ASEC Report 12월

® ASEC Report

2009. 1.

㈜안철수연구소의 시큐리티대응센터(AhnLab Security Emergency response Center)는 악성코드 및 보안위협으로부터 고객을 안전하게 지키기 위하여 바이러스 분석 및 보안 전문가들로 구성되어 있는 조직이다.

㈜안철수연구소의 시큐리티대응센터에서는 국내 인터넷 보안과 관련하여 보다 다양한 정보를 고객에게 제공하기 위하여 악성코드와 시큐리티의 종합된 정보를 매월 요약하여 리포트 형태로 제공하고 있다.

Ⅰ. 이달의 보안 이슈

(1) 악성코드 – IE 제로데이 취약점과 쿠폰을 가장한 악성코드

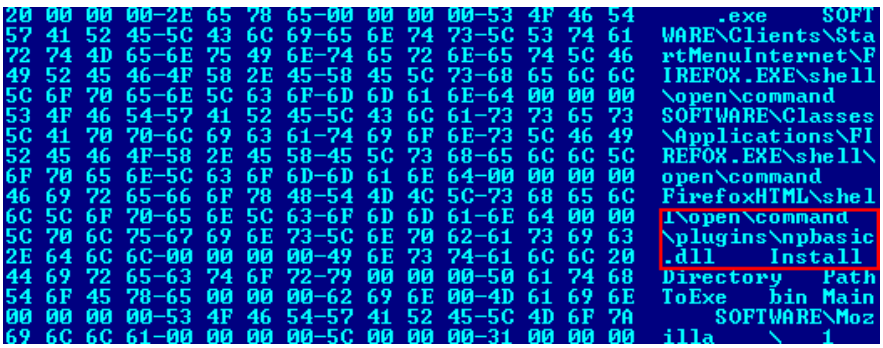
MS08-067 취약점을 이용한 Win32/Conficker.worm이 10월말 보고된 후, 12월 초에는 인터넷 익스플로러에 대한 제로데이 취약점이 발견, 보고되었고, 이를 악용한 악성코드가 제작되었다. 최근에는 상대적으로 인터넷 익스플로러와 비교하여 안전하다고 여겨졌던, 파이어폭스 웹 브라우저에도 동작하는 악성코드가 발견되었다. 또한 사용자들에게 쿠폰을 나눠주는 것처럼 속여 악성코드를 설치하는 사례도 이번 달에 발견되었다.

인터넷 익스플로러 제로데이 취약점

12월초 인터넷 익스플로러에 대한 제로데이 취약점이 알려졌다. 이는 모든 버전의 인터넷 익스플로러에 해당이 되어 큰 문제가 되었다. 또한 MS 의 긴급패치가 나오기 전에도 이를 악용한 악성코드와 제작도구가 만들어졌다. 이 취약점을 악용하는 악성 HTML 코드는 인터넷 익스플로러에서 데이터 바인딩 객체 배열을 생성하도록 하고, 일부를 해제한 다음, 이전에 해제된 객체를 참조하도록 한다. 이 취약점 유형은 유효하지 않은 포인터를 참조하기 전에 공격자가 힙 메모리의 데이터를 제어할 수 있기 때문에 공격이 가능하다. V3 는 JS/Mult 라는 진단명으로 해당 악성코드를 진단하고 있다.

파이어폭스 웹 브라우저를 노린 악성코드

인터넷 익스플로러보다는 비교적 안전하다고 알려진 파이어폭스 웹 브라우저만을 노린 악성코드[1]가 발견, 보고 되었다. 악성코드는 파이어폭스의 설치정보를 이용하며 자신을 플러그인으로 위장하여 실행되고, 플러그인 파일명은 npbasic.dll 이다.



[그림 1-1] 악성코드 실행 후 파이어폭스내 설치 정보

[1] V3는 Win-Trojan/Changehost.22115로 진단

해당 악성코드는 사용자가 파이어폭스를 실행할 때마다 함께 실행되어 악성코드에 하드코딩된 다음과 같은 사이트(주로 은행권으로 추정)에 대한 계정 정보를 훔쳐낸다.

[그림 1-2] 파이어폭스를 대상으로한 악성코드가 훔쳐내는 뱅킹 사이트

DNSChanger 류 악성코드

Win-Trojan/DNSChanger는 오래 전에 발견된 형태의 악성코드이지만, 12월에 발견된 변형은 은폐기법 및 자기보호 기능이 강화되었다. 일반적으로 해당 유형의 악성코드는 사용자 시스템의 DNS 주소를 특정한 곳으로 변경하여, 광고성 팝업, 배너, 피싱 또는 파밍 등을 통하여 사용자의 정보를 탈취하거나, 다른 악성코드를 감염시키고, 악성 DHCP(Dynamic Host Configuration Protocol) 서버를 생성하여 허위 DHCP 패킷을 보내기도 한다. 또한 감염 후 자신을 커널 레벨에서 은폐하고, 파일을 액세스 하지 못하도록 하는 등 변형에 따라서는 기존 파일 I/O를 무시하는 형태의 은폐기법을 사용하여 자신이 오랫동안 생존할 수 있게 하는 등 점점 지능적인 형태로 발전하고 있다.

연말연시 관련 악성코드

세계적인 경제불황에 콜라 및 햄버거의 쿠폰으로 위장한 악성코드가 유행하면서 국내에서도 발견되었다. 해당 악성코드(Win32/Ceein.worm)는 다음과 같은 첨부파일을 포함하여 메일로 전파되었다.

- coupon.zip, promotion.zip, postcard.zip

[그림 1-3] Win32/Ceein.worm.157184 웜이 보낸 메시지 (출처 *wordpress.com*)

실행 된 후 로컬 시스템에서 메일 주소를 수집하며 자체 메일발송 기능이 있어 수집된 메일 주소로 자신의 복사본을 전송한다. 또한 해당 악성코드는 백도어 모듈을 설치하여 시스템 정보 유출 및 제어 등에 악용될 수 있다.

(2) 스파이웨어 – 애드웨어의 새로운 시도

새로운 방법으로 광고를 노출하기 시작한 애드웨어

애드웨어는 소프트웨어 자체에 광고를 포함하거나 광고와 함께 묶여서 배포되는 프로그램을 말한다. 이러한 광고는 프로그래머가 소프트웨어를 개발하면서 개발 비용을 광고를 통해 충당할 목적으로 주로 사용된다. 이렇듯 모든 애드웨어가 악성코드는 아니지만, 광고를 강제적으로 사용자 PC에 띄워서 불편함을 유발하거나, 개인정보 침해를 야기하는 경우, 악성으로 분류하여 스파이웨어 제거 프로그램에서 진단한다. 이러한 악성 애드웨어는 주로 쇼핑, 포르노, 도박 사이트의 광고페이지를 노출하거나 강제로 연결을 시킨다.

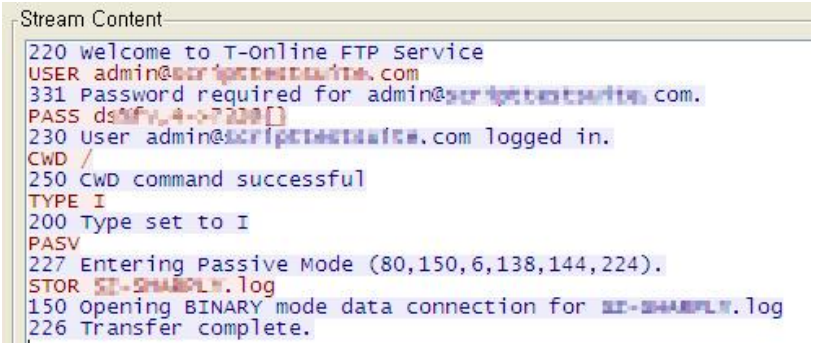
기존의 악성 애드웨어의 경우 인터넷 익스플로러에 광고를 시각적으로 노출했으나, 최근에 접수된 애드웨어 중에는 인터넷 익스플로러를 실행할 경우 스피커를 통해 광고로 추정되는 중국어가 나온다. ㈜안철수연구소로 접수된 의심파일을 확인결과 증상을 유발하는 애드웨어는 작업관리자(taskmgr.exe)와 유사한 파일명(taskmagr.exe)으로 동작하며 iframe을 인터넷 익스플로러에 삽입하는 형식으로 광고를 노출하는 애드웨어로 확인되었다. iframe을 통해 광고를 노출하는 것은 기존의 광고 방법과 유사한 형태지만 iframe 설정 값을 변경하여 화면에는 노출되지 않고 음성파일을 전송해 인터넷 익스플로러에서 음성파일이 실행되도록 한 것이다.

PC에 저장된 중요한 정보를 탈취하는 스파이웨어

공무원을 대상으로한 이메일을 통한 해킹이 문제가 되었다[1]. 전달된 이메일의 첨부파일을 실행하면 내부의 문서를 외부로 유출하는 스파이웨어를 이용한 것으로 지난 달 국외에서 신고된 샘플을 분석한 결과 스파이웨어 제작자는 개인의 PC들에 저장된 많은 정보들을 노리고 있었던 것으로 분석되었다.

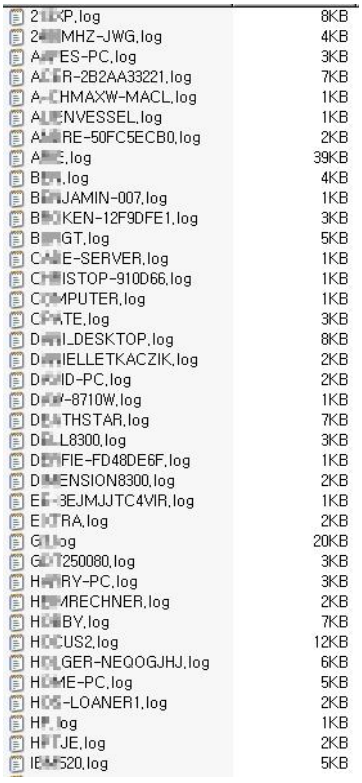
키생성기 형식으로 배포되는 것이 확인된 코드소프트(Win-Spyware/PWS.CodeSoft.1605120)는 사용자가 자신에게 필요한 키생성기를 찾아 실행할 때 PC에 감염이 된다. 코드소프트(Win-Spyware/PWS.CodeSoft.1605120)가 실행되면 실행된 PC에 설치된 모든 MS 관련 소프트웨어의 시리얼과 자동로그인이 설정된 각종 메신저의 계정 및 패스워드, 파이어폭스를 사용하는 경우 자동 로그인을 위해 저장된 웹사이트의 주소 계정 정보를 '컴퓨터이름.log'파일에 저장한 후 [그림 1-4]와 같이 특정 ftp사이트로 전송한다.

[1] http://www.boannews.com/media/view.asp?idx=11663&kind=1



[그림 1-4] 감염 PC에서 수집한 log를 ftp를 이용하여 서버로 전송

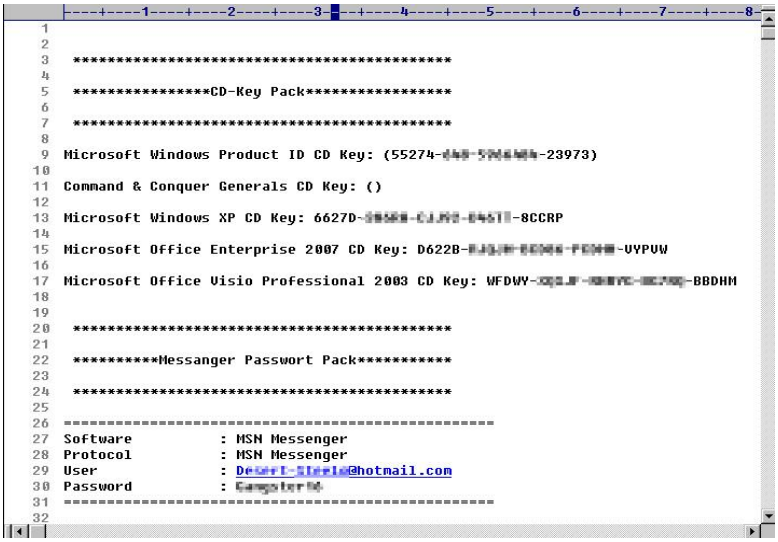
실제 해당 스파이웨어를 분석하여 사용되는 ftp 계정과 패스워드를 추출하여 확인한 결과 [그림 1-5]와 같이 많은 PC에서 성공한 것을 확인할 수 있었다.



