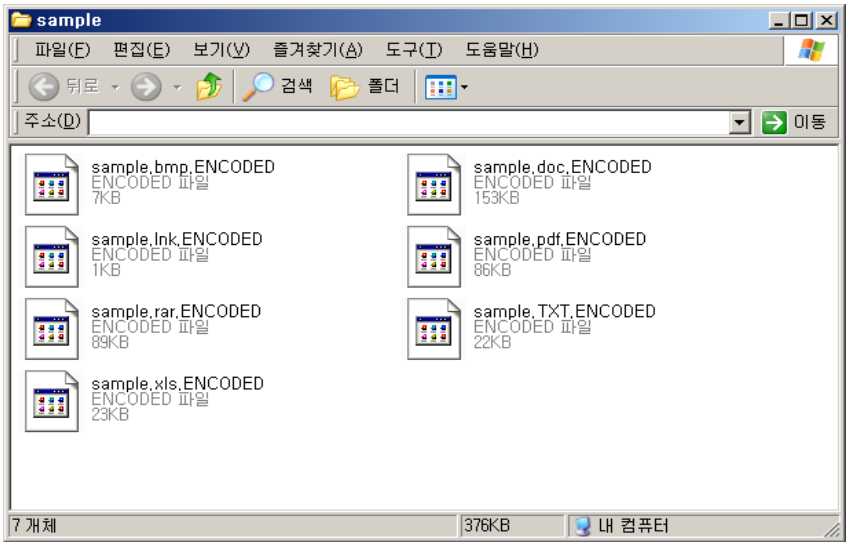
***.jpg, *.jpeg, *.psd, *.cdr, *.dwg, *.max, *.mov, *.m2v, *.3gp, *.doc, *.docx, *.xls, *.xlsx, *.ppt, *.pptx, *.rar, *.zip, *.mdb, *.mp3, *.cer, *.p12, *.pfx, *.kwm, *.pwm, *.txt, *.pdf, *.avi, *.flv, *.lnk, *.bmp, *.1cd, *.md, *.mdf, *.dbf, *.mdb, *.odt, *.vob, *.ifo, *.mpeg, *.mpg, *.doc, *.docx, *.xls, *.xlsx**

검색 중 자신이 찾는 확장자 존재 시 원본 파일을 암호화 시키고 확장자 뒤에 ".ENCODED" 문자열을 추가시킨다.



<악성파일이 정상적인 파일을 암호화 및 파일명을 변경하는 순서도>

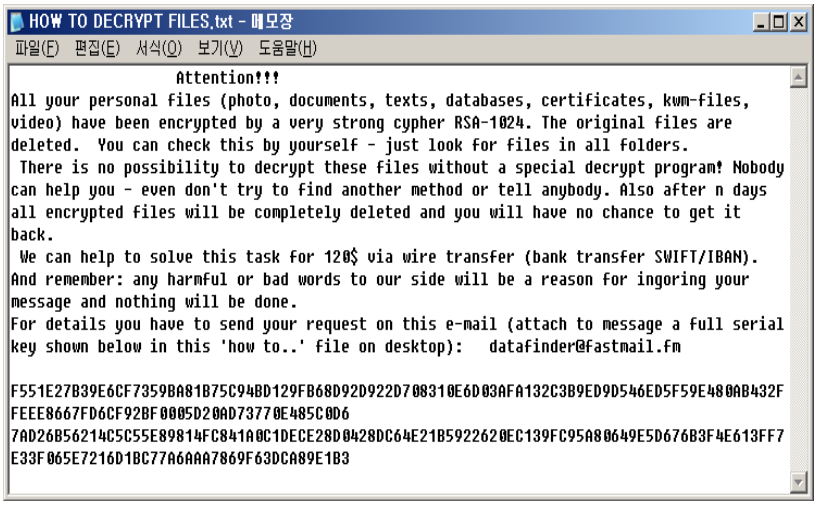
위 순서도에 따라 바뀌어진 파일들은 다음과 같은 모습으로 바뀐다.



<감염된 파일의 모습>

⑤ 스레드 생성

시스템 바탕화면에 HOW TO DECRYPT FILES.txt 파일을 생성하고, 처음에 실행 되었던 "cfg" 리소스에서 가져온 복호화 데이터를 txt파일에 삽입 후 사용자에게 보여준다.



<파일들은 RSA-1024로 암호화가 되어있으며, $120를 송금하라는 텍스트 파일 화면>

파일 리소스 중 "Wall"에 저장 된 데이터를 바탕으로 랜덤(16자리)의 BMP파일을 사용자 %TEMP% 폴더에 생성한다. 생성 된 BMP파일은 시스템의 바탕화면으로 사용된다.

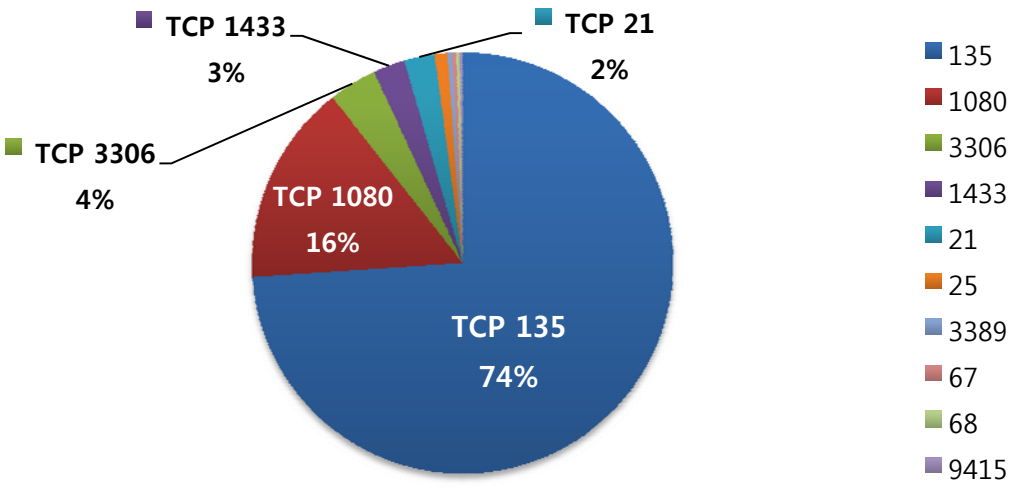
3) 유포 경로

이번 랜섬웨어에 감염 시 업무에 지장이 될 수 있는 문서파일과 그림파일, 압축파일 등이 암호화 되어 사용자의 불편을 일으키기 때문에 기업의 경우 막대한 손해가 발생 될 수 있다. 따라서 사용자는 확인되지 않은 메일에 첨부 된 파일을 실행해서는 안되며, 운영체제의 보안 업데이트 및 취약점이 존재하는 소프트웨어의 업데이트를 생활화해야 한다. 특히 중요한 문서 및 자료들을 항상 백업하는 습관을 가져야하겠다.

