안철수연구소에서 발행하는 월간 보안 보고서

ASEC 리포트

2009년 2월호

이달의 보안 이슈

ASEC 칼럼

이달의 통계

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 – AimBot 웜의 출현과 Virut 바이러스 변형 기승

콘피커 웜의 피해가 사라지기도 전에 같은 취약점(MS08-067)을 이용하여 전파되는 Win32/AimBot.worm(이하 에임봇 웜)이 발견 보고 되었다. 특히 시스템 날짜를 2090으로 변경하는 특이한 증상을 보여 많은 매스컴에서 관심을 받기도 하였다. 또한 지속적인 변형이 출현되었던 Win32/Virut(이하 바이럿) 바이러스 변형이 2월에 추가적으로 발견보고 되었다. 이와 함께 웹 브라우저와 인터넷 문서파일의 취약점을 이용하는 악성코드 2건이 보고 되었다. 끝으로 시스템 파일을 패치 하여 자신을 동작하는 Win-Trojan/Patched로 진단되는 악성코드가 증가하였다.

(1) 에임봇 웜 피해 급증

MS08-067 취약점을 이용하며 국내에 큰 피해를 주는 또 다른 악성코드가 발견, 보고되었다. 이 악성코드는 시스템 날짜를 2090년으로 변경하여, 일명 2090 바이러스라고 먼저 알려졌으며, 안철수연구소는 진단명을 Win32/AimBot.worm으로 명명하고 진단/치료를 하고 있다.

에임봇 웜은 자신을 윈도우 부팅시마다 실행 되도록 하기 위해서 특정 레지스트리 키 값을 이용하는데 이때 버그로 추정되는 현상으로 윈도우 로그인 진입 시 무한 재부팅 현상을 일으킬 수 있다. 또한 일부 시스템에서는 악성코드에서 생성되는 드라이버로 인하여 BSOD를 발생하는 등 버그로 인해 더 많은 피해를 일으켰다. 최근에는 시스템 날짜를 2070년으로 변경하는 악성코드 변형도 등장하였다. 특히 에임봇 웜은 근래 악성코드가 자기보호 기능을 가지는 추세에 맞 추어 백신 프로그램으로부터 자신을 보호하기 위한 쓰레드를 생성하고, 자신이 등록된 레지스트리 키 값을 보호 하고 있다.

(2) 바이럿 바이러스 변형 발견

2008년도에 많은 피해를 입혔던 바이럿 바이러스 변형이 보고 되었다. 안철수연구소는 새로운 변형을 Win32/Virut.E, F형으로 각각 명명하고, 진단 및 치료 기능을 제공하고 있다. 이 바이러스의 변형의 기준은 EPO(Entry-Point Obscuring - 시작 실행시점 불명확화) 형태인 경우에는 C , E형으로 분류하고 Entry Point 내 특정 크기만큼 바이러스 코드로 덮어쓴 형태를 D, F형으로 분류하고 있다. 이번에 발견된 E, F형 경우 기존의 진단 방식을 회피하고 있는 형태로 기본적인 형태는 달라지지 않았다. 해당 바이러스는 치료를 위해서는 메모리 치료가 반드시 선행되어야 하는데 이번 변형의 경우는 바이럿 바이러스가 Winlogon.exe에 악의

적인 쓰레드를 생성하고 특정 윈도우 함수를 후킹하고 있기 때문이다.
따라서, 메모리 치료와 같은 선행 치료를 하여야 재감염을 방지할 수 있다.

다른 특징으로는 특정 IRC서버로 접속하여 다른 악성코드를 다운로드하여 설치 할 수가 있다. 보고서를 작성하는 현재 국내에서는 해당 IRC 호스트로는 접속이 불가능하다. 또한 앞에서 언급 했듯이 다중 암호화 레이어를 가지고 있어 진단 및 치료가 매우 복잡하다. 특히 윈도우 파일 보호 기능을 무력화하여 윈도우 시스템 파일들도 감염 시킬 수가 있다.

(3) 취약점을 이용하는 악성코드 IE7 취약점과 PDF 문서 제로데이 취약점

IE7 취약점(MS09-002)을 이용하는 악성코드가 보고 되었다. 안철수연구소에서는 해당 취약점을 이용한 악성코드는 HTML/Exploit-XMLhttpd로 진단하고 있다. 취약점은 초기화 되지 않은 메모리 손상 취약점이며, 해당 취약점은 대부분의 윈도우 OS와 인터넷 익스플로러7 에서 동작한다. 취약점은 원격 코드 실행을 허용할 수 있으며, 메일 및 메신저에 삽입된 URL이나 문서에 URL을 첨부하는 형태로 악의적인 웹 사이트로 유도할 수 있다. 처음 해당 취약점을 이용하여 공격한 형태는 특정인 또는 단체에 메일을 보내어 공격하는 스피어 피싱 형태로 유포 된 것으로 보인다.

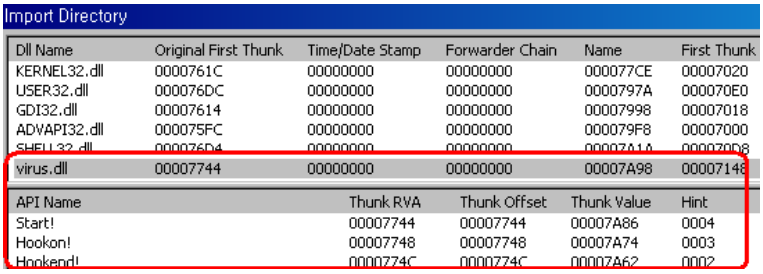
또한 어도비 PDF 문서에서 제로데이 취약점이 보고되었다. 어도비 리더와 어도비 아크로뱃 9.0 및 이하 모든 버전에서 JBIG2 이미지 스트림을 로딩하는 도중 버퍼 오버 플로우를 발생한다고 알려져 있다. 패치는 아쉽게도 3월11일 예정 되어 있기 때문에 그 동안 이 취약점을 악용한 조작된 PDF 문서를 통하여 악성코드 유포가 발생할 수 있다. 알려진 취약점 형태로는 자바스크립트를 이용한 쉘 코드에 Heap Spray(이하 힙 스프레이) 기법을 사용한 형태이며, 기본적인 예방법으로 어도비 리더에서는 자바 스크립트 기능을 꺼두는 것이 임시 방편으로 알려져 있다.

(4) 시스템 파일을 패치하는 악성코드

일반적으로 Win-Trojan/Patched로 명명되는 악성코드 중 일부는 다음과 같이 정상파일의 임포트 영역에 악성코드 모듈을 로드 하도록 추가하는 형태가 많다. 이와 같은 형태는 우선 악성코드 모듈의 동작 방식을 발견하기 어렵다는데 있다. 일반적으로 시스템에 수상한 virus.dll은 쉽게 발견될 수 있지만 이것을 실행하는 레지스트리는 별도로 존재하지 않는다.

다만 아래 [그림1-1] 처럼 정상파일의 임포트 영역을 수정하여 악성코드 모듈을 로드 하도록 한다. 이러한 경우 대부분이 윈도우 시작과 동시에 실행되는 시스템 파일이 주로 공격 대상이 된다. 정해진 윈도우 시스템 파일이 있는 것이 아니므로 이와 같이 시스템 파일이 패치

된 형태는 찾아내기 어렵다.


Import Directory

Dll Name	Original First Thunk	Time/Date Stamp	Forwarder Chain	Name	First Thunk
KERNEL32.dll	0000761C	00000000	00000000	000077CE	00007020
USER32.dll	000076DC	00000000	00000000	0000797A	000070E0
GDI32.dll	00007614	00000000	00000000	00007998	00007018
ADVAPI32.dll	000075FC	00000000	00000000	000079F8	00007000
SHELL32.dll	000076D4	00000000	00000000	00007A1A	00007008
virus.dll	00007744	00000000	00000000	00007A98	00007148

API Name	Thunk RVA	Thunk Offset	Thunk Value	Hint
Start!	00007744	00007744	00007A86	0004
Hookon!	00007748	00007748	00007A74	0003
Hookend!	0000774C	0000774C	00007A62	0002

[그림 1-1] 시스템 파일을 패치하는 유형의 악성코드

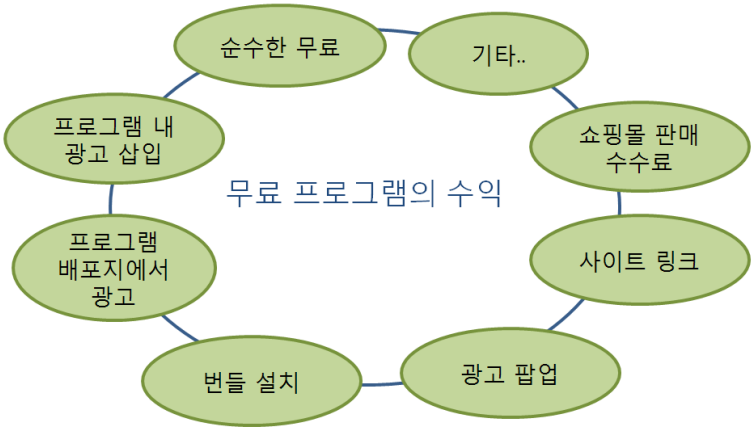
앞서 말했듯이 위와 같은 형태로 악성코드를 동작 시키는 경우 일반 사용자가 찾아내기 어렵고 악성코드를 찾더라도 패치 된 실행파일을 사용자가 수정할 수 없어 치료에 어려움이 있다. 일반적으로 위와 같은 경우 치료를 위해서는 virus.dll 모듈로 찾아 제거 해야 하고 수정된 시스템 파일의 임포트 영역도 원래와 같이 복구해야 한다.

2. 스파이웨어 – 스파이웨어 배포 방식의 지능화

최근 국내에서는 무료 프로그램을 배포할 때 약관의 허점을 교묘히 이용하여 스파이웨어 프로그램을 설치하는 방식이 증가하고 있다. 또한 국외에서는 BHO를 이용하여 검색결과를 조작해 스파이웨어 설치를 유도하는 이슈가 있었다. 그럼 이 두 가지 내용에 대해 좀 더 자세히 알아보자.

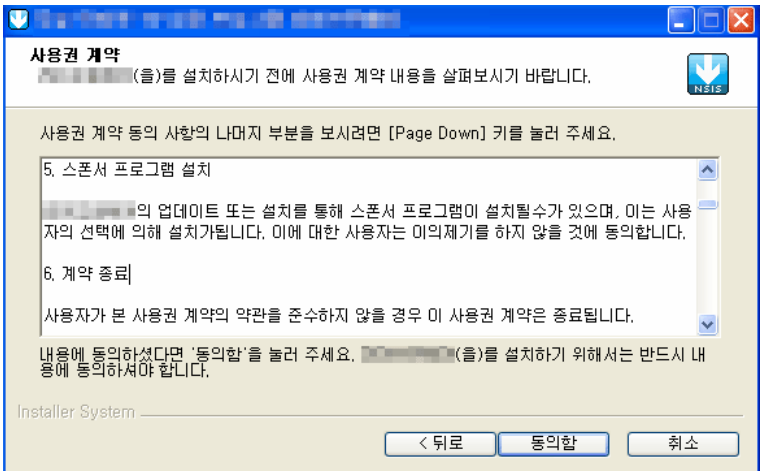
(1) 국내 – 약관의 허점을 이용한 스파이웨어 설치 증가

현재 우리가 사용하는 컴퓨터는 사용하고자 하는 프로그램을 하드디스크에 설치하고 실행하는 구조를 가지고 있다. 따라서 누구나 자신이 필요한 기능을 가진 프로그램을 설치하면 원하는 기능을 사용할 수 있다. 이런 프로그램은 크게 유료와 무료로 구분된다. 유료 프로그램의 경우 일반적으로 프로그램의 판매로 수익이 발생한다. 하지만 무료 프로그램은 유료 프로그램과는 달리 수익 구조가 명확하지 않다. 무료 프로그램의 수익 구조를 살펴보면 다음과 같다.



[그림 1-2] 무료 프로그램의 수익 구조

[그림1-2]에서 알 수 있듯 순수하게 무료로 제공되는 프로그램을 제외하면 매우 다양한 수익 구조를 가지고 있음을 알 수 있다. 물론 무료 프로그램이 수익 구조를 가져가는 것이 잘못된 것은 결코 아니다. 건전한 수익 구조를 가져 간다면 사용자는 보다 높은 품질의 무료 프로그램을 사용할 수 있는 기회를 얻기 때문이다. 하지만 일부 프로그램의 경우 사용자의 정당한 권리를 침해하는 수익 구조를 가지려고 하기 때문에 문제가 된다. 대다수의 경우 애드웨어(Adware) 또는 스파이웨어(Spyware)로 분류가 되어 컴퓨터 보안 제품에 의해 차단이 되지만 일부 프로그램의 경우 사용자들이 프로그램을 설치할 때 사용자 약관을 꼼꼼히 확인하지 않는 다는 점을 악용하는 사례가 지속적으로 발견 되고 있다. 이런 프로그램을 설치할 때 약관을 살펴보면 다음과 같은 부분을 확인할 수 있다.