[그림 1-5] ftp서버에 저장된 감염 PC의 정보 파일들

아이러니하게도 코드소프트(Win-Spyware/PWS.CodeSoft.1605120)를 배포한 해커는 무료로 소프트웨어의 키를 얻으려 하는 사용자를 노린다. 어떤 소프트웨어의 키가 필요한 PC 사용자가 인터넷 검색을 통해 자신이 필요로 하는 키생성기를 다운받아 실행하는 순간, 해커는 사용자의 PC에 저장된 수많은 계정과 패스워드는 물론이고 이미 설치된 소프트웨어의 CD

key까지 훔쳐가 버리는 것이다.



[그림 3-6] ftp서버에 저장된 정보파일의 내용

이러한 유형의 위협은 오래 전부터 지적되어온 보안의 위협 중 하나이지만, 이러한 프로그램의 경우 프로그램을 실행시킨 사람이 원하는 기능을 포함하고 있는 경우 자신의 PC에 저장된 어떤 정보가 외부로 유출되는 것을 알기 어렵다. 그러나, 코드소프트(Win-Spyware/PWS.CodeSoft.1605120)의 경우 실제 키생성기의 기능이 없는 상태에서 사용자를 속였기 때문에 ㈜안철수연구소로 신고가 접수되었으며, 악성코드 분석 환경에서 외부로 정보를 유출하는 기능이 그대로 분석되었다. 그러나, 개인 사용자가 사용하는 PC에서 그 사용자가 원하는 기능(예를 들어 키생성 등)을 제공하면서 동시에 PC에 저장된 정보를 외부로 전송한다면 그 프로그램을 사용한 사람은 스파이웨어의 기능에 만족하고, 다른 이에게 추천하는 일도 있을 수 있다.

빠른 속도로 변형을 생산하는 스파이웨어 패밀리의 지속적 증가

2008년 6월 ASEC Report에서는 빠른 속도로 변형을 생산하는 스파이웨어에 대해 다루었으며, 즐롭[1](Win-Spyware/Zlob)을 예로 들었다. 즐롭의 경우 동일한 배포 사이트를 통해 지속적으로 배포되며, 하루에도 수많은 변형 샘플을 배포하는 대표적인 스파이웨어이다.

이런 유형의 스파이웨어의 경우 기존 시그니처 기반의 백신 프로그램에서는 모두 다른 시그니처를 작성해야 하기 때문에 변형에 대한 대응이 어렵다.(2008년 7월 ASEC Report 참고)

[1] 즐롭(Win-Spyware/Zlob)은 동영상 재생을 위한 코덱을 가장해 배포되고 있으며, PC에 감염되면 허위감염 메시지 출력해 사용자로 하여금 가짜 백신을 설치하도록 유도하는 악성 코드다.

최근 즐롭(Zlob)을 제외하고도 씨피유에스에이치(Win-Dropper/Cpush), 티디에스에스(Win-Spyware/TDSS)와 같은 스파이웨어가 즐롭(Win-Spywar/Zlob)의 뒤를 이어 동일한 수법으로 변형을 배포하고 있으며. 동일한 사이트에서 변형을 배포하는 방법은 지속/확산되고 있다.

(3) 시큐리티 – MS08-078 IE XML 제로데이 취약점

MS08-078 IE XML 취약점

지난 12월 10일 어느 보안업체 직원의 실수로 마이크로소프트사로 전달되기 위한 인터넷 익스플로러 취약점 정보가 블로그에 포스팅되었다. 이렇게 외부로 알려진 인터넷 익스플로러 취약점은 거의 모든 익스플로러에 적용되는 아주 심각한 것으로써, 다음과 같은 형태의 XML 데이터를 처리하는 과정에서 발생한다.

```
<XML ID=I><X><C>
<![CDATA[
<image SRC=http://&#2570;&#2570;.AAAAA.lan
SRC=http://BBBB.lan >
]]>
</C></X></XML>
<SPAN DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
<XML ID=I> </XML>
<SPAN DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></SPAN>
</SPAN>
```

이러한 비정상적인 XML 태그는 인터넷 익스플로러가 메모리를 정상적으로 비우지 못하게 함으로써 원래 호출되어야 할 함수 대신 임의의 메모리 주소번지를 호출하게 만들 수 있다. 단지, 위와 같은 코드가 포함된 웹 페이지에 접근하는 것만으로도 사용자들은 피해를 입을 수 있기 때문에 아주 심각한 취약점이라 할 수 있다. 이러한 위험도가 높은 취약점들은 악성코드 제작자에게 매우 유용한 무기로 사용된다. 실제로 취약점이 발표된 후, 해당 취약점을 이용하는 악성코드가 접수되었으며, 국내외 크고 작은 웹사이트들에도 해당 취약점을 이용하는 악성 코드들이 삽입된 사례가 확인되었다. 또한, 대량 SQL Injection 공격으로 통해 삽입된 악의적인 URL에서도 해당 취약점을 이용하는 악성코드를 내포되어 있는 것이 발견되기도 하였다.

[그림 1-7] MS08-078 취약점을 이용한 실제 악성코드

문제의 심각성을 인지한 다수의 보안업체들은 임시방편으로 사용할 수 있는 비공식 패치를 발표하기도 하고, 해당 공격코드를 진단하거나 알려진 악성 URL들을 차단하는 등의 위협 확산을 위한 노력을 기울이기도 하였다. 마이크로소프트사에서 12월 18일에 제공한 긴급 보안 업데이트(Out-of-Band)를 적용하기 전까지 많은 사용자들이 일주일이 넘는 기간 동안 3rd party 업체에서 제공하는 패치를 사용하거나 익스플로러가 아닌 다른 브라우저를 사용하는 방법으로 웹 서비스를 이용할 수밖에 없었다. 하지만, 대부분의 사용자들은 이러한 취약점의 심각성을 인지하지 못하였기 때문에 윈도우 업데이트가 제공되기 전까지 평소와 마찬가지로 인터넷 익스플로러를 사용하였고, 이에 따라 보고되지 않은 수많은 피해자가 발생하였을 것으로 예상된다. 게다가, 패치가 공개된 후에도 적용하지 않은 채로 인터넷 익스플로러를 사용하고 있는 사용자들이 무수히 많고, 해당 취약점을 이용하는 악성코드의 공격도 증가되어 지속적인 피해가 발생되고 있을 것으로 추정된다.

SQL Server 취약점

마이크로소프트사는 SQL Server 2000과 2005의 일부 버전에 원격에서 코드를 실행할 수 있는 취약점이 존재한다고 발표하였다. 해당 취약점은 원격 혹은 로컬에서 인증된 사용자의 권한으로 확장 프로시저인 sp_replwritetovarbin에 존재하는 힙 오버플로우를 이용하여 임의의 코드를 실행할 수 있다. 현재(2009년 1월 초)까지는 공식적인 보안 업데이트가 발표되지 않았고, 블로그와 보안 권고문을 통해 sp_replwritetovarbin 확장 저장 프로시저의 권한 설정을 통한 해당 취약점 제거를 권고하고 있다

해당 취약점을 이용한 공격이 성공하려면 인증된 사용자의 권한이 필요하지만 웹 서비스처럼 사용자의 입력을 처리하는 경우 SQL Injection 등의 기법과 함께 사용된다면 인증 없이도 공격이 성공할 수 있다. 아직까지는 해당 취약점을 이용한 실제 공격이나 피해 사례가 보고되고 있지는 않지만 조속한 보안 패치가 제공되어야 할 것이다.

PS3를 이용한 SSL 공격

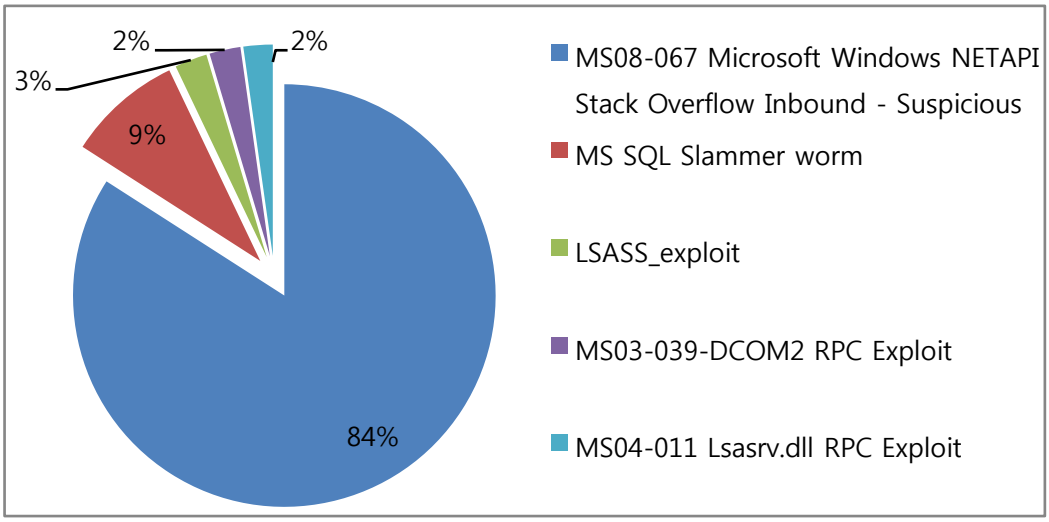
이번 독일에서 열린 컨퍼런스 CCC에서는 소니에서 만든 게임기인 PS3를 이용한 SSL 공격 성공에 대한 내용이 발표되었다. 발표 내용은 SSL 자체의 문제점이 아니라 인증서의 유효성을 검사할 때 사용되는 MD5의 문제점을 이용한 것이다. 발표자는 인증서를 발급해주는 인증 기관에서 사용하는 인증서의 MD5의 충돌 값을 찾기 위해 [그림 1-8]과 같이 200대의 PS3를 연결하여 사용하여 충돌이 일어나는 MD5 값을 찾아 정상적인 인증 기관의 인증서처럼 위조한 뒤 악용시킬 인증서를 발급하여 SSL에 사용하였다. 이렇게 만들어진 가짜 인증서는 사용자로 하여금 아무런 의심 없이 위조된 사이트에 접근하도록 만들 수 있다. 이러한 문제는 인증 기관에서 MD5 대신 안전한 해쉬 알고리즘 (SHA1 등)을 사용함으로써 어렵지 않

게 해결할 수 있다. 하지만, 이번 발표는 MD5와 같은 안전하지 못한 보안장치를 사용하는 서비스를 실제로 공략 가능함을 직접 보여줬음에 의미가 있다. 특히, PS3가 아니라 악성 코드 유포나 DDoS 공격에 사용되는 봇넷이 이러한 공격에 사용될 수 있기 때문에 보다 안전한 보안 장치를 개발하고 사용하는 것이 필요하다.

[그림 1-8] SSL 공격에 사용된 PS3

(4) 네트워크 모니터링 현황 – MS08-067 취약점 공격 트래픽

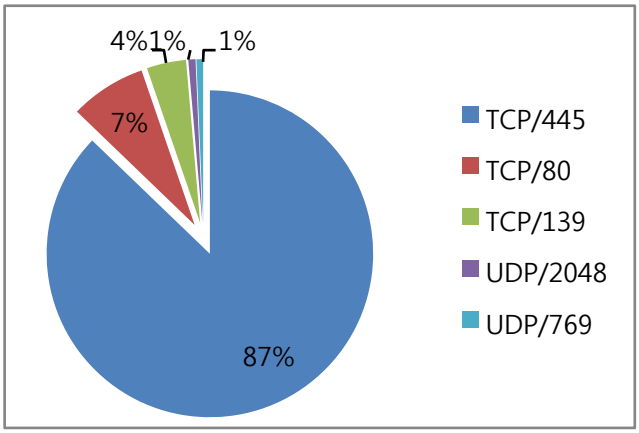
12월에 ㈜안철수연구소에서 운영중인 네트워크 모니터링 시스템의 로그를 분석하여 추출된 Top 5 보안 위협은 아래 [그림 1-9]와 같다.