Part I 12월의 악성코드 통계

3. 허니팟/트래픽 분석

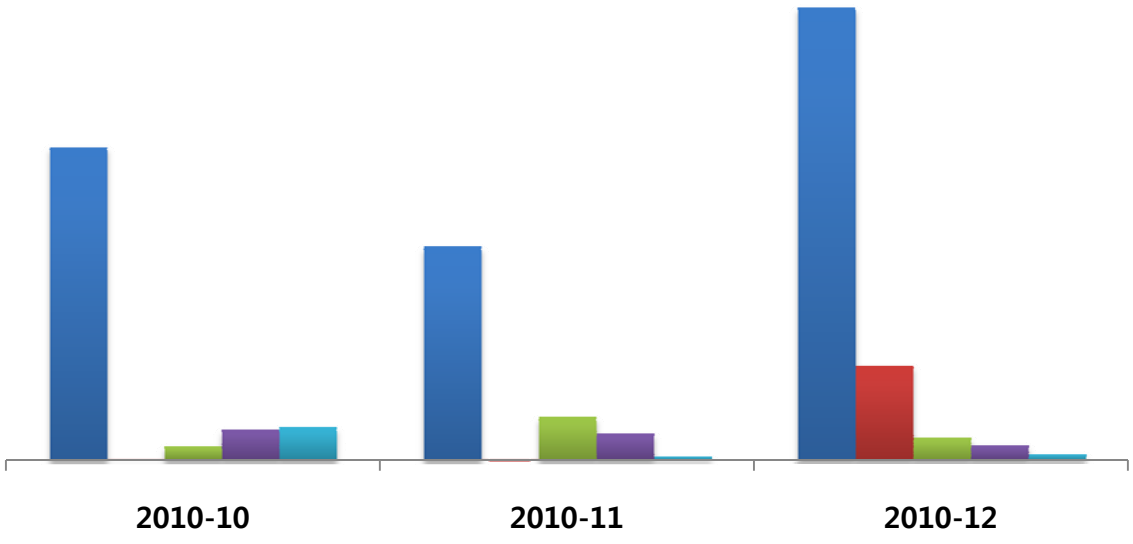
(1) 상위 Top 10 포트



12월 초부터 TCP 1080 포트를 통한 트래픽 유입이 크게 증가했다. TCP 1080 포트는 대표적으로 MyDoom, Proxmeg, Bugbear, Hagbard, Daemoni, Lixy 악성코드가 사용한 포트이다.
지난달과 비교했을 경우에는 TCP 135번 포트에 대한 비율 변동이 거의 없었다 (약 1% 감소)

(2) 상위 Top 5 포트 월별 추이

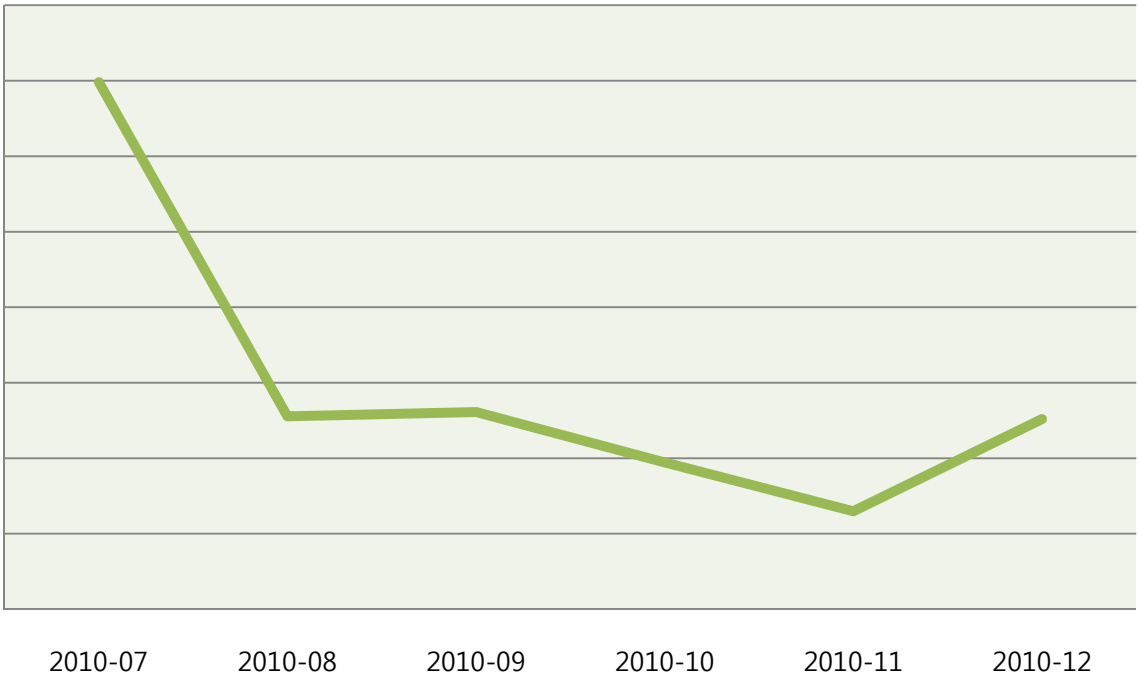
[2010년 10월 ~ 2010년 12월]



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 7월 ~ 2010년 12월]

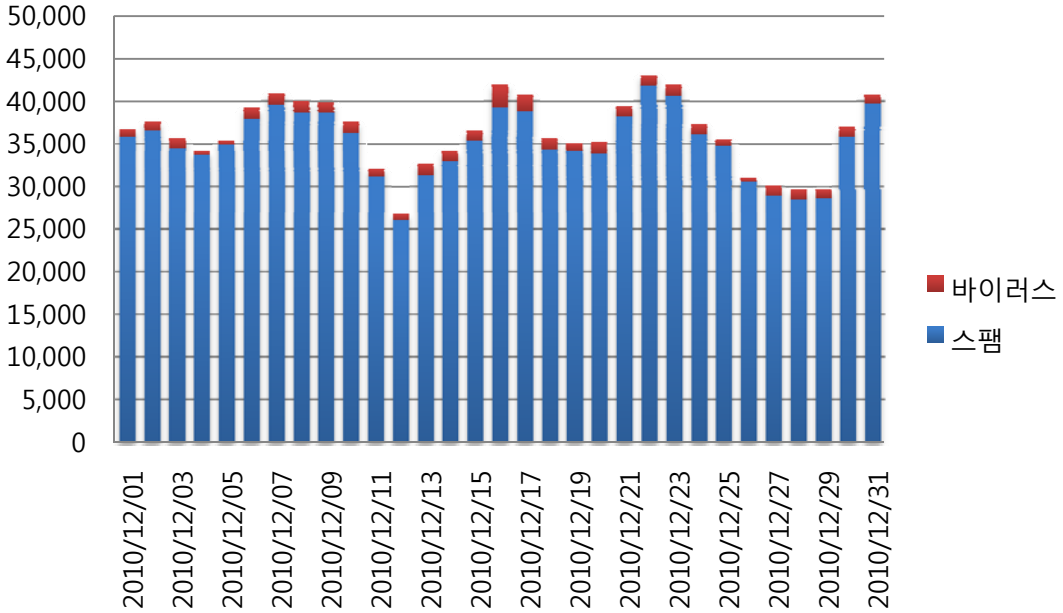


전체적인 악성 트래픽의 유입양은 전달에 비해 증가하였다.
최근 보안이 취약한 언론사 홈페이지나 인터넷 커뮤니티에 웹 해킹으로 악성 스크립트를 삽입한 후 웹사이트에 접속한 사용자들에게 악성코드를 유포시키는 사례가 자주 발견되고 있다. 한 가지 주목할 점은 현재 악성코드 제작자들이 홈페이지 관리자의 대응이 어려운 주말 기간을 집중적으로 노리고 있으며, 주말 기간 동안에도 모니터링이 이루어지지 않은 홈페이지는 사실상 방치 상태에 놓이게 된다.
홈페이지 관리자의 대응도 이루어지지 않고 주말에는 인터넷 커뮤니티의 활동이 늘어나기 때문에 악성코드 유포에 주말이 최적의 시간으로 자리잡게 되었다.