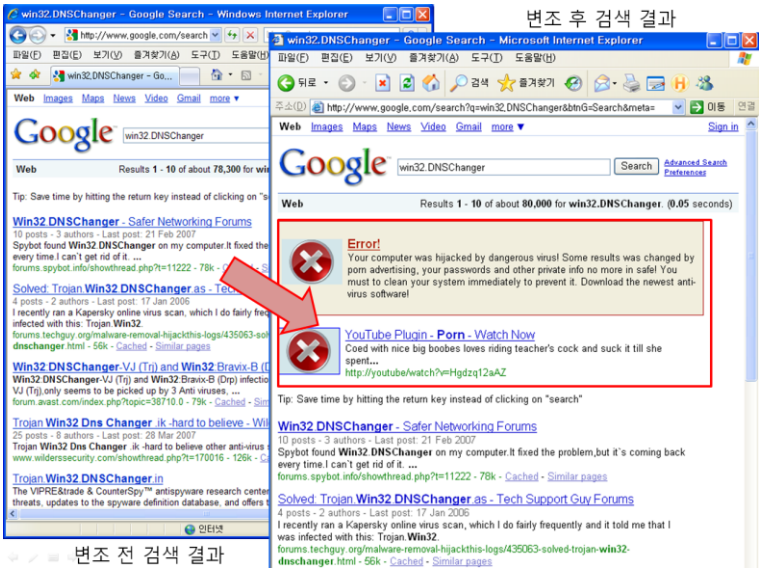
[그림 1-3] 스폰서 프로그램 설치에 관한 약관

이 프로그램이 설치된 이후 해당 프로그램의 업데이트는 스폰서 프로그램의 이름만 보여주기 때문에 해당 프로그램이 어떤 기능을 하는지 전혀 알 수 없으며 가장 중요한 사용자 약관을 제공하지 않는다는 큰 문제점이 존재 한다. 실제 이런 스폰서 프로그램 중 일부는 자신을 보호하기 위한 목적으로 루트킷(rootkit)을 설치해 정상적인 윈도우 동작을 방해하는 등 문제를 일으켰다. 하지만 사용자는 최초 프로그램을 설치할 때 "업데이트 또는 설치를 통해 스폰서 프로그램이 설치될 수가 있으며, 이는 사용자의 선택에 의해 설치가 된다. 이에 대한 사용자는 이의제기를 하지 않을 것에 동의합니다"에 동의 했으므로 해당 스폰서 프로그램으로 문제가 발생 하더라도 정당한 보상을 받을 수 없다.

최근 무료 프로그램을 배포하거나 무료로 게임을 제공하는 곳이 늘어나고 있다. 하지만 이들은 무료 제공을 이유로 위와 같이 애드웨어 또는 스파이웨어를 사용자의 적절한 동의를 받지 않고 번들로 설치하고 있다. 따라서 이런 피해를 예방하기 위해서는 무료 프로그램이나 서비스를 제공 받기 전 약관이 제공 되는지 확인하고 이를 꼼꼼히 확인하여 사용자에게 직간접적으로 피해가 되는 부분이 있는지를 확인하는 것이 좋다. 만약 설치과정에서 약관을 제공하지 않는다면 문제가 있을 소지가 매우 높으므로 각별한 주의가 필요하다.

(2) 국외 - 검색 결과를 조작한 스파이웨어의 배포

Win-Adware/Rogue.AntiVirus, Win-Adware/Rogue.AntiSpyware와 같은 외산 가짜 백신에 의한 국내 피해가 꾸준히 증가하고 있다. 이들은 가짜 백신을 보다 효과적으로 배포하기 위해 Active-X, Zero-day exploit와 같은 전통적인 방식과 YouTube와 같은 동영상 UCC 공유 사이트, 가짜 동영상 파일 등과 같은 새로운 방식을 사용한다. 최근 브라우저 BHO(Browser Helper Object)를 이용해 검색 사이트의 검색 결과를 조작해 스파이웨어 설치를 유도하는 사례가 발견되었다.



[그림 1-4] Win-Clicker/BHO.FakeAlert.106496에 의해 변조된 검색 결과

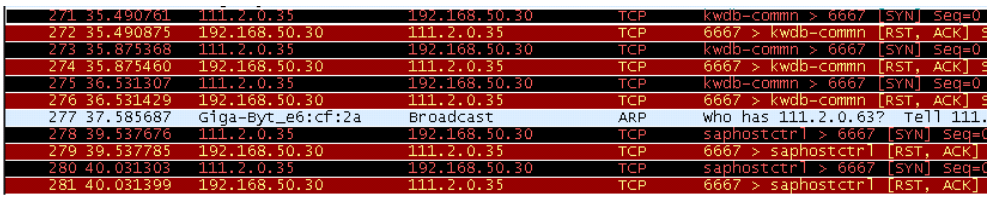
Win-Clicker/BHO.FakeAlert.106496의 경우 일정 시간마다 컴퓨터가 스파이웨어에 감염 되었다는 허위 경고 메시지 박스를 띄우며, 검색 사이트 구글(Google)에서 특정 악성코드(Win32.DNSChanger)의 검색 결과를 보여준다. 하지만 [그림 1-4]를 보면 알 수 있듯, 실제 구글의 검색 결과의 상단에 다른 내용이 추가된 것을 확인할 수 있다. 추가된 검색 결과를 클릭하면 가짜 백신을 설치하는 페이지로 이동하게 된다. 이는 일반적으로 사용자들이 신뢰할 수 있는 검색 사이트의 검색 결과를 조작해 가짜를 진짜인 것처럼 속여 가짜 백신을 직접 설치 하도록 유도한 사례이다. 따라서 내가 직접 입력하지 않은 검색어의 검색 결과가 나온다면 그 결과의 진위를 한번쯤 의심해 보는 것이 좋다. 또한 일정 시간을 간격으로 컴퓨터에 바이러스 또는 스파이웨어 감염 사실을 알리고 새로운 백신 제품의 설치를 유도한다면 가짜 백신의 설치를 유도하는 것이므로, 피해를 입지 않도록 주의해야 한다.

3. 시큐리티 – 다양한 취약점을 이용한 공격 증가

2-3년 전부터 일반 취약점들의 동향이 서비스 취약점 보다 어플리케이션 취약점 등으로 옮겨가고 있는데 이중 자주 공격대상이 되는 어플리케이션은 Internet Explorer, PDF, Office 및 ActiveX 등이다. 또한 Fuzzer 등과 같은 자동화된 도구를 이용한, 파일 포맷관련 취약점들도 많이 나타나고 있다. 시큐리티 이슈에서는 악성코드 이슈에서 언급한 에임봇 웜, IE7 취약점, Adobe사의 PDF 취약점에 대해서 상세히 알아보자.

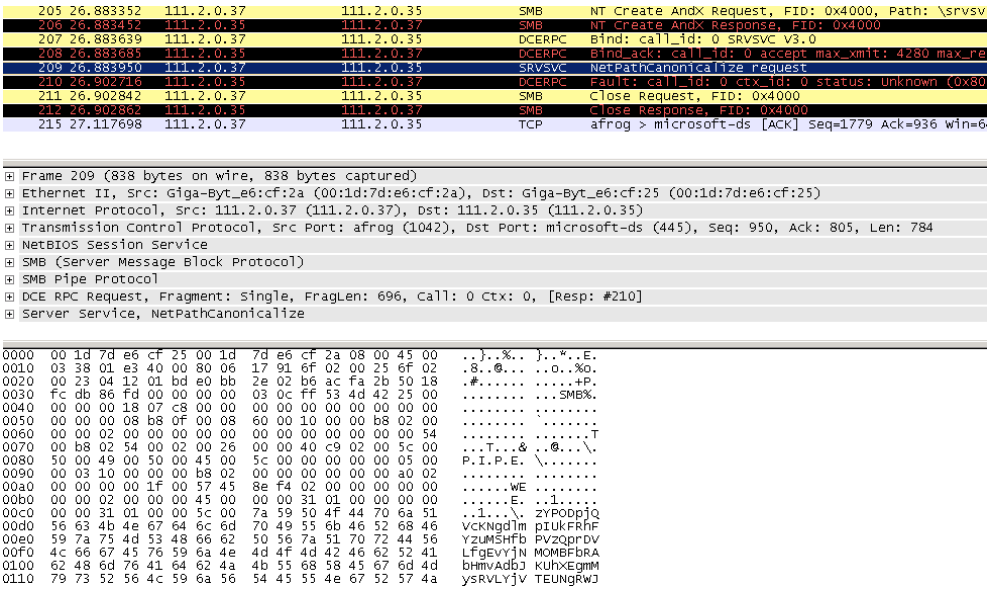
(1) MS08-067 취약점을 이용한 또다른 악성코드 에임봇 웜

지난 1월에 MS08-067 서버 서비스 취약점을 이용한 콘피커 웜이 발생한 이후에 2월에는 동일한 취약점을 이용한 악성코드인 에임봇 웜이 발견되었다. 에임봇 웜은 일반 IRCBot 웜과 유사하며, 아래 화면과 같이 특정 IRC 서버 채널(TCP Port 6667)에 접속을 시도 한다.



[그림 1-5] IRC 서버 채널 접속 시도

만약 IRC 서버 채널에 접속이 성공하면 봇넷 오퍼레이터의 명령을 받아 MS08-067 취약점을 이용하여 전파되며 전파되는 경로는 취약점, 네트워크 공유, USB등이다



[그림 1-6] MS08-067 취약점을 이용하는 패킷

위의 그림과 같이 콘피커 웜 에서 사용하는 MS08-067 취약점을 이용하는 것을 알 수 있다. 에이봇 웜은 콘피커 웜과 전체적인 Exploit 구조는 같으나, 쉘 코드 등의 부분이 다른 것이 특징이다.

(2) MS09-002 Internet Explorer7 Cloned Object 취약점

2월에 MS09-002 Internet Explorer7 Cloned Object 취약점에 대한 POC가 인터넷 상에 공개되어, 악성코드 유포 때 많이 악용되고 있다.

다음은 MS09-002 IE7 Cloned Object POC 코드의 일부이다.

```
<script language="JavaScript">
var c=unescape("%ue8fc%u0044%
var array = new Array();
var ls = 0xd00000;
var b = unescape(
while(b.length<ls/2) { b+=b;}
var lh = b.substring(0,ls/2);
delete b;
}
 CollectGarbage();
var s1=unescape(
var a1 = new Array();
function ok() {
  o1=document.createElement("tbody");
  o1.click;
  var o2 = o1.cloneNode();
  o1.clearAttributes();
  o1=null; CollectGarbage();
  o2.click;
}
```

[그림 1-7] MS09-002 IE7 Cloned Object POC 코드 내용

이 취약점은 mshtml.dll 에서 CFunctionPointer::PrivateAddRef 함수 포인터의 참조 카운트 증가부분에서 문제가 발생하는데, 공격원리는 다음과 같다.

객체(Object)를 생성하고 그 객체를 참조하는 경우, 참조 카운트가 증가한다. 해당 객체가 함수를 참조하는 객체에 속하는 경우, 함수의 참조 카운트와 부모 객체 또한 증가한다. 이때,

원래의 객체를 제거할 경우, 함수 포인터는 제거되지 않는다. 제거된 객체를 참조하는 함수 포인터를 사용하려고 하면, 원래 객체를 호출하게 되는데, 해당 객체는 이미 삭제된 객체이기 때문에, 잘못된 주소로 인한 Exception(예외)이 발생하게 된다.

해당 취약점은 악성코드 유포를 위한 방법으로 악용될 수 있으므로, Internet Explorer7을 이용하고 있으면, 즉시 보안 패치의 적용이 필요하다.

(3) PDF Adobe Acrobat Reader JBIG2 Buffer Overflow 취약점

2월에 Adobe사의 Acrobat Reader 의 PDF 문서의 취약점에 대한 제로데이 공격이 알려졌는데, 글을 쓰는 시점까지 보안 패치는 공개되고 있지 않아, 악성코드 유포 및 시스템 공격에 악용될 소지가 높다. Adobe사에서는 Advisory1을 통해 3월 중순쯤에 정식 보안 패치가 나올 것이라고 한다.

일반적으로 PDF 취약점은 특정 Object 등에서 자주 발생을 하는데, PDF 문서를 읽을 때 Acrobat Reader 가 JBIG2 Stream의 유효 검증 값을 체크를 하지 않아서 버퍼 오버플로우 취약점이 발생한다.

먼저 발견된 악성코드에서는 JBIG2b Stream에 다음과 같은 값이 들어가 있다.

```
.: 0D 0A 2F 48 65 69 67 68 74 20 33 32 0D 0A 2F 43 ; ../Height 32../C
.: 6F 6C 6F 72 53 70 61 63 65 20 2F 44 65 76 69 63 ; olorSpace /Devic
.: 65 47 72 61 79 0D 0A 2F 42 69 74 73 50 65 72 43 ; eGray../BitsPerC
.: 6F 6D 70 6F 6E 65 6E 74 20 31 0D 0A 2F 46 69 6C ; omponent 1../Fil
.: 74 65 72 20 2F 4A 42 49 47 32 44 65 63 6F 64 65 ; ter /JBIG2Decode
.: 0D 0A 2F 44 65 63 6F 64 65 50 61 72 6D 73 20 3C ; ../DecodeParms <
.: 3C 3E 3E 0D 0A 0D 0A 2F 4C 65 6E 67 74 68 20 36 ; <>>..../Length 6
.: 35 35 33 38 30 0D 0A 3E 3E 0D 0A 73 74 72 65 61 ; 55380..>>..strea
.: 6D 0D 0A E0 FF 40 61 44 00 00 20 20 40 00 0C 0C ; m..?@aD..  @...
```

[그림 1-8] JBIG2b Stream 코드 내용

해당 값으로 인하여, Acrobat Reader는 Crash가 발생을 하는데, Crash 발생지점은 아래와 같다.

```
00ffd887 8b0a            mov     ecx,[edx]            ds:0023:035ae6f8=044f2414
00ffd889 8b411c          mov     eax,[ecx+0x1c]   ** Segment Page Association
00ffd88c 85c0            test    eax,eax
00ffd88e 0f84ac020000    je      AcroRd32_950000!PDFLTerm+0x235ad0 (00ffdb40)
00ffd894 8b4e10          mov     ecx,[esi+0x10]
00ffd897 8d0480          lea     eax,[eax+eax*4]
00ffd89a 834481ec01      add     dword ptr [ecx+eax*4-0x14],0x1    Crash발생
00ffd89f 8d4481ec        lea     eax,[ecx+eax*4-0x14]
```

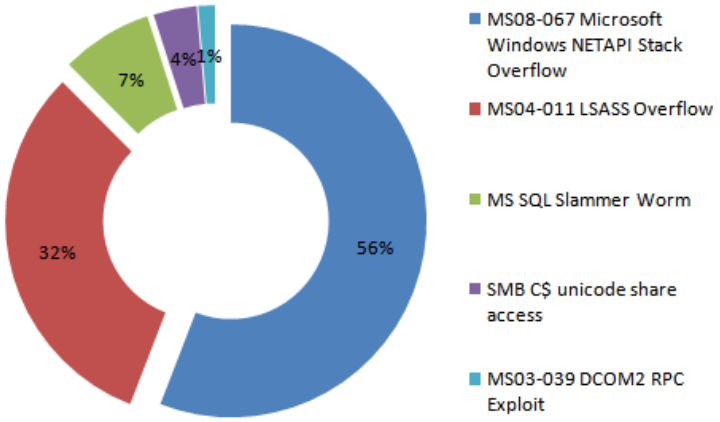
```
00ffd8a3 8b02                mov       eax,[edx]
00ffd8a5 8b4810              mov       ecx,[eax+0x10]
00ffd8a8 85c9                test      ecx,ecx
00ffd8aa 894c242c            mov       [esp+0x2c],ecx
```

악성코드는 Heap Spray 공격기법을 이용하여, Crash 지점의 Return Address 를 조작하여 쉘코드를 실행하는데, 이 때 아래의 API등을 사용하여 특정 파일을 생성한다.
GetCurrentProcess, GetTempPathA, TerminateProcess, CreateFileA, createFileW, SetFilePointer, ReadFile, WriteFile, WinExec, CloseHandle, GetCommandLineA, GetModuleFileNameA

현재까지는 패치가 나오지 않은 관계로 백신 소프트웨어 사용과 더불어, 신뢰되지 않는 사용자에게서 온 PDF 문서 파일을 열어보지 않거나, Acrobat Reader의 Javascript 사용기능을 해제하는 것이 필요하다.[Acrobat Reader - 편집(edit) - 기본설정 - Javascript - Acrobat Javascript 사용기능(체크해제)]

4. 네트워크 모니터링 현황 – MS08-067 취약점을 이용한 공격 증가

콘피커 웜의 공격은 2009년 1월을 거쳐 2월에도 자사의 네트워크 모니터링 시스템에서 탐지되고 있다. 콘피커 웜은 이전에 RPC 를 이용한 공격의 LSASS, DCOM의 공격만큼이나 큰 피해를 주고 있어, MS에서는 제작자를 신고하는 사람에게 현상금($250,000)을 걸 정도이다. 2월에는 1월과 같이 큰 변화는 나타나고 있지 않으며 MS08-067 취약점을 이용한 공격이 주요 탐지 이벤트에서 상위를 차지하고 있다.

