안철수연구소에서 발행하는 월간 보안 보고서

ASEC 리포트

2009년 4월호

이달의 보안 이슈

1. 악성코드 – 파워 포인트 제로데이 관련 취약점과 또 다른 Conficker 웜 변형 2
2. 스파이웨어 – Zlob 방식으로 배포되는 국내 애드웨어 6
3. 시큐리티 – PPT 0 day 취약점(CVE-2009-0556) 12
4. 중국 보안 이슈 – 중국의 정보보안 관련법 16

ASEC 칼럼

■ Ineternet Explorer 8.0의 편리함과 보안 위협 18

이달의 통계

1. 악성코드 26
2. 스파이웨어 36
3. 시큐리티 39
4. 사이트가드 42

안철수연구소의 시큐리티대응센터(ASEC, AhnLab Security Emergency response Center)는 바이러스 분석가 및 보안 전문가들로 구성된 글로벌 보안 대응 조직입니다. 이 리포트는 ㈜안철수연구소의 ASEC에서 작성하며, 매월 발생한 주요 보안 위협과 이에 대응하는 최신 보안 기술에 대한 요약 정보를 담고 있습니다.
자세한 내용은 안랩닷컴(www.ahnlab.com)에서 확인하실 수 있습니다.

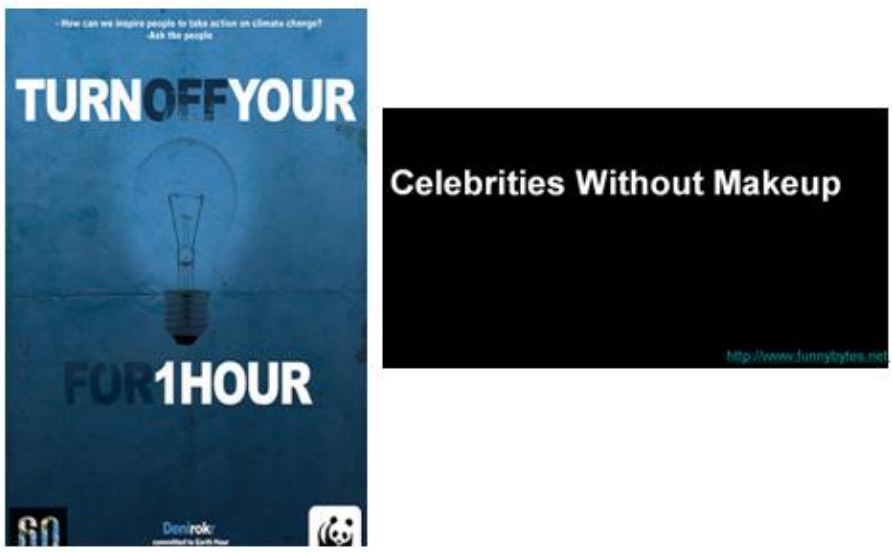
I. 이달의 보안 이슈

1. 악성코드 – 파워 포인트 제로데이 관련 취약점과 또 다른 Conficker 웜 변형

문서파일의 취약점은 곧잘 악성코드 제작에 이용되는데 이번 달 초 MS 파워포인트의 제로데이 취약점이 알려지고 이를 이용한 악성코드가 국외에서 보고 되었다. 또한 Conficker 변형이 또다시 보고 되었다. 이번 변형은 가짜백신을 설치하고 이전 변형인 Conficker.B 형을 설치 한다. 지난달에도 보고된 Waledac 웜 변형이 이번에는 SMS 문자 메시지를 훔쳐 볼 수 있는 내용을 담는 메일 형태로 광범위하게 퍼졌다. 이외에도 서버 서비스 취약점을 사용하는 Buzus 트로이목마가 국내에서 다수 보고 되었으며 국외의 유명 SNS인 Twitter 관련 웜이 보고 되기도 하였다.

(1) MS 파워 포인트 제로데이 취약점

Dropper/Exploit-PPT가 악용한 취약점은 조작된 파워 포인트 파일을 파싱하는 과정에서 발생하며 이는 메모리 상에서 삭제된 오브젝트(Object)를 다시 참조함으로 인해 유효하지 않은 메모리 참조가 발생하는 메모리 오류로 인한 코드 실행 취약점이다. 악의적으로 제작된 파워 포인트 문서들을 오픈 하면 다음과 같은 슬라이드 중 하나가 보여지게 된다.



[그림 1-1] 파워 포인트 제로데이 취약점 관련 문서 슬라이드 중 일부

위와 같이 취약점이 포함된 문서파일을 이용한 공격은 대부분 메일을 통하여 첨부파일로 전달 되므로 의심스러운 문서파일 종류는 절대로 실행하지 말아야 한다. 이처럼 취약점이 포함된 문서파일을 이용하여 메일을 보내어 공격하는 형태를 스피어 피싱이라고 불리며 일반 사

용자들을 노리기 보다는 기업 또는 공공기관처럼 신뢰 있는 기관을 공격하여 주요한 정보를 탈취하려는 목적이 강하기 때문에 주의가 요구된다.

(2) MS08-067 관련 취약점을 이용하는 Win-Trojan/Buzus

Win-Trojan/Buzus 는 유저모드 은폐기법을 이용하면서 자신의 프로세스를 숨기며 동작하는 악성코드이다. 해당 트로이목마는 다수의 국내 사용자로부터 보고 되었다. 트로이목마가 실행 되면 자신을 ₩Windows₩System 폴더에 1sass.exe 자신의 복사본을 생성한다. 그리고 특정 호스트로 자신을 접속하며 서버 서비스 취약점 (MS08-067)을 이용하여 자신을 전파하려고 한다. 트로이목마 자체는 실행 압축된 형태이므로 코드가 바로 보이지 않으며 실행을 위해서 자신을 특정 메모리 영역에 할당을 받은 뒤 이곳에 원래의 코드를 풀어내고 실행하게 된다.

파일명	검색 취약점
unp_1sass.bin	/ MS08-067

[그림 1-2] Win-Trojan/Buzus가 사용하는 서버 서비스 Exploit 코드 부분

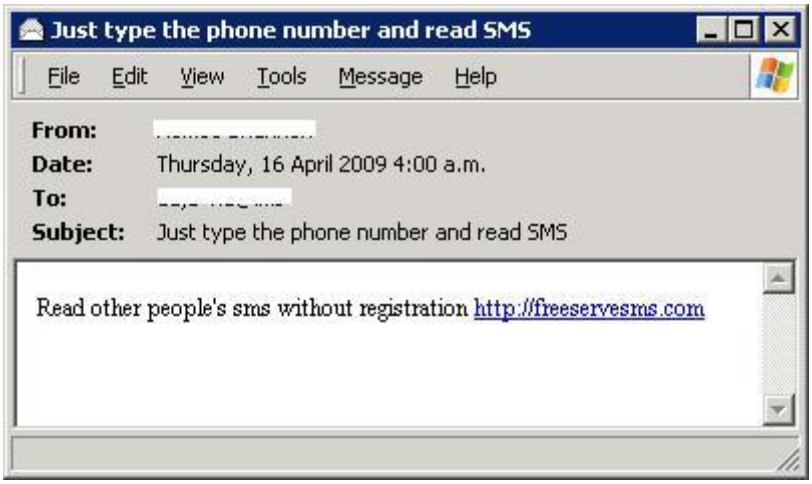
또한 트로이목마는 이동식 디스크에 자신의 복사본과 Autorun을 생성해둔다. 따라서 감염된 이동식 디스크를 감염되지 않는 곳이나 외부의 네트워크와 접근이 되지 않는 폐쇄망에 연결된 시스템에 디스크를 연결하는 경우 이와 같은 환경에서도 해당 악성코드 감염이 발생 하게 된다.

(3) 변형 또 다른 Conficker 웜 변형 출현

Conficker 웜 또 다른 변형이 발견, 보고 되었다. 이번에는 EXE 형태로 직접 실행 가능한 형태이다. 이번 변형은 아직 광범위하게 전파된 것은 아닌 것으로 추정된다. 실행 되면 가짜 백신을 설치하며 Conficker.B로 알려진 변형을 레지스트리에 숨겨둔다. 이와 같은 방법은 특정 레지스트리 키를 생성한 후 그 내용에 암호화된 Conficker.B를 데이터로 써두는 방법이다. 특정 조건이 되면 해당 파일이 복호화 되어 실행될 것으로 추정 된다. 새로운 Conficker는 취약점으로 전파는 물론 P2P 형태로 자신을 전파하거나 명령을 제어할 수 있는 것으로 알려져 있다.

(4) SMS Spy 메일로 위장한 Waledac 웜 관련

Win32/Waledac.worm의 또 다른 변형이 발견, 보고 되었다. Waledac 웜은 지난 달 특정 도시에 테러가 발생 했다는 뉴스로 가장하여 전파되기도 하였다. 이번에는 SMS 를 온라인에서 해킹할 수 있는 프로그램을 제공하는 것처럼 사용자를 특정 웹 페이지로 유도한다.



[그림 1-3] SMS Spy 메일로 위장한 Waledac 관련 메일

[그림 1-4] SMS Spy 메일로 위장한 Waledac 관련 메일

웹 페이지 내 'DownloadFreeTrial' 링크를 클릭하면 Waledac 웜 파일을 다운로드 하는 창이 보여진다. Waledac 웜은 지금까지 국제적인 이슈나 기념일등과 관련된 내용을 가진 메일로 광범위하게 전파되고 있다. 또한 Server-Side Polymorphism 기법을 이용하여 매번 다른 변형을 배포하고 있어 안티바이러스 진단을 피하도록 하고 있기도 하다. 이후 Waledac 웜은 다른 국제 및 사회적인 이슈 등으로 가장하여 스팸성 메일로 전파될 소지가 많은 만큼 이와 같은 거짓정보에 현혹 되어서는 안된다.

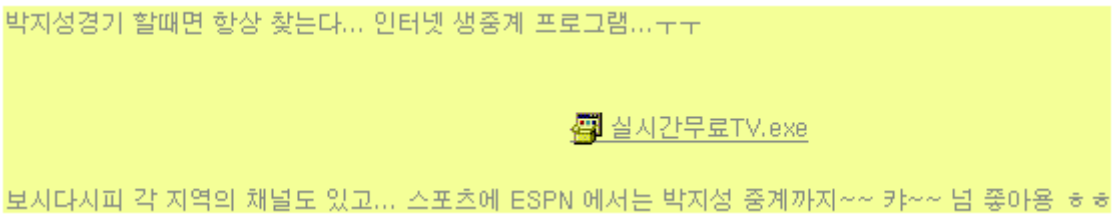
2. 스파이웨어 – Zlob 방식으로 배포되는 국내 애드웨어

Zlob 이라고 하면 코덱 형식을 가장하여 배포되는 악성 프로그램으로, 실행하면 다수의 애드웨어 또는 스파이웨어를 설치하는 특징을 가지고 있다. 이들은 사람들의 관심을 끌만한 동영상으로 사용자의 접속을 유도한 후 감상을 시도할 때 코덱 설치 메시지를 보여주며 악성 프로그램의 설치를 유도한다. 이러한 사회공학적인 방식에 속아 사용자들은 악성 프로그램들을 스스로 설치하게 된다.

지금까지 이러한 Zlob 들은 대부분 해외에서 발견되었으며 국내에서는 거의 이용되지 않았는데, 이것은 국산 애드웨어의 배포 역사와 밀접한 관련이 있다. 국산 애드웨어 배포 방식은 과거에 ActiveX 를 통한 배포가 주를 이루다가 보안 업체의 진단이 많아지자 번들 설치로 넘어가는 단계에 있다. 이런 시점에 국산 Zlob 이 나타난 것은 시사하는 바가 크다고 할 수 있다.

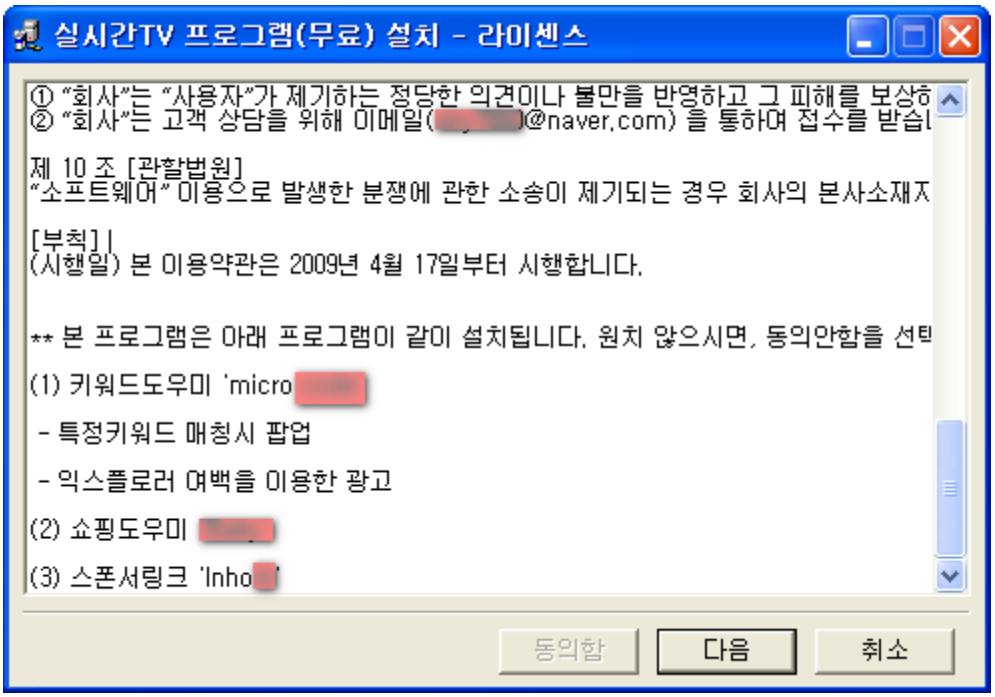
현재 활성화되어 있는 국산 Zlob 배포지는 그리 수가 많지 않으며, 블로그 형태와 홈페이지 형태가 확인되었다. 블로그를 이용한 형태는 포털 사이트의 주요 검색 키워드 관련 영상을 이용하거나 코덱 팩을 위장하여 다운로드를 유도한다. 그와 달리 홈페이지를 이용한 방식은 사이트 특성에 맞춰 음악 감상 사이트의 경우 MP3 다운로드를 위장하고, 동영상 감상 사이트의 경우 코덱을 위장한다. 구체적으로 살펴보면 아래와 같다.