Part I 12월의 악성코드 통계

3. 스팸 메일 분석

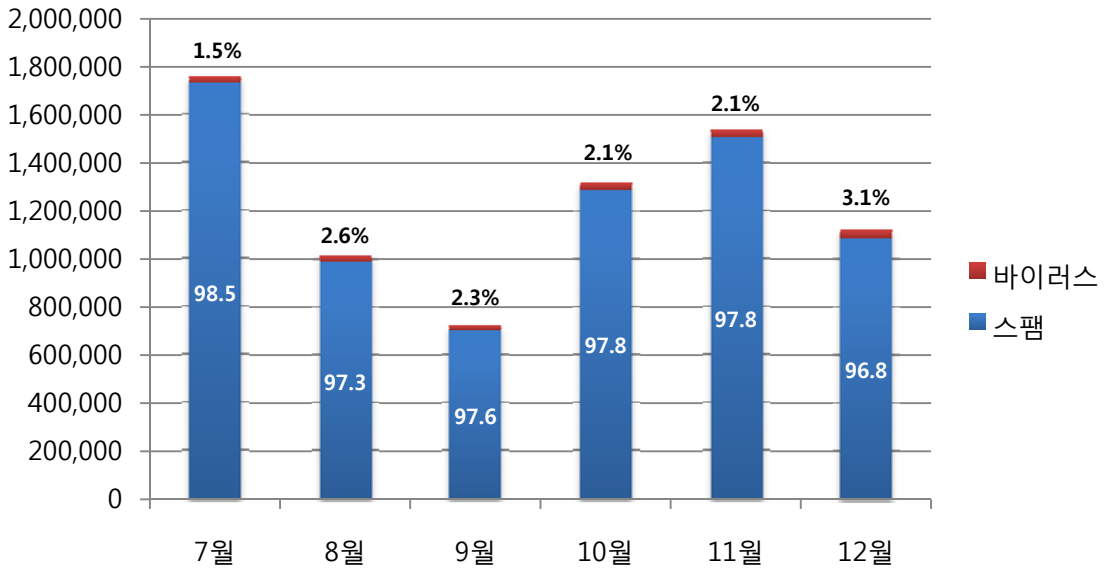
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 수신된 악성코드 첨부, 스팸메일의 개수를 나타낸 그래프이다. 12월에는 크리스마스 연하장을 위장한 악성코드 메일이 많이 발견되었다. 이번에 발견된 "1st Christmas Card"라는 제목의 메일은 SnowFairy.zip라는 첨부 파일을 포함하고 있으며, 이 파일을 실행 했을 때 시스템 설정 정보와 개인 정보를 수집해 외부로 유출시킨다. 또한 PC에서 이메일 주소를 수집한 후 웜(Worm)이 첨부된 메일을 발송한다.

(2) 월별 통계 현황

[2010년 7월 ~ 2010년 12월]



월별 통계 현황은 악성코드 첨부 및 스팸메일이 전체메일에서 차지하는 비율을 나타내는 그래프이다. 12월의 스팸 메일은 96.8%, 바이러스 메일은 3.1%를 차지하였다. 12월에 비해서는 바이러스 메일 비율이 약간 증가하였고, 스팸메일은 소폭 줄어들었다. 또한 전체적인 메일 수신양은 감소하였다.

(3) 스팸 메일 내의 악성코드 현황

[2010년 12월 1일 ~ 2010년 12월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	14,202	39.54%
2	W32/MyDoom-H	5,868	16.34%
3	Mal/ZipMal-B	5,012	13.95%
4	W32/Virut-T	3,906	10.88%
5	W32/Bagz-D	2,581	7.19%
6	W32/AutoRun-BHX	925	2.58%
7	W32/MyDoom-Gen	786	2.19%
8	W32/Bagle-CF	444	1.24%
9	W32/Netsky-N	344	0.96%
10	Troj/CryptBx-ZP	242	0.76%

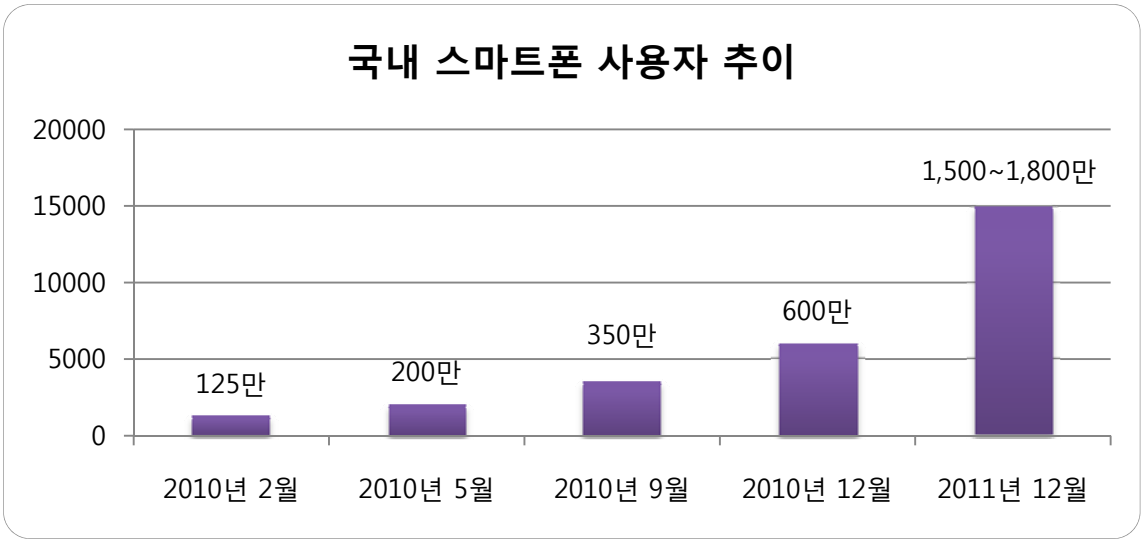
스팸 메일 내의 악성코드 현황은 12월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프이다. 현재 W32/Mytob-C가 39.54%로 1위를 차지하였다.
2위는 16.34%를 차지한 W32/MyDoom-H, 3위는 13.95%를 차지한 Mal/ZipMal-B이다.
12월에는 W32/Netsky-N와 Troj/CryptBx-ZP 악성코드가 새롭게 순위에 등장하였으며,
1~5위까지는 전달과 비교해 변동이 없다.