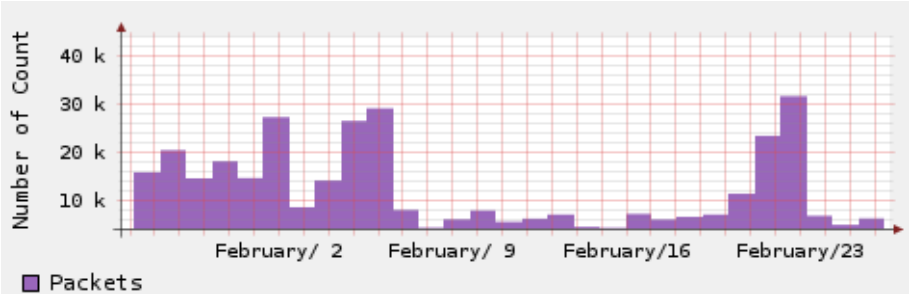


[그림 1-9] 주요 탐지 이벤트 현황 TOP 5

MS08-067이 이렇게 빠르게 사용될 수 있었던 이유는 다음과 같다.

① 비교적 최신의 취약점인 점
② 기본적인 서비스로 동작중인 점
③ 취약점 자체로 주로 전파를 시도했던 것과 달리 공유 폴더, USB와 같은 외장매체를 통한 감염 등 다양한 방식을 이용하고 있는 점.

이번 MS08-067취약점은 당분간 상위를 차지하며 지속될 것으로 보인다.



[그림 1-10] TCP/445 트래픽

이외 FTP(File Transfer Protocol)서버로 많이 이용되는 ProFTPd에서 SQL Injection 취약점이 보고되어 이와 관련한 공격이 2월 중순 이후부터 탐지되는 것으로 보고되었다. 공격코드가 공개되어 있어, ProFTPd에서 인증을 DB로 사용하는 경우 발생될 수 있다. 현재 이 공격이 감지되기 시작하였으므로 ProFTPd 사용자는 TCP/21 번으로 들어오는 트래픽에 대해 특별한 주의가 필요하다.

5. 중국 보안 이슈 – 가짜 경품 웹 사이트 사기단 검거

(1) 가짜 경품 웹 사이트 사기단 검거

2009년 2월 3일 중국 언론에는 가짜 경품 웹 사이트를 통해 경품 당첨에 따른 배송료 등의 명목으로 개인들로부터 10만 위엔(한화 약 2,900만원)을 갈취한 일당 4명의 구속 사건이 보도되었다.

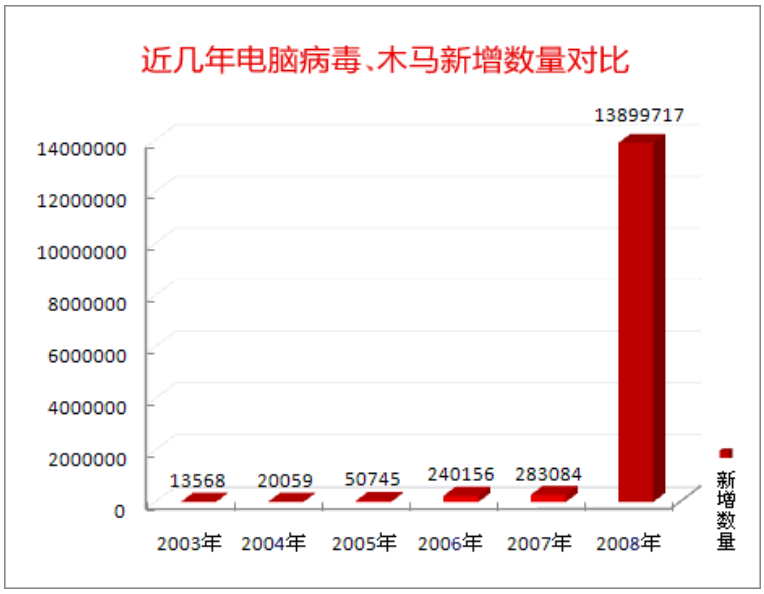
[그림 1-11] 구속된 가짜 경품 웹 사이트 사기단

이번에 구속된 가짜 경품 웹 사이트 사기단 일당은 2008년 4월 중국 대륙에서 유명한 물품 거래 사이트인 알리바바(www.alibaba.com)와 유사한 가짜 웹 사이트를 만든 뒤 진짜 알리바바 웹 사이트에 물품을 공개한 판매자들에게 휴대전화로 알리바바 웹 사이트의 직원으로 사칭하여 경품이 당첨되었다는 안내 전화를 했다. 안내 전화를 통해 3만 8천 위엔(한화 약 1,100만원)의 현금과 소니에서 제공되는 최신 노트북을 주는 경품에 당첨 되었다라고 속인 뒤 해당 경품의 배송에 따른 경비를 입금하라는 거짓 안내를 하였다. 이러한 수법으로 약 400명의 사람들로부터 약 10만 위엔(한화 약 2,900만원)에 달하는 금액을 갈취했다.

이번 중국에서 발생한 가짜 경품 웹 사이트 사기단은 사회공학(Social Engineering) 기법을 이용한 Voice Phishing(이하 보이스 피싱)과 동일한 수법을 사용하였을 뿐만 아니라 유사한 형태의 가짜 웹 사이트까지 준비하였다는 점에서 보이스 피싱과 전통적인 피싱 수법이 결합된 형태라고 볼 수 있다. 이러한 사회공학 기법을 이용한 전화사기를 예방하기 위해서는 평소 개인 정보 관리와 보호에 세심한 노력을 기울이고 의심스러운 전화를 받을 경우에는 직접 관계 기관에 문의하는 자세가 필요하다.

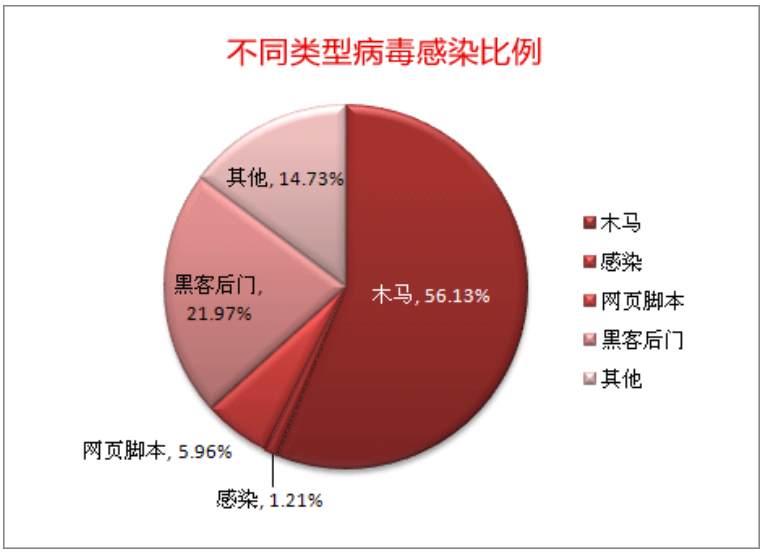
(2) 중국 보안 업체 금산(KingSoft, 金山)의 2008년 악성코드 동향 분석 발표

중국의 3대 보안 업체 중 하나인 금산(KingSoft, 金山)에서 2008년 한 해 동안의 악성코드 동향에 대해서 종합 정리한 보고서를 2009년 2월 5일 발표하였다. 이번에 발표한 동향 보고서에는 악성코드의 급증과 트로이목마 형태의 급속한 증가를 2008년의 특징으로 보았으며 2008년 주요 10대 악성코드들로는 온라인 게임의 사용자 정보 유출 형태의 트로이목마를 첫 번째로 지적하였다.



[그림 1-12] 년도 별 악성코드 발견 수치

먼저 [그림 1-12]와 같이 2008년 한 해 동안 총 13,899,717건의 악성코드가 발견이 되었으며 이 수치는 2007년의 48배에 달한다.



[그림 1-13] 2008년 악성코드 유형별 분포

이렇게 급증한 악성코드 수치 중에서 분포도로 구분 한 것이 [그림 1-13]과 같다. 이 분포도에서는 트로이목마가 7,801,911건으로 전체의 56.13%를 차지하고 있으며 그 다음으로 백도어 류의 악성코드가 전체의 21.97%를 차지하고 있다. 그리고 스크립트 악성코드가 5.96%, 파일을 감염시키는 전통적인 바이러스 형태가 1.21% 차지하고 있는 것으로 밝혔다. 그리고 기타 형태의 악성코드가 14.73% 차지하고 있다. 그리고 온라인 게임의 사용자 정보를 유출하는 OnlineGameHack 트로이목마와 각종 보안 제품들의 정상적인 실행을 방해하는 AVKiller, 트로이목마 그리고 중국 대륙 내에서 많이 사용되는 QQ 메신저의 사용자 정보를 유출하는 QQ 관련 트로이목마들을 2008년의 10대 주요 악성코드들 중 하나로 분석하고 있었다. 이와 더불어 2009년 예상되는 보안 이슈로는 “제로데이 공격의 가속화”, “웹 사이트를 통한 악성코드의 유포 증가”와 “윈도우 7과 비스타 등의 새로운 운영체제를 노리는 악성코드의 등장”들을 주요 보안 이슈로 선정하였다.

II. ASEC 칼럼

■ 주요 백신 프로그램의 오진 사례와 원인

2009년에도 매일 2-3 만개의 신종 악성코드가 발견되고 있다. 악성코드 수가 급격히 증가하면서 시그니처(진단 값, 패턴) 기반의 백신 프로그램이 가지고 있는 문제인 오진도 따라서 증가하고 있다.

본 칼럼에서는 주요 오진 사례와 원인에 대해서 알아보자.

(1) 오진! 오진! 오진!

백신 프로그램의 오진, 오동작 문제는 백신 프로그램 탄생 때부터 존재했으며 최근 악성코드가 급격히 증가하고 진단하는 악성코드 수도 증가하면서 오진 문제도 자주 언급되고 있다.

주요 오진 사례는 다음과 같다.

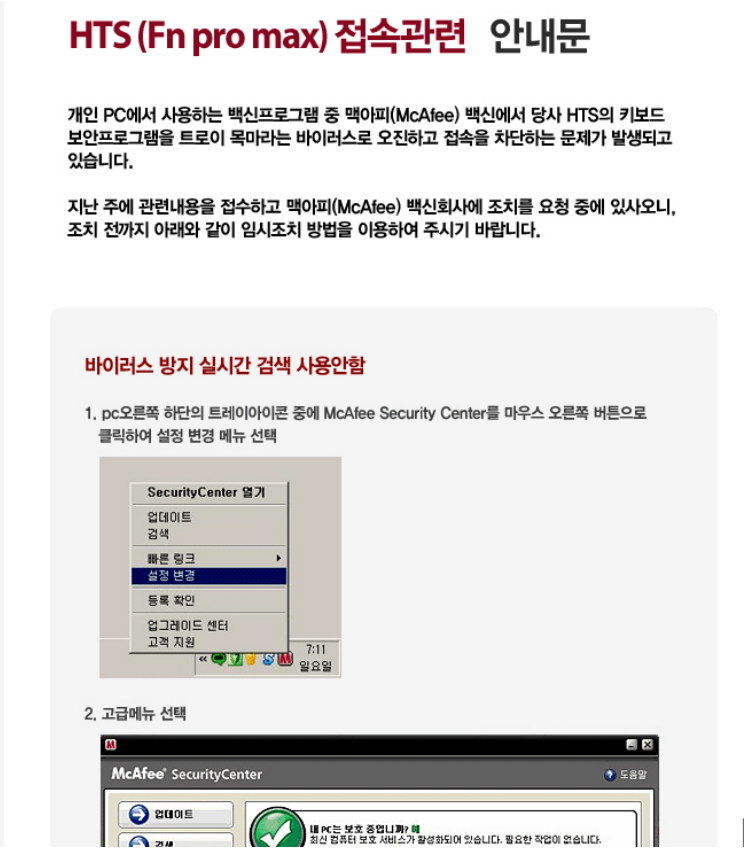
2005년 4월 23일 트렌드마이크로 사에서 배포한 패턴 2.594.00에서 시스템 자원을 100% 사용하여 시스템이 느려지며, 윈도우 XP 서비스 팩2 혹은 윈도우2003 서버에서는 시스템 운영이 불가능해질 수 있는 문제가 발생했다.