[그림 1-9] 상위 TOP5 위협 탐지 이벤트

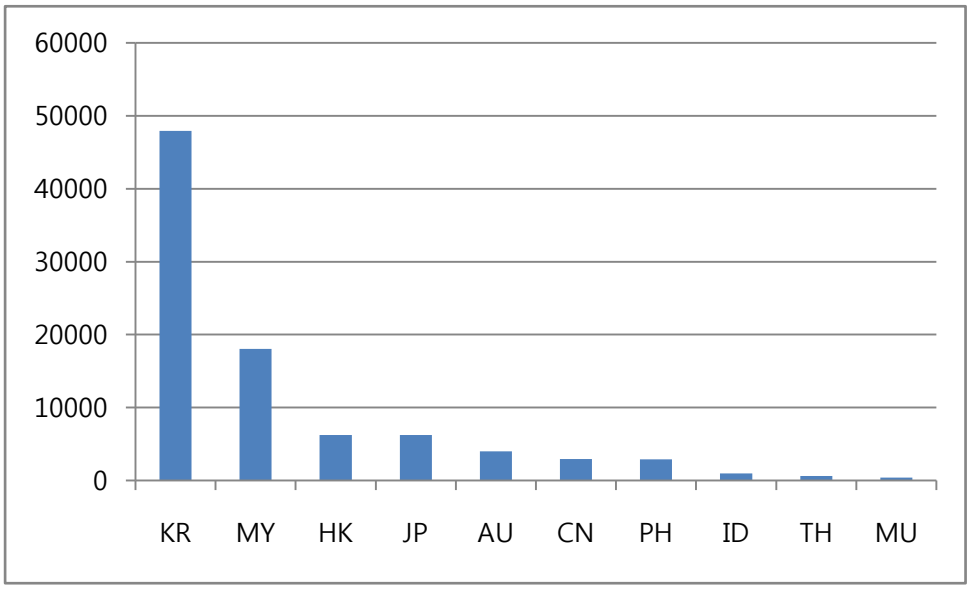
지난 10월 말 MS08-067 서버 서비스 취약점이 발표된 이후, 해당 취약점 공격으로 분석된 트래픽이 급격히 증가하여, 지난 11월 2위를 차지하였으나 이번 달에는 가장 최상위 이벤트로 랭크 되었다. 최근 새로운 취약점이 발표되면, 그에 따른 악성코드가 제작되는 시간이 점점 짧아지고 있어 해당 취약점을 이용하는 공격 트래픽 또한 급격히 증가되는 현상을 확인할 수 있다.

[그림 1-10]의 포트별 공격 트래픽 탐지 부분에서도 MS08-067 서버 서비스 취약점과 관련된 TCP/139, TCP/445 포트가 큰 비중을 차지하였다. 특히, TCP/445 포트는 직접적인 공격 트래픽 외에도 사전 공격에 발생되는 트래픽을 포함하여 87%라는 네트워크 모니터링 시작 이후 가장 큰 수치를 나타내기도 하였다. 네트워크 관리자는 사용자 시스템의 패치 권고를 비롯하여 방화벽과 같은 보안 솔루션을 통해 해당 TCP/139, TCP/445 포트에 대한 설정을 강화할 필요가 있다.



[그림 1-10] 상위 TOP 5 포트

국가별 공격 발생지 현황[1]을 살펴보면, 한국(KR), 말레이시아(MY), 홍콩(HK), 일본(JP), 오스트레일리아(AU), 중국(CN) 등의 국가들이 차례로 높은 비중을 차지하였다. 국내로부터 발생되는 트래픽 급증 현상 및 주요 국가 외에 말레이시아와 같은 제 3국으로부터 발생되는 트래픽이 증가되는 점이 특이하다.



[그림 1-11] 국가별 공격 탐지 통계

[1] 해당 결과는 ㈜안철수연구소에서 운영중인 네트워크 모니터링 시스템의 모니터링 결과로 전체를 대표하지는 않는다.

(5) 중국 보안 이슈 – 광범위하게 판매되는 악성코드 생성기

인터넷 익스플로러 0-Day 취약점을 악용한 악성코드의 발생

12월 10일 새벽 1시경, 중국으로부터 인터넷 익스플로러 7에 대한 패치가 제공되지 않은 제로데이 취약점인 "MS08-078 포인터 참조 메모리 손상 취약점"이 알려졌다. 이와 거의 동시에 중국과 대만을 비롯하여 유럽 등 전세계적으로 해당 취약점을 공격하는 악성코드[1]가 급속하게 유포되기 시작하였다.

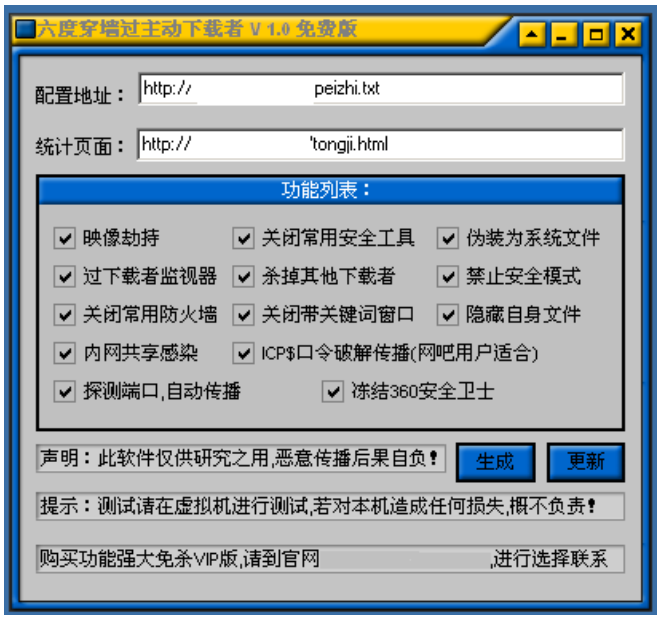
[그림 1-12] MS08-078 취약점을 악용하는 스크립트 악성코드 생성기

해당 보안 취약점을 악용한 악성코드가 발생한 몇 시간 뒤에는 중국 언더그라운드 웹 사이트들에서는 이미 [그림 1-12]와 같이 해당 취약점을 악용하여 다른 악성코드를 다운로드 할 수 있도록 설정이 가능한 JS/Mult 악성코드 생성기가 공유되기 시작하였고, 몇몇 언더그라운드 웹 사이트에서는 해당 악성코드 생성기를 판매하기도 하였다. 외국의 특정 보안 업체의 정보에 따르면 해당 취약점은 지난 10월에 언더그라운드에 알려지기 시작하여 실제 미화 15,000 달러에 거래되었다는 보고가 있었던 것으로 미루어 공개적으로 알려지기 전에 더욱 은밀하게 악용되었을 가능성이 높을 것으로 분석 된다.

상용으로 판매 중인 다양한 기능의 다운로더 생성기

12월 들어 중국 언더그라운드 웹 사이트들에서는 스크립트 악성코드를 생성하는 웹쉘(WebShell)과 다른 악성코드를 다운로드하는 기능을 가진 다운로더(Downloader) 형태의 악성코드 생성기가 많이 발견되었다.

[1] V3 진단명: JS/Mult

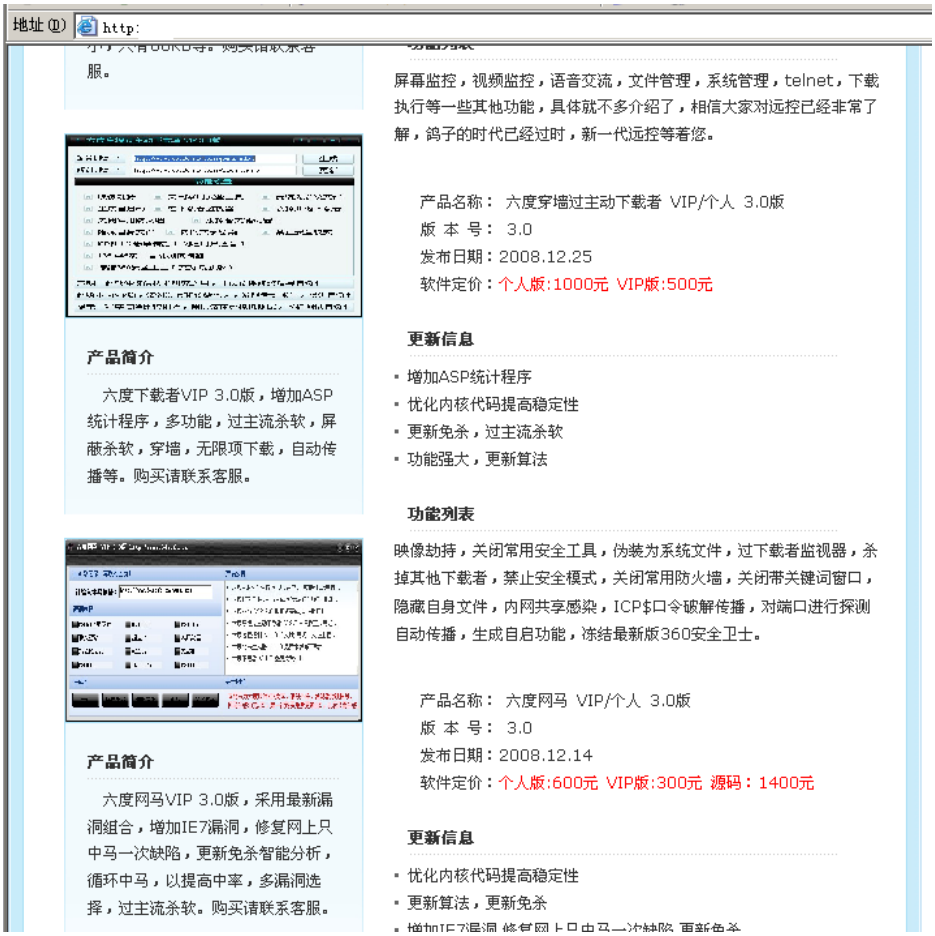


[그림 1-13] 상용으로 판매 되는 다운로더 생성기

여러 웹 사이트 중에서도 특히 전문적인 프로그래머를 고용하여 판매하고 있는 것으로 추정되는 웹 사이트에서 발견된 [그림 1-13]과 같은 다운로더 생성기[1]는 다양한 보안 프로그램을 우회할 수 있는 기능을 포함하고 있어 중국 내 블랙 마켓의 심각성을 여실히 보여주었다. 해당 다운로더 생성기는 구매자가 다운로드 할 악성코드 리스트가 존재하는 텍스트 파일의 웹 사이트 주소만 지정해주고 추가할 악의적인 기능들만 선택하면 새로운 악성코드가 생성되었다. 해당 다운로더 생성기가 가지고 있는 악의적인 기능들은 다음과 같다.

1. 다운로더의 은폐 기능
2. 윈도우 방화벽의 기능 강제종료 기능
3. 네트워크 내부의 공유폴더를 통한 전파
4. 알려진 보안 제품 및 시스템 분석 툴 강제종료 기능
5. 다른 다운로더 악성코드의 강제 삭제
6. 안전모드 부팅 방해
7. 안전360(중국 내에서 널리 사용되는 무료 백신) 강제 종료 기능

[1] 해당 다운로더 생성기로 생성한 악성코드는 V3에서 휘피곤 변형(Win-Trojan/Hupigon.Gen)으로 진단 및 치료 가능하다.



[그림 1-14] 다양한 악성코드 생성기를 판매하고 있는 웹 사이트

이러한 다양한 악의적인 기능을 가지고 있는 다운로더 생성기를 판매하고 있는 웹 사이트에서는 해당 다운로더 생성기외에도 MS08-078 취약점을 공격하는 스크립트 악성코드 생성기와 웹쉘(WebShell) 생성기 등 다양한 악성코드 생성기 등이 한화 약 54,000원에서 252,000원 사이에 판매되고 있었다. 그리고 구매자에게 중국의 QQ 메신저를 통해서 기술지원을 하고 있다고 광고 중이었다. 이렇게 중국 내 블랙마켓에서 판매되고 있는 악성코드 생성기 들은 기술적인 지식이 없더라도 다른 시스템을 충분히 공격할 수 있어 금전을 목적으로 한 악성코드의 양산을 부추기고 있는 것으로 분석 된다.

II. 연간 보안 이슈

2008년 1월부터 12월까지의 악성코드/스파이웨어 동향을 분석한 결과 올 1년간 새로 발견된 악성코드(바이러스, 웜, 트로이목마의 통칭)는 17,652개로 전년 동기 대비 약 2.9배로 증가했으며, 스파이웨어는 6,815개가 새로 발견돼 지난해 동기 대비 약 2.9배로 증가했다. 이런 폭증세의 주요 원인은 악성코드 자동 제작 툴이 인터넷 상에 공개되어 일반인들도 쉽게 입수해 악성코드를 제작할 수 있기 때문인 것으로 분석된다.