Part Ⅱ 보안 이슈 돋보기

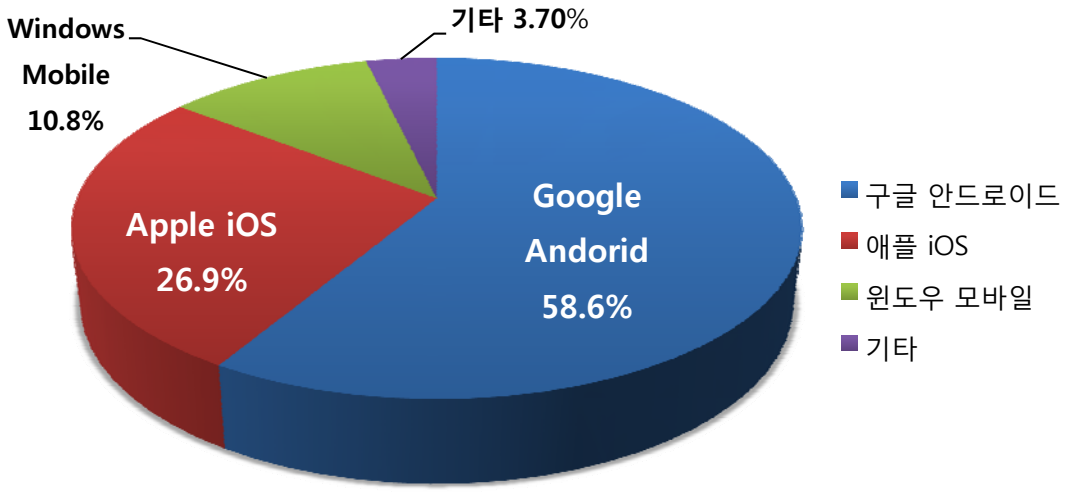
1. 2011년 보안 위협 전망 보고서

① 대중화된 스마트폰 서비스를 이용한 보안 위협

국내 스마트폰 사용자가 올해말 600만을 돌파하였으며, 내년에는 1,500~1,800만명의 스마트폰 사용자가 생겨날 것으로 예측되고 있다. 가히 "우리나라 국민 절반이 스마트폰을 들고 다닌다."고 말할 수 있을 만큼 스마트폰 대중화 속도가 매우 빠른 상황이다.



특히 국내 스마트폰 OS 중에서 구글 안드로이드의 점유율(58.6%, 353만명)이 절대적으로 높게 나타난 가운데 안드로이드를 기반으로 한 악성코드가 올해 최초로 발견되었고, 국내 백신 회사들을 중심으로 안드로이드 백신 출시가 연이어 있었다.



출처 : 국내 이동통신3사 집계 데이터

<참고>

국내 스마트폰 총 사용자 : 602만

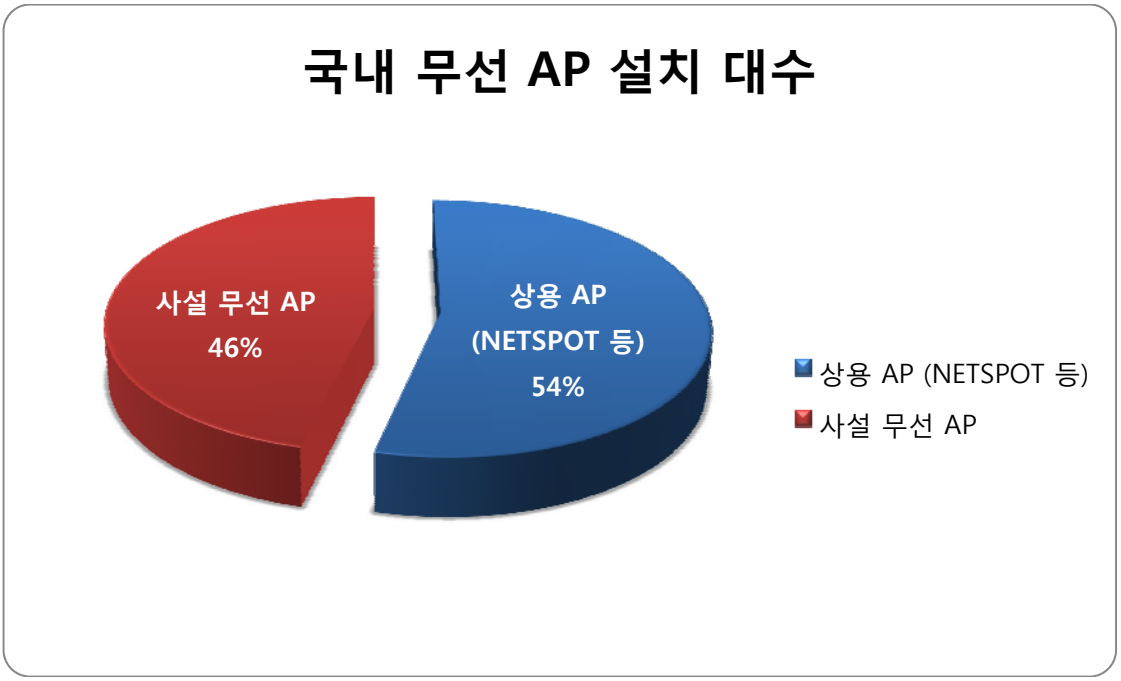
스마트폰 OS 점유율 : 안드로이드(353만), Apple iOS (162만), 윈도우 모바일(65만), 기타(22만)

내년에는 스마트폰 대중화 추세와 국내에 독보적인 안드로이드 OS의 점유율, 안드로이드의 앱(App) 설치 및 배포 특성을 고려했을 때 **안드로이드 OS에 대한 악성코드 유포가 크게 늘어날 것으로 예측되며**, 안드로이드 OS 기반의 태블릿 PC, 구글TV 같은 셋톱박스 등으로 악성코드의 활동 범위가 늘어날 수 있다.

<스마트폰 악성코드에 대비하기 위한 이스트소프트의 알약 안드로이드 백신>

② 무선랜의 대량 보급으로 새로운 위협 발생

국내 495만대에 Access Point 중 일반 개인이나 기업이 설치한 사설 무선 AP가 절반에 가깝다는 통계가 발표되었다. 대다수 사설 무선 AP는 상용 AP에 비해 상대적으로 보안이 취약한 상태로 운영되고 있으며, AP 패스워드가 아예 없거나 공장 초기 값, 취약한 암호화 알고리즘을 사용(WEP)하는 경우가 많다.



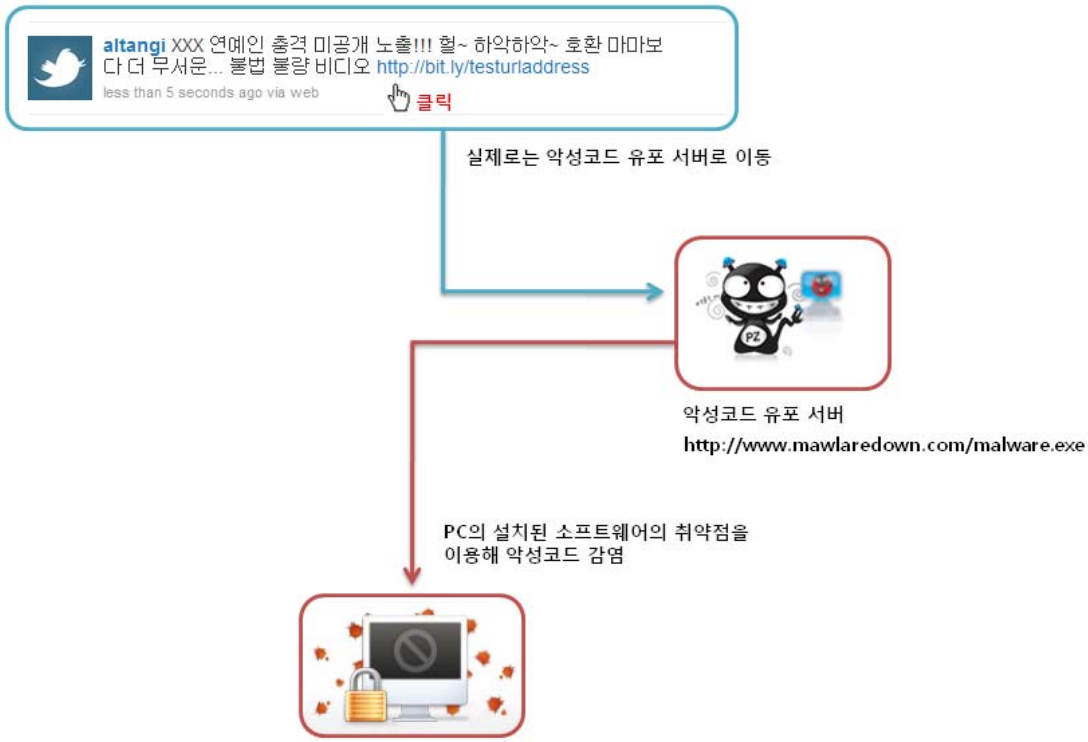
출처 : 한국인터넷진흥원 (2010년 4월 사업자 문의를 통해 간접 파악)