2006년 3월 맥아피 DAT 4715는 마이크로소프트 엑셀, 플래쉬 플레이어(Macromedia Flash Player), 어도브 업데이트 매니저(Adobe Update Manager), 구글 툴바 설치 파일(Google Toolbar Installer)를 악성코드로 진단했다.

2007년 5월 18일 시만텍 노턴 안티 바이러스 제품에서 중국어 윈도우 XP 서비스 팩2 파일인 netapp32.dll과 lasass.exe를 Backdoor.Haxdoor로 오진하고 시스템 파일을 삭제해 버려 시스템이 부팅되지 않는 문제가 발생했다. 그리고 2008년 7월 10일 안철수연구소는 윈도우 XP 서비스 팩 3의 LSASS.EXE 파일을 악성코드로 진단해 삭제해버려 시스템이 부팅되지 않는 문제가 발생했다.

2008년 11월 30일 어베스트!(Avast!)는 네이트온 및 기타 프로그램을 Win32:Search로 진단하고 12월 8일 알약이 알약에 포함된 AYUpdate.exe를 S.SPY.Lineag-GLG로 진단해 자신이 자신을 진단하는 해프닝도 있었다.

2009년 2월 16일 맥아피 바이러스 스캔에서 삼성증권 홈트레이딩시스템(HTS:Home Trading System)의 키보드 보안 프로그램을 악성코드로 오진하였다.



[그림 2-1] 맥아피의 삼성증권 홈트레이딩 시스템 오진

위의 예는 언론 등을 통해 알려진 오진 사례이며 언론에 잘 알려져 있지 않지만 개인 혹은 특정 기업에서 사용하는 프로그램을 악성코드로 오진하는 경우도 종종 있다.

(2) 오진이란?

오진(False Positives)은 줄여서 FP로 표현하거나 'False Alarm'과 같은 표현도 사용하며 사전적 의미로는 '긍정 오류', '양성 오류'로 해석되며 흔히 '오진', '오탐'으로 부른다. 보안 프로그램에서 오진은 정상을 비정상이라고 식별하는 것으로 스팸 검사에서는 정상 이메일을 스팸으로 잘못 식별하는 것, 백신 프로그램에서는 정상 프로그램을 악성코드로 잘못 식별하는 것이다.

(3) 오진의 피해

백신에서 정상 실행 파일이나 데이터 파일을 악성코드로 진단해 삭제하거나 치료를 시도하면 파일 변조가 발생한다. 이로 인해 파일이 삭제되거나 손상이 일어나 특정 프로그램 실행이 안될 수 있다. 만약, 시스템 파일이 삭제되거나 손상되면 단순 시스템 운영 장애뿐 아니라 최악의 경우 시스템 자체가 부팅되지 않을 수 있다. 또, 자사의 프로그램이 백신 프로그램에서 악성코드로 진단될 경우 고객들로부터 악성코드를 퍼뜨리는 회사로 오인을 받아 대외 신인도가 하락할 수 있다.

(4) 오진 종류

오진 발생 요인은 크게 '잘못된 분석'과 '잘못된 진단 값'으로 나뉘어 진다. 잘못된 분석은 분석가나 분석 시스템이 정상 파일을 악성코드로 분석한 경우이며 잘못된 진단 값은 악성코드를 정확하게 진단했지만 진단 위치를 잘못 선정해 악성코드뿐 아니라 정상 파일까지 진단하는 경우이다.

가) 분석가 오판

분석은 보통 자동 분석 시스템 혹은 분석가에 의해 이뤄진다. 분석가가 정상 파일을 악성코드로 오판하는 경우는 다양하다.

1) 악성코드와 유사한 프로그램

분석가가 오판하기 쉬운 대표적인 프로그램은 악성코드와 유사한 행동을 하는 프로그램들로 '보안 프로그램', '원격제어 프로그램', '인터넷 관련 프로그램' 등이 있다.

만약 이들 프로그램이 프로그램 보호를 위해 패커(Packer)를 사용하거나 자신의 존재를 숨기는 기능 그리고 분석가가 이해할 수 없는 언어로 된 문자열을 포함하고 있다면 악성코드로 오판할 가능성은 더 높아진다. 보안 프로그램 중 백신 프로그램은 진단에 사용하는 진단 문자열을 암호화하지 않거나 다른 백신에서 동일한 진단 문자열을 검색할 경우에는 진단 의심스러움 혹은 악성코드로 진단될 수 있다. 실제로 백신 프로그램간 오진도 종종 발생한다.

2007년에는 중국 백신 업체인 라이징과 러시아 카스퍼스키 연구소간 법정 문제로 비화된 오진 사건이 있었다. 카스퍼스키가 중국 라이징 제품을 악성코드로 오진하였는데, 빠른 조치가가 이루어지지 않아 결국 영업 방해로 법정까지 간 것이다. 라이징은 2006년 11월터 2007

년 5월까지 카스퍼스키 제품이 22 번의 오진을 일으켰다고 주장했다.[1]

체코 어베스트(Avast)는 2008년 4월 30일 국내 금융권 웹사이트 보안 프로그램으로 널리 사용되는 잉카 인터넷의 엔프로텍트 네티즌을 악성코드로 진단했다.[2] 특히 키보드 보안 프로그램은 사용자가 중간에 키보드 입력 내용을 가로채므로 기능만 보면 악성코드로 오해 할 수 있다.

2008년 7월에는 안철수연구소 V3의 시스템 드라이브 파일을 일부 백신 프로그램에서 오진한 적이 있었다.

2) 악성코드에서 이용하는 파일

악성코드 제작자가 모든 파일을 자신이 제작하는 경우가 있지만 때로는 정상 프로그램을 가져다 사용하는 경우가 있다. 키로깅 기능을 위해 키보드 내용을 가로채는 DLL 등이 대표적인 예이다.

이 경우 해당 DLL을 분석가가 악성코드로 판단할 수 있지만 실제로 정상적인 용도로 사용되는 프로그램의 구성 파일일 수 있다. 악성코드와 정상 프로그램 모두 사용 가능한 파일의 경우 오진이 발생한다.

나) 잘못된 진단 값

잘못된 진단 값이 악성코드에만 존재할 것으로 생각하고 진단한 부분이 정상 파일에도 동일하게 존재할 경우 발생한다.

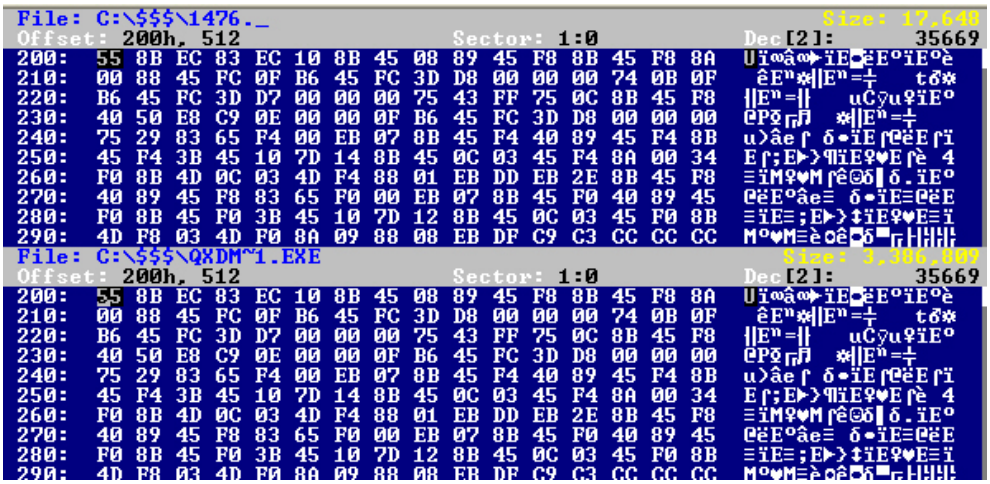
1) 컴파일러 공통 영역

고급 언어로 프로그램을 만들면 최소 수십 킬로바이트의 실행 파일이 생성되는데 생성되는 파일 중 컴파일러가 만든 공통 영역이 존재한다. 이 공통 영역은 악성코드와 정상 파일 모두 존재하며 파일들마다 코드가 매우 흡사하다. 만약 진단 위치를 컴파일러 공통 영역을 잡게 되면 심한 경우 특정 컴파일러로 제작한 모든 파일을 악성코드로 진단 할 수 있다. 보통 진단 위치를 자동으로 선정해주는 도구는 이런 부분을 피할 수 있지만 정의되지 않은 컴파일러의 경우 공통 영역 내용을 진단 값으로 삼을 수 있다.

[1] http://www.pcadvisor.co.uk/news/index.cfm?newsid=10067
[2] http://www.moneytoday.co.kr/view/mtview.php?type=1&no=2008050113133856164&outlink=1

2) 앞부분이 동일한 파일

앞부분이 동일하고 뒷부분에 데이터가 붙는 형태의 파일을 공통 영역을 시그니처로 잡을 때 발생한다. 보통 인스톨러, 오토잇!(AutoIt!), 자체 압축 풀림 파일(SFX, Self-extracting archive) 등이 이런 형태로 되어 있다. 보통 알려진 유형의 파일은 공통 영역을 피해 진단 값을 선정하지만 미리 정의되지 않은 파일은 공통 영역을 진단 값으로 정할 수 있다.



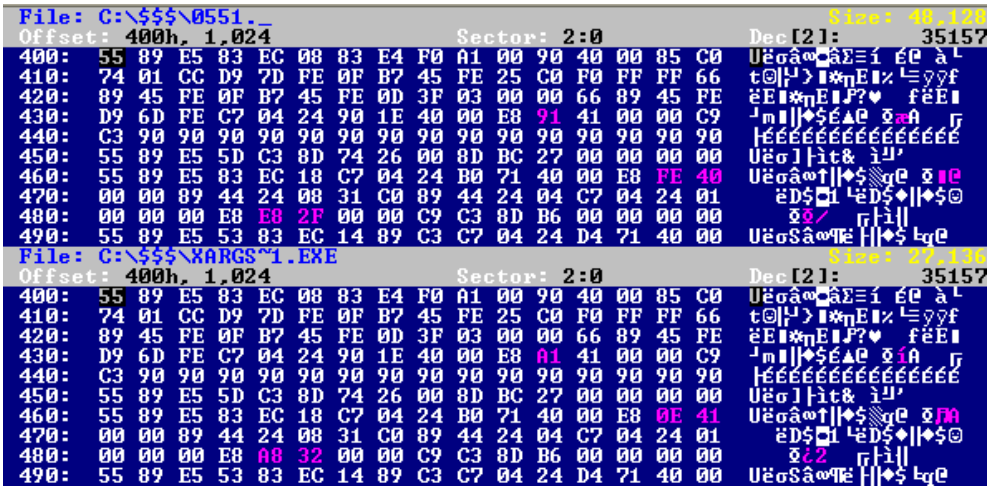
[그림 2-2] 앞 부분이 동일한 인스톨러 파일

3) 바이러스 감염 파일이나 변조된 파일

바이러스에 감염된 파일이나 윈도우 시스템 파일을 변조 시키는 악성코드의 경우에도 오진이 발생할 가능성이 높다. 주로 윈도우 시스템 파일을 변조 시키는 악성코드는 보통 Win-Trojan/Patched와 같은 이름이 붙여진다.

감염되거나 변형된 파일은 원본 파일과 공통 영역이 많이 존재하게 된다. 이때 진단위치를 원래 파일과 공통 영역으로 선정하면 정상 파일까지 진단될 수 있다.

다음 예는 xargs.exe에 바이러스가 감염되었는데 이 파일 자체를 트로이목마로 잘못 분석했고 진단 값을 앞부분으로 잡아서 코드가 유사한 xargs.exe의 다른 버전인 4.3.1-3를 악성코드로 오진한 경우이다.



[그림 2-3] 버전은 다르나 코드가 유사하여 오진한 경우

다) 진단명에 포함된 '의심스러움(Suspicious)'이란?

'의심스러움'은 엄밀히 말하면 오진은 아니다. 흔히 휴리스틱 진단으로 알려져 있으며 악성코드로 의심되는 파일을 진단한 것이다. 하지만, 사용자들은 '의심스러움'을 악성코드 진단으로 생각할 수 있다.

최근에는 백신 프로그램에서 패커나 비정상적인 실행 파일을 진단하는 경우가 증가하고 있는데 '크랙(Crack)'이나 키젠으로 불리는 제품번호 생성기가 패커로 압축되어 있는 경우 악성코드로 진단되거나 의심스럽다고 진단 될 수 있다.

'의심스러움'은 오진 가능성을 항상 포함하고 있으므로 백신 업체에 보내 분석 결과를 받아야 한다.

(5) 오진을 낮추기 위한 노력

오진 증가는 악성코드만큼 백신 업체 최대의 골치거리로 어떤 제품도 오진으로부터 자유로울 수는 없다. 이에 백신 업체는 오진을 낮추기 위해 엔진을 배포하기 전에 보유하고 있는 정상 파일을 검사해 오진 유무를 확인하고 있다. 하지만, 사용자가 사용하고 있는 모든 정상 파일을 모두 보유할 수 없어 문제 해결이 쉽지는 않은 실정이다. 이러한 문제점을 해결하기 위해 백신 업체간 정상파일에 대한 정보를 공유하는 방안에 대해 논의하는 중이다.

(6) 사용자 대처 방안

백신 프로그램에서 악성코드로 진단했을 때는 진단명을 통해 정확한 진단인지 '의심스러움' 인지를 파악할 필요가 있다.

보통 '의심스러움'으로는 표시하는 진단명에 'Heuristic(줄여서 Heur)', 'New Malware', 'Suspicious'(줄여서 Sus) 등이 포함된다. 이 경우 악성코드 추정이므로 파일 삭제나 치료 전에 백신 업체에 오진여부를 확인하는 게 좋다.정확한 진단명으로 진단할 경우에는 파일명을 확인해 그 동안 잘 사용하던 파일인지 확인 할 필요가 있다. 잘 사용하던 파일을 갑자기 악성코드로 진단하는 경우라면, 다른 백신에서 검사를 추가로 해보고, 만약 자신이 사용하는 백신 프로그램에서만 해당 파일을 진단한다면 오진일 가능성이 높다. 이때에는 자신이 사용하는 백신프로그램 제조 회사로 연락해 오진 유무를 최종 확인할 필요가 있다.