블로그의 경우는 매 기사마다 사용자의 관심을 끌만한 컨텐츠를 제공한다. 그 중에 특히 유용한 프로그램의 다운로드를 제공하는 경우가 일반적이다. 예를 들면 아래의 [그림 1-5]은 축구선수 박지성의 인기를 이용한 것으로 경기 시청을 원하는 국내 팬들을 대상으로 하고 있다.



[그림 1-5] 인터넷 TV로 위장한 국내 Zlob

위에서 제공하는 파일을 실행하면 아래와 같은 사용자 이용 동의 창을 확인할 수 있다.



[그림 1-6] 국산 Zlob 설치 시 사용자 동의 창

사용자가 자세히 확인하지 않고 동의 버튼을 누를 경우 실시간 TV 시청 프로그램과는 전혀 관련 없는 다수의 리워드(적립금), 키워드 프로그램이 설치된다.

이와는 달리 사람들의 관심을 끄는 무료 동영상을 위장하여 애드웨어의 설치를 유도하는 방법도 이용된다. 예를 들면 아래와 같이 유명 무료 동영상의 이미지를 긁어와서 설치 프로그램과 연결시켜 놓는 경우도 있다.

[그림 1-7] 웹 동영상 창으로 위장한 다운로드 링크

위의 이미지는 동영상 플레이어를 위장하고 있지만, 실제로는 이미지이다. 이미지와 연결된 다운로드 링크는 웹 브라우저의 상태 바에서 확인할 수 있다.

블로그와 달리 웹 사이트는 하나의 컨텐츠 성격을 갖고 있다. 그 때문에 어떻게 보면 단순해 보일 수도 있으나, 예를 들면, MP3 공유 사이트의 경우 음악 정보들을 위장하여 애드웨어를 배포하며, 동영상 감상 사이트의 경우 코덱을 위장하여 애드웨어의 설치를 유도한다. 예를 들면, [그림 1-8]를 보면 국내 가요들의 MP3를 다운로드 할 수 있도록 서비스를 제공하는 것으로 보인다. 그러나 실제 모든 음악 링크들은 동일한 애드웨어 설치 프로그램을 다운로드 하도록 연결되어 있다.

[그림 1-8] MP3 감상 사이트로 위장한 Zlob 배포지

페이지 소스를 보면 아래와 같다. [그림 1-9]의 인기차트의 맨 위에 있는 음악 링크를 누를 경우 함수 locationOK() 가 호출되며 파라미터로 선택된 음악 제목이 전달된다.


```
<td width='30' align='center'><img src='images/boxbtn_mp3.gif' align='absmiddle'
onclick="locationOK('Mission No.4 (With 김현중, 김준) - 손담비')"
style='cursor:hand'></td>
```

[그림 1-9] 노래 제목을 누를 시 활성화되는 스크립트

함수 locationOK() 에서는 [그림 1-10]과 같이 전달된 음악과 무관하게 함수 BigPopup() 이 호출된다.

```
function locationOK(name)
{
    var msg = document.mp3Frm.cment.value;
    if(msg) alert(msg);
    hiddenframe.location.href='qry/click.php?id=isthex_mp3&type=mp3&name='+name;

        BigPopup('MusicPOP');
}
```

[그림 1-10] 어떤 제목을 클릭해도 'BigPopup' 호출

함수 BigPopup() 은 [그림 1-11]에서 볼 수 있듯이 다운로드 URL 을 창으로 Open 한다.

```
function BigPopup(target)
{
    var OpenURL = document.mp3Frm.openURL.value;
    var Width = (screen.width);
    var Height = (screen.height);
    var open =
window.open(OpenURL,target,'width='+Width+',height='+Height+',top=0,left=0,
scrollbars=yes');
    open.focus();
}
```

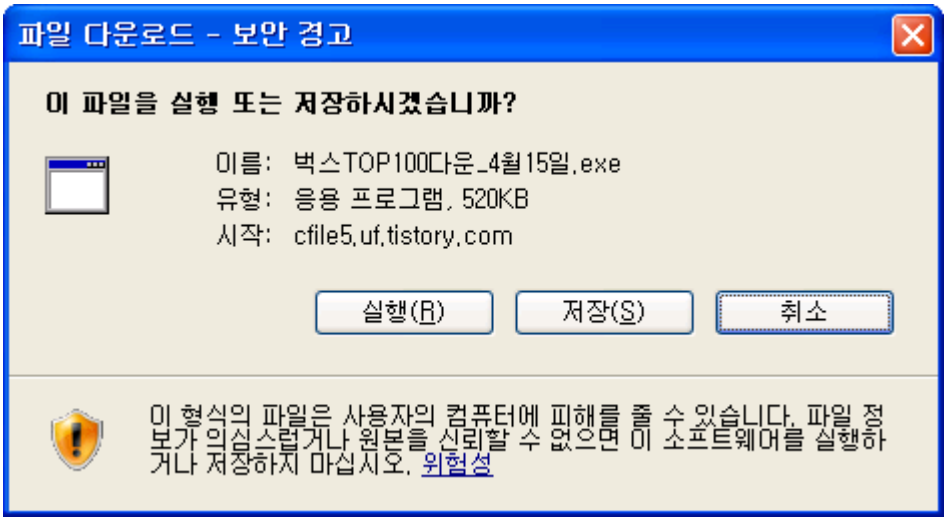
[그림 1-11] 다운로드 링크를 Open 함

다운로드 URL 은 아래의 [그림 1-12]과 같이 애드웨어의 설치 프로그램이 연결되어 있다.

```
<form name="mp3Frm">
<input type="hidden" name="openURL"
value="http://[redacted].tistory.com/attachment/cfile5.uf@205D4A1649E58A9B61F23C.exe">
<textarea name="cment" style="display:none">※ 100곡의 인기가요 MP3가 설치됩니다
※</textarea>
</form>
```

[그림 1-12] 'mp3Frm' 에 있는 다운로드 링크

실제로 마우스 클릭 시 아래의 [그림 1-13]와 같은 다운로드 창을 확인할 수 있다.



[그림 1-13] 국산 Zlob 다운로드 창

이와 유사하게 동영상 감상의 경우 아래의 [그림 1-14]과 같은 홈페이지 구성을 갖고 있다.

앞서 살펴본 MP3 공유 사이트와 동일하게 영상 클릭 시 애드웨어 설치 프로그램의 다운로드 창을 보여준다. 다만 코덱을 설치하도록 유도한다는 점에서 차이가 있다.

[그림 1-14] 동영상 감상 사이트로 위장한 Zlob 배포지

3. 시큐리티 – PPT 0 day 취약점(CVE-2009-0556)

MS Office는 이번 달에도 많은 보안 패치가 나올 만큼 최근 이슈가 되고 있다.
안철수연구소가 ASEC 보안 권고문을 통해 이미 사용자에게 주의를 알렸으나, 아직 보안 패치가 나오지 않았으며 악성코드에 이용되는 PowerPoint 0 day 취약점에 대해 상세히 알아보자.

(1) CVE-2009-0556 PPT 0 day 취약점

PowerPoint PPT 파일은 다음 스트림들로 구성되어 있다.

- ✓ Current User - 해당 프리젠테이션을 마지막으로 연 사용자의 이름이 저장된다.
- ✓ PowerPoint Document - PowerPoint 프리젠테이션에 대한 모든 정보가 저장된다.
- ✓ Pictures(선택사항) - 그림 관련 데이터가 저장된다.(메타파일, PNG, JPG 등)
- ✓ Summary Information 및 DocumentSummaryInformation(선택사항) - 문서에 관한 통계가 저장된다.

PowerPoint Document 스트림에는 프리젠테이션 정보가 포함되어 있으며, 다음과 같은 공통 구조를 가진 일련의 레코드로 구성된다.

Offset	Size	Field
0x00	WORD	Record Version (4 bits MSBs), Record Instance (12 bit LSBs)
0x02	WORD	Record type
0x04	DWORD	Record length, n
0x08	BYTE[n]	Data

[그림 1-15] 레코드 공통 구조

atom과 container라는 두 종류의 레코드가 존재한다.
atom은 실제 정보를 저장하는 파일과 같고, container는 다른 디렉토리와 파일을 포함하는 디렉토리와 같다.

TextHeaderAtom(3999) - 동일한 텍스트에 속한 일련의 atom 중 가장 앞에 위치한다.

Offset	Size	Field
0x00	WORd	Record Version (4 bits MSBs), Record Instance (12 bit LSBs)
0x02	WORD	Record type, 3999 (0xf9f) for *TextHeaderAtom*
0x04	DWORD	Record length, 4
0x08	DWORD	Text Type (enum)

[그림 1-16] 레코드 공통 구조

OutlineTextRefAtom(3998) - 슬라이드 내에서 해당 문서에 이미 포함된 텍스트를 나타내는데 사용된다.

Offset	Size	Field
0x00	WORD	Record Version (4 bits MSBs), Record Instance (12 bit LSBs)
0x02	WORD	Record type, 3998 (0xf9e) for *OutlineTextRefAtom*
0x04	DWORD	Record length, 4
0x08	DWORD	Text Type

[그림 1-17] 레코드 공통 구조

PowerPoint는 container 내에서 TextHeaderAtom을 만나면 해당 텍스트를 위한 임시 개체를 할당한다.
다음 atom들은 일반적으로 이 텍스트 개체의 콘텐츠를 수정하는데 사용된다.
PowerPoint는 OutlineTextRefAtom를 만나면, 참조되는 텍스트 개체가 이미 내부 데이터 구조 내 어딘가에 존재한다고 가정하고 임시 텍스트 개체에 대해 할당된 메모리를 해제한다.

만일 이 두 이벤트가 동일 container 내에서 발생되면, PowerPoint는 동일 container 내의 나머지 atom들을 처리할 때 이미 해제된 임시 텍스트 개체를 사용하려고 시도하게 되고, 결국 메모리 손상이 발생하게 된다.

아래 예제는 위 취약한 방법으로 실행되는 PowerPoint의 파일 포맷을 분석한 내용이다.

```
2C00h: 02 3C 03 0F 00 0D F0 40 00 00 00 00 00 9F 0F 04
2C10h: 00 00 00 04 00 00 00 00 00 A0 0F 02 00 00 00 2A
2C20h: 00 00 00 9E 0F 16 00 00 00 02 00 00 00 00 00 00
2C30h: 08 00 00 02 00 02 00 00 00 00 00 02 00 0E 00 00
```

struct PPT_CONTAINER MSOClientTextbox[4]		2C03h
struct PPT_RECORD_HEADER hdr		2C03h
USHORT recVer : 4	15	2C03h
USHORT recInstance : 12	0	2C03h
USHORT recType	61453	2C05h
LONG recLen	64	2C07h
struct PPT_RECORD TextHeaderAtom[6]		2C0Bh
struct PPT_RECORD_HEADER hdr		2C0Bh
USHORT recVer : 4	0	2C0Bh
USHORT recInstance : 12	0	2C0Bh
USHORT recType	3999	2C0Dh
LONG recLen	4	2C0Fh
BYTE data[4]	┘	2C13h
struct PPT_RECORD Atom[71]		2C17h
struct PPT_RECORD OutlineTextRefAtom		2C21h
struct PPT_RECORD_HEADER hdr		2C21h
USHORT recVer : 4	0	2C21h
USHORT recInstance : 12	0	2C21h
USHORT recType	3998	2C23h
LONG recLen	22	2C25h
BYTE data[22]	┐	2C29h

[그림 1-18] Power Point 파일 포맷

MSOClientTextbox container의 길이는 (40 00 00 00)으로 64바이트이고, 그 안에

TextHeaderAtom (9F 0F) 3999와 OutlineTextRefAtom (9E 0F) 3998이 포함되어 있어 취약한 부분을 가진 PowerPoint 파일이라고 할 수 있다.

아래와 같이 취약한 부분을 통해 다른 메모리 위치에서 쉘 코드가 실행되는 것을 확인할 수 있다.

```
0:000> t
eax=0089bac4 ebx=00000000 ecx=0089e640 edx=0089ebd4 esi=001336cc
edi=00000000
eip=300501cd esp=001335ec ebp=00133680 iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00200202
PowerPoint+0x501cd:
300501cd ff501c call dword ptr [eax+1Ch] ds:0023:0089bae0=0089bb54
```

➔ **악의적인 쉘 코드 분기 부분**

```
0:000> t
eax=0089bac4 ebx=00000000 ecx=0089e640 edx=0089ebd4 esi=001336cc
edi=00000000
eip=0089bb54 esp=001335e8 ebp=00133680 iopl=0 nv up ei pl nz na po nc
cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00200202
<Unloaded_ed20.dll>+0x89bb53:
0089bb54 0d00000000 or eax,0
```



```
0089bb54 0d00000000 or eax,0
0089bb59 0000 add byte ptr [eax],al
0089bb5b 0000 add byte ptr [eax],al
0089bb5d 0000 add byte ptr [eax],al
0089bb5f 0000 add byte ptr [eax],al
0089bb61 0000 add byte ptr [eax],al
0089bb63 0000 add byte ptr [eax],al
0089bb65 0018 add byte ptr [eax],bl
0089bb67 00c0 add al,al
0089bb69 0000 add byte ptr [eax],al
0089bb6b 00c0 add al,al
0089bb6d 90 nop
0089bb6e 90 nop
0089bb6f 90 nop
0089bb70 eb2b jmp <Unloaded_ed20.dll>+0x89bb9c (0089bb9d)
```

```
0089bb72 33c0              xor     eax,eax
0089bb74 50                push    eax
0089bb75 648920            mov     dword ptr fs:[eax],esp
0089bb78 33ff              xor     edi,edi
0089bb7a 81c700100000      add     edi,offset <Unloaded_ed20.dll>+0xfff (00001000)
0089bb80 b8d0cf11e0        mov     eax,0E011CFD0h
0089bb85 3b07              cmp     eax,dword ptr [edi]
0089bb87 75f1              jne     <Unloaded_ed20.dll>+0x89bb79 (0089bb7a)
0089bb89 40                inc     eax
0089bb8a 3b87000a0000      cmp     eax,dword ptr <Unloaded_ed20.dll>+0x9ff
(00000a00)[edi]
0089bb90 75e8              jne     <Unloaded_ed20.dll>+0x89bb79 (0089bb7a)
0089bb92 81c7000a0000      add     edi,offset <Unloaded_ed20.dll>+0x9ff (00000a00)
0089bb98 83c704            add     edi,4
0089bb9b ffe7              jmp     edi
0089bb9d e8d0ffffff        call    <Unloaded_ed20.dll>+0x89bb71 (0089bb72)
```

위 코드를 통해, 취약점을 이용하는 쉘 코드 부분을 PowerPoint 파일에서도 확인할 수 있다.


```
A:D870h: 00 00 A0 0F 96 00 00 00 C0 90 90 90 EB 2B 33 C0
A:D880h: 50 64 89 20 33 FF 81 C7 00 10 00 00 B8 D0 CF 11
A:D890h: E0 3B 07 75 F1 40 3B 87 00 0A 00 00 75 E8 81 C7
A:D8A0h: 00 0A 00 00 83 C7 04 FF E7 E8 D0 FF FF FF 8B 54
A:D8B0h: 24 0C 33 C0 B4 10 33 DB B3 9C 01 04 13 33 C0 C3
A:D8C0h: CD 01 05 30 52 FF 49 FF 56 FF 41 FF 54 FF 45 FF
```

[그림 1-19] 쉘 코드

원격의 공격자가 대상 사용자로 하여금 동일 container 내에 TextHeaderAtom 다음에 OutlineTextRefAtom이 따라 오도록 조작된 프리젠테이션 파일을 열도록 유도하는 방법으로 이 취약성을 공격할 수 있을 것이다.