월	트로이목마	드롭퍼	웜	스크립트	파일	기타	소계	스파이웨어	총계
1월	1,272	160	111	123	1	33	1,700	276	1,976
2월	579	48	82	110	3	23	845	300	1,145
3월	739	77	87	78	9	38	1,028	415	1,443
4월	1,063	112	98	181	8	10	1,472	369	1,841
5월	743	49	86	216	2	19	1,115	352	1,467
6월	1,800	111	67	123	4	29	2,134	572	2,706
7월	1,399	144	77	117	5	21	1,763	615	2,378
8월	1,094	195	55	88	1	10	1,443	745	2,188
9월	867	97	64	91	2	13	1,134	684	1,818
10월	899	130	58	145	3	16	1,251	784	2,035
11월	1,162	197	57	151	19	6	1,592	821	2,413
12월	1431	370	85	263	3	23	2,175	882	3,057
합계	13,048	1,690	927	1,686	60	241	17,652	6,815	24,467

[표 2-1] 2008년 신종 악성코드 발견 건수

(1) 2008년 10대 이슈 및 2009년 전망

올 한해 악성코드 동향은 중국 발 해킹과 악성코드로 인한 피해가 극심하고 국지적인 특성이 매우 뚜렷하다고 정리할 수 있다.

폭증하고 있는 악성 코드

몇해 전부터 폭증하는 추세를 보이고 있는 악성 코드 수가 올해도 폭증세를 이어가고 있다. 이러한 현상의 주요 원인으로는 악성코드 자동 제작도구를 일반인들도 쉽게 입수할 수 있을 정도로 일반화되어 이를 이용하여 너무나도 쉽게 악성코드를 제작할 수 있는 환경이 구축된 것으로 추정된다. 특히 웹 사이트 로그인 계정 정보나 시스템 정보와 같은 개인 정보를 훔쳐

내는 트로이목마 유형의 악성코드는 전체 악성코드 75% 를 차지 할 만큼 많았으며 그 피해 또한 컸다.
이러한 악성코드들이 지속적으로 PC를 공격하고, 감염된 PC에 의해서 거대한 봇넷을 구성하여 스팸과 DDoS 공격에 지속적으로 사용되고 있고, 이를 사이버 범죄에 악용하고 있는 현상이 지속되고 있다.

악성화/교묘화로 발달하고 있는 스파이웨어

2008년 상반기 국내 스파이웨어 제작사에 대한 경찰의 대대적인 수사로 국내 허위 안티-스파이웨어 프로그램 제작자가 서울경찰청 사이버 수사대에 무더기로 검거되는 사건이 있었다. 이를 계기로 한때 국내 제작 스파이웨어 수가 주춤하는 것으로 보였으나, 악성화와 교묘화하는 방법으로 스파이웨어가 발달하고 있다.
설치과정에서 교묘하게 형식적으로나마 사용자 동의를 받는 형태로 스파이웨어 기준을 살짝 벗어나는 형태가 많이 제작되고 있고, 이들은 주로 무료게임, 무료소프트웨어 설치과정에서 번들형태로 설치된다.
또한 2008년 1월 발견된 스파이웨어 하이드 프록(Win-Spyware/HideProc)은 악성 다운로더의 프로세스를 숨기는 기능을 수행하여 많은 피해를 입혔으며, 스파이웨어의 삭제를 방해하는 루트킷(Rootkit) 드라이버를 설치하는 스파이웨어가 많이 발견되었다. 이 외에도 다운로더 Kwsearch(Win-Downloader/Kwsearch)는 EXECryptor와 같은 프로텍터로 실행압축하여 분석도구 실행을 방해하고 역분석(Reverse-Engineering)을 어렵게 하는 등의 특징이 있으며, 2008년 12월 까지도 꾸준한 피해를 입히고 있다.

외산 가짜 백신으로 인한 피해

해외에서 제작된 스파이웨어는 성인사이트, 스팸메일을 통해 국내에 유입되어 많은 피해를 입혔다. 스파이웨어 즐롭(Win-Spyware/Zlob)의 경우 성인사이트나 선정적인 이미지가 포함된 스팸메일을 이용하여 가짜 동영상 코덱 설치를 유도한다. 이 외에도 상용 프로그램의 크랙 또는 키젠(Keygen) 프로그램으로 위장하여 설치되거나, 응용프로그램의 취약점을 이용하여 설치되기도 한다. 즐롭에 감염되면 클리커 훼이크얼럿(Win-Clicker/FakeAlert), 스파이웨어 크립터(Win-Spyware/Crypter) 등이 2차 감염될 수 있으며 허위 안티-스파이웨어 프로그램을 설치하고 스팸메일을 대량 발송하여 또 다른 사용자에게 피해를 입힐 수도 있다.
특히 가짜백신 AntiVirusXP2008(Win-Adware/Rogue.AntiVirusXP2008, Win-Trojan/Fakeav)에 감염되면 바탕화면이 허위 경고 메시지가 포함된 이미지로 변경되며, AntiVirusXP2008과 함께 설치된 블루스크린을 흉내낸 화면보호기로 인하여 사용자는 시스템에 오류가 있는 것으로 착각하기 쉽다. 이와 함께 디스플레이 설정을 변경하여 사용자가 바탕화면과 화면보호기를 변경할 수 없도록 한다. AntiVirusXP2008은 변형이 다양하며 랜덤한 경로명을 사용하여 설치하기 때문에 안티-바이러스 프로그램과 같은 보안 프로그램에서

진단이 어려운 특징이 있으며, 제거한 경우에도 다른 악성코드에 의해 재감염되는 경우가 많다.

MASS SQL Injection을 비롯하여 활발한 웹 공격

웹 서핑을 즐겨하는 사용자라면 최근 웹 페이지를 여는 순간 백신 프로그램의 경고창이 실행되는 사례를 자주 경험하였을 것이다. 이는 웹 페이지 속에 삽입된 악의적인 스크립트를 탐지해내어 차단하는 것으로 지난 1월부터 본격적으로 시작된 중국발 대량 웹 페이지 변조 공격으로 인하여 최근까지도 국내외 많은 사이트들이 피해를 입고 있다.
SQL Injection으로 인하여 데이터베이스 데이터 손상을 유발하였을 뿐만 아니라 웹 서버에 삽입된 스크립트를 통해서 사용자를 악의적인 사이트로 연결시킴으로써 최근 발표된 Flash Player 취약점 및 기타 ActiveX 취약점 Exploit을 통해 또 다른 2차 공격을 수행하고 있다. 또한 그 이외에도 웹 사이트에 존재하는 다수의 취약점을 이용하여 해당 웹 사이트를 해킹하고 악성코드의 유포지 혹은 경유지로 악용하는 사고가 지속적으로 발생하고 있다.

3rd party 어플리케이션 취약점에 대한 공격

올해 다수의 마이크로소프트사의 취약점들이 발표 되었음에도 불구하고, 최근 발생하고 있는 보안 사고의 상당 부분이 대중적으로 사용되고 있는 3rd party 어플리케이션 상에서 발견된 취약점들을 이용한 공격으로 파악되고 있다.
Adobe 플래쉬 플레이어 취약점을 악용하여 홈페이지를 'www.3929.cn'으로 고정하는 스파이웨어 및, Adobe Reader 취약점을 악용하여 PDF 파일 속 자바스크립트 기능으로 파일이 오픈 될 때, 악성 스크립트를 실행해서 ARP 스푸핑 공격, 악성 스파이웨어 Antivirusxp2008 등을 비롯한 각종 다운로더 및 트로잔 파일들을 다운로드하여 실행하는 공격들이 다수 발생하였다.

끊임없이 나오는 MS 보안 패치와 이를 악용한 공격

2008년 한해 동안 MS에서 발표된 보안 패치는 총 78건으로 작년 69건에 비하여 13%가량 증가하였다. 일반적으로 MS의 정기 보안 패치는 매월 두번째 화요일에 제공되는데, 연말에 크게 이슈가 되었던 MS08-078과 MS08-067이 상황의 긴급성으로 인하여 긴급 패치로 제공되었다.
올해 주요하게 이슈가 되었던 취약점으로는 (MS08-041) Microsoft Access Snapshot Viewer에서 사용하는 ActiveX 컨트롤의 취약점으로 인한 원격 코드 실행 문제점, (MS08-067) 서버 서비스의 취약점으로 인한 원격 코드 실행 문제점, (MS08-078) Internet Explorer 보안 업데이트(IE7 제로데이 취약점)을 꼽을 수 있다.

ARP 스푸핑의 재등장

올 상반기에 다시 등장한 ARP 스푸핑 공격은 과거 중국 발 웹 해킹에 의한 악성코드 전파의 새로운 패러다임을 제공하였다. 즉, 수동적인 웹 접속으로는 감염대상을 많이 확보 할 수는 없지만, ARP 스푸핑 공격을 활용하여 인트라넷의 모든 시스템을 공격 대상으로 삼았다. 이러한 ARP 스푸핑 공격으로 인하여 수많은 기업의 네트워크가 마비되고, 악성코드로 인하여 피해를 입었다.

유출된 개인 정보 악용

올 초 국내 최대 온라인 쇼핑몰에서의 사용자 DB 유출 사건을 시작으로, 국내 유명 포털의 메일 계정, 메신저, 쪽지함 등에서 악성코드 링크가 포함된 URL과 악성 첨부파일을 포함한 메일이 대량 발견되었다. 특히 이런 메일들은 공공기관을 사칭하는 한글로 된 메일내용을 포함하고 있었기 때문에 사용자들이 첨부파일이나 URL을 클릭할 확률이 더욱 더 높았다. 또한 메신저의 경우 사용자의 계정을 훔쳐내도록 되어 있어서 훔쳐낸 계정이 다른 목적으로 사용될 위험성도 예상 해볼 수 있다. 이처럼 이제는 국내 사용자들만을 노리는 스피어 피싱 성격의 메일과 악성코드의 기승이 활발해지지 않을까 예상 된다.

악성코드의 고도화와 사라지지 않는 바이러스

올해 초 파일이나 레지스트리에는 자신의 흔적을 남기지 않으며 대신 과거 부트 바이러스처럼 물리적인 디스크 영역에 자신의 코드를 숨겨놓고 동작하는 MBR Rootkit이 발견되었다. 이처럼 악성코드에 대한 은폐, 코드 가상화, 난독화, 실행압축 등 자체 보호 기능 적용이 일반화되고 있다.
실행 파일을 감염 시키는 전통적인 파일 감염 바이러스도 여전히 피해가 꾸준하다. 특히 Win32/Kashu.B 바이러스 변형이 꾸준히 발견되었는데, 이들 변형은 메모리 치료가 선행 되지 않으면 재감염되며 시작 실행 시점 불명확 기법과 다형성 기법 등을 사용하여 진단과 치료가 매우 까다로웠다. 또한 바이러스는 아니지만 윈도우의 중요한 시스템 파일을 패치한 후 악의적인 모듈이 실행 되도록 한 Win32/Liger, CIH 바이러스처럼 파일의 빈 공간에 자신을 기록하여 감염 후 파일 사이즈가 증가하지 않는 Win32/Huhk.C 도 발견, 보고 되었다.

사회공학적 트릭을 이용한 공격

사회적 관심 사항이 포함되어 있는 메일, 특정 조직에 대하여 신뢰할만한 사람이 발신인인 것처럼 가장한 스피어 피싱 메일, 메신저를 통한 지인으로 가장한 대화를 통한 개인정보 유출하는 다양한 scam 등 일반인을 속이기 위한 트릭이 꾸준히 다양화되어 지속적으로 사용자를 노리고 있다.

악성코드는 2009년에도 폭발적으로 증가 할 것으로 보인다. 이에 따라 2008년도 악성코드 동향을 위와 같이 정리하면서 여기서 예측 가능한 2009년 악성코드 흐름을 예상해 보았다.

전통적인 바이러스의 피해는 꾸준할 것으로 전망

악성코드 발생이 국지적인 경향이 뚜렷한 가운데 2008년에도 실행파일을 감염시키는 Win32/Virut 바이러스 변형들과 Win32/Kashu.B(Win32/Sality 변형)가 큰 피해를 발생시켰다. Win32/Virut 바이러스 경우는 2007년도에도 꾸준히 변형이 발견 되고 피해를 지속적으로 입혔다. 따라서 신규 바이러스에 의한 피해도 예상 해볼 수 있지만 이 바이러스들에 감염된 파일이 여전히 인터넷 공간을 떠돌고 있기 때문에 보안제품 사용에 신경쓰지 않는 사용자들에게는 잠재적으로 계속 위협이 될 수가 있다.