안철수연구소에서는 '바이러스 신고센터' 외에 [그림 2-4]와 같이 '오진 신고센터[1]' 도 운영하고 있으며 타 백신에서 진단하는 파일 중 오진으로 추정되는 샘플은 이곳으로 접수하면, 분석결과와 함께 오진여부를 안내해준다.

[그림 2-4] 안철수연구소의 오진 신고센터

[1] http://kr.ahnlab.com/info/customer/reportCenterForward.ahn?ct=01&center=diagnosis

III. 이달의 통계

1. 악성코드 – Autorun 기능을 이용한 악성코드 2차 감염증가

(1) 2월 악성코드 통계

순위		악성코드명	건수	비율
1	-	Win-Trojan/Agent.67678	13	16.5%
2	new	Win-Trojan/Xema.variant	11	13.9%
3	new	Win-Trojan/SpamMailer.349696	10	12.7%
4	new	Win-Trojan/Buzus.224256	8	10.1%
4	new	Win-Trojan/Fakealert.85504.B	8	10.1%
5	new	Dropper/Autorun.171298	6	7.6%
5	new	Dropper/OnlineGameHack.171283	6	7.6%
5	new	Win-Trojan/Agent.175644	6	7.6%
5	new	Win-Trojan/Downloader.10240.LD	6	7.6%
10	new	Dropper/OnlineGameHack.33280.D	5	6.3%
합계			79	100%

[표 3-1] 2009년 1월 악성코드 피해 Top 10

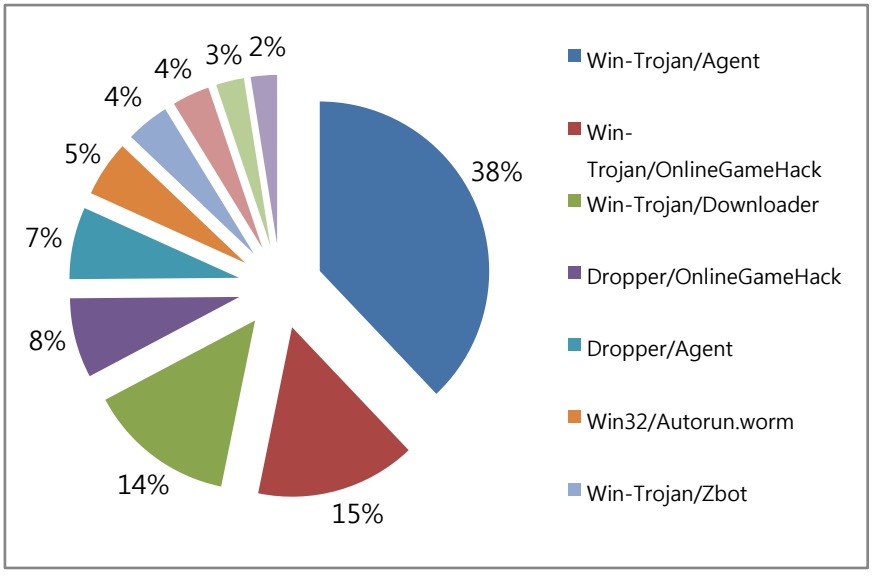
순위		악성코드명	건수	비율
1	new	Win-Trojan/Backdoor.33365	9	19.6%
2	new	Win32/Autorun.worm.175277	5	10.9%
2	new	Win32/Spammer.worm.395264	5	10.9%
4	new	Win-Trojan/Downloader.88576.H	5	10.9%
5	new	Win32/Autorun.worm.174030	4	8.7%
6	new	Win-Trojan/Agent.26112.IG	4	8.7%
7	new	Win-Trojan/Bagle.806912.D	4	8.7%
7	new	Win-Trojan/Webdor.425984	4	8.7%
9	new	Dropper/Agent.1176615	3	6.5%
10	new	Dropper/Agent.66048.J	3	6.5%
합계			46	100%

[표 3-2] 2009년 2월 악성코드 피해 Top 10

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

1월의 경우 10위까지의 악성코드 종류는 모두 Trojan류였으나, 2월 Top10에서 특이 할만한 것은 Top10중 Win32/Autorun.worm(이하 오토런 웜) 이 Top10의 2자리를 차지한 것이다. 오토런 웜은 윈도우의 자동실행 기능을 이용하여 전파하며, 악의적인 행동을 수행하는 악성코드다. 오토런 웜이 실행 되면 모든 드라이브 루트에 autorun.inf (악성코드 원본을 실행시키기 위해 파일명과 파일경로가 저장되어 있음)와 악성코드 원본을 생성한다. 감염된 시스템에 USB 등의 이동형 저장장치가 연결되어 있는 경우, 이동형 저장장치를 통해 전파될 수 있다. 국가정보원에서 배포하는 USB Guard[1]를 사용하면 이동형 저장장치를 통한 전파를 막을 수 있다..

아래의 그림과 표는 변형 악성코드를 묶어서 대표진단명 기준으로 통계를 뽑은 것이며, 개별 악성코드 통계보다 전체적인 악성코드 통계양상을 알 수 있다. 이는 많은 변형의 출현 및 빠른 악성코드 엔진대응으로 개별 악성코드 생명주기가 짧아져서 이를 보강하기 위해 참고로 작성한 것이다.



[그림 3-1] 2009년 2월 악성코드 대표진단명 Top 10

[1] http://www.ncsc.go.kr/data/usbguard.exe

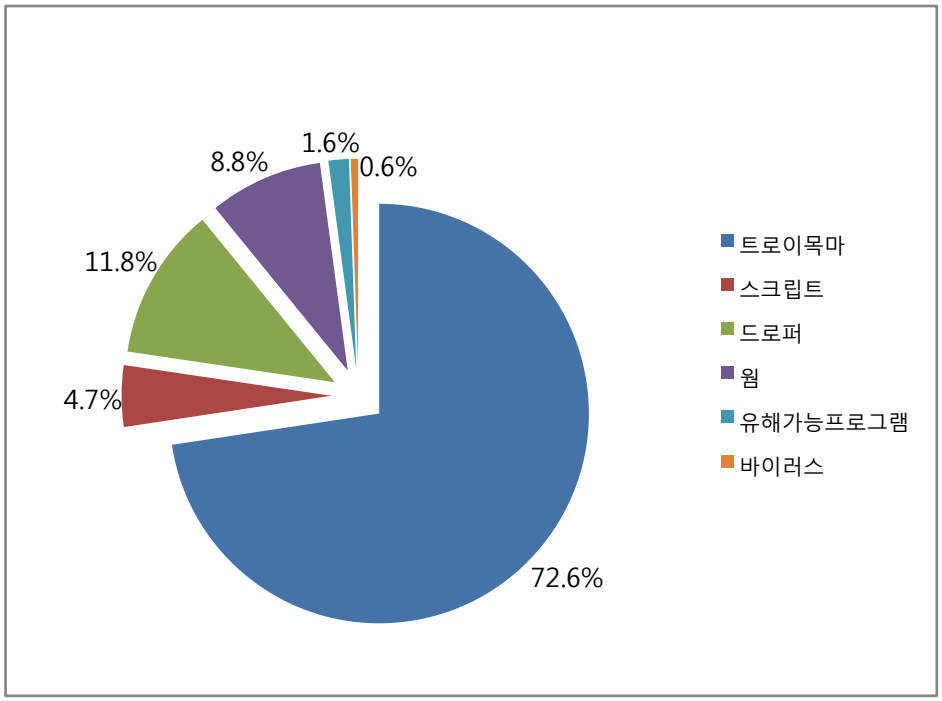
순위		악성코드명	건수	비율
1	↑1	Win-Trojan/Agent	667	37.9%
2	↓1	Win-Trojan/OnlineGameHack	269	15.3%
3	-	Win-Trojan/Downloader	247	14.0%
4	-	Dropper/OnlineGameHack	134	7.6%
5	↑5	Dropper/Agent	121	6.9%
6	↑3	Win32/Autorun.worm	94	5.3%
7	-	Win-Trojan/Zbot	73	4.2%
8	new	Win-Trojan/Waledac	63	3.6%
9	new	Win-Trojan/Fakeav	47	2.7%
10	new	Win-Trojan/Fraudload	44	2.5%
합계			1,759	100%

[표 3-3] 2009 2월 악성코드 대표진단명 Top 10

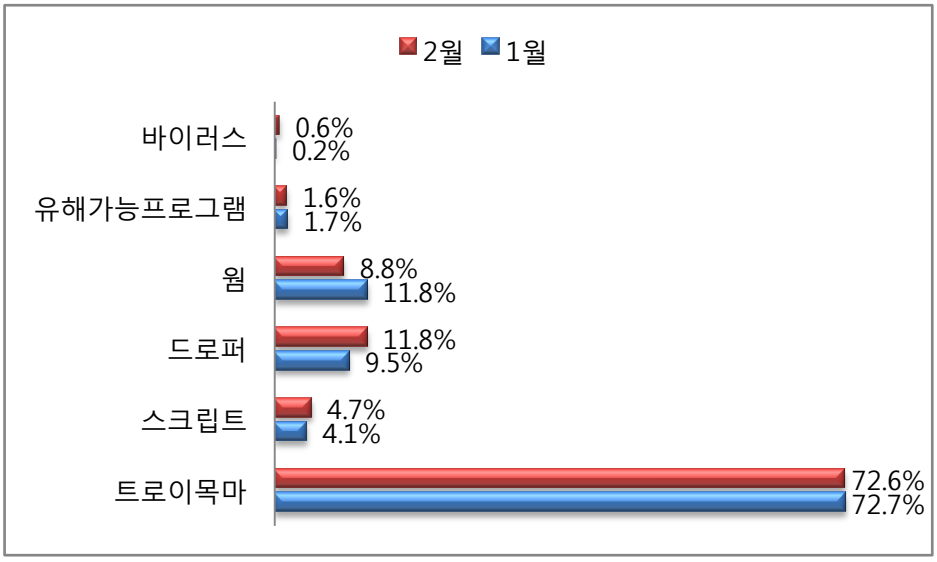
[그림 3-1]과 [표 3-3]은 2009 2월 악성코드의 대표진단명을 기준으로 유형별 피해 순위 Top 10을 나타내고 있다. 유형별 Top 10에 포함된 악성코드 총 피해건수는 1,759건이며 1월의 1,883건에 비해 소폭 감소하였다.

2월 악성코드 대표진단명 Top 10을 살펴 보면 OnlineGameHack이 2위와 4위를 차지하고 있으며, 그 비율을 합치면 29.3%로 1월과 마찬가지로 많은 비율을 차지하고 있다. 1월에 9위를 차지했던 오토런 웜은 6위로 올라갔다. OnlineGameHack과 마찬가지로 오토런 웜은 중국발 해킹을 이용해 유포되며, 감염된 시스템은 2차적으로 이동형 저장장치를 통해 전파될 수 있다. 작년 4분기부터 11월까지 기승을 부리다가 12월 이후로 잠잠하던 가짜백신 프로그램인 페이크 안티바이러스(Fakeav)는 다시 10위권으로 진입했으며, 작년 10월부터 꾸준히 늘어나 1월 악성코드 대표진단명 TOP10에 2위를 차지했던 콘피커 웜(Win32/Conficker.worm)은 10위권 밖으로 밀려났다.

아래의 [그림 3-2]는 2009년 2월 전체 악성코드 유형별 피해신고 건수를 나타내고 있는 그래프이다. 트로이 목마 프로그램은 72.6%로 다른 악성코드보다 월등히 많은 비율을 차지하고 있으며, 드롭퍼와 웜이 각각 11.8%와 8.8%를 차지하고 있으며, 그 뒤를 이어 스크립트 4.7%, 유해가능 프로그램이 1.6%를 차지하고 있다. 저번 달과 동일하게 바이러스는 0.6%로 극히 낮은 비율을 유지하고 있다.

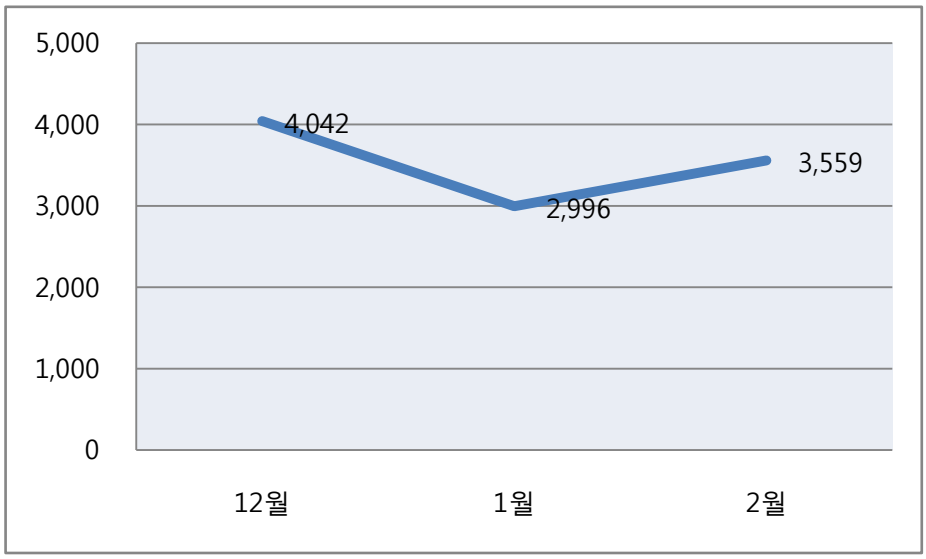


[그림 3-2] 2009년 2월 악성코드 유형별 피해신고 비율



[그림 3-3] 2009년 2월 악성코드 유형별 피해신고 비율 전월 비교

위의 [그림 3-3]은 전월과 비교한 악성코드 유형별 피해신고를 나타낸 것이다. 증가한 것은 트로이 목마의 경우 전월과 거의 다름없는 비율이며, 웜은 8.8%로 전월에 비해 3%가 줄어들었다. 웜이 줄어 든 것은 앞에서 언급된 콘피커 웜 감소와 연관된 것으로 보인다. 드로퍼는 11.8%로 전월에 비해 2.3% 소폭 증가하였으며, 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 작년 12월에서 1월에는 중국 춘절의 영향으로 중국발 악성코드가 다소 감소하였다가 2월에 들어 다시 증가하였다. 온라인 게임핵, 오토론 웜 등 악성코드의 1/3이상이 중국에서 제작된 것을 감안하면, 춘절 연휴의 영향이 반영된 것으로 보인다.