공격에 성공하면, 공격자가 현재 로그인 된 사용자의 보안 컨텍스트에서 임의의 코드를 실행할 수 있다.

4. 중국 보안 이슈 – 중국의 정보보안 관련법

■ 강화된 중국의 정보보안 관련 형법

2009년 2월 중국에서는 제 11회 중화인민공화국 전국인민대표회의 상무의원 회의가 개최되었다. 전국인민대표회의는 한국으로 비교하자면 현재 시행되고 있는 법령을 현실에 맞게 개정하기 위해 국회의원들이 모여 법령을 개정하기 위한 회의라고 할 수 있다.

[그림 1-20] 개정된 중화인민공화국 형법 수정 건 7호

이번에 개정된 법령은 중화인민공화국 주석령으로 한국과 비교하자면 대통령령 정도 볼 수 있다. 개정된 법령은 모두 2월 28일자로 시행되며 총 15건에 대한 형법이 개정되었다. 이 중에는 해외 상품에 대한 밀수 관련 처벌 사항과 유가증권을 통한 증시조작 그리고 세금 포탈 등과 관련된 형법들이 개정되었다.
이 중에서도 정보 보안을 다루는 보안 업체에서 관심을 가져야 할 수정된 형법은 바로 9조에 표기한 정보 시스템 보호 관련 형법이다. 아래는 이 번에 개정된 정보 시스템 보호 관련 형법 전문을 정리하면 다음과 같다.

9조, 형법 제 285조에 근거하여 2차와 3차 개정안에 다음의 사항들을 추가한다.

“반국가규정에 근거해서, 컴퓨터 시스템 또는 기타 기술수단을 이용하여 침입(해킹)을 하거나, 컴퓨터 시스템에 저장한 데이터 또는 전송되는 데이터를 획득 또는 가로채거나 컴퓨터 시스템을 불법 제어 할 경우, 상황의 심각성에 따라 3년 이하의 징역 또는 구금에 처하며 이와 동시에 벌금도 부과된다. 상황이 특수하게 심각할 경우, 3년 이상 7년 이하의 징역 또는

구금에 처하며 이와 동시에 벌금도 부과된다.”

”전문적으로 침입(해킹)하기 위해 불법으로 컴퓨터 시스템의 프로그램 또는 도구(유틸리티)를 제어 및 제공하거나 명백하게 알려진 타인의 컴퓨터 시스템에 대해 범죄의 목적으로 침입(해킹) 및 제어하거나 프로그램 및 유틸리티를 제공할 경우 상황의 심각성에 따라 법령에 대한 불이행으로 간주하고 처벌 한다.”

이번 형법 개정안에 포함된 정보 시스템 보호 관련 형법을 본다면 전반적으로 불법적인 해킹과 악성코드 유포 및 소스코드 거래에 대해 정국 정부의 엄격한 법령 적용을 하겠다는 의지로 볼 수 있다. 그러나 이번 형법의 개정으로 인해 중국발 해킹이 감소 할 지는 조금 더 시간을 두고 지켜 볼 필요가 있을 것이다.

II. ASEC 칼럼

■ Ineternet Explorer 8.0의 편리함과 보안 위협

지난 3월 IE8(Internet Explorer 8.0)이 정식 출시 되었다. 과거 7.0 버전에 비해 많은 기능들이 추가되고 성능도 좋아졌다는 평가를 받고 있어, 타 브라우저들과의 경쟁에서 여전히 우위를 고수할 것으로 전망된다.

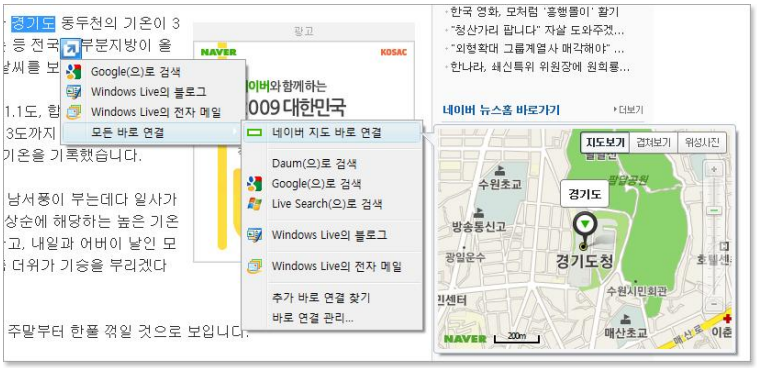
그러나 보안적인 측면에서 바라본다면 IE8에서도 여전히 많은 문제점들이 남아있고, 사용자 편의를 위해 제공되는 기능들이 스파이웨어에 의해 악용될 가능성이 있어 우려가 된다. 이 글에서는 IE8에서 새로이 추가된 기능들과 그 기능들이 앞으로의 스파이웨어에 의해 어떻게 악용될 수 있는지, 그리고 여전히 남아있는 IE의 보안 헛점을 알아보도록 한다.

1. IE8에 새로이 추가된 기능들

(1) 더 쉽고 빠르게

➢ **바로 연결(Accelerator)**

브라우징 도중, 웹 페이지의 단어를 번역하거나 그 단어로 검색을 하고자 할 때, 과거 IE7이하의 버전에서는 상당히 많은 작업을 거쳐야만 했다. 이제는 IE8의 '바로 연결' 기능을 이용하면 보다 손쉽고 빠른 작업 처리가 가능해졌다.



[그림 2-1] 바로 연결(Accelerator)

단순히 내가 원하는 특정 단어나 문자열을 드래그하여 선택하였을 때 나타난 '바로 연결' 아

이콘을 클릭하면 지도 검색, 번역, 쇼핑몰 검색 등의 다양한 서비스를 간편하게 이용할 수 있다.

➢ **비주얼 검색(Visual Search)**

검색창에 특정 단어를 입력하면 그와 관련한 연관 검색어를 보여주는 기능은 이미 많은 사용자들에게 익숙해져 있을 것이다. 그런데 '비주얼 검색'은 이보다 한 단계 더 나아가 단어를 입력하는 즉시 관련 정보를 제시해주어 검색에 낭비되는 많은 시간이 절약될 수 있다.

[그림 2-2] 비주얼 검색(Visual Search)

'비주얼 검색'은 단순히 문자만 보여주는 데서 그치지 않고 이미지까지 표시해주기 때문에 보다 상세한 정보를 얻을 수 있다.

➢ **웹 조각(Web Slice)**

인터넷 쇼핑몰을 이용해본 사람이라면 누구나 주문한 상품이 어디쯤 배송되었는지 확인하기 위해 몇 번이고 배송정보 페이지를 확인한 경험이 있을 것이다. 또 자신의 블로그나 홈페이지에 달린 댓글을 확인하기 위해 매번 그 페이지를 열어야 하는 번거로움을 한 번쯤은 겪었을 것이다. '웹 조각' 기능을 이용하면 이렇게 귀찮았던 작업을 간편하게 해결할 수 있다.

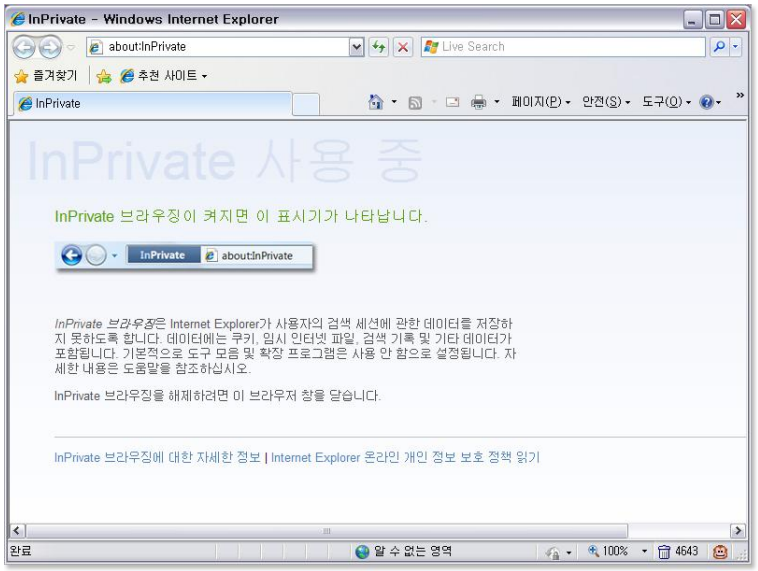
[그림 2-3] 웹 조각(Web Slice)

웹 페이지 상의 특정 영역을 '웹 조각'으로 등록하면 그 페이지의 내용이 바뀔 때마다 브라우저에서 알려준다.

(2) 안전한 보안

➢ **InPrivate**

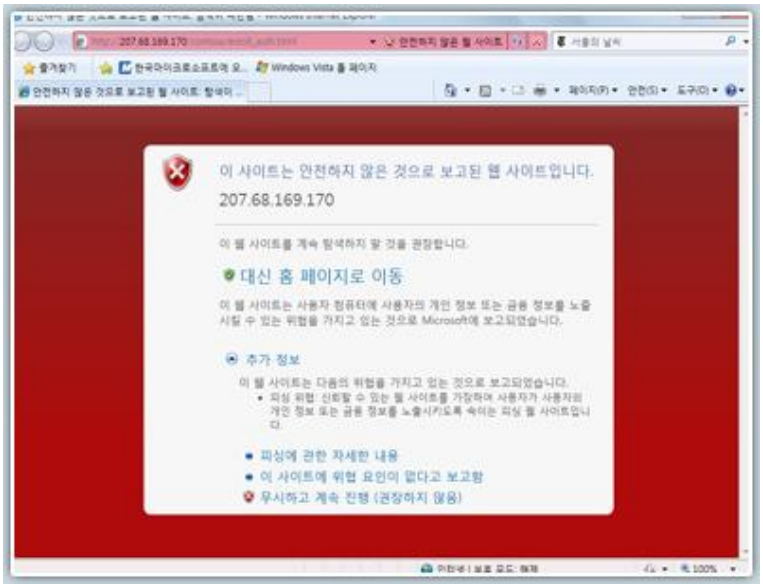
InPrivate' 기능을 이용하면 사용자의 인터넷 검색 기록, 임시 인터넷 파일, 양식 데이터, 쿠키 및 사용자 이름/암호 기록이 브라우저에 의해 남지 않아 은밀한 웹 서핑이 가능해진다.



[그림 2-4] InPrivate

➢ **SmartScreen**

인터넷을 사용하다 보면 자신도 모르게 악성코드가 삽입되었거나 악의적인 목적으로 제작된 사이트에 접속하게되는 경우가 허다하다. SmartScreen 기능을 사용하면 이러한 위협으로부터 보다 안전해질 수 있다.



[그림 2-5] SmartScreen

2. 그러나, 독이 될 수 있는 기능들

'더 쉽고 빠르게'라는 슬로건처럼 IE8에서는 인터넷을 사용하는데 편리한 기능이 많이 추가되었다. 그러나 이러한 기능들이 과연 편하기만 할까? 기우일지는 모르겠으나 아마도 이러한 기능을 악용하는 애드웨어들이 앞으로 많이 출현하지 않을까 하는 걱정이 앞선다. 특히 '바로 연결'과 '웹 조각' 기능은 수많은 애드웨어 제작자들이 군침을 흘릴만한 기능이 아닐 수 없다.

과거 IE를 타깃으로 하는 애드웨어들은 주로 주소표시줄, 즐겨찾기, 표준 단추 등을 이용하여 광고를 표시하거나 자신의 웹 사이트로의 방문을 유도하는 형태로 동작하였다. 그러나 이제 IE8부터는 '바로 연결', '웹 조각', '비주얼 검색' 이라는 먹잇감이 더 늘게 된 것이다.

➢ **바로 연결**

2006년 이후 한국에는 엄청난 '툴바' 열풍이 불었고 그 열기는 지금도 계속 이어져 오고 있다. 그 열기가 한창일 때는 PC 한 대에 여러 개의 툴바가 동시에 설치되어 [[그림 2-6] 화면의 절반을 채운 툴바

]과 같이 IE 화면의 절반을 툴바로 가득 채울 정도였다.

[그림 2-6] 화면의 절반을 채운 툴바

'바로 연결'도 툴바와 마찬가지로 애드웨어들의 치열한 다툼의 자리가 될 것으로 예상된다. '바로 연결'을 선택하면 화면 전체 세로 길이와 맞먹을 정도로 수많은 연결 메뉴가 나타나고 사용자는 어떤 서비스를 선택해야 할지 몰라 난감하게 될지도 모른다.

- **웹 조각**

과거 많은 애드웨어들이 광고를 보여주기 위한 방법으로 '팝업창'을 많이 이용하였다. 매시간마다 혹은 매초마다 주기적으로 뜨는 '팝업창'은 사용자들을 무척이나 괴롭혀왔다. 애드웨어의 입장에서 '웹 조각' 기능은 새로운 창으로 뜨는지 그렇지 않은지의 차이일 뿐, '팝업창'과 별반 다를 것이 없다. 그러나 현재 사용자가 보고 있는 브라우저 안에서 보여주는 광고이기에 '팝업창'보다 더 효과적인 광고 방법이 될 것이다.

[그림 2-7] 애드웨어에 의해 등록된 웹 조각 예제

8.0 이전의 IE에서 새로운 창을 띄우지 않고 광고를 보여주기 위해서는 BHO를 이용하여 웹 페이지 안에 광고를 삽입하는 방법을 이용하였는데, 이 방법은 복잡한 기술을 이용해야 했다. 그러나 '웹 조각' 기능은 그럴 필요 없이 비교적 간단한 방법으로 등록되어 IE 상단에 표시되기 때문에 더할 나위 없이 좋은 광고 수단이 된다. 아마도 애드웨어 제작자들이 가장 좋아하게 될 기능으로 예상된다.