자기보호 고도화를 통한 악성코드의 생존성의 극대화

악성코드의 자기보호는 이미 몇 번 언급 된 적이 있었다. 그러나 2008년 초 알려진 MBRRootkit과 은폐형 스팸 메일러들(Runtime3, Siberia2 등)을 확인해보면 자기보호의 고도화가 얼마나 앞서 있는지 알 수가 있다. 악성코드는 자신이 발각되지 않고 안티 바이러스 제품으로부터 생존시간을 늘려야만 더 많은 악성행위를 할 수 있다. 따라서 자기보호 고도화 기법은 잘 알려진 은폐기법부터 보안 프로그램 무력화, 가상 머신 탐지, 분석을 방해할 목적의 코드 난독화, 시그니처 및 Generic 진단 탐지 회피 등이 포괄적으로 사용되거나 특정 악성코드들에게는 집중될 가능성이 높다.

봇넷(BotNet) 역동적인 활동

2008년 상반기에 Win32/Zhelatin.worm이 극성을 부렸다. 이 웜은 대표적인 P2P 봇넷을 구성하는 악성코드 이다. 봇넷은 크게 4가지 카테고리로 분류한다. IRC, HTTP, P2P, 그리고 독자적인 프로토콜을 이용하는 CS (Client & Server) 봇들이 존재 한다. IRC 봇넷은 거의 쇠퇴 하고 있고, 국내의 경우에는 중국산 악성코드들의 영향으로 CS 봇들이 기승을 부리고 있다. 봇넷의 가장 큰 위협은 스팸 메일과 DDoS 공격을 꼽을 수가 있는데 이러한 위협은 내년에도 꾸준할 것으로 보인다. 그러한 가장 큰 이유는 다양한 공격도구가 중국 내 사이버 블랙마켓에서 거래되고 그 시장은 점점 커지고 있기 때문이다. 비단 중국 내 문제를 떠나서 이러한 도구들은 점점 일반 사용자들을 공격자로 만들어준다는데 있어서 문제가 되고 있다. 이러한 도구의 판매는, 사용자들 쉽게 자극하고 사이버 범죄에 끌어드린다는 점에서 2차적인 문제를 안고 있다.

스피어 피싱 및 스팸성 사기 메일등 증가

봇넷과 관련이 깊은 위협 중 가장 많은 비중을 차지 하는 것이 바로 스피어 피싱과 스팸성 사기메일이다. 스피어 피싱은 특정 단체나 인물을 노리고 보내는 메일로서 악성코드가 첨부되어 있거나 악성코드가 올려진 사이트로 방문을 유도한다. 스팸성 사기 메일도 이와 유사하다. 메일에 악성코드를 첨부하는 전통적인 방식은 거의 사용되지 않고 있으며 메일 본문에 링크를 걸어 악의적인 사이트로 유도한다. 대부분의 사용자들은 이러한 공격에 쉽게 당한다. 이러한 메일의 증가는 봇넷의 활동이 왕성해지면 더욱 더 극에 달 할 것으로 보인다.

국내 SNS 및 대형 포털 메일계정 사용자를 노리는 악성코드

올해 초 대형 쇼핑몰의 개인정보 유출로 인하여 더욱 더 개인 정보의 보호의 중요성이 대두되었다. 작년 초부터 서서히 선보이기 시작한 국내 유명 메신저와 포털의 메일 사용자를 노리는 악성코드는 계속 진화할 것으로 보인다. 특히 국내의 경우 영어로 작성된 스피어 피싱이나 스팸성 사기메일에 대하여 국내 사용자들은 영어에 대한 거부감으로 일반적으로 열어보지 않기 때문에 감염률이 낮다. 그러나 사용자들을 그럴듯하게 속이기 위하여 한글로 작성된 메일 내 첨부파일이나 링크를 통하여 클릭을 유도할 것으로 보인다. 또한 국내 유명 메신저의 경우 계정을 탈취하는 사례가 발생했었기 때문에, 탈취된 계정이 메신저의 로그온뿐만 아니라 관련 SNS까지 동일하게 악용 된다면, 유출된 개인정보를 통해 악의적인 스팸, 광고성 댓글 및 방명록 작성은 물론이고 메신저에 등록된 리스트들을 목표로 하는 실제 사기사건과 같은 피해가 발생할 가능성이 매우 높다.

가상 재산 및 정보를 노리는 악성코드

온라인 뱅킹과 온라인 게임 그리고 SNS 를 통하여 사이버 세상에는 자신이 만들어 놓은 무형의 자산과 정보들이 산재해 있다. 이러한 무형의 자산 중 일부는 현금화 될 수 있기 때문에 온라인 게임의 사용자 계정을 탈취하는 악성코드가 계속 기승을 부릴 것으로 보고 있다. 나아가 단지 온라인 게임 내에 국한 되지 않고 SNS를 이용한 자산 정보와 무형의 지적 가치들도 훼손 될 가능성이 높다. 따라서 이것을 안전하게 보호하는 서비스 또는 새로운 형태의 제품이 나올 가능성이 높다.

취약점, 취약점, 취약점

올해 문서파일(MS 오피스 문서와 PDF 취약점, HWP 취약점)에 대한 취약점이 극심할 정도로 위협이 되었다. 여기에 플래쉬 파일 취약점도 한몫 거들어 웹 상에서 쉽게 표현되는 이미지 파일에 대한 취약점도 큰 이슈가 되었다. 과거와 달리 윈도우 OS 자체를 공격하는 취약점은 그다지 큰 효과를 발휘 하지 못한다. 그 만큼 윈도우 자체를 공격하는 것이 어려워지고

있다. 그러나 문서파일과 플래쉬 파일 그리고 이미지 파일에 대한 취약점으로 인한 피해가 극심하였던 만큼 향후에도 웹 브라우저 관련 취약점과 문서 및 이미지 파일에 대한 취약점은 끊임없이 보고되고, 이로 인한 피해가 발생할 것으로 예상된다. 그러한 이유는 이러한 파일들이 스피어 피싱 및 스팸성 사기메일에 적절히 이용 되고 있기 때문이다. 한편 응용 프로그램들에 대한 취약점들도 꾸준히 보고될 가능성이 높지만 사용자 수를 많이 확보 하지 못한 응용 프로그램의 취약점이라면 그다지 효과적인 공격 목적으로 사용되기는 어렵다고 전망된다.

포터블 및 이종기기에 대한 공격과 악성코드 출현은 보합 or 진보

아이폰과 오픈 플랫폼 스마트폰인 구글폰의 경우 컨버전스 기기들의 복잡성으로 인한 취약점이나 이를 비정상적으로 사용하는 해킹 등이 선보이고 있다. 구글폰의 경우 아직 국내 시판 되고 있지 않지만 여기에 사용되는 오픈 플랫폼 자체가 보안에 취약 할 수가 있다. 아이폰의 경우 이미 다양한 해킹방법을 통하여 점점 기기 내부에 접근하고 있으며 아이폰용 프로그램을 제작할 수 있는 SDK가 배포 되고 있기 때문에 악성코드도 얼마든지 제작할 수 있는 단계에 와 있다고 볼 수 있다. 스마트폰에 사용된 대표적 OS인 심비안의 경우 지금은 인증제도를 도입하여 심비안의 인증을 받은 응용 프로그램만 사용하도록 하여 급증하던 심비안용 악성코드를 주춤하게 만들었다. 기기의 복잡성과 컨버전스 그리고 오픈 플랫폼 등이 점점 해킹과 취약점이 존재할 수 있는 가능성을 열어두고 있기 때문에 시간이 문제일 뿐 악성코드 출현의 길은 이미 열려있다.

(2) 악성코드 연간 동향

올 해 한국의 악성코드 동향은 중국 발 해킹과 악성코드로 인한 피해가 극심하고 국지적인 특성이 매우 뚜렷하였다. 이러한 특징은 중국산 악성코드가 국내 유입되어 피해를 입히고 있는 지난 3~4년 동안 비슷한 양상을 보이고 있고, 앞으로도 계속될 것으로 전망된다.

대부분의 악성코드가 그 대상을 일반적인 엔드포인트(개인 PC)에 집중하고 있고, 무엇보다도 취약점 및 악성코드 제작도구 그리고 배포 자동화로 인하여 악성코드들 변형 제작에 소요되는 시간은 점점 짧아지고 있고, 이에 따라 악성코드의 수가 폭발적으로 증가하고 있다.

악성코드피해 TOP 20

2007 년		
순위	악성코드 명	건수
1	Win-Trojan/Xema.variant	1448
2	Win32/Virut	351
3	Win32/IRCBot.worm.variant	341
4	Dropper/QQPass.23599.B	298
5	Dropper/QQPass.23599.D	293
6	Dropper/OnlineGameHack.23087	272
7	Win-Trojan/KorGameHack.17920.BR	272
8	Win-Trojan/KorGameHack.26624.AI	267
9	Win-Trojan/KorGameHack.14848.FO	195
10	Win-Trojan/KorGameHack.6430	149
11	Win-Trojan/Downloader.38400.I	141
12	Dropper/OnlineGameHack.15988	130
13	Win-Trojan/OnlineGameHack.15360.I	120
14	Win-Trojan/Downloader.169984.D	116
15	Win-Trojan/KorGameHack.19456.BM	113
16	Win-Trojan/KorGameHack.7295	102
17	Win-Trojan/KorGameHack.43072	96
18	Dropper/OnlineGameHack.29743	95
19	Win-Trojan/KorGameHack.12800.EI	88
20	Win-Trojan/KorGameHack.15064	88

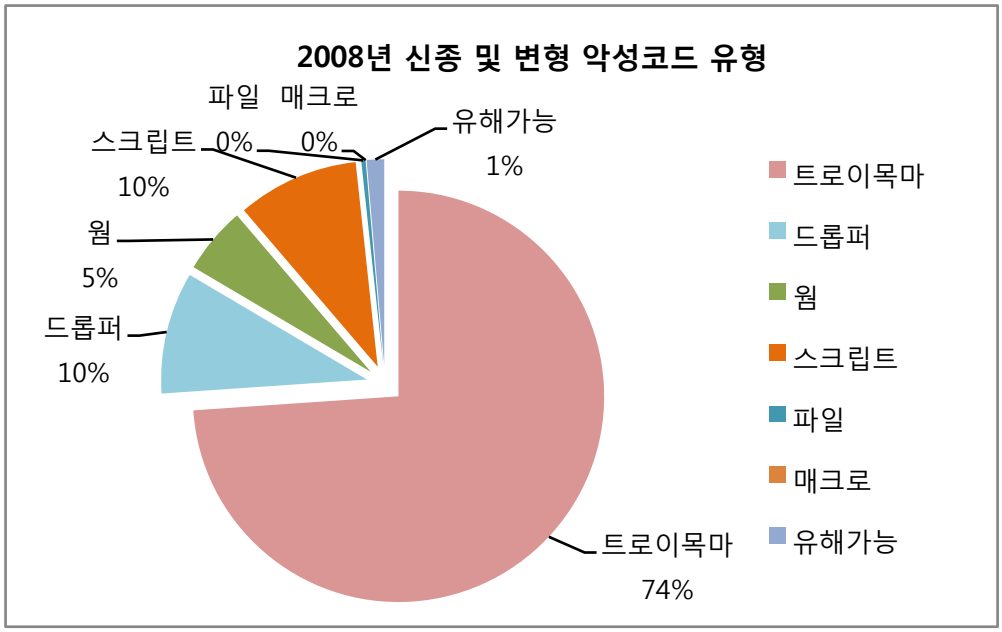
2008 년		
순위	악성코드 명	건수
1	Dropper/OnlineGameHack.20100	310
2	Win-Trojan/Downloader.16384.FS	267
3	Win-Trojan/Agent.60416.Z	221
4	Win-Trojan/Noupdate.36864	199
5	Dropper/OnLineGameHack.17143	183
6	Dropper/OnLineGameHack.17412	179
7	Dropper/OnLineGameHack.17799	178
8	Win-Trojan/KorGameHack.16121.D	169
9	Win-Trojan/OnlineGameHack.19208	159
10	Win32/IRCBot.worm.variant	153
11	Win-Trojan/OnlineGameHack.18768.B	150
12	Dropper/OnlineGameHack.17632	148
13	Win-Trojan/OnlineGameHack.19938	132
14	Dropper/OnLineGameHack.16767	129
15	Win-Trojan/KorGameHack.16972	113
16	Win-Trojan/OnlineGameHack.34304.P	104
17	Win-Trojan/Downloader.27136.BH	103
18	Dropper/OnLineGameHack.16531	103
19	Win-Trojan/KorGameHack.19589	97
20	Win-Trojan/Hidd.43008	94

[표 2-2] 2007/2008 피해 악성코드 Top 20

2005년 2006년의 TOP 20의 대부분을 웜이 차지하였던 것과는 전혀 다르게 게임핵을 비롯하여 트로이목마 류가 2007, 2008년의 TOP 20의 대부분을 차지하였다. 다만 2008년은 2007년과는 또 다르게 Win32/Virut 바이러스에 대한 피해신고건수가 TOP 20에서 제외되었다는 차이가 있으는데, 이는 백신업체들의 Virut 바이러스 치료기능 강화와 전용백신 제공 등이 Virut 바이러스의 피해신고가 감소하는데 큰 영향을 미친 것으로 보인다. 그리고 2007년과 마찬가지로 2008년도 TOP 20의 순위권에 랭크된 대부분의 악성코드 유형이 온라인게임핵이이고, 4위에 랭크된 Win-Trojan/Noupdate.36864는 특정 백신제품의 웹 페이지가 인터넷 익스플로러에 의해서 오픈 되었을 때 이를 종료하게 하는 증상을 갖는 악성코드로 2008년 3월을 기점으로 매우 많은 피해신고가 접수되었었다.