이동형 저장장치를 이용하는 다양한 악성코드가 출몰함에 따라 피해를 막기 위해서 이동형 저장 장치를 사용하기 전에 반드시 최신엔진으로 업데이트한 백신 프로그램으로 검사하는 습관이 필요하다.

(2) 국내 신종(변형) 악성코드 발견 피해 통계

2월 한 달 동안 접수된 신종(변형) 악성코드의 건수 및 유형은 [표 3-4]와 같다.

월	트로이목마	드롭퍼	스크립트	웜	파일	유해가능	합계
12 월	1431	370	263	85	3	23	2175
01 월	1361	195	87	260	3	24	1930
02 월	1691	261	105	166	11	22	2256

[표 3-4] 2008 ~ 2009년 최근 3개월 간 유형별 신종 (변형) 악성코드 발견 현황

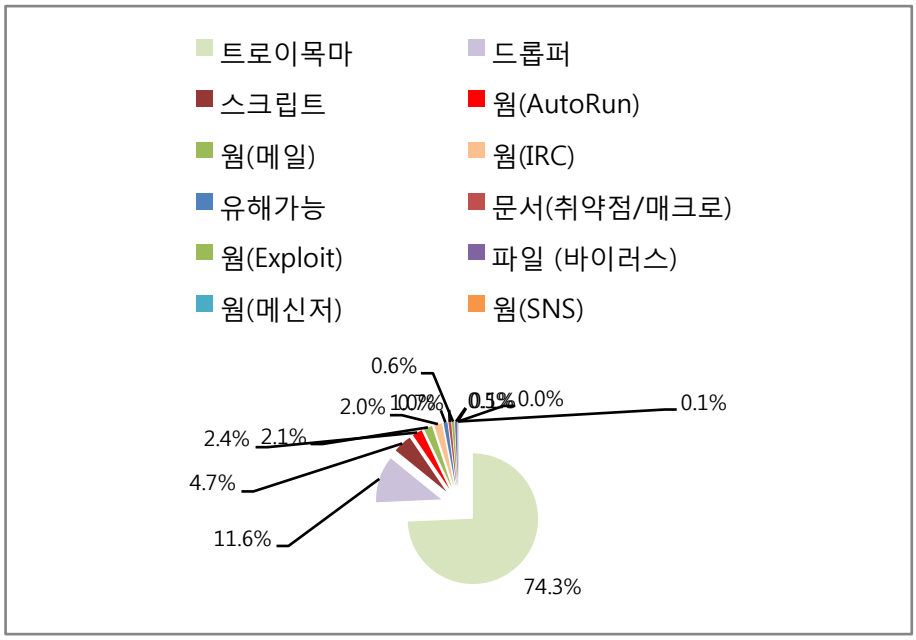
이번 달 신종 및 변형 악성코드는 전월에 대비하여 17% 증가 하였다. 위 [표 3-4]에서 알 수 있듯이 웜을 제외한 모든 악성코드 유형에서 발견 건수는 증가 하였다. 하지만, 웜은 전

월 대비 36% 감소를 하였다. 이는 지난 달에 폭발적으로 증가 했던 콘피커 웜의 확산으로 웜 유형의 발견건수가 많았지만, 2월에는 해당 악성코드가 진정국면으로 접어든 것이 전체적인 웜 유형의 발견건수 감소로 이어졌다. 특히 백신 업체들이 해당 악성코드를 Generic 하게 탐지 하도록 탐지기법을 수정하였기 때문에 광범위한 진단으로 콘피커 웜의 발견건수가 줄어든 것으로 보인다.

그러나 일반 사용자들이 해당 악성코드에 많이 감염 되었음을 알 수가 있었다. 이는 콘피커 웜에 감염 시 백신 업체와 같은 보안 업체의 인터넷 홈페이지 접속을 방해 하기 때문에 보안 업체 홈페이지에 접속하지 못한다는 피해를 신고하는 일반 사용자 문의가 2월 동안 끊이지 않은 것을 통해 알 수 있었다. 또한 이와 같은 문제를 해결하기 위해 임시 도메인을 통해 전용백신을 배포하는 방법을 사용하기도 하였다.

이와 같이 웜 유형은 콘피커 웜의 감소로 인하여 2월에 비하여 줄었지만 작년 12월 비해서는 여전히 높은 편이다. 한 때 큰 피해를 주었던 웜 유형은 다른 악성코드 유형에 밀려서 그 세력이 작아졌지만, 근래 들어 취약점과 Autorun 기능을 통해 급속히 시스템을 감염 시킬 수 있는 잠재력이 있는 만큼 여전히 관심을 가지고 피해 예방에 힘써야 할 것이다.

다음은 이번 달 악성코드 유형을 상세히 분류 하였다.



[그림 3-5] 2009년 02월 신종 및 변형 악성코드 유형

[그림 3-5]와 같이 트로이목마 유형은 74.3%로 전월 대비 23%증가 하였다. 일반적으로 트로이목마 유형의 증가는 온라인 게임의 사용자 계정을 훔쳐내는 악성코드 유형의 증가로 상

승하는데 이번 달에는 다른 양상을 보였다. 이번 달 트로이목마들은 전체적으로 고르게 상승하였으며, 주로 다음과 같은 악성코드가 많이 보고 되었다.

- Win-Trojan/Agent
- Win-Trojan/Downloader
- Win-Trojan/Fakeav

특히 Win-Trojan/Fakeav는 가짜 백신을 다운로드 하는 Win-Trojan/Vundo 트로이목마의 증가로 인하여 전월에 비해 급속히 증가 되고 있다. Win-Trojan/Agent와 Win-Trojan/Downloader류는 일반적인 형태로 가장 많은 유형을 차지 하였다. 이외에도 백신을 무력화 하는 Win-Trojan/AVKiller, Win-Trojan/Rootkit 형태가 많이 보고 되었다.

드롭퍼 유형은 전월 대비 34% 증가 하였다. 제일 많은 온라인 게임 유형을 제외하고는 전체적으로 평이하다. 다운로더 트로이목마를 드랍하는 형태와 Rootkit 및 Crypter 트로이목마와 관계있는 형태가 그 다음으로 많았다.

스크립트 유형 역시 소폭 상승하였다. 12월 경우 인터넷 익스플로러 관련 취약점으로 인하여 상승하다가 지난 달 급격한 감소를 맞았다. 그러나 이번 달은 앞서 말 한 것처럼 소폭 증가하였는데 특이한 형태는 발견 되지 않았다. 대부분 기존에 알려진 취약점을 이용한 형태나 iframe 태그를 이용한 형태와 VBS 류 웜이 대부분을 차지 하였다.

웜 유형은 앞서 말했듯이 콘피커 웜의 급격한 감소로 전체적으로 급격히 감소 하였다. 그래도 지난 12월 보다는 여전히 높은 수치이며, 지속적으로 콘피커 웜 변형 또는 같은 MS08-067 취약점을 사용하는 에임봇 웜 등이 보고 되고 있다. 그러나 이와 같이 취약점을 갖는 웜 유형은 전체 악성코드에서 1% 밖에 지나지 않는다. 이번 달 웜 유형은 대부분 Autorun 유형과 이메일 웜, 그리고 IRCBot 웜 유형이 차지 했다.

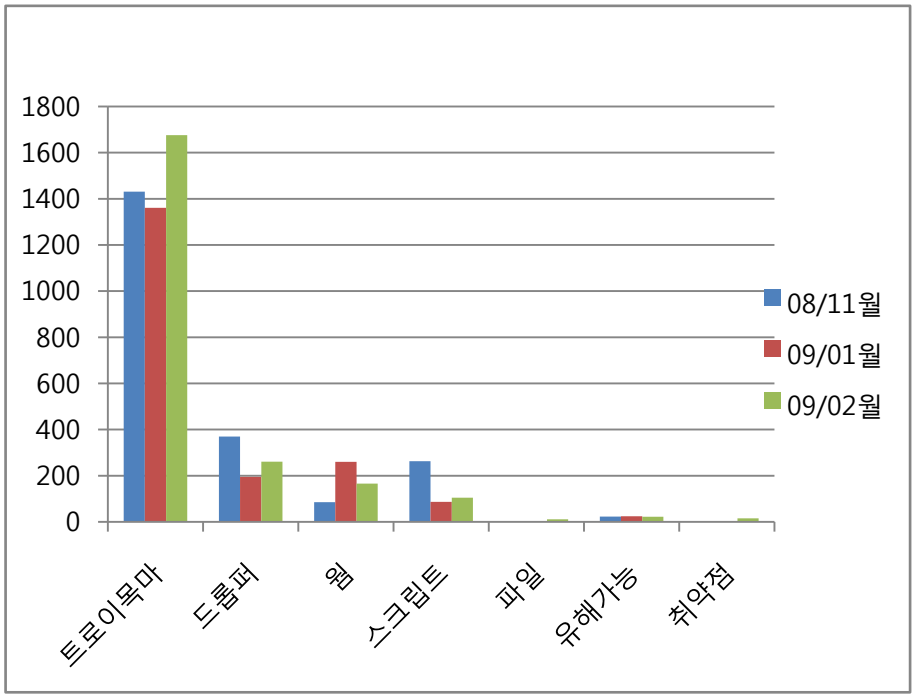
유해가능 프로그램류는 전월과 비슷한 수치가 보였는데 무료로 제공되는 키로거류가 주를 이루었다. 그 외에는 시스템을 셧다운 시키는 프로그램, 원격제어 툴 등이 주로 확인 되었다.

2월부터 취약점을 악용하여 악성코드로 제작된 유형들도 통계에 포함하였다. 2월에는 특히 PDF 문서 취약점을 사용하여 악의적으로 조작된 PDF 문서가 많이 보고 되었다. 해당 취약점은 기존에 알려진 형태로 시간이 지난 지금도 꾸준히 사용되고 있는 것으로 보인다.

바이러스 유형은 Win32/Virut 바이러스 변형이 계속적으로 보고 되었다. 특히 기존 안철수

연구소의 C(EPO), D형의 벗어난 E(EPO), F형이 보고 되었다.

다음은 최근 3개월간 신종 및 변형 악성코드 분포이다.

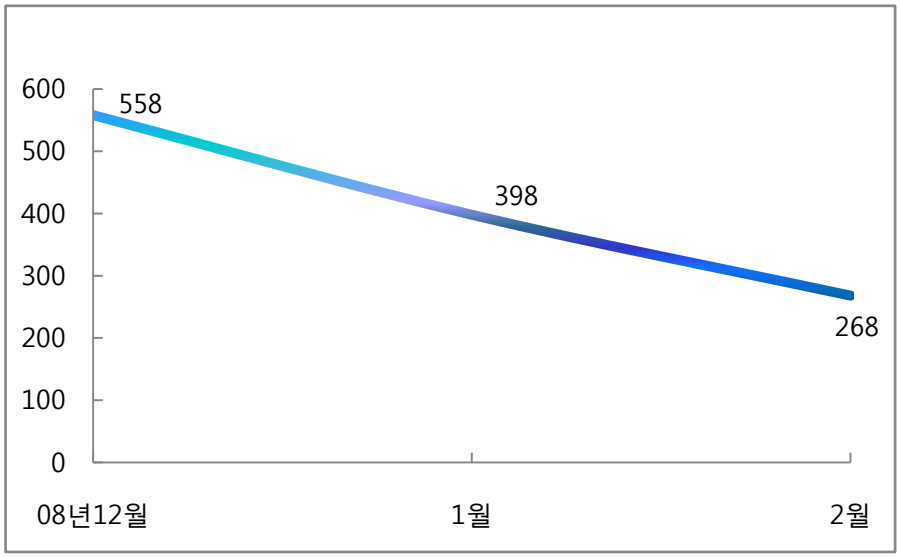


[그림 3-6] 2009년 최근 3개월간 악성코드 분포

[그림 3-6]에서도 알 수 있듯이 전월에 대비하여 웜 유형을 제외한 다른 악성코드 유형이 소폭 상승 하였다. 특히 트로이목마 유형이 큰 폭으로 상승하였고 이후 드롭퍼, 스크립트 악성코드 유형으로 상승 하였다.

웜 유형은 전월 대비 감소 했지만 여전히 Autorun 관련 악성코드와 IRCBot 웜 등이 활개를 치고 있다. 특히 MS08-067 취약점이 드문드문 발견 된 IRCBot 웜 변형 제작을 이끌어 내고 있다. 또한 국산 메신저를 노리는 악성코드도 점차 발견, 보고 되고 있어 메신저를 경로로 전파 되는 웜 유형도 증가할 것으로 예상 된다.

다음은 온라인 게임의 사용자 계정을 탈취하는 악성코드의 추세를 살펴보았다.



[그림 3-7] 온라인 게임 사용자 계정 탈취 트로이목마 현황

온라인 게임의 사용자 계정을 탈취하는 형태의 악성코드는 전월 대비 33% 감소하였다. 이는 1월을 기점으로 감소 추세에 있다. 감소의 가장 큰 원인은 지난 달 보고서에서도 언급 했듯이 그 동안 해당 악성코드에서 주로 사용되었던 특정 실행압축 형태의 악성코드가 진단되면서 감소율이 높았던 것으로 보인다. 그러나 최근에 보고 되는 형태는 진단을 회피할 목적으로 제작된 Custom[1] 압축 형태의 악성코드 비율이 점차 높아지고 있는 추세이다.

또한 여전히 백신 프로그램에 의한 진단을 회피 하기 위하여 파일 진단을 우회하거나 백신 프로그램 관련 파일을 무력화 하는 형태도 여전히 많이 사용 되고 있다. 참고로 해당 악성코드를 다운로드 및 실행 되는 방식은 주로 인터넷 익스플로러의 오래된 취약점을 사용하는 방식과 iframe 태그를 이용한 형태가 많다. 이런 경우 사이트가드[2]를 이용하면 안전하게 웹 서핑을 하면서 보안을 챙길 수가 있다.