- **비주얼 검색**

검색 서비스 공급자로 포르노 검색 사이트가 등록된다면 어떻게 될까? 이 기능 역시 과거 주소표시줄과 마찬가지로 수많은 애드웨어들이 서로 기본 검색 서비스 공급자로 등록되기 위해 치열한 전쟁을 벌일 전쟁터가 될 것이다.

[그림 2-8] 성인광고가 표시되는 비주얼 검색

3. 여전히 문제가 되는 ActiveX와 BHO

IE8이 성능이나 사용자 편의 면에서는 많은 개선이 이루어진 것으로 인정할 수 있겠으나 보안과 관련한 부분에서만큼은 합격점을 주기가 어렵다. 특히 ActiveX와 BHO에 관련해서는 이전 버전과 같이 개선된 부분이 없어 아쉬움이 크다.

ActiveX와 BHO는 IE에서 플러그인 형태로 등록되어 막강한 기능을 제공해준다. 우리가 여느 웹 사이트에서 흔히 볼 수 있는 Flash 역시 ActiveX로 IE에 등록되어 동작한다. 이 밖에도 보안 프로그램, 웹 하드디스크 등 수많은 프로그램들이 ActiveX나 BHO의 형태로 등록되어 사용자에게 많은 편의를 제공한다.

그런데 이런 ActiveX나 BHO는 매우 강력한 만큼 그에 따른 위험이 뒤따른다. 일단 IE에 설치된 ActiveX나 BHO는 시스템에 설치된 여느 프로그램과 다름없이 무엇이든 다 할 수 있기 때문이다. 프로그래머가 나쁜 마음을 먹는다면 악성코드를 다운로드 하여 실행할 수도 있고, 심지어는 그 자체가 악성코드가 되어 시스템을 망가뜨릴 수도 있다. 실제로 BHO는 2008년 한해 동안 V3에 진단 추가되는 스파이웨어 중 4.8%나 될 만큼 그 비중이 크다. 하지만, IE8에서 이전 버전과 비교해 ActiveX나 BHO와 관련해 보안상 나아진 부분이 사실상 없다고 봐도 무관하다. 여전히 이로 인한 위협이 남아 있는 것이다.

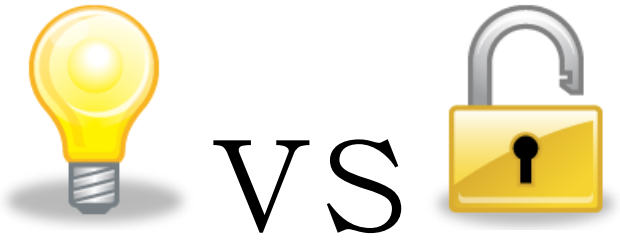
IE8에서 피싱 필터 기능을 보다 개선한 'SmartScreen' 기능을 내놓았으나, 전적으로

Microsoft에 등록된 데이터베이스에 의존하는 것이기에 등록되지 않은 사이트에 접속하거나 그 사이트로부터 악성코드를 다운로드 받을 경우엔 효과를 보지 못한다. 게다가 'SmartScreen' 기능은 단지 접속만 차단하는 것이기에 ActiveX나 BHO가 내부적으로 어떤 동작을 하든 그 것을 차단할 수는 없다.

'바로 연결'과 '웹 조각' 그리고 '비주얼 검색' 모두 매우 유용한 기능임에는 틀림없다. 하지만 그 유용한 만큼 애드웨어에 노출될 위협은 커졌다. ActiveX와 BHO 역시 막강한 부가기능을 제공하지만 그만큼 악성코드로부터 내 시스템이 위험해질 수 있다.

4. 편리함 VS 보안

이러한 경우처럼 가끔 우리는 무언가를 얻기 위해 다른 어떤 하나를 포기해야만 하는 경우가 있다. 보안과 편리함의 관계가 바로 그러한 관계일 것이다. 집안의 중요한 물건을 안전하게 지키기 위해서는 겹겹이 자물쇠를 채우는 방법이 있다. 그러나 매번 집을 들어설 때마다 수많은 자물쇠를 하나하나 풀어야 하는 번거로움이 생긴다.



[그림 2-9] 편리함 VS 보안

그러나 IE8에서 편리함과 보안 모두 이전 버전 보다는 많은 개선이 이루어진 것임은 틀림없다. 그렇지만 향상된 편리함에 비해, 보안에 있어서는 갈수록 커져만 가는 위협들로부터 사용자를 지키기에 그 진보가 미약하다고 느껴진다.

물론 IE가 다른 브라우저들에 비해 유독 보안에 취약하거나 한 것은 결코 아니다. 또한, 다른 브라우저라고 해서 많은 보안 위협으로부터 안전한 것은 아니다. 다만 IE는 가장 많은 사람들이 사용하는 브라우저이기에 항상 악성코드의 주요 타깃이 될 수밖에 없는 것이다. 다음 버전에서는 브라우저 시장의 강자답게 편리함과 보안, 이 두 마리 토끼를 모두 잡을 수 있기를 기대해본다.

III. 이달의 통계

1. 악성코드

(1) 4월 악성코드 통계

순위		악성코드명	건수	비율
1	new	Dropper/Agent.170797	9	11.7%
1	new	Dropper/OnlineGameHack.173857	9	11.7%
1	new	Win-Trojan/Agent.1470464.B	9	11.7%
1	new	Win-Trojan/Autorun.86016.E	9	11.7%
2	new	Win-AppCare/HackTool.13531	8	10.4%
3	new	Win32/IRCBot.worm.126976.AI	7	9.1%
3	new	Win-Adware/Elog.365568	7	9.1%
3	new	Win-AppCare/Agent.8704.B	7	9.1%
4	new	Dropper/OnlineGameHack.174326	6	7.8%
4	new	Win-Downloader/Rogue.XPPoliceAntivirus.52230	6	7.8%
합계			77	100.0%

[표 3-1] 2009년 3월 악성코드 피해 Top 10

순위		악성코드명	건수	비율
1	new	Win-AppCare/Keylogger.205824	11	13.6%
2	new	Win-Trojan/Agent.9728.OI	10	12.3%
2	new	Win-Trojan/Downloader.23552.OD	10	12.3%
3	new	Dropper/Agent.172913	8	9.9%
4	↓2	Win-AppCare/HackTool.13531	7	8.6%
4	new	Win-Trojan/Downloader.97416	7	8.6%
4	new	Dropper/OnlineGameHack.173553	7	8.6%
4	new	Dropper/OnlineGameHack.172748	7	8.6%
4	new	Win-Trojan/Agent.11264.KL	7	8.6%
4	new	Dropper/OnlineGameHack.171819	7	8.6%
합계			81	100.0%

[표 3-2] 2009년 4월 악성코드 피해 Top 10

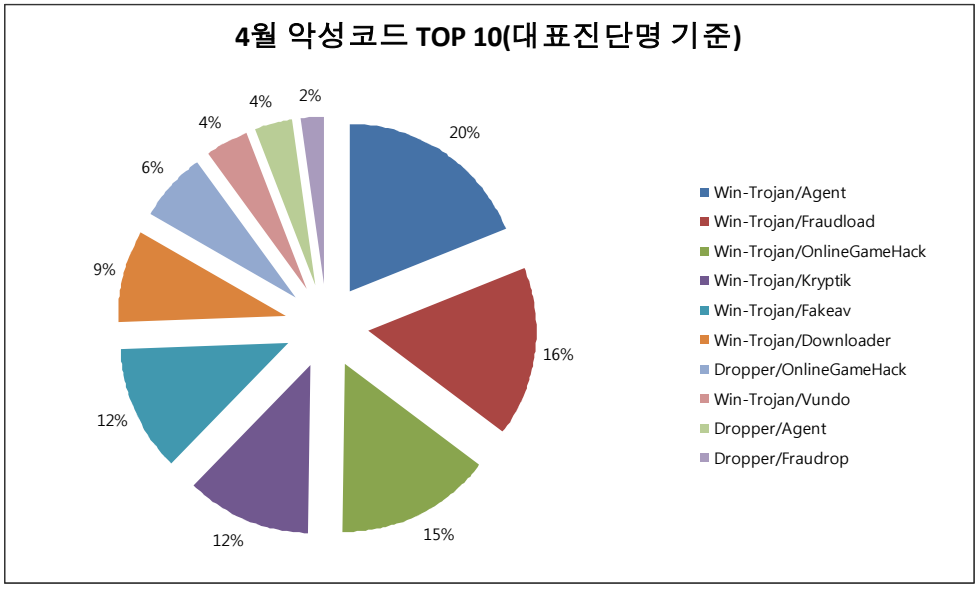
[표 3-1]은 2009년 3월 악성코드 피해 Top 10이며, [표 3-2]는 2009년 4월 악성코드로 인한 피해 Top 10을 나타낸 것이다.

4월에 이슈가 된 악성코드로는 'Win-Trojan/Downloader.97416'을 들 수 있다. 해당 악성코드가 실행되면서 생성되는 파일이 Autorun 웜, OnlineGameHack, AVKiller등 다양한 악의적인 기능을 수행한다. Autorun 웜 기능으로 인하여 USB저장장치를 많이 사용하는 국내에서는 매우 확산도가 컸으며, AVKiller 기능으로 인해 엔진업데이트가 이뤄진다고 하더라도 V3가 실행되지 않는 증상으로 인해 불만을 호소하는 고객의 문의가 다수 접수되었다. 또한 일부 시스템의 경우 스마트업데이트 파일이 손상되어 업데이트조차 진행되지 않아 부득이 감염된 시스템의 경우 전용백신과 함께 제품을 재 설치해야 하는 번거로움을 겪을 수 밖에 없었다. 나날이 악성코드는 발전하고 있다. 안티바이러스의 진단을 회피하는 기법과 함께 안티바이러스 제품을 무력화 시키는 악성코드에 대항하기 위해서는 진단율 향상과 더불어 자체보호기능을 강화시켜 나가야 할 것이다.

아래의 표와 그림은 대표진단명을 기준으로 변형들을 묶어 통계를 뽑은 것이다. 근래 악성코드의 활동 주기가 짧아짐-악성코드 제작자와 진단율 향상 등에 의해-에 따라 변형을 다룬 악성코드에 대한 통계보다 대표진단명을 통해서 전체적인 악성코드 감염 양상을 알 수 있다.

순위		악성코드명	건수	비율
1	↑1	Win-Trojan/Agent	445	19.0%
2	new	Win-Trojan/Fraudload	379	16.2%
3	-	Win-Trojan/OnlineGameHack	352	15.0%
4	new	Win-Trojan/Kryptik	285	12.2%
5	↑3	Win-Trojan/Fakeav	282	12.0%
6	↓5	Win-Trojan/Downloader	212	9.0%
7	↓2	Dropper/OnlineGameHack	152	6.5%
8	new	Win-Trojan/Vundo	101	4.3%
9	↓3	Dropper/Agent	84	3.6%
10	new	Dropper/Fraudrop	51	2.2%
합계			2,343	100.0%

[표 3-3] 2009 4월 악성코드 대표진단명 Top 10



[그림 3-1] 2009년 4월 악성코드 대표진단명 Top 10

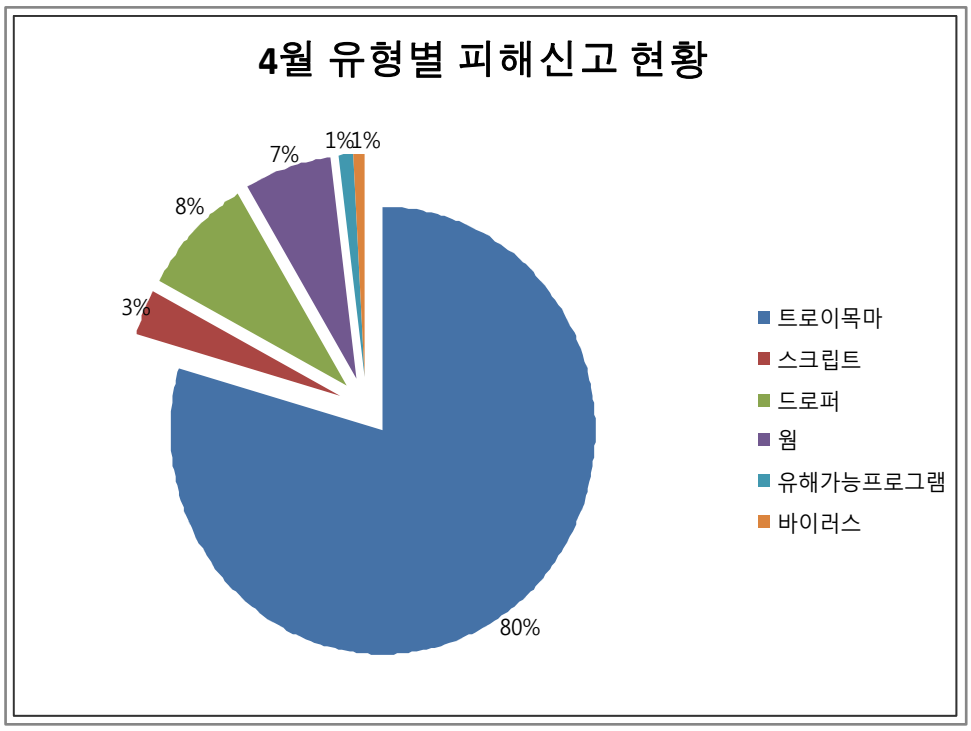
[표 3-3]과 [그림 3-1]은 2009 4 월 악성코드의 대표진단명을 기준으로 유형별 피해 순위 Top 10 을 나타내고 있다.

4월 악성코드 대표진단명 Top 10을 살펴 보면 OnlineGameHack이 여전히 강세를 보이며 전체 약 21.5%(3위와 7위)의 비율을 차지하고 있다. 그러나 4월 대표진단명에서 눈여겨 볼 만한 사항은 FakeAV, Zlob, Vundo, Kryptik, Fraud등으로 불리우는 허위 안티스파이웨어류이다.