악성코드 유형에 따른 분석

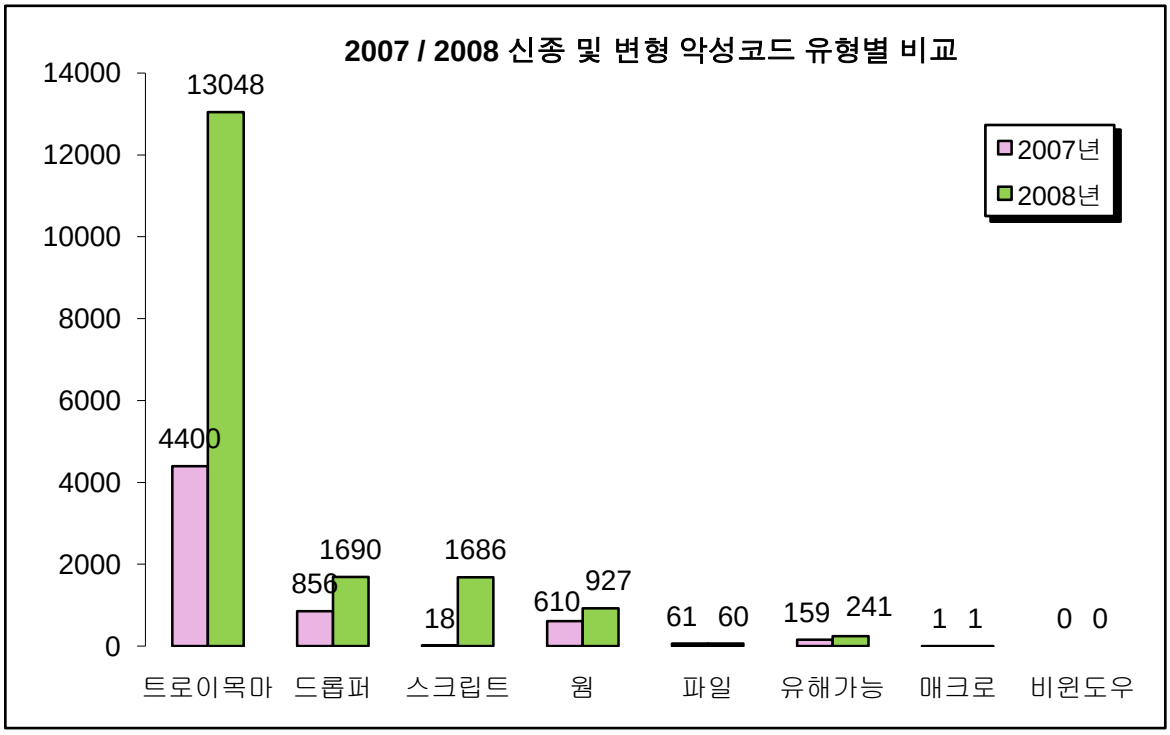
다음은 안철수연구소가 2008년 엔진에 반영한 악성코드 유형에 대한 분포이다.



[그림 2-1] 2008년 신종 및 변형 악성코드 유형

2008년 악성코드는 전년대비 폭발적으로 증가하였다. 매년 증가하는 추세인데 올해는 작년대비 3배 가까이 증가하였다. 특히 웹 사이트 로그인 계정 정보나 시스템 정보와 같은 사용자들의 정보를 훔쳐내는 유형과 다운로더, Agent 등과 같은 트로이목마 유형의 악성코드가 전체 악성코드의 74%를 차지할 만큼 많았으며, 그 피해 또한 매우 심각하였다. 특히 악성코드가 지속적으로 엔드포인트단을 공격하고, 감염에 의해서 확보된 시스템들을 네트워크로 묶고 이를 조정하여 하나의 거대한 봇넷을 구성하여 스팸과 DDoS 공격에 지속적으로 사용하고 있는 현상은 이전과 동일하게 계속되고 있다.

다음 [그림 2-2]는 2007, 2008년 악성코드를 유형별로 분류를 한 것이다.



[그림 2-2] 2007, 2008년 신종 및 변형 악성코드 유형별 비교

중국 발 악성코드 영향으로 웹 애플리케이션에 대한 공격이 거세지고 그에 따른 여파로 트로이목마, 드롭퍼, 스크립트 유형의 악성코드들이 작년과 다르게 많은 수가 보고가 되었다.

2008년 말쯤에 국외의 악의적인 유명 호스팅 업체의 서비스가 중지 되면서 스팸 메일이 일시적으로 줄었다는 보고가 있었는데, 이처럼 악성코드에 감염된 엔드포인트뿐만 아니라 악의적인 호스팅 업체들이 앞다투어 검은 돈을 얻기 위해서 사이버 범죄와 밀착되고 있다. 이와 맞물려 악성코드 고도화 역시 지속적으로 발전하고 있다.

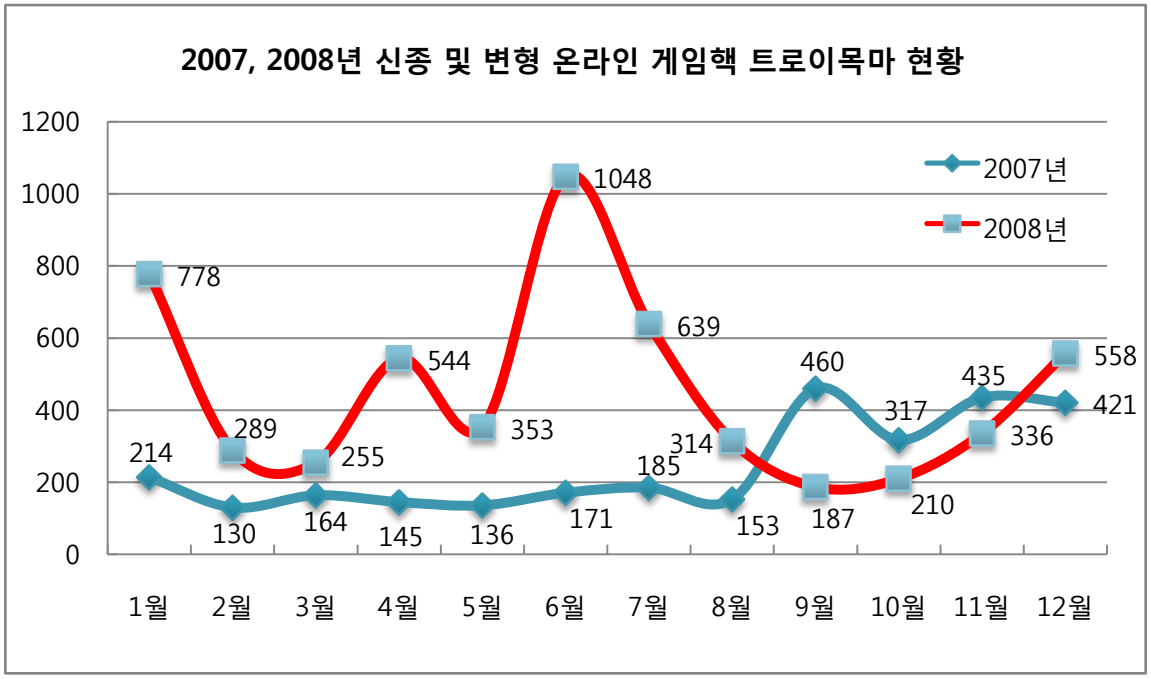
올해 초 파일이나 레지스트리에는 자신의 흔적을 남기지 않으며, 과거 부트 바이러스처럼, 물리적인 디스크 영역에 자신의 코드를 숨겨놓고 동작하는 MBR Rootkit이 PoC 형태가 아닌 인터넷상에서 처음 발견되기도 하였다. 취약점을 이용하는 악성코드 역시 더욱 기승을 부렸는데, 특히 대중적으로 많이 사용되는 PDF 문서파일 취약점과 플래쉬 파일 (SWF) 취약점을 이용한 악성코드가 폭발적으로 쏟아져 나왔다.

일반적으로 잘 알려진 오피스 문서류는 물론이고 윈도우 서버 서비스 취약점과 연말에 알려진 IE7 0-Day가 큰 피해를 가져오기도 하였다. 특히나 중국 및 러시아 등으로부터는 취약점

을 이용한 악성코드 제작 툴킷과 취약점 공격 툴킷 등이 이미 오래 전부터 제작, 판매 되고 있었으며, 이는 일반 사용자들에게도 호기심을 자극하여 사이버 범죄의 나락으로 이끌고 있다.

몇 년 전부터 한국을 강타하고 있는 중국발 웹 해킹 역시 위와 같은 취약점 등을 이용하여 끊임없는 공격이 시도되고 있으며, 많은 인터넷 사용자들이 지뢰밭이 되어 버린 국내 인터넷 환경에 조심해야 하는 상황이 되었다. 특히 ARP 스푸핑 공격을 포함하고 있는 악성코드로 인하여 많은 수의 기업 네트워크가 마비가 되기도 하였으며, 많은 악성코드 들이 특정 게임만을 노리는 것이 아니라 국내 대형 포털의 메일 계정 정보나 메신저 계정 정보 등을 타겟으로 하는 현상이 두드러졌다. 이와 같은 공격은 내년에는 더욱 더 기승을 부릴 것으로 예상된다.

다음 [그림 2-3]은 중국 발 악성코드의 영향으로 국내 발견 트로이목마 중 가장 많은 변형과 비율을 차지하는 온라인 게임의 사용자 계정을 훔쳐내는 악성코드를 전년도와 비교해 보았다.



[그림 2-3] 2007, 2008년 신종 및 변형 온라인 게임핵 트로이목마 발견 수

SWF 관련 취약점이 극심할 때인 6월에 해당 악성코드가 폭발적으로 증가하는 현상을 보였는데, 이는 취약점과 악성코드 유포가 밀착되어 있는 것을 여실히 보여주는 사례라고 할 수 있다.

한편 자기보호 고도화 악성코드는 2007년에 이미 충분히 예상을 한 형태였는데, 위에서 언

급한 MBR Rootkit을 비롯하여 일반적인 안티 루트킷 기술을 회피하는 형태가 2008년에 일부 악성코드에서 선 보였으나 비교적 쉽게 분석, 진단 기술을 개발 할 수 있었다. 그리고 은폐와 같은 자기 보호 이외 에도 코드 가상화, 난독화, 실행압축 등은 악성코드 제작에 꾸준히 사용 되었다.

다음은 2008년에 있었던 대표적인 악성코드 이슈들이다.