전체 : 495만대 (사설무선AP 233만대, 상용AP : 262만대)

취약한 무선 AP를 통한 예상 공격 방법으로는 무선 AP의 직접적인 취약점을 이용하여 해킹이나 DDoS 수행, 무선 AP에 연결된 클라이언트들의 공격 및 악성코드 감염 등을 대표적으로 꼽을 수 있다.

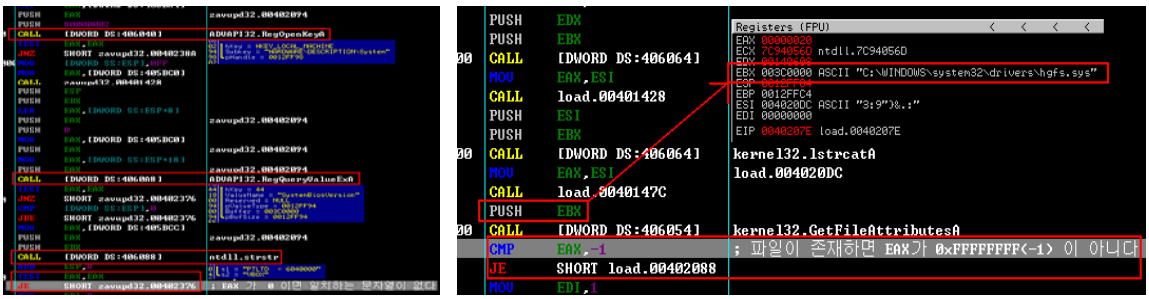
③ 고도화된 악성코드의 공격 지속

2011년에도 주로 MS Internet Explorer와 Adobe Acrobat 제품을 대상으로 한 제로데이(Zeroday) 취약점 공격이 계속 이어질 것으로 보여지며, 홈페이지 해킹과 변조 이외에도 SNS(트위터, 페이스북 등)의 단축 URL 서비스를 통한 악성코드 유포 방식이 대세를 이룰 것으로 예측되고 있다.



<SNS의 단축URL 서비스를 통한 악성코드 유포 개념도>

또한, 악성코드가 PC에 설치된 백신과 보안 제품을 무력화시키고, 백신으로부터 탐지와 제거를 회피하기 위해 악성코드의 자가보호나 루트킷(Rootkit) 기법을 이용한 은폐기법, 바이러스 분석가들의 분석을 방해하는 기술(가상 PC에서의 동작 여부 확인이나, 분석도구의 강제 종료 등) 또한 계속 발전할 것이다.



<악성코드의 VMWare 가상 PC 실행 탐지기법의 예>

악성코드의 백신 무력화 기법의 하나로 최신 엔진 업데이트의 방해(hosts 파일 변조, 백신 업데이트 프로세스의 실행 차단, 보안 회사 홈페이지의 해킹 및 변조 혹은 업데이트 서버에 대한 DDoS 공격)가 주로 사용되고 있으며, 2011년에 이 기술이 중국의 악성코드 제작자들을 중심으로 더욱 일반화될 것이다.

```
if ( !_vbaStrCmp(CurrentProcessName, L"AYUpdate.aye", *(_DWORD *)(*(_DWORD *)(v80 + 0xC) + CurrentProcessName)) )
{
  v91 = 0xEu;
  if ( v80 && *(_WORD *)v80 == 1 )
  {
    v28 = i - *(_DWORD *)(v80 + 0x14);
    v75 = i - *(_DWORD *)(v80 + 0x14);
    if ( (unsigned int)v75 >= *(_DWORD *)(v80 + 0x10) )
      v58 = _vbaGenerateBoundsError(v75, v28);
    else
      v58 = 0;
    v57 = 4 * v75;
  }
  else
  {
    v57 = _vbaGenerateBoundsError(v27, v26);
  }
  v29 = _vbaStrCat(*(_DWORD *)(v80 + 0xC), v57, *(_DWORD *)(*(_DWORD *)(v80 + 0xC) + v57), L"taskkill /f /im \"");
  v30 = _vbaStrMove(&v79, v29);
  v78 = _vbaStrCat(v27, v26, byte_40479C, v30);
  v77 = 8;
  v76 = rtcShell(&v77, 0);
  _vbaFreeStr(&v79);
  _vbaFreeVar(&v77);
}
```

<백신 업데이트 파일의 실행 차단 사례>

```
127.0.0.1 www.symantec.com
127.0.0.1 securityresponse.symantec.com
127.0.0.1 symantec.com
127.0.0.1 www.sophos.com
127.0.0.1 sophos.com
127.0.0.1 www.mcafee.com
127.0.0.1 mcafee.com
127.0.0.1 liveupdate.symantecliveupdate.com
127.0.0.1 f-secure.com
127.0.0.1 www.f-secure.com
127.0.0.1 kaspersky.com
127.0.0.1 www.avp.com
127.0.0.1 www.kaspersky.com
127.0.0.1 avp.com
127.0.0.1 www.networkassociates.com
127.0.0.1 networkassociates.com
127.0.0.1 www.ca.com
127.0.0.1 ca.com
```

Win32.Bagle.BD의 hosts 파일 변조 사례

```
00000EE0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000EF0  00 00 00 00 00 00 00 00  00 00 50 00 00 00 FF 07  ..........P.....
00000F00  00 00 32 00 00 00 00 00  00 00 00 00 00 00 58 88  ..2...........X.
00000F10  E3 40 00 00 00 00 78 88  E3 40 1E 00 00 00 03 00  .@....x..@......
00000F20  00 00 1E 00 00 00 50 00  00 00 1D 00 00 00 E0 57  ......P........W
00000F30  14 00 77 77 77 2E 61 6C  74 6F 6F 6C 73 2E 63 6F  ..www.altools.co
00000F40  2E 6B 72 3B 38 30 3B 67  65 74 3B 2F 3B 3B 00 0C  .kr;80;get;/;;..
00000F50  00 77 77 77 2E 61 68 6E  6C 61 62 2E 63 6F 6D 00  .www.ahnlab.com.
```