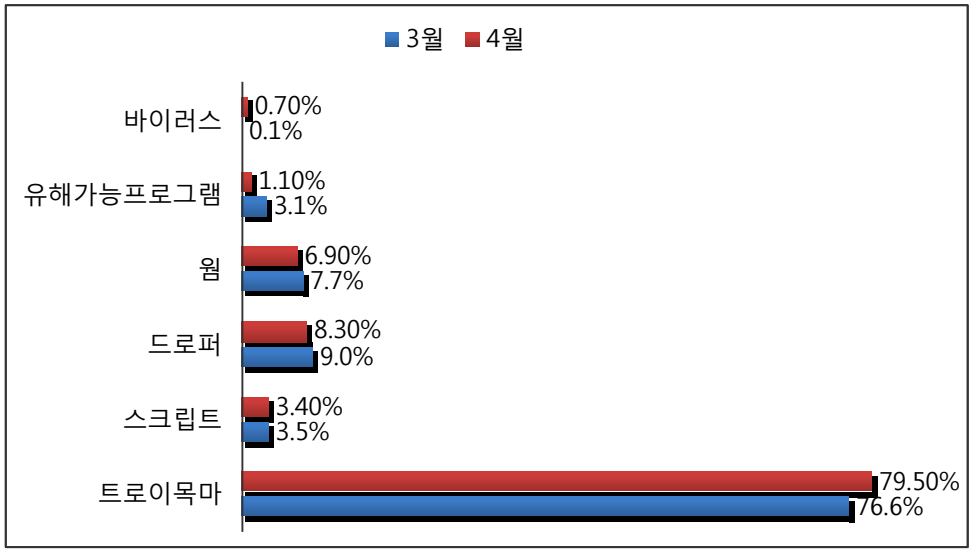
그 동안 하위권에 머물렀던 허위 안티스파이웨어류가 4월에는 전체 약 46.9%라는 엄청난 비율을 차지하고 있다. 이러한 허위 안티스파이웨어류에 감염되면 유사류의 악성코드를 다수 다운로드하는 특징이 있으며, 사용자가 설치 및 검사하지 않았음에도 감염되었다는 Alert을 띄워주고 허위로 진단하여 마치 시스템이 많은 악성코드가 감염된 것처럼 보여준다. 이에 사용자들을 유혹해 온라인 결제로까지 유도하여 금전적인 목적을 취하고 있다. 이를 예방하기 위해서는 게시판, 자료실, E-mail등 의심되는 파일은 가급적 실행하지 말고 감염되었다 하더라도 허위 안티스파이웨어임을 인지하여 백신프로그램을 이용한 진단/치료 및 [바이러스신고센터]로 신고하여 피해를 줄일 수 있다.

아래의 [그림 3-2]는 2009년 4월 전체 악성코드 유형별 피해신고 건수를 나타내고 있는 그래프이다. 트로이목마 프로그램은 80%로 다른 악성코드보다 월등히 많은 비율을 차지하고 있으며, 드롭퍼와 웜이 각각 8%와 7%를 차지하고 있으며, 그 뒤를 이어 스크립트 3%, 유해가능 프로그램이 1%를 차지하고 있다. 저번 달과 동일하게 바이러스는 0.7%로 극히 낮은

비율을 유지하고 있다.

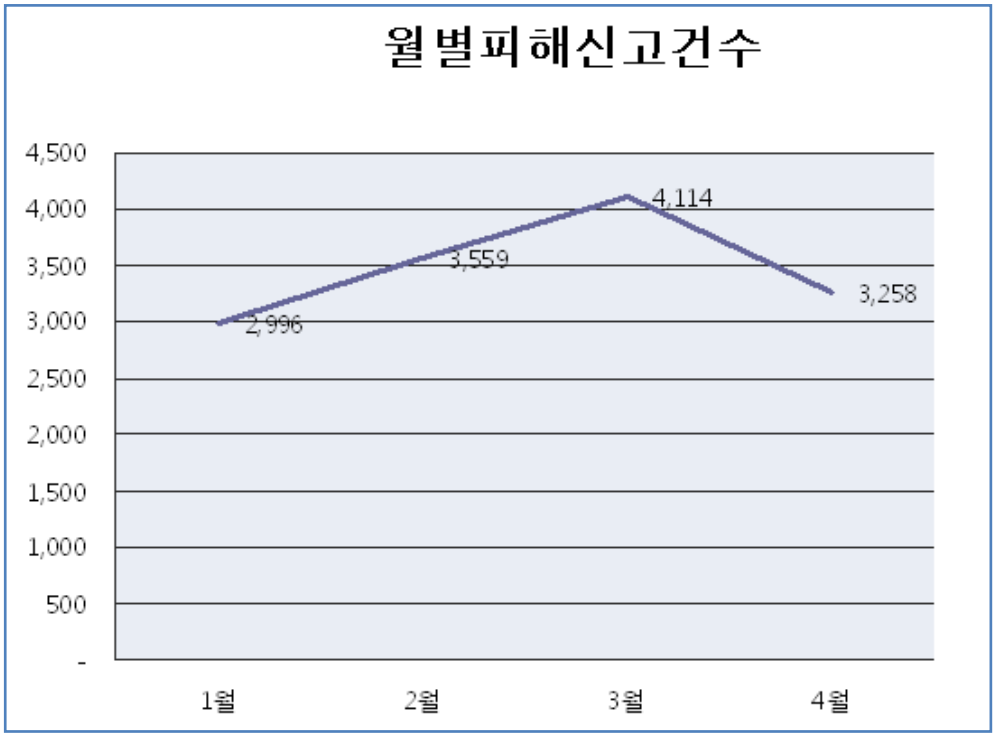


[그림 3-2] 2009년 4월 악성코드 유형별 피해신고 비율



[그림 3-3] 2009년 월 악성코드 유형별 피해신고 비율 전월 비교

위의 [그림 3-3]은 전월과 비교한 악성코드 유형별 피해신고를 나타낸 것이다. 증가한 것은 트로이목마의 경우 전월과 비교하여 2.9%가 늘어났으며, 웜은 6.9%로 전월에 비해 0.8%가 줄어 들었다. 드롭퍼도 8.3%로 전월에 비해 소폭 감소하였으며, 스크립트, 유해가능 프로그램과 바이러스는 약간의 수치 차이는 있겠으나 전월과 많은 차이가 없었다.



[그림 3-4] 월별 피해신고 건수

[그림 3-4]는 월별 피해신고 건수를 나타내는 그래프로 2월부터 피해가 증가하였으나 4월에는 전달에 비해 엔진에 반영된 샘플수가 전달에 비해 약 2배정도 증가함에 따라 사전대응이 높았던 것으로 추정된다. 참고로, 4월에 반영된 엔진은 3월 대비 트로이목마는 55,133개에서 98,990개로, 웜은 2,115개에서 4,441개로, 트로이목마는 55,133에서 98,990개로 증가하였다.

그러나, 엔진 진단률 향상만으로는 시스템을 안전하게 보호할 순 없다. 악성코드의 유형이 점차 은폐형 악성코드 및 최신 취약점을 이용하는 악성코드가 늘어남에 따라 피해를 막기 위해서는 최신 보안패치와 함께 최신 버전의 백신프로그램으로 주기적으로 검사하는 습관이 필요하다.

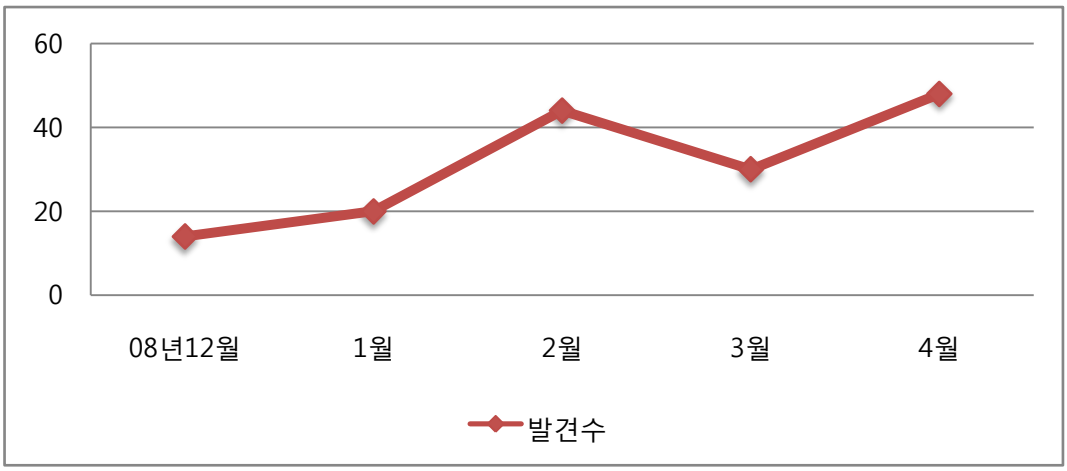
(2) 국내 신종(변형) 악성코드 발견 피해 통계

4월 한 달 동안 접수된 신종(변형) 악성코드의 건수 및 유형은 [표 3-4] 과 같다.

월	트로이목마	드롭퍼	스크립트	웜	파일	유해가능	합계
02 월	1691	261	105	166	11	22	2256
03 월	1385	237	80	151	1	14	1868
04 월	1700	202	92	190	1	24	2209

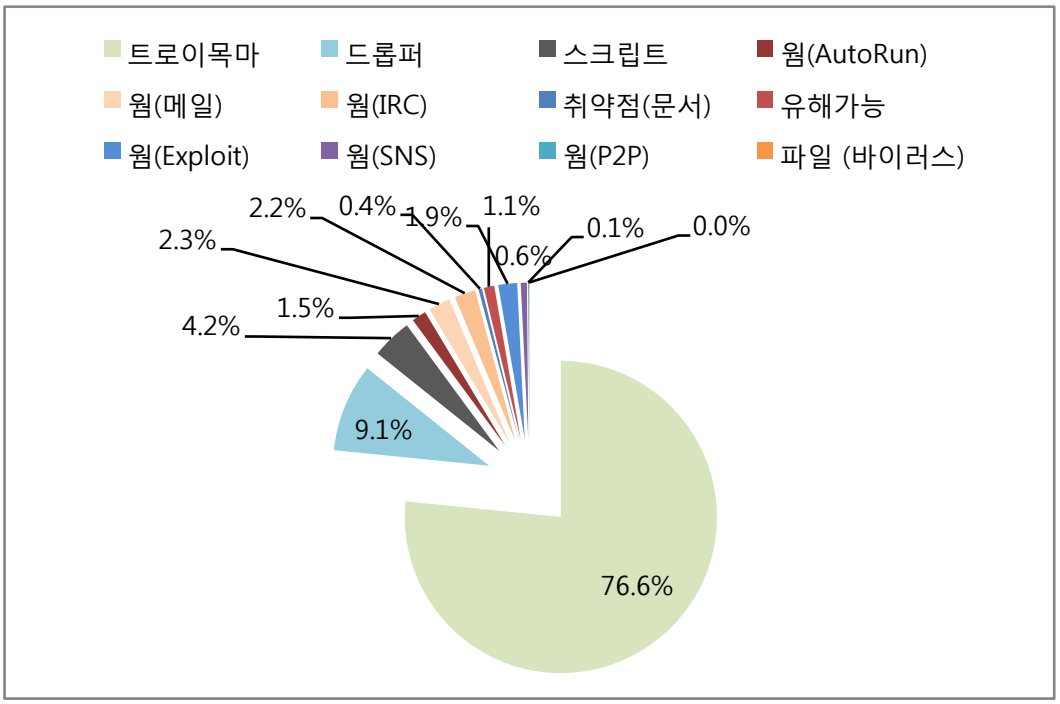
[표 3-4] 2009년 최근 3개월 간 유형별 신종(변형) 악성코드 발견 현황

이번 달 악성코드 전월 대비 18% 증가 하였다. 이는 올해 들어 두 번째로 많은 악성코드가 보고 되었다. 특히 트로이목마와 웜 유형이 증가 하였는데 트로이목마는 전월 대비 25% 증가 하였고 웜은 26% 증가 하였다. 이 두 가지 유형의 악성코드가 증가한 원인은 명확하지는 않다. 보통 트로이목마의 증가에 연관이 있는 드롭퍼의 경우 오히려 그 수가 소폭 감소하였다. 웜 유형에서는 IRCBot 웜이 최근 3개월간 많은 수가 보고 되고 있는데 이유 역시 명확하지 않다. 작년 말과 올해 1월의 경우 작년과 비슷한 수치를 보이고 있는데 최근 3개월간은 부쩍 증가 하였다. 서버 서비스 취약점인 MS08-067 과 어느 정도 연관성도 배제할 수는 없다고 생각된다. 다음은 최근 Win32/IRCBot.worm에 대한 통계이다.



[그림 3-5] 2009년 최근 5개월 간 Win32/IRCBot.worm 현황

이외에도 Win-Trojan/Buzus라고 불리는 악성코드도 동일 취약점을 이용하여 자신을 전파하는데 사용되고 있다. 서버 서비스 취약점이 원격 코드 실행이 가능한 취약점이므로 Win-Trojan/Conficker를 비롯해서 다수의 악성코드에서 사용 되고 있음을 알 수 있다.
다음은 이번 달 악성코드 유형을 상세히 분류 하였다.



[그림 3-6] 2009년 04월 신종 및 변형 악성코드 유형

트로이목마 유형은 전월 대비 23% 증가 하였다. 그러나 많은 감염보고가 있는 온라인 게임의 사용자 계정을 탈취하는 형태는 전월 대비 11% 감소 하였다. 증가 추세를 보인 트로이목마는 다음과 같다.

- Win-Trojan/Downloader
- Win-Trojan/Vundo
- Win-Trojan/Rustock

Win-Trojan/Downloader(이하 다운로더 트로이목마)는 진단명 그대로 다른 악성코드를 특정 호스트로부터 다운로드 및 설치하는 형태를 말한다. 과거와 달리 현대의 다운로더 트로이목마는 정상 시스템 프로세스에 리모트 쓰레드를 생성하거나 정상 시스템 파일을 실행 후 메모리 로드 된 이미지를 자신과 교체하여 방화벽과 HIPS(Host Intrusion Prevention System)로 부터 우회기법을 사용하는 등 지능적으로 발전하고 있는 추세이다. Win-Trojan/Vundo(이하 번도 트로이목마)는 스팸 메일 형태로 전파 되기도 하며 외산 가짜백신과도 관련이 있다. 번도 트로이목마의 경우 치료가 어려운데 이는 시스템 프로세스에 인젝션 되어 있기 때문이다. 따라서 동작 중에는 깔끔한 치료가 어렵고 대부분 재부팅 후 삭제하거나 BootTimeScan 기능을 이용하여 치료 될 수 있다. Win-Trojan/Rustock(이하 러스톡 트로이목마)는 잘 알려진 은폐형 스팸 메일러이다. 진단/치료 하기가 까다롭고 다수의 다른 악성코드를 설치하여 시스템을

복구하기 어려운 상태로 만들어둔다. 해당 트로이목마는 정상적인 NDIS.SYS나 Beep.SYS의 메모리 이미지를 자신으로 교체하거나 자신이 직접 NDIS.SYS 역할을 하면서 스팸 메일을 발송한다. 또한 별도의 SYS 형태로도 동작하는 형태도 있는 만큼 변형이 다양하고 유사한 악성코드가 많다. 시스템 프로세스에 커널모드 쓰레드를 만들어 자기 보호를 하는 변형도 존재하는데 역시 진단/치료가 까다롭다.