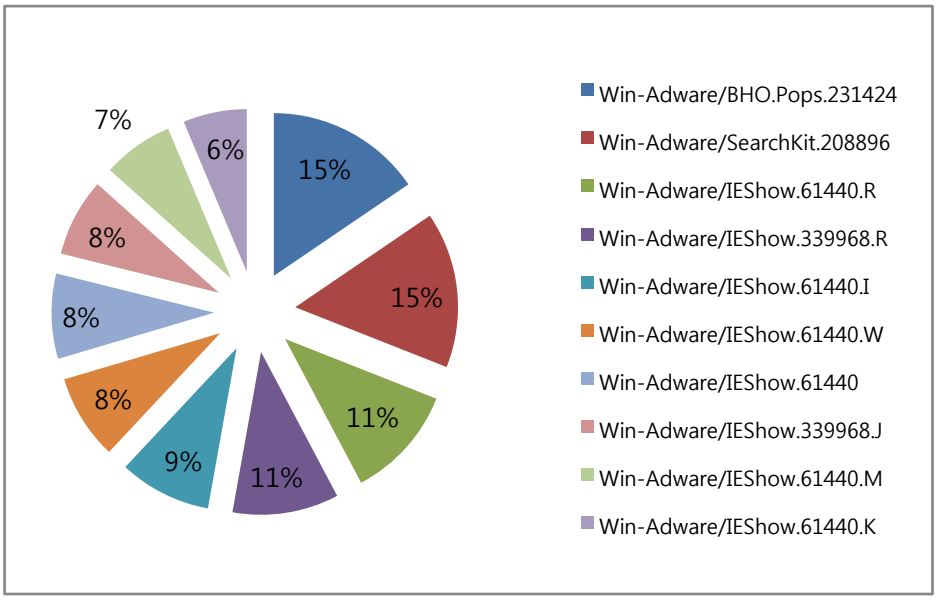
[1] 악성코드 제작자가 직접 제작한 압축 알고리즘
[2] www.siteguard.co.kr

2. 스파이웨어 동향 – 애드웨어 IEShow 변형 증가

(1) 2월 스파이웨어 피해 현황

순위		스파이웨어 명	건수	비율
1	New	Win-Adware/BHO.Pops.231424	22	15%
2	New	Win-Adware/SearchKit.208896	22	15%
3	New	Win-Adware/IEShow.61440.R	16	11%
4	New	Win-Adware/IEShow.339968.R	15	11%
5	New	Win-Adware/IEShow.61440.I	13	9%
6	New	Win-Adware/IEShow.61440.W	12	8%
7	New	Win-Adware/IEShow.61440	12	8%
8	New	Win-Adware/IEShow.339968.J	11	8%
9	New	Win-Adware/IEShow.61440.M	10	7%
10	New	Win-Adware/IEShow.61440.K	9	6%
합계			**142**	**100%**

[표 3-5] 2009년 2월 스파이웨어 피해 Top 10



[그림 3-8] 2009년 2월 스파이웨어 피해 Top 10

2009년 2월 스파이웨어 피해 Top10에 오른 스파이웨어는 모두 대량의 변형을 배포하는 국산 스파이웨어이다. 지난 1월에 피해 Top10에 등록된 스파이웨어의 총 피해건 수는 65건이었으나 2월 현재 집계결과는 142건으로 나타났다. 또한 스파이웨어 Top10에 등록된 진단명

은 모두 2가지 스파이웨어의 변형으로 확인되었다. 지난 1월에 이어 가장 많은 이름을 올린 Win-Adware/IEShow(이하 아이쇼우)의 경우 모두 2009년 1월 최초 발견된 이후로 지속적으로 대량의 변형을 유포하고 있다. 이번에 새롭게 Top 10에 등장한 Win-Adware/BHO.Pops 와 Win-Adware/SearchKit은 동일 제작자가 제작한 프로그램으로 사용자의 키워드 입력을 가로채 입력된 키워드에 관련된 광고를 노출하는 기능을 가지고 있다.

순위	대표진단명	건수	비율
1	Win-Adware/IEShow	220	35%
2	Win-Spyware/PWS.OnlineGame	74	26%
3	Win-Downloader/Zlob	66	7%
4	Win-Spyware/Crypter	57	6%
5	Win-Downloader/Rogue.SystemSecurity	45	6%
6	Win-Downloader/Rogue.XPPoliceAntiVirus	37	6%
7	Win-Spyware/Agent	37	4%
8	Win-Clicker/FakeAlert	35	4%
9	Win-Spyware/ZBot	34	3%
10	Win-Spyware/Xema	33	3%
합계		**638**	**100%**

[표 3-6] 2월 대표진단명에 의한 스파이웨어 피해 Top10

[표 3-6]은 변형을 고려하지 않은 대표 진단명을 기준으로 한 피해 건수이다. 2009년 2월에는 과거 외산 스파이웨어가 항상 피해신고 1위에 올랐던 것과는 다르게 국산 스파이웨어인 아이쇼우가 전체 문의의 1/3을 차지하고 있다. 이는 아이쇼우의 다양한 변형이 대량으로 배포되었으며, 실행 시 유저모드 루트킷으로 동작하여 백신프로그램에서 Suspicious BHO로 진단되어 사용자가 피해사실을 인지할 수 있었기 때문이다.

2009년 2월 유형별 스파이웨어 피해 현황은 [표 3-7]과 같다.

구분	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
08'12월	291	437	193	419	3	22	3	4	0	1372
1월	370	286	162	384	1	29	0	1	0	1233
2월	421	521	151	355	2	48	0	0	0	1500

[표 3-7] 2009년 2월 유형별 스파이웨어 피해 건수

스파이웨어류의 피해가 1월보다 다소 높아졌으며, 대량의 변형을 생산하는 국산 애드웨어의

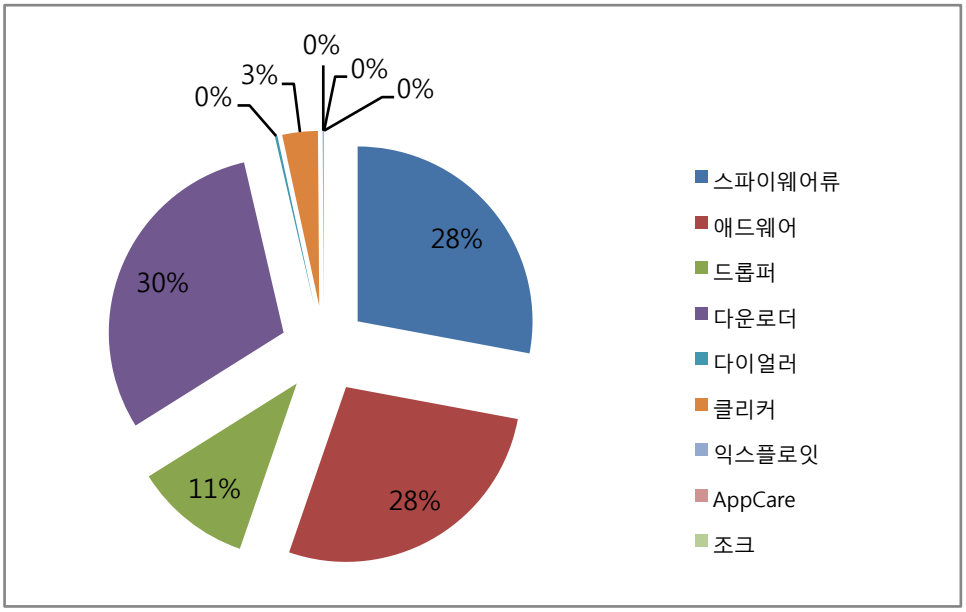
등장으로 인해 애드웨어류의 피해가 급격히 증가해 전체 피해건수가 급격하게 증가했다.

(2) 2월 스파이웨어 발견 현황

2월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 3-8], [그림 3-9]와 같다.

구분	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
08'12월	202	269	132	235	2	19	2	3	0	882
1월	264	139	76	244	0	24	0	1	0	748
2월	238	233	92	258	2	28	1	0	0	852

[표 3-8] 2009년 2월 유형별 신종(변형) 스파이웨어 발견 현황



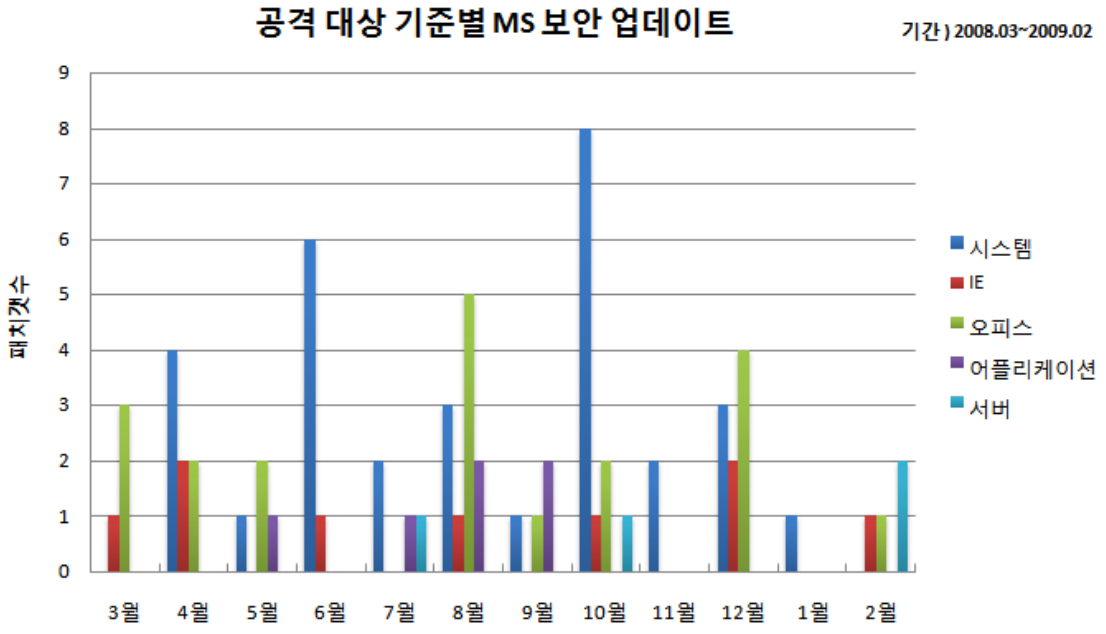
[그림 3-9] 2009년 2월 발견된 스파이웨어 프로그램 비율

애드웨어 피해신고는 증가하였으나 신종(변형) 애드웨어는 크게 증가하지 않았다. 이는 국내 애드웨어가 많은 변형을 배포하여 많은 PC를 감염시키기 때문에 피해신고는 증가하였지만 동일한 방법을 이용하는 애드웨어가 많지 않기 때문에 변형이 크게 증가하지는 않았기 때문이다.

3. 시큐리티 – MS09-002 취약점

(1) 2월 마이크로소프트 보안 업데이트 현황

2월에는 마이크로소프트사가 총 4건의 보안 업데이트를 발표했고, 긴급(Critical) 2건, 중요(Important) 2건으로 구성되어 있다.



[그림 3-10] 2009년 2월 발견된 스파이웨어 프로그램 비율

위험도	취약점	PoC
긴급	(MS09-002) Internet Explorer 누적 보안 업데이트	유
긴급	(MS09-003) Microsoft Exchange의 취약점으로 인한 원격 코드 실행 문제점	무
중요	(MS09-004) Microsoft SQL Server의 취약점으로 인한 원격 코드 실행 문제점	유
중요	(MS09-005) Microsoft Office Visio의 취약점으로 인한 원격 코드 실행 문제점	무

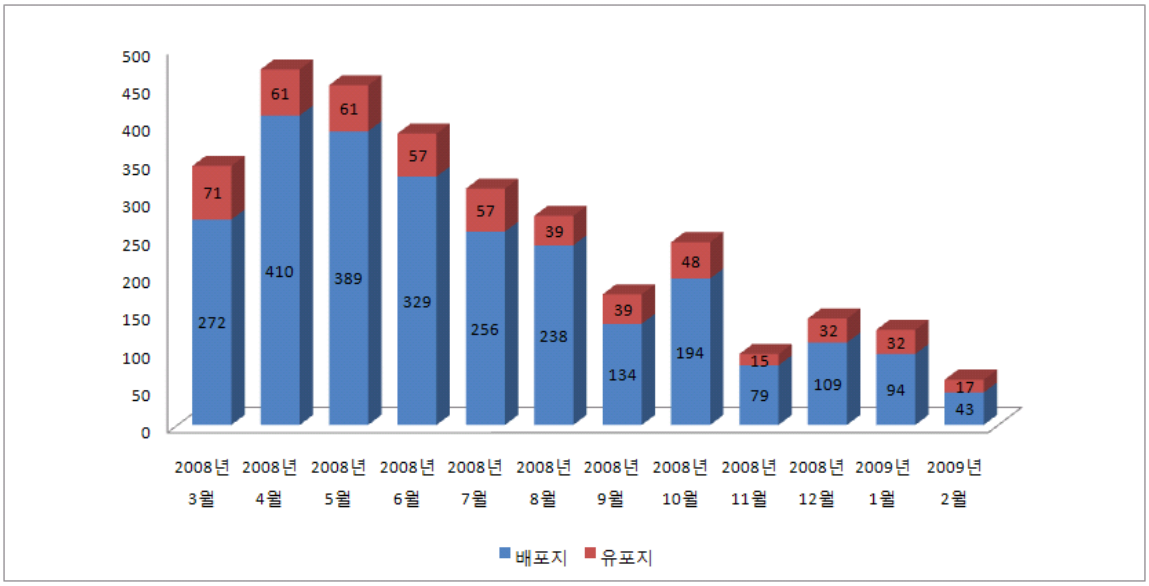
[표 3-9] 2009년 02월 주요 MS 보안 업데이트

MS09-004 MS SQL 서버 취약점은 해당 취약점 공격 코드(Exploit)가 이미 12월부터 공개되었으나, 제로데이 취약점으로 남겨진 채 두달여의 시간이 흘렀고, 드디어 2월에 관련 업데이트가 발표되었다. 업데이트 발표까지 많은 시간이 소요되었으나 해당 취약점을 통한 실제 악용사례는 아직까지 보고된 바가 없다.