<7.7 DDoS의 uregvs.nls 파일>

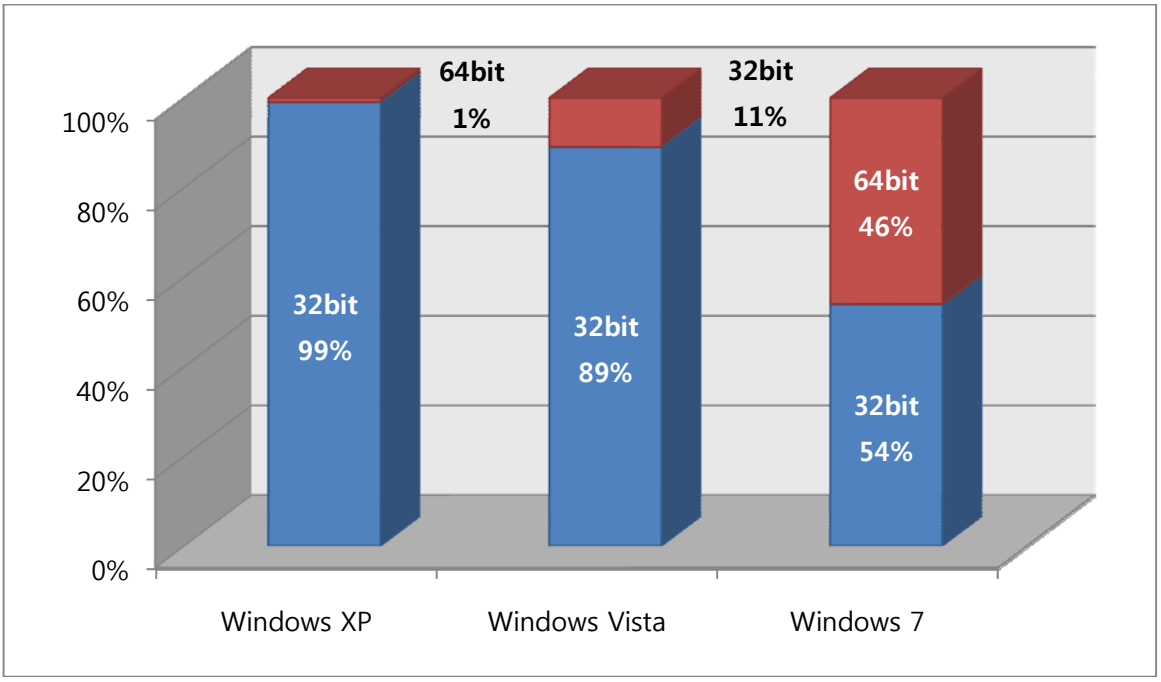
최근에는 바이러스 토탈(VirusTotal)이나 VirScan 같은 멀티 스캐너 사이트를 통해 미리 악성코드가 백신에 진단되는지 확인하고, 진단되지 않는 경우에 최종적으로 악성코드를 유포하는 사례들이 나타나고 있으며(심지어 전문 악성코드 제작자를 대상으로 한 백신 진단 유료 서비스도 존재한다) 앞으로 사전 방역 기능이 지원되지 않는 백신은 신종 악성코드에 대한 진단과 대응이 더욱 어려울 것으로 전망된다.

<대표적인 멀티 백신 스캐너 사이트 – VirusTotal, VirScan>

④ 윈도우 7의 보급 확대로 인한 64비트 악성코드의 전환점

64bit CPU 보급과 함께 대표적인 64bit PC OS인 윈도우7의 도입 속도가 빠르게 증가하면서 본격적인 64bit 컴퓨팅 시대로 옮겨가고 있으며, 이에 악성코드도 64bit 환경에서 동작하도록 진화하고 있다.

Microsoft의 자료에 의하면 2010년 전세계 Windows 7 OS 시장에서 64bit 모드(64bit mode)가 차지하는 비율이 46%에 달하는 것으로 나타났으며, 이전 버전인 Windows Vista와 비교했을 때 4배 이상 급성장하였다.



<전세계 Windows 운영모드 현황 - 출처 : Microsoft>

2010년에 하드디스크 MBR까지 감염되는 Alureon 악성코드가 64bit CPU 및 OS 환경에서 작동하도록 새롭게 업그레이드 되었으며, Shruggle, Rugrat도 64bit 환경에서 동작하는 대표적인 악성코드로 유명하다.

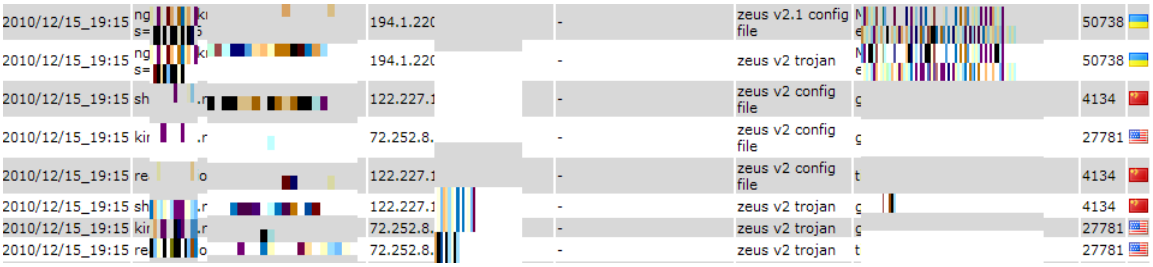
Microsoft는 이미 Windows 2008 Server R2 버전부터 64bit 전용 OS만 출시하고 있으며, 앞으로 32bit OS의 비중을 점진적으로 감소시킬 것으로 예측되는 만큼 64bit 환경에 완전히 적응한 악성코드들이 내년에 점차 늘어날 것으로 전망 된다.

⑤ 사이버 범죄 그룹의 표적화 공격 증가

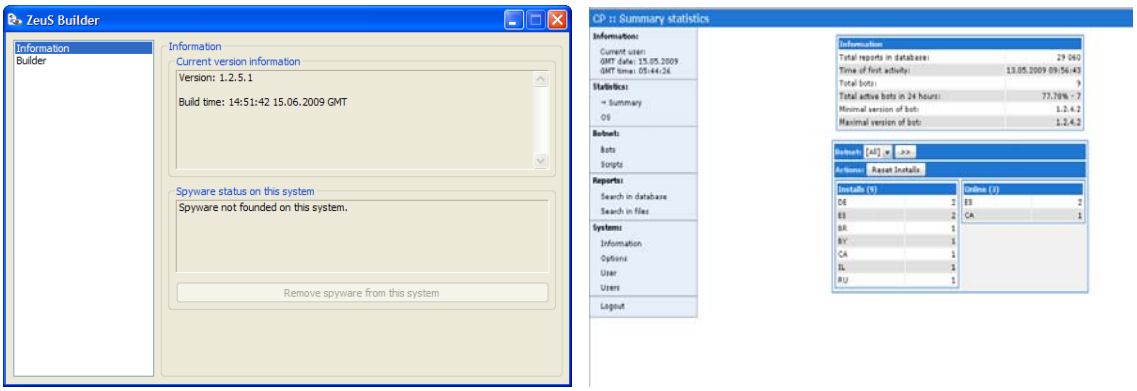
주로 해외의 인터넷 뱅킹 계정 정보를 빼내는 제우스(Zeus or Zbot) 계열 악성코드나 온라인 게임 계정 해킹 같은 형태로 금전적 이득을 얻는 사이버 범죄 집단이 계속 성장할 것이다.

제우스의 경우 새로운 C&C(Command & Control) 서버와 전파 목적의 스팸메일, 변종 악성코드 샘플이 계속 발견되고 있으며, 제우스 봇넷(Botnet)을 구성할 수 있는 종합 툴킷(Tool Kit)들이 지하 경제에서 $3,000~$5,000 사이의 가격대로 거래되고 있다.