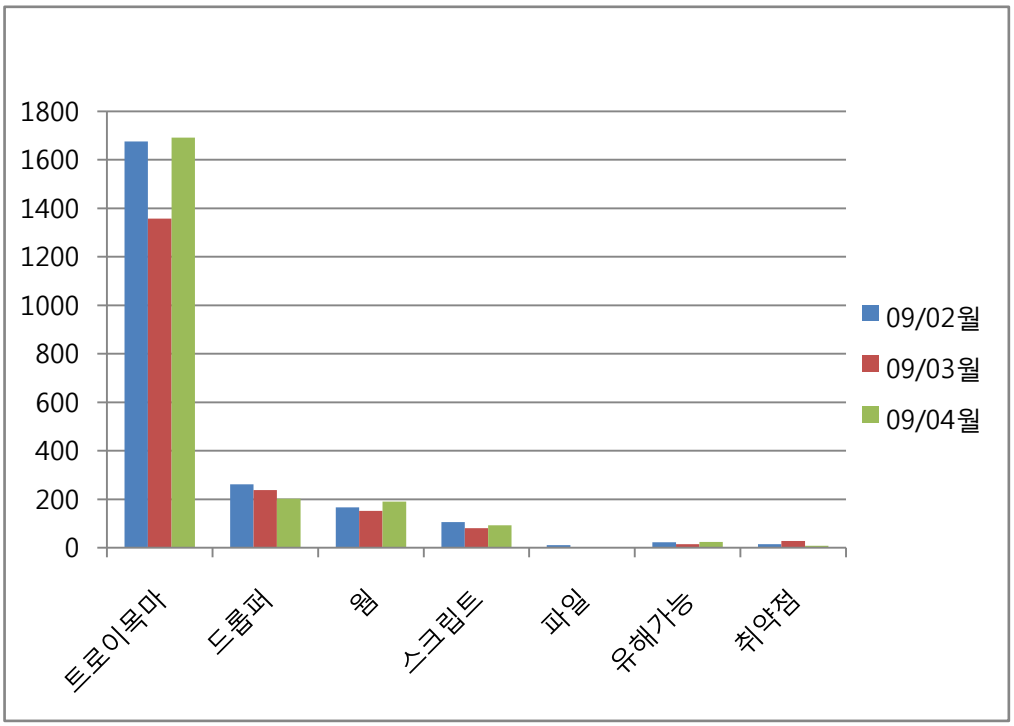
이처럼 최근 발견되고 있는 악성코드는 진단을 회피할 목적으로도 자신을 매번 다른 형태로 변형 시키지만 일단 감염 되면 진단하거나 제거하는데 어려움에 겪게 만들기도 한다. 매우 간단하지만 잘 지켜지지 않는 메일 및 메신저 특정 웹사이트 내 의심스러운 링크나 첨부파일은 실행 하지 않는 것만 지켜도 위해서 언급한 교활하고 지능적인 악성코드는 예방하는데 충분한 도움이 된다.

드롭퍼 유형은 전월 대비 15% 정도 감소 하였다. 일반적으로 트로이목마와 드롭퍼 유형이 동시에 증가하는게 일반적인데 이번 달은 달랐다. 드롭퍼 유형 역시 온라인 게임의 사용자 계정 정보를 탈취하는 형태의 악성코드 영향을 많이 받게 된다. 전체의 40% 넘는 형태가 온라인 게임 관련 악성코드 이기 때문이다. 따라서 이번 달 드롭퍼 유형이 감소하는 어느 정도 영향이 있었던 것으로 추정 된다.

스크립트 형태는 전월과 비교하여 큰 차이를 보이지 않았다. 웜 유형은 전월 대비 26% 증가 했다. 위에서 언급 했듯이 악성 IRCBot 웜 유형도 증가 했고 Win32/Waledac.worm 처럼 메일로 전파 되는 유형도 증가 했다. 또한 국외의 SNS(Social Networking Site)를 노리는 웜 형태의 악성코드 눈에 띄게 보고가 되었다.

취약점 관련 악의적인 문서 파일의 경우 PDF 관련 취약점이 전월에 이어서 다수 보고가 되고 있다. 대부분 작년에 알려진 오래된 취약점을 이용하는 형태가 많았다. 따라서 PDF 리더기가 업데이트가 되었거나 JavaScript를 사용하지 않도록 옵션을 변경 했다면 악의적인 문서를 오픈 하여도 별다른 문제가 되지 않는다. PDF와 같이 인터넷상에 표준이 되어 버린 문서의 경우 많은 사용자들이 이용하므로 그 만큼 많이 노출 되어 있기 때문에 앞으로도 취약점이 계속 보고 될 확률이 높으며 악성코드 제작자들에게 악용 될 소지가 많다. 문서 파일을 이용하여 악성코드를 설치 하는 형태는 사용자들이 문서파일과 같은 데이터 파일에 악성코드가 포함 될 수 있다는 것 자체에 의구심을 갖는 경우가 많다. 그리고 윈도우와 같은 OS 및 웹 브라우저에 대한 보안 업데이트만 신경을 쓰고 관련 프로그램의 보안 업데이트에 소홀히 할 수밖에 없다는 게 문제이다. 간단히라도 요즘 PDF 관련 뷰어들은 자동 업데이트 기능을 제공하므로 이를 이용하여 최신버전으로 유지만 하더라도 이러한 악의적인 PDF 를 이용한 공격에 최소한의 예방은 될 수 있다.

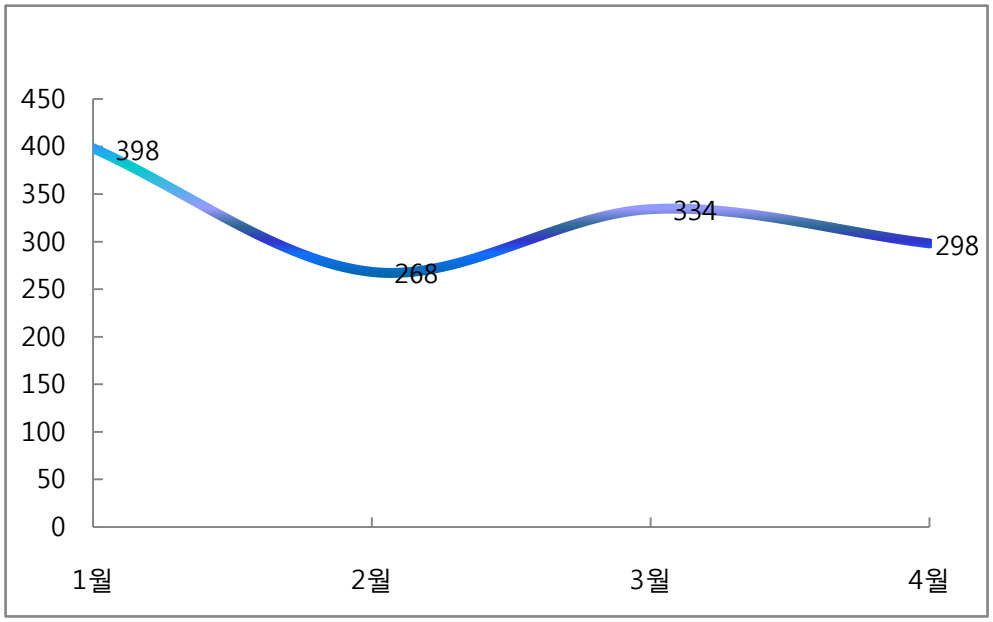
다음은 최근 3개월간 신종 및 변형 악성코드 분포이다.



[그림 3-7] 2009년 최근 3개월간 악성코드 분포

트로이목마 유형과 웜 유형은 최근 3개월 사이 가장 많은 보고가 있었다. 실행 파일을 감염시키는 바이러스는 새롭게 보고된 형태가 국내에서는 없었지만 Win32/Virut 바이러스 변형이 전월처럼 계속적인 변형이 나왔다. 드롭퍼 유형의 악성코드는 최근 3개월 사이에는 하락하는 추세를 보이고 있다. 앞서 말 했듯이 드롭퍼 유형 역시 상당수가 온라인 게임의 사용자 계정을 탈취 하는 형태가 40% 넘게 차지하므로 해당 악성코드가 감소하면 그에 따라서 변화 하므로 기복이 있는 편이다. 유해가능 및 스크립트 유형의 악성코드는 큰 변화는 없는 편이다. 취약점을 이용하는 형태는 비교적 최근에 알려진 PDF 관련 취약점을 이용하는 형태와 작년에 보고된 취약점이 혼재 되어 있는 형태가 보고 되었다.

다음은 온라인 게임의 사용자 계정을 탈취하는 악성코드의 추세를 살펴보았다.



[그림 3-8] 온라인 게임 사용자 계정 탈취 트로이목마 현황

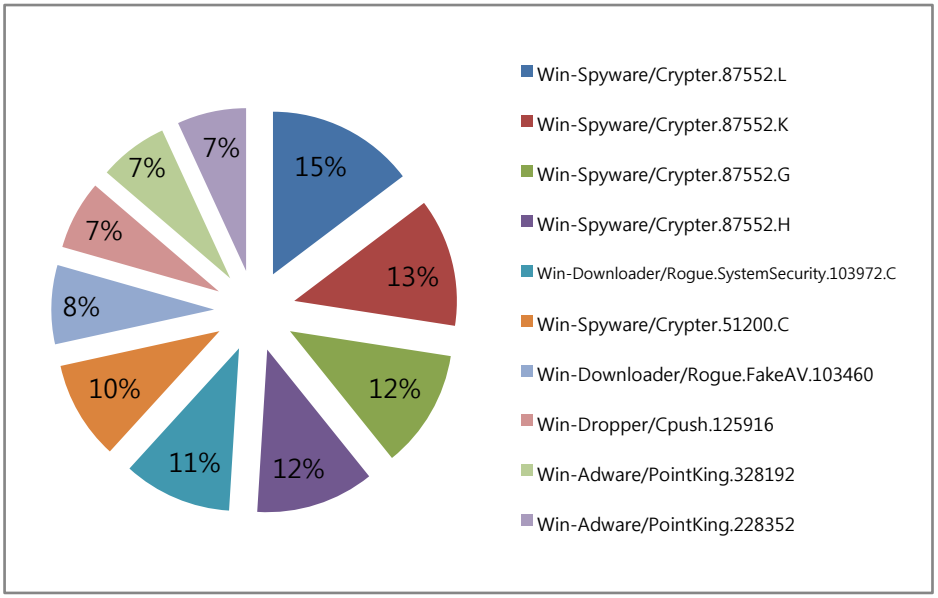
해당 악성코드는 전월 대비 11% 감소 하였다. 해당 악성코드 유형 역시 전월과 비교하여 감소 이외에 큰 영향을 보이고 있지 않다. 대부분이 국산 및 외산 온라인 게임의 사용자 계정을 노리고 있으며, 감염 후 다른 악성코드를 설치하는 등 이전과 크게 다르지 않았다.

2. 스파이웨어

(1) 4월 스파이웨어 피해 현황

순위		스파이웨어 명	건수	비율
1	New	Win-Spyware/Crypter.87552.L	15	15%
2	New	Win-Spyware/Crypter.87552.K	13	13%
3	New	Win-Spyware/Crypter.87552.G	12	12%
4	New	Win-Spyware/Crypter.87552.H	12	12%
5	New	Win-Downloader/Rogue.SystemSecurity.103972.C	11	11%
6	New	Win-Spyware/Crypter.51200.C	10	10%
7	New	Win-Downloader/Rogue.FakeAV.103460	8	8%
8	New	Win-Dropper/Cpush.125916	7	7%
9	New	Win-Adware/PointKing.328192	7	7%
10	New	Win-Adware/PointKing.228352	7	7%
합계			**102**	**≒100%**

[표 3-5] 2009년 4월 스파이웨어 피해 Top 10



[그림 3-9] 2009년 4월 스파이웨어 피해 Top 10

2009년 4월 스파이웨어 피해 Top 10에서는 스파이웨어 크립터(Win-Spyware/Crypter)로 인한 피해가 증가 한 것으로 나타났다. 허위감염 메시지를 노출해 외산 가짜백신 설치를 유도하거나 인터넷 익스플로러에 광고를 노출하는 스파이웨어 크립터는 꾸준히 피해 TOP 10에 나타나고 있다. 국내 애드웨어의 경우 자신의 정상적인 동작을 보장하기 위해 다른 프로

그램의 동작을 방해하는 경우가 계속해서 보고되고 있다. 4월 피해리스트에 등록된 리워드프로그램인 애드웨어 포인트킹(Win-Adware/PointKing)은 국산 애드웨어로 설치과정에서 다른 BHO를 삭제하는 기능이 있다. BHO가 삭제된다면 브라우저확장기능을 사용해 동작하는 그룹웨어와 같은 프로그램의 정상적인 실행이 불가능하다.

순위	대표진단명	건수	비율
1	Win-Downloader/Rogue.FakeAV	2018	82%
2	Win-Spyware/Crypter	149	6%
3	Win-Downloader/Rogue.SystemSecurity	70	3%
4	Win-Adware/IEShow	57	2%
5	Win-Clicker/FakeAV	41	2%
6	Win-Adware/BestLink	28	1%
7	Win-Adware/PointKing	26	1%
8	Win-Dropper/Zlob	24	1%
9	Win-Spyware/Xema	20	1%
10	Win-Spyware/Agent	19	1%
합계		**2452**	**100%**

[표 3-6] 4월 대표진단명에 의한 스파이웨어 피해 Top 10

[표 3-6]은 변형을 고려하지 않은 대표 진단명을 기준으로 한 피해 건수이다. 4월에는 2018건의 피해신고가 접수된 다운로드 로그 페이크에이브이(Win-Downloader/Rogue.FakeAV)가 피해가 가장 많이 접수된 것으로 확인되었다. 다운로드 로그 페이크에이브이는 스파이웨어 크립터에 감염되는 경우 나타나는 광고 사이트를 통해 배포되고 있다. 배포 사이트에서 다운로더 페이크에이브이가 다운로드 될 경우 파일의 하단에 사이트주소와 타임스탬프를 추가해 MD5를 다르게 하고 있다. 이런 이유로 수없이 많은 프로그램을 배포하는 것처럼 보인다. 그러나, 다운로더 페이크에이브이에 의해 설치되는 가짜백신은 다운로드 페이크에이브이에 보다 다양하지 않다.

지난 2월부터 꾸준히 감염신고가 되는 아이쇼우(Win-Adware/IEShow)도 계속해서 변형을 생성하며 대표진단명에 의한 스파이웨어 피해 Top 10에 꾸준히 이름을 등록하고 있다.