전통적인 바이러스의 피해발생 여전

취약점이 포함된 악의적인 스크립트 파일과 온라인 게임의 사용자 계정을 훔쳐내는 악성코드가 여전히 기승을 부리고 있는 가운데 실행 파일을 감염 시키는 전통적인 파일 감염 바이러스도 여전히 피해가 꾸준한 것으로 보인다. 특히 Win32/Kashu.B 바이러스는 꾸준히 변형이 발견되었는데, 메모리 치료가 선행되지 않으면 재감염되며, 시작 실행 시점 불명확 기법과 다형성 기법 등을 사용하여 진단과 치료가 매우 까다로웠다. 또한 바이러스는 아니지만 윈도우의 중요한 시스템 파일을 패치한 후 악의적인 모듈이 실행되도록 한 Win32/Liger 도 있었다. 이외에도 CIH 바이러스처럼 파일의 빈 공간에 자신을 기록하여 감염 후 파일 사이즈가 증가하지 않는 Win32/Huhk.C 도 발견, 보고 되었다.

봇넷(BotNet) 활동과 스피어피싱 및 스팸성 사기 메일의 증가

봇넷은 감염된 시스템에서 악의적인 일련의 행동을 수행하는 악성코드로 구성된 일련의 네트워크를 말한다. 이러한 봇넷들은 P2P 또는 HTTP, IRC 프로토콜을 이용하면서 감염된 시스템들을 제어한다. 다양한 변형을 가지고 있는 Win32/Zhelatin.worm 등에 감염된 경우 봇넷에 연결되어 악의적인 용도에 사용되었다. 또한 올 3분기 가장 기승을 부린 Win-Trojan/Fakeav(일명 antivirusxp2008)는 다양한 경로로 감염되는데, 일반적으로 외국의 유명 연예인을 사칭하는 스팸성 사기 메일을 통하여 주로 감염이 이루어졌다. 이처럼 봇넷의 활동력 증가로 인하여 악성코드를 설치를 통한 금전적인 이익을 얻으려는 형태가 일반화 되어가고 있다. 스피어 피싱은 조직 내 신뢰할 만한 대상인 것처럼 속여서 아이디와 비밀번호를 알아내도록 가짜 사이트로 유도하거나, 악성코드 설치를 목적으로 가짜 사이트의 방문을 유도 또는 취약점이 담긴 문서 파일을 보내어 실행을 요구하는 등의 일종의 피싱 공격이다.

국내 대형 포털 메일계정에 유포된 악성코드

올 초 국내 온라인 쇼핑몰에 대한 사용자 DB 유출 사건을 시작으로 국내 유명 포털의 메일 계정과 메신저 또는 쪽지함 등으로 악성코드가 포스팅 된 URL 또는 첨부파일이 포함된 메일이 대량 발견 되었다. 이렇게 국내 포털 사용자를 노린 악성코드는 이전까지 사례가 없었다. 특히 이들은 공공기관을 사칭하는 한글로 된 메일내용을 가지고 있기 때문에 사용자들이

더욱 더 첨부파일이나 URL을 클릭할 확률이 높았다. 또한 메신저의 경우 사용자의 계정을 훔쳐내도록 되어 있어서 훔쳐낸 계정이 다른 목적으로 사용될 위험성도 예상해 볼 수도 있었다. 이처럼 이제는 국내 사용자들만을 노리는 스피어 피싱 성격의 메일과 악성코드의 기승이 활발해지지 않을까 예상 된다.

올림픽과 중국 내 사회적인 이슈를 다룬 악성코드

티벳 독립시위 관련하여 이를 지지하거나 또한 중국의 무력진압에 반대하는 등의 내용을 다룬 악성코드가 종종 발견되었다. 또한 북경 올림픽도 악성코드 제작자들의 중요한 소재거리였다. 이러한 성향은 핵티비즘과는 다르고 단지 사회공학적 기법을 이용하여 악성코드를 설치 후 제작자들의 소기의 이익을 달성하는데 그 목적이 있다.

중국 발 SWF 취약점과 ARP 스푸핑

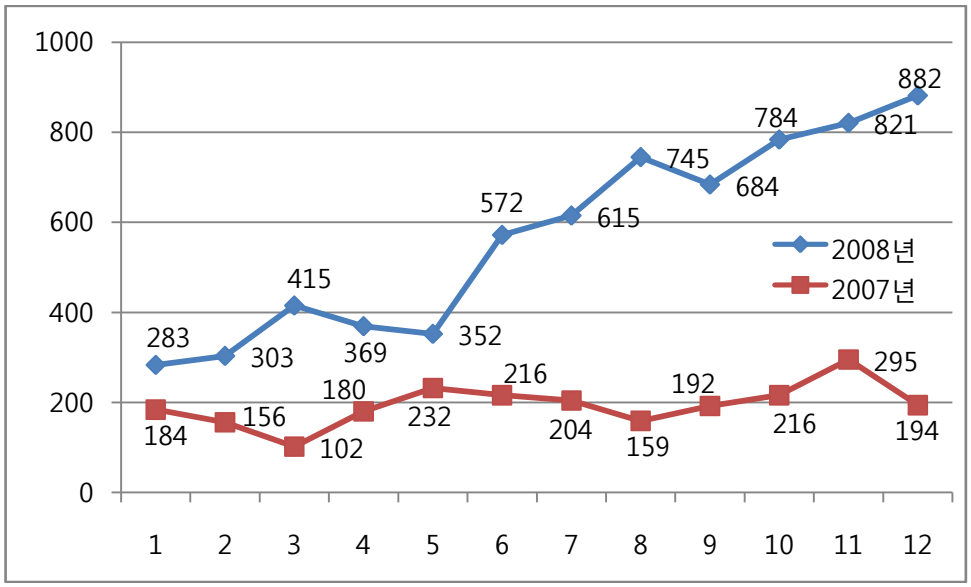
올 상반기에 있었던 SWF 취약점과 ARP 스푸핑 공격은 과거 중국 발 웹 해킹에 의한 악성코드 전파의 새로운 패러다임을 제공하였다. 즉, 수동적인 웹 접속으로는 감염대상을 많이 확보할 수는 없지만 ARP 스푸핑 공격으로 인한 인트라넷의 모든 시스템을 공격 대상으로 삼았다. 나아가 SWF 취약점은 대표적인 어플리케이션 취약점이라 할 수 있고 웹과 밀접한 관련이 있어 그 피해는 극심하였다. 무엇보다도 이러한 어플리케이션 취약점과 ARP 스푸핑 공격 그리고 자동화로 인한 공격도구 및 악성코드 대량양산은 더욱 더 많은 이들을 사이버 범죄자로 만들고 있다. 또한 불 보듯 뻔한 이러한 현실을 제대로 인지하지 못하고 강 건너 불구경 하는 보안 불감증에 걸린 관리자 및 사용자들에게는 크리스마스의 악몽과 같은 현실로 다가올 것으로 예상 되므로 부단한 주의가 필요하다.

대중적인 애플리케이션의 취약점들

PDF 관련 취약점, SWF 파일 취약점, 윈도우 서버 서비스 취약점, IE 0-Day 등은 올 한 해를 흔들어 놓았던 대표적인 취약점이다. 특히 해당 취약점은 많은 사용자들이 쉽게 접할 수 있었기 때문에 그 피해가 더욱 컸다. 또한 중국 발 악성코드와 맞물려 수 많은 웹 페이지가 공격 당했으며, 이로 인한 악성코드의 수는 올 6월 폭발적으로 증가하기도 하였다.

(3) 스파이웨어 연간 동향

2008년 신종 및 변형 스파이웨어 발견 현황



[그림 2-4] 2007년, 2008년 신종 및 변형 스파이웨어 증감 비교

2008년 신종 및 변형 스파이웨어 발견 현황에서 가장 주목할 점은 양적인 증가이다. 2008년에는 애드웨어, 스파이웨어가 안티-스파이웨어, 안티-바이러스와 같은 보안 프로그램의 탐지를 피하기 위한 다양한 방법을 동원하였으며, 2008년 초기에는 주로 탐지 회피를 위한 루트킷(Rootkit)을 사용하였고, 루트킷과 함께 2008년 중순부터는 보안프로그램의 탐지를 회피하기 위한 방법으로 변형을 양산하기 시작하였다. 대표적으로 스파이웨어 즐롭(Win-Spyware/Zlob), 스파이웨어 크립터(Win-Spyware/Crypter) 그리고 안티바이러스XP(Win-Adware/Rogue.AntiVirusXP2008)등이 다양한 변형으로 많은 피해를 입혔다.

신종 및 변형 스파이웨어 발견 건수가 2008년에 급격히 증가한 반면, 스파이웨어로 인한 피해 동향은 2007년과 비슷한 양상을 보였다. 신종 및 변형 발견 건수는 증가하였으나 이들 변형 스파이웨어에 대한 모니터링과 제너릭 진단법의 개발로 피해가 확산되지 않은 것으로 풀이된다.

2007년과 2008년 피해 동향이 수치상으로는 비슷하지만 구체적인 피해 내용은 차이가 있다. 2007년 하반기부터 많은 피해를 입힌 국내제작 애드웨어 및 다운로더는 2007년 개정된 정부의 스파이웨어 기준과 2008년 초 경찰의 대대적인 수사로 2008년 상반기에는 크게 줄어들었다. 그러나 2008년 중반부터 스팸메일과 성인사이트를 중심으로 확산되는 스파이웨어 즐롭 변형의 양산으로 현재까지 많은 피해를 입히고 있다. 2007년과 비교하여 중국에서 제작된 온라인게임계정유출 목적의 스파이웨어는 2008년 들어 피해가 다소 감소하였다.

스파이웨어로 인한 주요 이슈를 월별로 정리하면 아래 [표 2-3]과 같다.

	주요 이슈
1월	국내 제작 스파이웨어 피해 급증
2월	스파이웨어 즐롭 변형 배포 시작
3월	국내제작 스파이웨어에 루트킷(Rootkit) 드라이버 사용 증가
4월	해외 제작 허위 안티-스파이웨어(가짜백신) 피해가 증가하기 시작
5월	스팸메일, 성인사이트 중심으로 스파이웨어 즐롭 확산 시작
6월	허위 안티-스파이웨어, 스파이웨어 즐롭 등 다수의 변형 배포
7월	가짜백신 안티바이러스XP2008(Win-Adware/Rogue.AntiVirusXP2008) 피해 증가
8월	가짜백신 변형 피해 증가
9월	불법 인터넷 도박사이트 방문을 유도하는 애드웨어 증가
10월	스팸메일러 피해 증가, 가짜백신(Fakeav) 전용백신 배포
11월	가짜백신 피해 감소
12월	국내제작 애드웨어 배포 방식의 변화

[표 2-3] 2008년 월별 스파이웨어 주요 이슈

국내 허위 안티-스파이웨어 제작자 적발과 국내제작 스파이웨어 감소

2005년경 등장하기 시작한 국내제작 스파이웨어는 2008년 초까지 많은 사용자에게 직, 간접적인 피해를 입혔으며, 특히 허위 안티-스파이웨어 프로그램은 게시판이나 블로그 등의 불특정 웹사이트에서 ActiveX 방식으로 사용자 동의 없이 설치되어, 허위 과장된 검사 결과를 보여주거나, 정상 파일을 진단하여 사용자를 속이는 방법으로 금전적인 피해를 입히기도 하였다. 2007년 12월 정부에서 발표한 강화된 “스파이웨어 기준”과 2008년 상반기 경찰의 대대적인 수사로 국내 허위 안티-스파이웨어 프로그램 제작자가 서울경찰청 사이버 수사대에 무더기로 검거되는 사건이 있었다. 이러한 영향으로 국내제작 스파이웨어의 발견과 피해가 2008년 들어 전년도에 비하여 감소하는 양상을 보였다. 하지만 설치과정에서 사용자 동의를 받는 적립금제공(리워드) 형태의 애드웨어는 현재도 많은 피해를 입히고 있으며 이들은 주로 무료 게임, 무료 소프트웨어 설치과정에서 번들 형태로 설치된다. 비록 형식상 사용자 동의[1]를 받는다고 하나 소프트웨어 사용 약관이 허술하거나 사용자에게 불합리한 부분이 있어 주의해야 한다. 향후 이런 방식으로 설치되는 스파이웨어는 더욱 증가할 것으로 예상되지만, 허술한 제도와 규정으로 인하여 이러한 유형의 스파이웨어를 진단하기 어려운 상황이기 때문에 사용자들의 많은 피해가 예상된다.