또한, 간단한 설정으로 다양한 변종을 만들 수 있는 빌더(Builder)와 감염(좀비) PC에서 실행되는 봇(bot), 대량의 감염 PC들을 중앙에서 관리할 수 있는 C&C 역할의 컨트롤 패널(Control Panel)으로 각자의 영역이 세분화되어 있어 해커는 쉽게 제우스 변종을 유포하고 좀비 PC들을 중앙에서 편안하게 관리할 수 있다.
게다가 덤으로 인터넷 뱅킹의 계정 정보를 빼내 불법적인 계좌 이체까지 가능하다.



<Zeus 악성코드 유포 서버 주소 – 유포 서버 주소는 부득이 모자이크 처리>



<Zeus Builder(좌), Zeus Control Panel(우)>

최근 중국에서 제작되는 대부분의 악성코드들은 국내 온라인 게임들을 목표로 하고 있으며, PC에 감염되면 온라인 게임에 접속할 때 계정 정보를 유출시키는 역할을 한다.
2010년에 크게 유행했던 ARP Spoofing 공격 관련 악성코드는 사실 국내 온라인 게임의 계정 유출을 주된 목적으로 제작된 것이 특징이다.

국내 온라인 게임의 아이템들은 게임 유저들간의 매매를 통해 이미 현금화 할 수 있는 좋은 수단으로 잘 알려져 있으며, 중국 해커들도 게임 아이템 거래로 금전적 이득을 얻기 위해 더욱 조직화되고 전문화되는 양상을 보이고 있다.

```
  GetModuleFileNameA(0, &Filename, 0x104u);
  v2 = strrchr(&Filename, '\\') + 1;
  if ( strcmp(v2, "pcotp.exe") )
  {
    result = ByPass_Authentication(v1);
  }
  else
  {
    if ( strcmp(v2, "dnf.exe") )
    {
      *v2 = 0;
      ((void (*)(_DWORD, const char *, ...))wsprintfA)(&dword_10013C08, "%sHShield\\ehsvc.dll", &Filename);
      result = Hook_For_Account_Steal(v1);
    }
    else
    {
      result = 0;
    }
  }
  return result;
}
```

<국내 온라인게임을 대상으로 한 악성코드 분석 화면 일부>

중국 이외의 러시아에서 제작된 악성코드들의 경우 상당수가 금전적 목적을 위해 활동하고 있지만 다행히 현재까지 국내에 별다른 영향을 끼치지 않았다.
러시아 악성코드 제작자들은 중국 이상으로 세련된(?) 악성코드 제작 기술을 선보이고 있지만, 아직까지 우리나라를 주된 목표로 생각하지 않는 것으로 보인다.
하지만 이들이 국내 인터넷 환경을 주목한다면 강력한 악성코드들을 무기로 중국에 못지 않은 피해를 발생시킬 수 있다고 생각된다.

Part Ⅱ 12월의 이슈 돋보기

② 12월의 취약점 이슈

• Microsoft 12월 정기 보안 업데이트

Internet Explorer 누적 보안 업데이트, Exchange 와 SharePoint 서버의 원격코드 실행, 커널모드 드라이버 취약점으로 인한 권한 상승, 윈도우의 취약점으로 인한 원격코드 실행 문제점 등을 해결한 Microsoft 12월 정기 보안 업데이트를 발표하였습니다.

<해당 제품>

- Internet Explorer 6~8
- Windows XP Service Pack 3
- Windows Server 2003, 2008
- Windows Vista, 7
- Microsoft Office XP~2010
- Microsoft Office SharePoint Server 2007
- Microsoft Exchange Server 2007 SP2

<취약점 목록>

Internet Explorer 누적 보안 업데이트(2416400)

이 보안 업데이트는 Internet Explorer의 비공개적으로 보고된 취약점 4건과 일반에 공개된 취약점 3건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

OTF(OpenType 글꼴) 드라이버의 취약점으로 인한 원격 코드 실행 문제점(2296199)

이 보안 업데이트는 원격 코드 실행을 허용할 수 있는 비공개적으로 보고된 여러 건의 Windows OTF(Open Type Font) 드라이버 취약점을 해결합니다. 공격자는 네트워크 공유 위치에 특수하게 조작된 OpenType 글꼴을 호스팅할 수 있습니다. 그러면 사용자가 Windows 탐색기에서 공유 위치로 이동할 때 영향을 받는 제어 경로가 트리거되어 특수하게 조작된 글꼴이 영향을 받는 시스템을 완전히 제어할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치할 수 있을 뿐 아니라 데이터를 보거나 변경하거나 삭제할 수 있고 모든 사용자 권한이 있는 새 계정을 만들 수도 있습니다.

작업 스케줄러의 취약점으로 인한 권한 상승 문제점(2305420)

이 보안 업데이트는 Windows 작업 스케줄러의 공개된 취약점을 해결합니다. 이 취약점으로 인해 공격자가 영향을 받는 시스템에 로그온한 후 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.

Windows Movie Maker의 취약점으로 인한 원격 코드 실행 문제점(2424434)

이 보안 업데이트는 Windows Movie Maker의 공개된 취약점을 해결합니다. 이 취약점으로 인해 공격자가 사용자로 하여금 특수하게 조작된 라이브러리 파일과 동일한 네트워크 디렉터리에 있는 합법적인 Windows Movie Maker 파일을 열도록 유도할 경우 원격 코드 실행이 허용될 수 있습니다. 공격에 성공하려면, 사용자가 신뢰할 수 없는 원격 파일 시스템 위치 또는 WebDAV 공유를 방문하거나 이러한 위치에서 취약한 응용 프로그램이 로드되는 문서를 열어야 합니다.

Windows Media Encoder의 취약점으로 인한 원격 코드 실행 문제점(2447961)

이 보안 업데이트는 Windows Media Encoder의 공개된 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 라이브러리 파일과 동일한 네트워크 디렉터리에 있는 합법적인 Windows Media 프로필(.prx) 파일을 열도록 유도할 경우 원격 코드 실행이 허용될 수 있습니다. 공격에 성공하려면, 사용자가 신뢰할 수 없는 원격 파일 시스템 위치 또는 WebDAV 공유를 방문하거나 이러한 위치에서 취약한 응용 프로그램이 로드되는 문서를 열어야 합니다.

Microsoft Windows의 취약점으로 인한 원격 코드 실행 문제점(2385678)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 라이브러리 파일과 동일한 네트워크 폴더에 있는 .eml 및 .rss(Windows Live 메일) 또는 .wpost(Microsoft Live Writer)와 같은 파일 형식을 열 경우 원격 코드 실행이 허용될 수 있습니다. 공격에 성공하려면, 사용자가 신뢰할 수 없는 원격 파일 시스템 위치 또는 WebDAV 공유를 방문하거나 이러한 위치에서 취약한 응용 프로그램이 로드되는 문서를 열어야 합니다.

Windows 주소록의 취약점으로 인한 원격 코드 실행 문제점(2423089)

이 보안 업데이트는 Windows 주소록의 공개된 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 라이브러리 파일과 동일한 네트워크 폴더에 있는 Windows 주소록 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 취약한 응용 프로그램이 로드되는 문서를 열어야 합니다.

인터넷 연결 등록 마법사의 안전하지 않은 라이브러리 로드로 인한 원격 코드 실행 문제점(2443105)

이 보안 업데이트는 Microsoft Windows 인터넷 연결 등록 마법사의 공개된 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.

이 취약점으로 인해 사용자가 특수하게 조작된 라이브러리 파일과 동일한 네트워크 폴더에 있는 .ins 또는 .isp 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 공격에 성공하려면, 사용자가 신뢰할 수 없는 원격 파일 시스템 위치 또는 WebDAV 공유를 방문

하거나 이러한 위치에서 취약한 응용 프로그램이 로드되는 문서를 열어야 합니다.

Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점(2436673)

이 보안 업데이트는 Microsoft Windows의 공개된 취약점 1건과 비공개적으로 보고된 여러 취약점을 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.

라우팅 및 원격 액세스의 취약점으로 인한 권한 상승 문제점(2440591)

이 보안 업데이트는 비공개로 보고된 Microsoft Windows의 라우팅 및 원격 액세스 NDProxy 구성 요소의 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.

이 취약점으로 인해 공격자가 영향을 받는 시스템에 로그온한 후 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.

동의 사용자 인터페이스의 취약점으로 인한 권한 상승 문제점(2442962)

이 보안 업데이트는 동의 사용자 인터페이스(UI)의 비공개적으로 보고된 취약점을 해결합니다. 이 취약점으로 인해 공격자가 영향을 받는 시스템에서 특수 조작된 응용 프로그램을 실행하면 권한 상승이 허용될 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그온 자격 증명 및 SeImpersonatePrivilege를 가지고 로컬로 로그온할 수 있어야 합니다. 익명의 사용자에 의해서나 원격으로는 이 취약점을 악용할 수 없습니다.

Windows Netlogon 서비스의 취약점으로 인한 서비스 거부 문제점(2207559)

이 보안 업데이트는 도메인 컨트롤러로 작동하도록 구성된 영향을 받는 Windows Server 버전에서 Netlogon RPC 서비스의 비공개적으로 보고된 취약점을 해결합니다. 이 취약점으로 인해 공격자가 특수하게 조작된 RPC 패킷을 영향을 받는 시스템의 Netlogon RPC 서비스 인터페이스로 보낼 경우 서비스 거부가 발생할 수 있습니다. 공격자는 이러한 취약점을 이용하기 위해 영향 받는 도메인 컨트롤러와 동일한 도메인에 가입된 시스템에 대한 관리자 권한이 있어야 합니다.

Hyper-V의 취약점으로 인한 서비스 거부 문제점(2345316)

이 보안 업데이트는 Windows Server 2008 Hyper-V 및 Windows Server 2008 R2 Hyper-V에서 발견되어 비공개적으로 보고된 취약점을 해결합니다. 이 취약점으로 인해 Hyper-V 서버에서 호스팅하는 게스트 가상 컴퓨터 중 하나의 인증된 사용자가 특수하게 조작된 패킷을 VMBus로 보낼 경우 서비스 거부가 발생할 수 있습니다. 공격자는 이 취약점을 악용하기 위해 유효한 로그온 자격 증명이 있어야 하며 특수하게 조작된 콘텐츠를 게스

트 가상 시스템에서 전송할 수 있어야 합니다. 익명의 사용자에 의해서나 원격으로는 이 취약점을 악용할 수 없습니다.

Microsoft Publisher의 취약점으로 인한 원격 코드 실행 문제점(2292970)

이 보안 업데이트는 비공개적으로 보고된 취약점 5건을 해결합니다. 사용자가 특수하게 조작된 Publisher 파일을 열면 이 Microsoft Publisher 취약점을 통해 원격 코드 실행이 허용될 수 있습니다. 이러한 취약점 중 어느 것이든 성공적으로 악용한 경우 공격자는 영향을 받는 시스템을 완전히 제어할 수 있습니다. 이렇게 되면 공격자가 프로그램을 설치할 수 있을 뿐 아니라 데이터를 보거나 변경하거나 삭제할 수 있고 모든 사용자 권한이 있는 새 계정을 만들 수도 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Microsoft SharePoint의 취약점으로 인한 원격 코드 실행 문제점(2455005)

이 보안 업데이트는 비공개적으로 보고된 Microsoft SharePoint의 취약점을 해결합니다. 이 취약점으로 인해 문서 변환 부하 분산 서비스를 사용하는 SharePoint 서버 환경에서 공격자가 특수하게 조작된 SOAP 요청을 문서 변환 시작 관리자 서비스에 보낼 경우 게스트 사용자의 보안 컨텍스트에서 원격 코드 실행이 허용될 수 있습니다. 기본적으로 문서 변환 부하 분산 서비스 및 문서 변환 시작 관리자 서비스는 Microsoft Office SharePoint Server 2007에서 사용되지 않습니다.

Microsoft Office 그래픽 필터의 취약점으로 인한 원격 코드 실행 문제점(968095)

이 보안 업데이트는 Microsoft Office에서 발견되어 비공개적으로 보고된 취약점 7건을 해결합니다. 이러한 취약점은 사용자가 Microsoft Office를 사용하여 특수하게 조작된 이미지 파일을 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.

Microsoft Exchange Server의 취약점으로 인한 서비스 거부 문제점(2407132)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Exchange Server의 취약점을 해결합니다. 이 취약점으로 인해 인증된 공격자가 Exchange 서비스를 실행하는 컴퓨터에 특수하게 조작된 네트워크 메시지를 보낼 경우 서비스 거부가 발생할 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.

<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/ms10-dec.mspx

영문 : http://www.microsoft.com/technet/security/Bulletin/ms10-dec.mspx

• MS Internet Explorer 원격 코드 실행 취약점 주의

CVE Number : CVE-2010-3971

MS Internet Explorer에서 mshtml.dll 라이브러리가 재귀적으로 CSS @import 규칙을 포함하는 웹페이지를 처리할 때 원격코드 실행되는 문제가 발견되었습니다.

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

<해당 제품>

• Internet Explorer 6/7/8 (Internet Explorer 9는 이번 취약점에 해당하지 않음)

<임시 해결책>

EMET((Enhanced Mitigation Experience Toolkit) 설치한 후 Internet Explorer를 EMET 설정에 추가합니다. 또한 인터넷 및 로컬 인트라넷 보안 영역을 높음으로 설정합니다.

(이 설정으로 ActiveX 컨트롤과 Active Scripting 사용이 비활성되어 일부 사이트에서 정상적인 접속이 어려울 수 있습니다.)

<참고 사이트>

http://www.microsoft.com/technet/security/advisory/2488013.mspx

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c6f0a6ee-05ac-4eb6-acd0-362559fd2f04

http://blogs.technet.com/b/srd/archive/2010/12/22/new-internet-explorer-vulnerability-affecting-all-versions-of-ie.aspx

• MS WMI 관리도구 원격 코드 실행 취약점 주의

CVE Number : CVE-2010-3962

MS WMI 관리도구에서 "WBEMSingleView.ocx"ActiveX 컨트롤이 메모리 오류로 인한 원격 코드 실행되는 문제가 발견되었습니다.

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

<해당 제품>

• MS WMI Administrative Tools 1.1 및 이전 버전

<임시 해결책>

다음 CLSID에 대해 "kill bit"를 적용하여 취약점이 존재하는 ActiveX 실행 차단을 설정합니다. CLSID : {2745E5F5-D234-11D0-847A-00C04FD7BB08}

<참고 사이트>

http://support.microsoft.com/kb/240797

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

• 애플 퀵타임 플레이어 및 iOS 4.2 최신 보안 업데이트 권고

애플(Apple) 사의 퀵타임 플레이어(Quicktime) 7.6.8 및 iOS 4.2에 대한 최신 보안 업데이트가 발표되었습니다.

Contact us…

㈜이스트소프트 알약보안대응팀

Tel : 02-881-2364

E-mail : help@alyac.co.kr

알약 사이트 : www.alyac.co.kr