2009년 4월 유형별 스파이웨어 피해 현황은 [표 3-7]과 같다.

구분	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
2월	421	521	151	355	2	48	0	0	0	1500
3월	243	248	105	185	2	8	4	0	0	795

4월	275	230	104	2171	0	47	3	0	0	2830

[표 3-7] 2009년 4월 유형별 스파이웨어 피해 건수

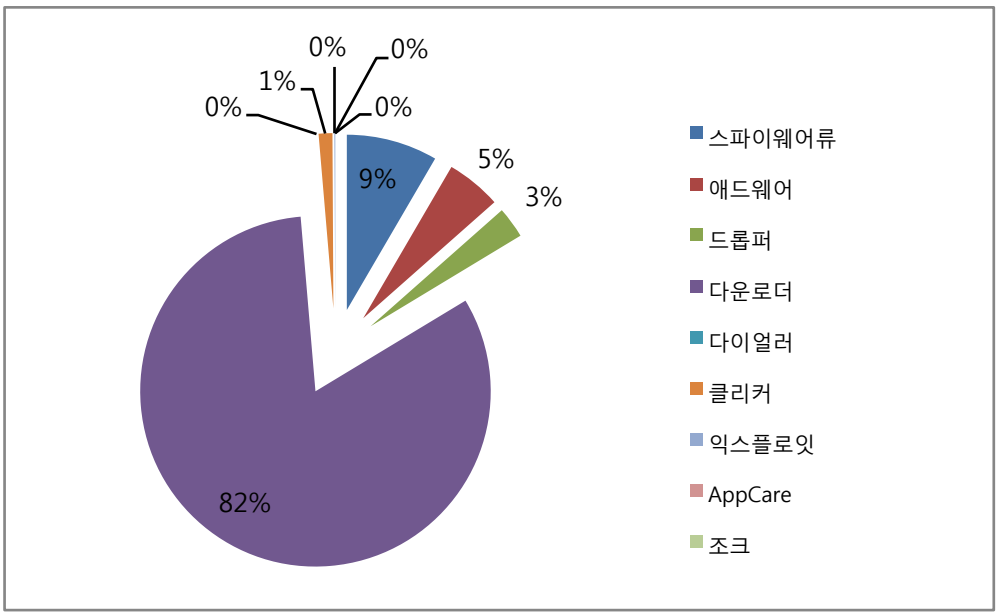
2009년 4월에는 스파이웨어 다운로더의 피해가 2171건으로 전월 비 2000건 이상 증가 해 전체 피해 수치가 크게 증가했다. 다운로더의 피해수치가 증가한 것은 한 가짜백신을 배포하는 사이트에서 사이트주소와 타임스탬프 등을 이용해 MD5를 변경하는 변형 다운로더의 신고접수가 증가했기 때문이다.

(2) 4월 스파이웨어 발견 현황

4월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 3-8], [그림 3-10]와 같다.

구분	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
2월	238	233	92	258	2	28	1	0	0	852
3월	184	139	60	143	2	6	4	0	0	538
4월	199	120	68	1948	0	30	2	0	0	2367

[표 3-8] 2009년 4월 유형별 신종(변형) 스파이웨어 발견 현황



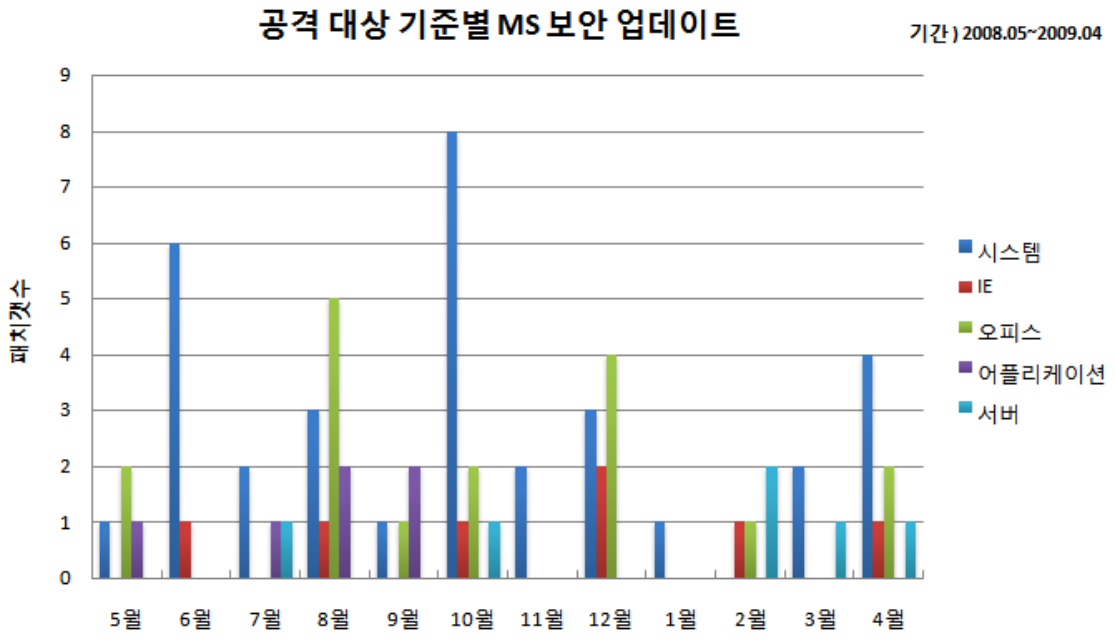
[그림 3-10] 2009년 4월 발견된 스파이웨어 프로그램 비율

4월에는 가짜백신을 설치하는 다운로더 신고의 증가로 인해 다운로더의 비율이 높았다. 크립터, 즐롭에 의해 설치되는 외산 가짜백신 다운로더의 배포 방법은 당분간 동일할 것으로 예상된다. 시스템 경고나 갑작스런 팝업창에 의해 백신 설치 사이트가 나타난다면 해당 사이트에서 설치되는 프로그램은 가짜백신으로 의심해야 한다.

3. 시큐리티

(1) 4월 마이크로소프트 보안 업데이트 현황

마이크로소프트사는 4월에 긴급(Critical) 5건, 중요(Important) 2건, 보통(Moderato) 1건으로 구성된 총 8건의 보안 업데이트를 발표하였다.



[그림 3-11] 2009년 4월 MS 보안 업데이트 현황

위험도	취약점	PoC
긴급	(MS09-009) Microsoft Office Excel의 취약점으로 인한 원격 코드 실행 문제점	유
긴급	(MS09-011) Microsoft DirectShow의 취약점으로 인한 원격 코드 실행 문제점	유
긴급	(MS09-014) Internet Explorer 누적 보안 업데이트	유

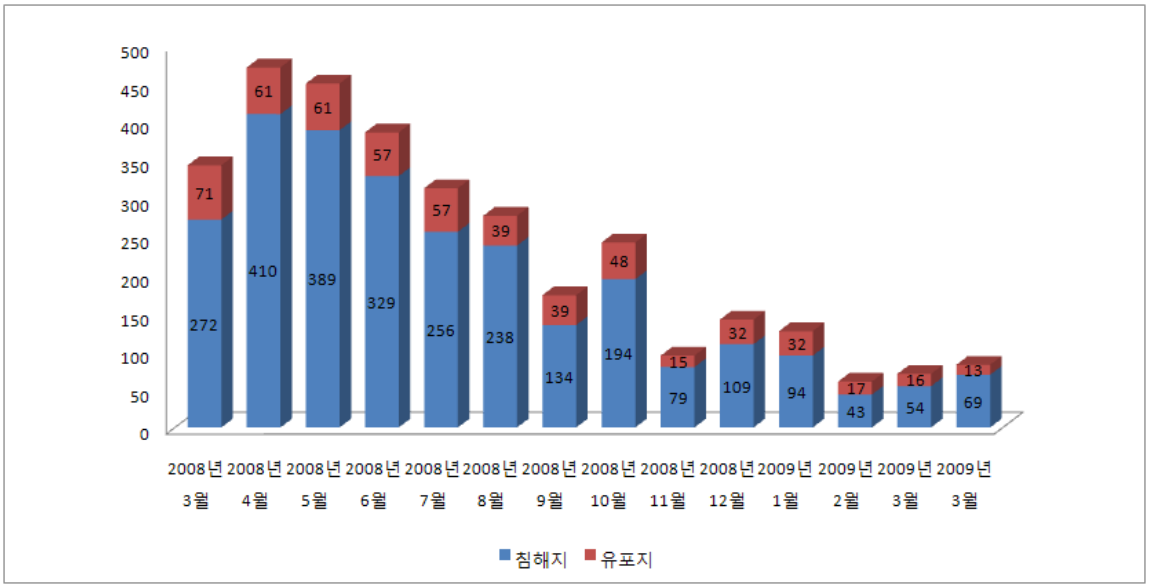
[표 3-9] 2009년 03월 주요 MS 보안 업데이트

이번 달에는 지난 달에 비해 2배 이상 증가한 비교적 많은 수의 보안 업데이트가 발표되었다. 그러나, 일부 취약점들에 대한 공격코드가 공개 되었으나 아직까지 실제 해당 취약점들에 대한 피해는 보고된 바가 없다.

특히, MS09-009 Office Excel 취약점 보안 업데이트는 지난 2월에 공개된 Excel 0-day 취약점에 관한 업데이트로, 해당 취약점을 이용하는 악의적인 파일이 실제로 보고 되었으나 공개된 지 10여 일 후인 정기 보안 업데이트를 통해 패치가 발표되었다. 지난 4월 초에 공개된 Office PowerPoint 0-day 취약점 또한 4월 보안 업데이트에 포함되지 않았으며, 이미 취

약점 정보가 공개된 지 한 달이 넘은 현재까지 MS사로부터 발표된 보안업데이트가 존재하지 않는다. 따라서, 사용자들은 신뢰되지 않은 Office 파일을 열어보는 과정에서 각별히 주의를 기울여야 할 것이다.

(2) 2009년 4월 웹 침해사고 및 악성코드 배포 현황



[그림 3-12] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

2009년 4월 악성 코드를 위해 침해된 웹사이트의 수와 악성 코드 유포지의 수는 69/13로 2009년 3월의 54/16 에 비해 소폭 증가했다. 특별히 브라우저와 관련된 어플리케이션의 취약점 발표가 없었던 것을 감안하면 이와 같은 추세는 계속될 것으로 보인다.

웹을 이용하여 배포되는 악성코드는 갈수록 그 패턴이 지능화 되고 있다. 특히 사용자에게 악성코드가 노출되는 것을 방지 하기 위해 사회 공학적 기법이 사용 되는 등 다양한 기법이 사용되고 있다. [그림 3-13]는 4월에 발견된 악성코드의 예시이다.

```
<script type="text/jscript">
function init() {
document.write("No web site is configured at this address");

}
window.onload = init;
</script>
<SCRIPT LANGUAGE="JavaScript">
function aa(str,m){
```

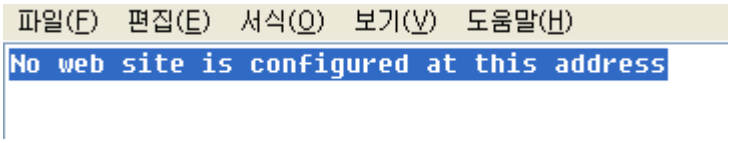
[그림 3-13] 악성코드 예시

이 코드는 악성 스크립트 코드를 먼저 실행한 후 document.write 함수를 사용해 웹페이지의 단순 텍스트(이 코드에서는 “No web site is configured at this address”)로 바꾸어 사용자를 속이는 코드이다. 따라서 사용자는 이러한 메시지가 서버쪽의 오류를 나타내는 메시지라고 생각하여 실제로 악성코드가 실행되었다고 생각하지 못한다.

사용자가 이 페이지가 게시된 웹서버에 접속하면 사용자는 브라우저에서 다음과 같은 화면을 보게 된다

[그림 3-14] 웹서버 접속하면

실제로 소스코드를 확인해도 역시 내용은 같다.



[그림 3-15] 소스코드

이렇듣 다양한 악성코드가 인터넷에 게시되어 있으므로 웹을 사용하는 사용자들은 이러한 위협에 항상 노출되어 있다. 따라서 사용자들은 자신의 시스템을 보호하기 위해 항상 보안패치를 적용하고 제품의 상태를 최신으로 유지하는 노력을 아까지 말아야 한다.

4. 사이트가드

(1) 2009년 4월 웹 사이트 보안 요약

구분	건수
악성코드 발견 건수	103,207
악성코드 유형	902
악성코드가 발견된 도메인	790
악성코드가 발견된 URL	7,748

[표 3-10] 1월 웹 사이트 보안 요약

웹 사이트를 통한 사용자의 피해를 막기 위해 안철수연구소가 제공하는 인터넷 보안 무료 서비스인 "사이트가드[1]"의 통계를 기반으로 본 자료는 작성되었다.

[표 3-10]은 2009년 4월 한달 동안 웹 사이트를 통해 발견된 악성코드 동향을 요약해서 보여주고 있다.

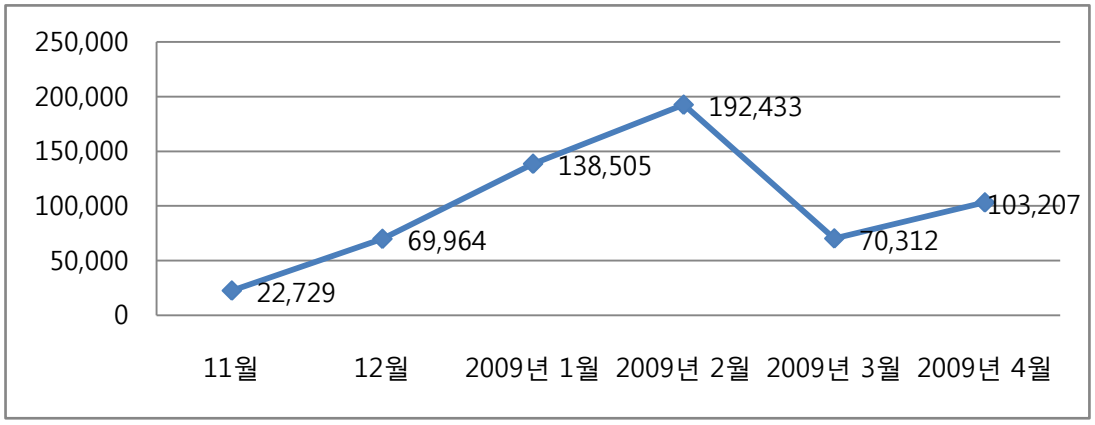
사이트가드의 집계에 따르면 4월 한달 동안 악성코드는 902종 103,207건 발견되었으며, 악성코드 유형은 902건, 악성코드가 발견된 도메인은 790건, 악성코드가 발견된 URL은 7,748건으로 전반적으로 증가세를 보였다. 이는 지난달의 감소세가 일시적인 현상이였음을 의미하는 것으로 판단된다. 이번 달은 신종 악성코드의 증가와 함께 중국 춘절의 여파가 사라진 것이 악성코드 발견 건수, 악성코드가 발견된 URL 등이 다시 증가세로 돌아선 주요 원인으로 보인다.