한편, 이달에 발표된 MS09-002 인터넷 익스플로러 누적 업데이트에는 복제된 오브젝트 처리상의 문제로 발생하는 코드 실행 취약점 관련 패치가 포함되어 있다. 해당 취약점은 충분

한 코드 실행 가능성을 가지고 있기 때문에, 발표 이후, 국내외 언론에서도 많은 관심을 받았다. 드디어 이달에 실제로 힙 스프레이 기법과 결합되어 해당 취약점을 악용하는 악성코드 배포 사례들이 보고되기 시작하였다. 해당 취약점은 기존의 많은 취약점과 마찬가지로 웹 공격을 위한 좋은 방법론이 될 수 있기 때문에 해당 취약점에 대한 주의와 업데이트 적용을 통한 빠른 조치가 필요할 것이다.

(2) 2009년 2월 웹 침해사고 및 악성코드 배포 현황



[그림 3-11] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

2009년 2월 악성코드 배포를 위해 침해를 당한 웹사이트의 수와 악성 코드 유포지의 수는 43/17로 2008년 12월이래 계속 감소하는 추세를 나타낸다. 2009년 2월 Internet Explorer와 관련된 MS09-002취약점의 공격코드가 발표가 되었기 때문에 이러한 추세가 계속 될지는 조금 더 지켜보아야 한다. MS09-002 취약점은 함수의 레퍼런스를 관리하는 함수인 MSHTML.DLL의 PrivateAddRef 함수의 취약점을 이용한 것으로, 함수가 제거될 때, 함수 포인터를 제대로 관리하지 못해 생기는 취약점이다. 해당 공격 코드의 모습은 다음과 같다.

```
o1.click;
var o2 = o1.doneNode();
[redacted]es();
[redacted];
CollectGarbage();
```

[그림 3-12] MS09-002 공격 코드 중 일부

하지만 이 취약점의 공격도 힙 스프레이 기법을 사용하기 때문에 항상 공격이 성공한다고

볼 수 없기 때문에, 이전의 다른 취약점들(MS07-017 등)과 같이 큰 피해를 줄 것으로는 보이지 않는다. 하지만, 안철수연구소에서는 지속적으로 해당 코드를 사용한 침해결과를 감시할 예정이다.

4. 사이트가드 – 악성코드 증가 추세

(1) 2009년 2월 웹 사이트 보안 요약

구분	건수
악성코드 발견 건수	192,433
악성코드 유형	857
악성코드가 발견된 도메인	933
악성코드가 발견된 URL	10,135

[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 2월 한달 동안 웹 사이트를 통해 발견된 악성코드 동향을 요약해서 보여주고 있다.

사이트가드의 집계에 따르면 1월 한달 동안 악성코드는 857종 192,433건 발견되어 지난 2009년 12월부터 증가세를 보이고 있으며, 이런 악성코드를 포함하고 있는 웹사이트도 계속 증가하여 도메인 933개, 배포 URL 10,135개로 확인되었다.

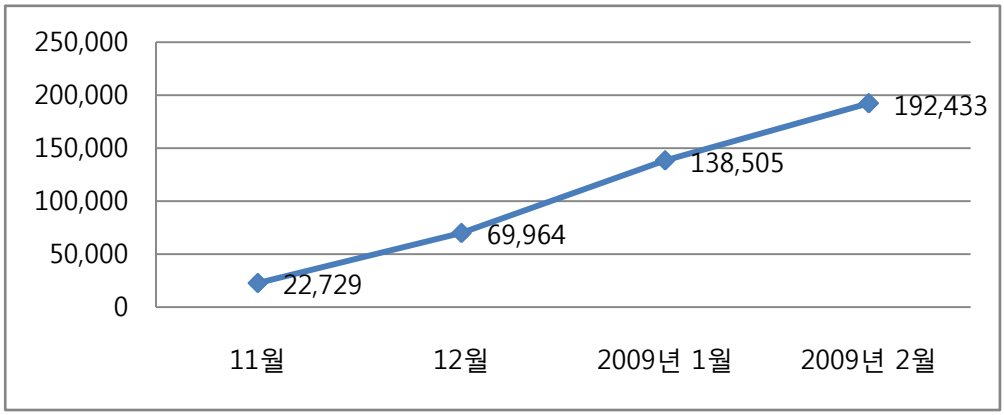
전체적으로 2월 한달 동안 악성코드 종류와 발견 건수, 도메인 그리고 URL 모두 지속적인 증가세를 보였다.

세부내용을 보면 다음과 같다.

[1] www.siteguard.co.kr

(2) 악성코드 월간 통계

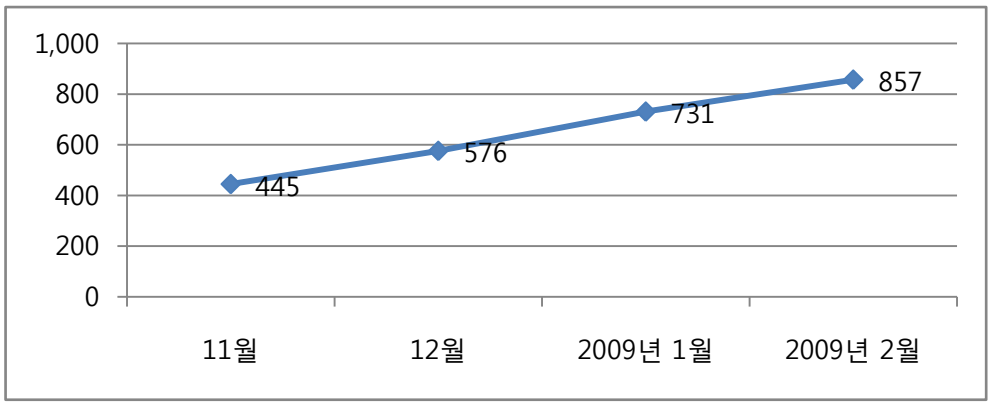
가) 악성코드 발견건수



[그림 3-13] 월별 악성코드 발견건수

[그림 3-13]는 최근 4개월인, 2008년 11월부터 2009년 2월까지의 악성코드 발견 건수의 추이를 나타내는 그래프로 1월 악성코드 발견 건수는 192,433건으로 지난달에 비해 약 40% 정도의 증가세를 보였다.

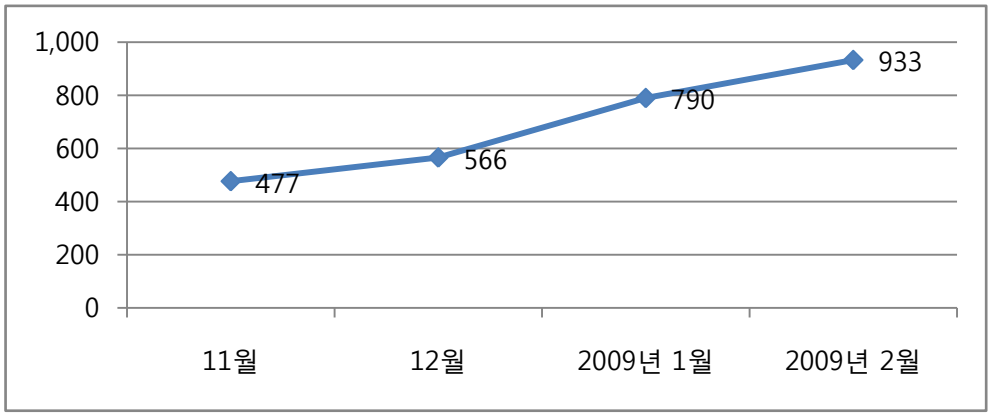
나) 악성코드 유형



[그림 3-14] 월별 악성코드 유형

[그림 3-14]는 최근 4개월간 발견된 악성코드의 유형을 나타내는 그래프로 역시 지난 1월의 731종에 이어 2월에 857종이 발견되어 지속적인 증가세를 보이고 있다.

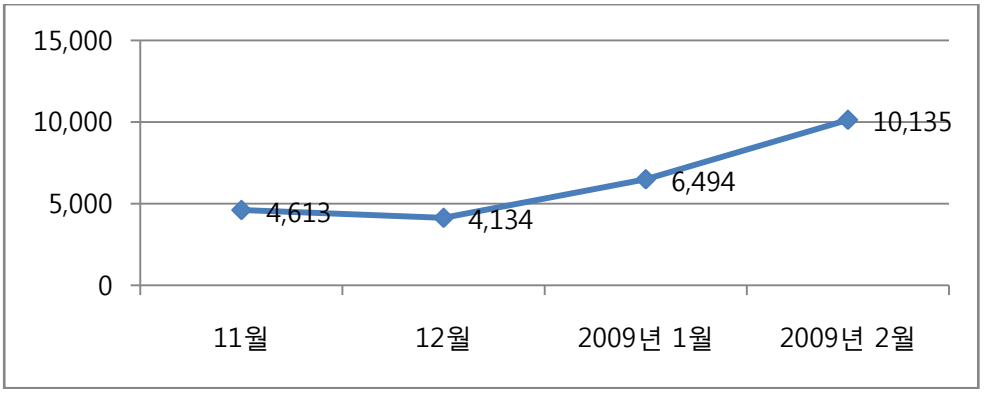
다) 악성코드가 발견된 도메인



[그림 3-15] 월별 악성코드가 발견된 도메인

[그림 3-15]는 최근 4개월간 악성코드가 발견된 도메인 수의 변화 추이를 나타내는 그래프로 2월 악성코드가 발견된 도메인은 933개로 전월에 비해 약 18%가 증가하였다. 이는 1월의 증가세에 비해서는 낮으나 지속적으로 악성코드를 웹을 통해 전파하는 경우가 증가함을 알 수 있다.

라) 악성코드가 발견된 URL



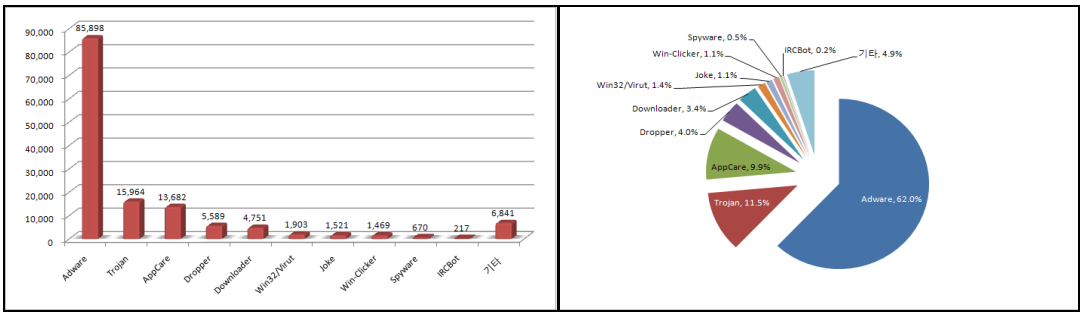
[그림 3-16] 월별 악성코드가 발견된 URL

[그림 3-16]은 최근 3개월간 악성코드가 발견된 URL 수의 변화 추이를 나타내는 그래프로 1월 악성코드가 발견된 URL은 6,494개로 전월에 비해 36%의 증가세를 보였다.

(3) 악성코드 유형별 악성코드 배포 수

유형	건수	비율
Adware	81,768	42.5%
Downloader	39,418	20.5%
Trojan	27,546	14.3%
AppCare	15,707	8.2%
Dropper	9,098	4.7%
Win32/Virut	3,194	1.7%
Joke	3,073	1.6%
Spyware	1,657	0.9%
Win-Clicker	906	0.5%
IRCBot	397	0.2%
기타	9,669	5.0%
합계	192,433	100%

[표 3-11] 악성코드 유형별 악성코드 배포 수



[그림 3-17] 악성코드 유형별 분포

[표 3-11]와 [그림 3-17]은 2월 한달 동안 발견된 악성코드를 유형별로 구분하여 발견 건수와 해당 비율(%)를 보여주고 있다.

2월 한달 동안 총 192,433개의 악성코드가 발견되었으며 이중 Adware류가 81,768개로 지난달에 이어 부동의 1위를 차지하였으며, 지난달에 2위였던 Trojan이 27,546개로 3위로 밀려나고, 그 자리에 Downloader가 39,418개로 2위를 차지하였다. Downloader가 2위를 차지한 것을 보면, 계속적으로 증가하는 변형들을 무차별적으로 다운 받기 위해 해커들이 전용 Downloader를 지속적으로 만든 것으로 추정된다.

(3) 악성코드 배포 순위

순위		악성코드명	건수	비율
1	new	Win-Downloader/NavigateAssister.282624	34,852	27%
2	new	Win-Adware/Shortcut.IconJoy.642048	26,985	21%
3	-	Win-Adware/Onclub.446464	25,552	20%
4	-	Win-Trojan/Xema.variant	10,559	8%
5	new	Win-Adware/Shortcut.ItemPFLauncher.36864	6,750	5%
6	↓1	Win-AppCare/WinKeyfinder.542720	5,908	5%
7	↓1	Win-AppCare/WinKeygen.94208	5,578	4%
8	new	Dropper/Agent.87552.G	4,778	4%
9	new	Win-Adware/WStory.94208	3,852	3%
10	↓6	Win-Appcare/RemoveWGA.49664	2,893	3%
합계			128,615	100%

[표 3-12] 악성코드 유형별 악성코드 배포 Top 10

[표 3-12]는 2월 한달 동안 웹 사이트에서 사이트가드를 통해 확인된 악성코드 배포 Top 10을 보여주고 있다. Top 10에 포함된 악성코드들의 총 배포건수는 128,615건으로 2월 한달 총 배포건수 192,433건의 약 67%에 해당되며, 지난달의 72%보다 약간 줄어들었다. 원인은 악성코드 유형수가 변종으로 인해 증가하여 점유율이 분산된 것으로 보인다.

특이한 점은 1위와 2위가 처음으로 Top10에 진입한 악성코드(Win-Downloader/NavigateAssister.282624와 Win-Adware/Shortcut.IconJoy.642048)가 차지했다는 것이다. 또한, 신규로 진입한 악성코드가 5개로써, 지난달의 2개에 비해 증가하였다. 이는 1월에 비해 악성코드 유형이 증가한 것이 주요 원인으로 보인다.

요컨대, 지난달 2월과 같이 drive by download 들이 지속적으로 증가하는 추세이다. 확산을 방지하기 위해서는 개인 사용자의 주의가 필요하지만, 먼저 웹 사이트 관리자는 적극적인 예방 조치(보안패치 및 백신프로그램 엔진 업데이트, 정기적인 소스 점검)를 통해 자신이 운영하는 사이트가 악성코드를 배포하는 agent로 악용되는 것을 방지하여야겠다.