세부내용을 보면 다음과 같다.

[1] www.siteguard.co.kr

(2) 악성코드 월간 통계

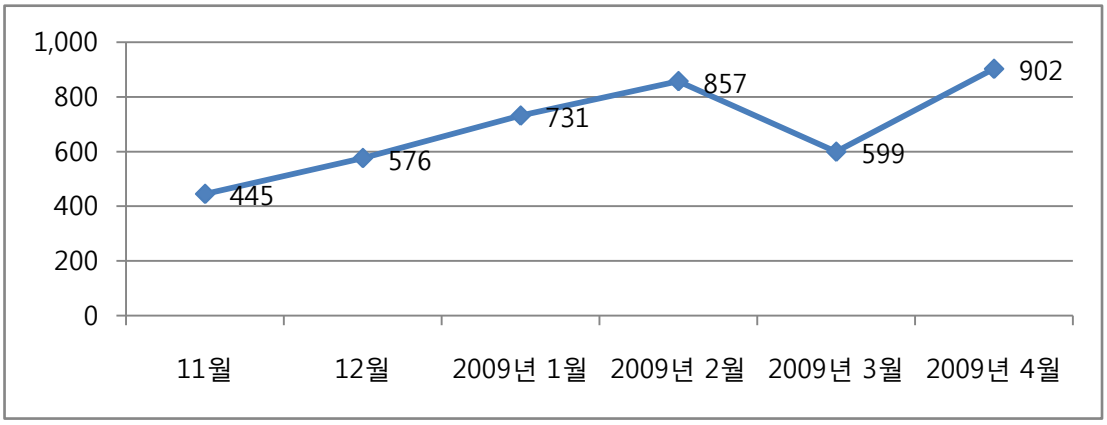
가) 악성코드 발견 건수



[그림 3-16] 월별 악성코드 발견 건수

[그림 3-16]는 최근 6개월인, 2008년 11월부터 2009년 4월까지의 악성코드 발견 건수의 추이를 나타내는 그래프로 4월 악성코드 발견 건수는 103,207건으로 지난달에 비해 약 32%의 증가세를 보였다.

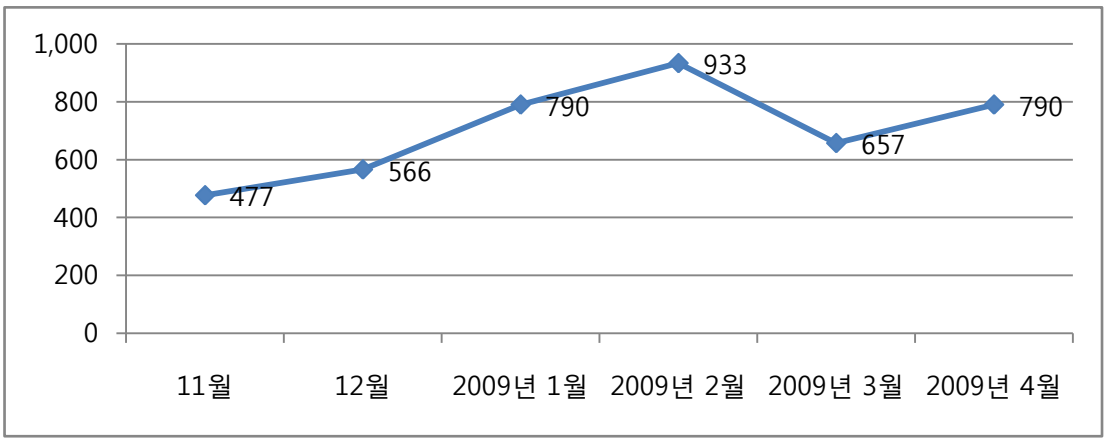
나) 악성코드 유형



[그림 3-17] 월별 악성코드 유형

[그림 3-17]는 최근 6개월간 발견된 악성코드의 유형을 나타내는 그래프로 역시 지난 달 599건으로 잠시 증가세가 주춤하였으나, 4월에 902건으로 급속한 증가세를 보였다. 이는 지난달에 비해 34% 증가한 수치이다.

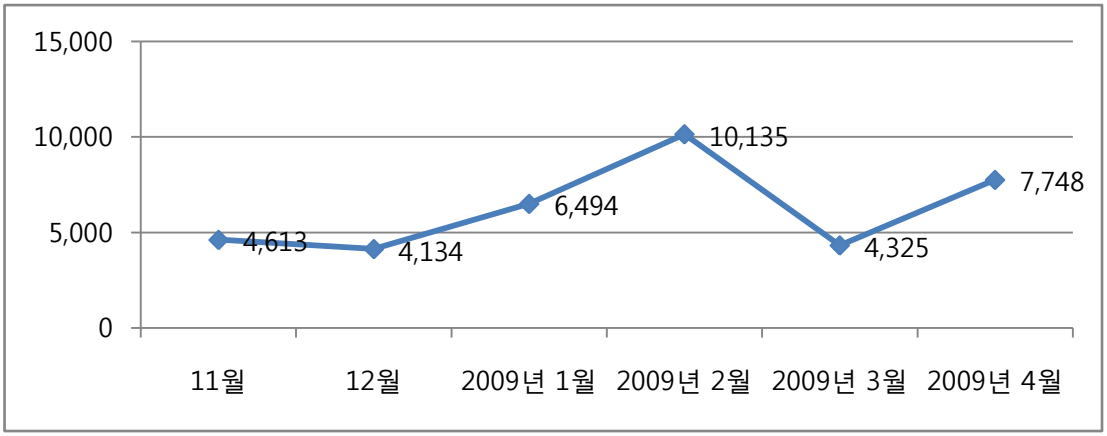
다) 악성코드가 발견된 도메인



[그림 3-18] 월별 악성코드가 발견된 도메인

[그림 3-18]는 최근 6개월간 악성코드가 발견된 도메인 수의 변화 추이를 나타내는 그래프로 4월 악성코드가 발견된 도메인은 790개로 전월에 비해 약 17% 증가하였다.

라) 악성코드가 발견된 URL

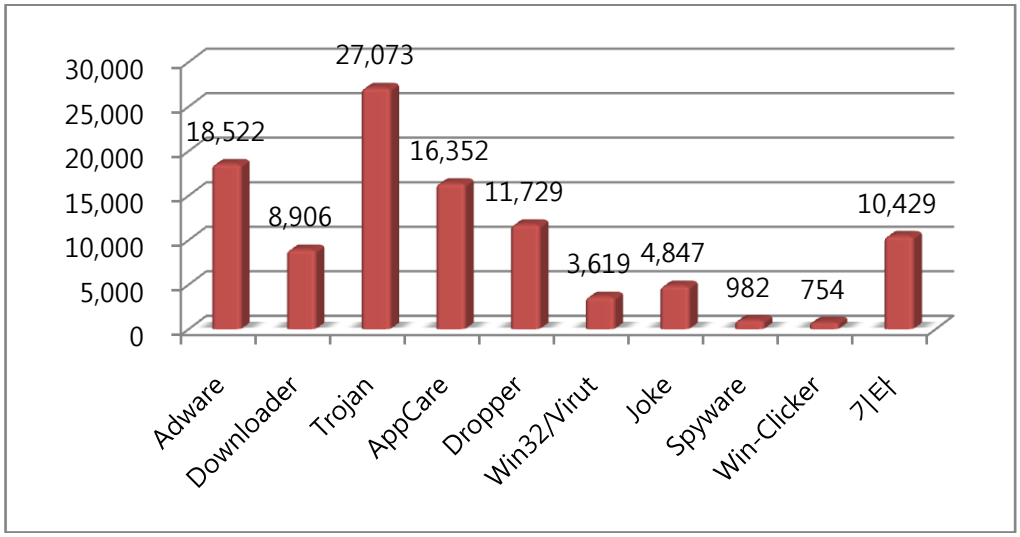


[그림 3-19] 월별 악성코드가 발견된 URL

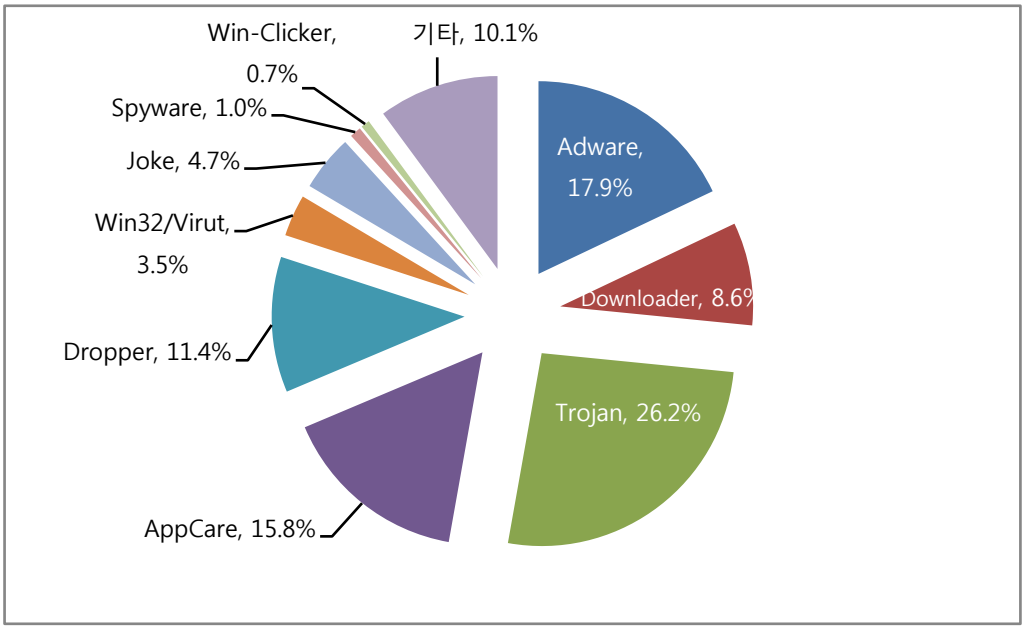
[그림 3-19]은 최근 6개월간 악성코드가 발견된 URL 수의 변화 추이를 나타내는 그래프로 4월 악성코드가 발견된 URL 수는 7,748개로 전월에 비해 44% 증가하였다.

(3) 유형별 악성코드 배포 수

유형	건수	비율
Trojan	27,073	26.2%
Adware	18,522	17.9%
AppCare	16,352	15.8%
Dropper	11,729	11.4%
Downloader	8,906	8.6%
Joke	4,847	4.7%
Win32/Virut	3,619	3.5%
Spyware	982	1.0%
Win-Clicker	754	0.7%
기타	10,429	10.1%
합계	103,213	100%



[표 3-11] 유형별 악성코드 배포 수



[그림 3-20] 유형별 악성코드 분포

[표 3-11]과 [그림 3-20]은 4월 한달 동안 발견된 악성코드를 유형별로 구분하여 발견 건수와 해당 비율(%)를 보여주고 있다.

4월 한달 동안 총 103,213개의 악성코드가 발견되었으며 이중 Trojan류가 27,073개로 지난 달 잠시 1위에 올랐던 Downloader류(8,906개)를 멀리 밀어내고 1위를 차지하였다. 2위는 2월까지 1위였던 Adware류가 18,522개로 2위를 차지하였다. 그 다음으로는 AppCare류가 Dropper류(11,729개)를 4위로 한 계단 밀어내고 16,352개로 3위를 차지하였다. 상위 1~4위까지는 기존과 큰 변화 없이 Trojan류, Adware류, AppCare류, Dropper류 등이 계속적으로 상위권을 차지하고 있다. 이는 금전적 목적으로 특정 기능을 수행하기 위한 악성코드들이 다수 생성되어 주요 배포지로 웹 사이트를 이용함에 따른 필연적인 결과임을 알 수 있다

(3) 악성코드 배포 순위

순위		악성코드명	건수	비율
1	↑1	Win-Adware/Onclub.446464	10642	17%
2	new	Win-Trojan/Bho.270336.D	8879	14%
3	↓2	Win-Downloader/NavigateAssister.282624	7520	12%
4	↑2	Win-AppCare/WinKeygen.94208	5753	9%
5	-	Win-AppCare/WinKeyfinder.542720	5616	9%
6	↓3	Win-Trojan/Xema.variant	5505	9%

7	-	Packed/Upack	5445	9%
8	new	Win-Joke/Stressreducer.1286147	4560	7%
9	-	Win-Adware/Shortcut.IconJoy.642048	4034	7%
10	new	Dropper/Xorer.142535	3700	6%
		합계	61,654	100%

[표 3-12] 유형별 악성코드 배포 Top 10

[표 3-12]는 4월 한달 동안 웹 사이트에서 사이트가드를 통해 확인된 악성코드 배포 Top 10을 보여주고 있다. Top 10에 포함된 악성코드들의 총 배포건수는 61,654건으로 4월 한달 총 배포건수 103,213건의 약 60%에 해당되며, 지난달의 75%보다 감소하였다. 원인은 다양한 신종 악성코드들이 출몰함에 따른 악성코드의 분포가 다양해진 것이 주요원인으로 분석된다.

요컨대, 지난달의 악성코드의 증가세가 주춤한 현상은 일시적인 현상이었으며, 춘절의 여파가 사라지고 다양한 악성코드들의 발견에 따라서, 다시 웹 사이트를 통한 악성코드 침해 건수가 증가 추세로 돌아선 4월이었다. 앞으로 5월, 6월에는 방학으로 인한 Script Kids들이 돌아오는 시기로, 당분간 웹사이트 침해 건수는 증가할 것으로 예상된다.

ASEC REPORT 작성을 위하여 다음과 같은 분들께서 수고하셨습니다.

2009년 4월호

편집장	선임 연구원	허 종 오
집필진	선임 연구원	정 진 성
	선임 연구원	심 선 영
	선임 연구원	허 종 오
	주임 연구원	장 영 준
	주임 연구원	강 동 현
	주임 연구원	이 재 호
	주임 연구원	임 채 영
	주임 연구원	김 민 성
	주임 연구원	주 설 우
감 수	상 무	조 시 행
참여연구원		ASEC 연구원분들
		SiteGuard 연구원분들