[1] ASEC report 2008년 11월호 컬럼 참조

스파이웨어의 악성화

국내제작 스파이웨어가 2008년 들어 감소한 반면 악성화 되는 경향이 뚜렷하였다. 2008년 1월에 발견된 스파이웨어 하이드 프록(Win-Spyware/HideProc)은 악성 다운로더의 프로세스를 숨기는 기능을 수행하여 많은 피해를 입혔으며, 스파이웨어의 삭제를 방해하는 루트킷(Rootkit) 드라이버를 설치하는 스파이웨어가 많이 발견되었다. 이 외에도 다운로더 Kwsearch(Win-Downloader/Kwsearch)는 EXECryptor와 같은 프로텍터로 실행압축하여 분석도구 실행을 방해하고 역분석(Reverse-Engineering)을 어렵게 하는 등의 특징이 있으며, 2008년 12월 까지도 꾸준한 피해를 입히고 있다.

스파이웨어 Zlob 변형의 확산, 외산 스파이웨어의 증가

해외에서 제작된 스파이웨어가 증가하여 많은 피해를 입혔다. 이러한 스파이웨어들은 성인사이트, 스팸메일을 통해 국내에 유입되어 많은 피해를 입혔다. 스파이웨어 즐롭(Win-Spyware/Zlob)의 경우 성인사이트나 선정적인 이미지가 포함된 스팸메일을 이용하여 가짜 동영상 코덱 설치를 유도한다. 이 외에도 상용 프로그램의 크랙 또는 키젠(Keygen) 프로그램으로 위장하여 설치되거나, 응용프로그램의 취약점을 이용하여 설치되기도 한다. 즐롭에 감염되면 클리커 훼이크얼럿(Win-Clicker/FakeAlert), 스파이웨어 크립터(Win-Spyware/Crypter) 등이 2차 감염될 수 있으며 허위 안티-스파이웨어 프로그램을 설치하고 스팸메일을 대량 발송하여 또 다른 사용자에게 피해를 입힐 수도 있다.

AntiVirusXP 2008, 훼이크AV

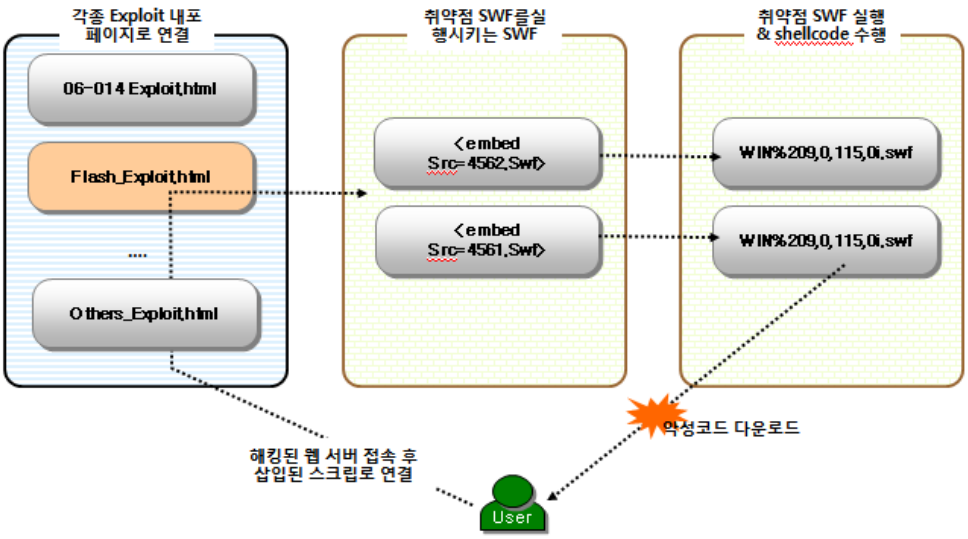
가짜백신(허위 안티-스파이웨어 프로그램) AntiVirusXP2008(Win-Adware/Rogue.AntiVirusXP2008, Win-Trojan/Fakeav)은 2008년에 발견된 가장 많은 피해를 입힌 허위 안티-스파이웨어 프로그램이다. AntiVirusXP2008에 감염되면 바탕화면이 허위 경고 메시지가 포함된 이미지로 변경되며, AntiVirusXP2008과 함께 설치된 블루스크린을 흉내낸 화면보호기로 인하여 사용자는 시스템에 오류가 있는 것으로 착각하기 쉽다. 이와 함께 디스플레이 설정을 변경하여 사용자가 바탕화면과 화면보호기를 변경할 수 없도록 한다. AntiVirusXP2008은 변형이 다양하며 랜덤한 경로명을 사용하여 설치하기 때문에 안티-바이러스 프로그램과 같은 보안 프로그램에서 진단이 어려운 특징이 있으며, 제거한 경우에도 다른 악성코드에 의해 재감염되는 경우가 많았다. AntiVirusXP2008 이외에도 스파이웨어 즐롭이나 클리커 훼이크얼럿에 의해 감염되는 다른 여러 허위 안티-스파이웨어 프로그램이 발견되어 많은 피해를 입혔다.

(4) 시큐리티 연간 동향

2008년에는 MS에서 발표한 보안 패치가 전년도에 비하여 13%가량 늘어난 78건이 발표되었다. 또한 MS 취약점뿐만 아니라 대중적인 3rd party 어플리케이션의 취약점이 다수 발견되어 공격에 악용되었다.

대중성이 높은 특정 애플리케이션 취약점을 악용하는 공격 사례 증가

올해 다수의 윈도우 시스템 관련 취약점이 발표 되었음에도 불구하고 대중적으로 사용되는 특정 애플리케이션의 취약점이 공격 대상으로 집중되는 현상을 보이고 있다. 이에 해당하는 가장 대표적인 사례가 Adobe Flash Player DefineSceneAndFrameLabelData 취약점을 이용하는 중국발 공격이다. 해당 Adobe Flash Player 취약점은 Scene와 Frame 레이블 정보를 담고 있는 DefineSceneAndFrameLabelData TAG 중 SceneCount 값에 대한 올바르지 못한 유효성 검사로 인하여 발생하였으며, 아래 [그림 2-5]와 같은 시나리오로 악성코드를 유포하는 공격이 발생하였다.



[그림 2-5] SWF 파일을 이용하는 공격 시나리오

11월에는 인터넷 익스플로러의 시작 페이지가 “www.3929.cn”으로 고정되며, 각종 광고 삽입, 툴바 설치, 팝업광고 노출 등의 피해사례를 호소하는 고객들의 신고가 급증하기 시작하였다. 해당 피해의 원인은 상반기에 발표되어 많은 피해 사례를 입혔던 Adobe 플래쉬 플레이어(SWF) 취약점을 이용하여 배포된 악성코드로 밝혀졌다. 해당 취약점은 이미 제품벤더에 의해서 문제를 해결하는 보안 패치가 발표되었음에도 불구하고, 다수의 사용자들이 해당 보안 패치를 적용하지 않았기 때문에 발생하였다.

플래쉬 파일을 사용하는 웹 서버가 증가하면서 대부분의 사용자 시스템에 플래쉬 플레이어가 설치되어 있는 환경에서 웹 공격과 연계하여 손쉽게 공격이 성공을 거두고 있다. 또한, 최근 이슈가 되고 있는 ARP 스푸핑 악성코드를 flash 파일을 이용해서 다운로드 하는 사례도 보고되고 있다.

진화와 다양성으로 지속력을 잃지 않는 웹 사이트 공격

올 초부터 시작된 대량 중국발 웹사이트 공격이 지속되고 있다. 대표적인 구글 검색 엔진을 통해 공격대상을 수집하고, 취약한 웹 서버와 연계된 데이터베이스의 모든 테이블에 공격자가 원하는 악의적인 스크립트를 삽입할 수 있도록 설계된 자동 SQL Injection 툴을 통해 이루어진 대량의 SQL Injection 방식을 비롯하여, 뒤이어 발표된 Adobe 플래쉬 플레이어(Flash Player) DefineSceneAndFrameLabelData 취약점은 최근까지도 웹 사이트에 삽입되는 주요 공격 방식으로 애용되고 있다. 또한, MS-Access 스냅샷 뷰어(Snapshot Viewer) 취약점[1]은 지난 7월말 처음 공격 Exploit 공개되었고, 10여 일이 지난 다음달 8월 MS 정기 보안업데이트를 통해 패치가 공개되었다. 취약점이 공개된 직후 바로 해당 Exploit을 이용한 웹 침해 사례가 실제로 발견될 정도로 새로운 취약점을 통한 웹 공격 방식의 적용이 매우 빠르다는 점을 짐작할 수 있다. 최근에는 악의적인 PDF 파일을 자동으로 생성해 주는 툴킷(Tool Kit)도 개발되어, 악의적인 PDF 파일이 삽입된 침해 사이트의 수가 크게 증가한 것으로 추정된다.

다시 발견된 마이크로소프트 서버 서비스 취약점으로 인한 피해 확산

지난 10월에는 마이크로소프트사로부터 이례적인 긴급 보안업데이트(Out-of-Band)가 발표되었다. 이는 MS06-040 취약점[2] 이후, RPC 기반 네트워크를 통한 파일 인쇄 지원 및 명명된 파이프 공유를 제공하는 서버 서비스에서 또 다시 치명적인 제로데이(0-day) 취약점인 MS08-067 서버 서비스 취약점[3]이 발견되었기 때문이다. 해당 취약점은 서버 서비스에서 사용하는 NetprPathCanonicalize 함수에 전달된 조작된 파라미터를 파싱하는 과정에서 발생하는 버퍼 오버플로우 취약점이다. MS08-067 취약점은 기본적으로 TCP 139/445 포트 상의 악의적인 메시지 전달을 통해서 공격을 수행하기 때문에 디폴트 방화벽 설정 및 패치를 적용하는 방법으로 그 내포된 위험성에 비해 확산 가능성을 낮출 수 있을 것으로 예상하였다. 그러나, 해당 취약점으로 인한 국내/외 피해고객 신고가 증가하고 네트워크 모니터링 시스템을 통해 탐지되는 공격 네트워크 트래픽량이 급증하는 등 빠르게 피해가 확산되기 시작하였다. 또한, 웹 상에서는 중국에서 제작된 다수의 자동화된 MS08-067 취약점 자동 제작 툴들이 공유되기도 하였다. 악의적인 공격 메시지에 포함된 다양한

[1] http://www.microsoft.com/technet/security/Bulletin/MS08-041.mspx
[2] http://www.microsoft.com/korea/technet/security/Bulletin/ms06-040.mspx
[3] http://www.microsoft.com/korea/technet/security/Bulletin/ms08-067.mspx

쉘코드(ShellCode)를 통해서 각종 트로이목마 및 또 다른 취약한 시스템을 공격하기 위한 악성코드[1] 등이 다운로드 되어 시스템에 피해를 가하게 된다.

IE7 제로데이(0-day) 취약점

IE7 제로데이 취약점은 DATASRC 속성을 갖는 HTML 태그 처리를 담당하는 함수인 mshtml!CXfer::TransferFromSrc에서 발생하는 메모리 오류 취약점으로, Windows XP, Windows 2003 Server, Windows Vista 등의 다양한 운영체제에서 인터넷 익스플로러 7 버전을 사용하는 사용자에게 영향을 줄 수 있는 것으로 밝혀졌다. 이미 해당 취약점은 공개되기 이전부터 자동화된 툴을 통해서 조용히 확산되기 시작한 것으로 알려졌고, 다양한 취약점 공격코드(PoC)가 공개된 이후에도 한동안 마이크로소프트사로부터 업데이트가 발표되지 않았기 때문에 집계되지 않은 피해사례는 엄청날 것으로 예상된다. 알려진 공격 코드는 기존의 웹 취약점 공격 기술과 동일하게 쉘코드를 내장한 힙 스프레이(Heap Spray) 기술을 취약점에 결합하는 방식으로 이루어졌고, 쉘코드 실행 시 각종 게임핵을 포함하여 다양한 악성코드들을 다운로드 받아 실행한다. 보안 업체들은 마이크로소프트사로부터의 보안 업데이트가 발표되기 전까지 취약점 공격 스크립트 진단 및 악의적인 배포지 URL들을 차단하는 방식으로 발 빠르게 대응하였고, 12월 셋째 주에 MS사에서 긴급보안업데이트(Out-of-Band)가 제공되었다.

DNS 캐쉬 포이즌 공격

우리는 과거 1.25 대란을 겪으면서 DNS 서버의 기능이 현재의 인터넷 환경에 얼마나 큰 영향을 미쳤는지 확실히 경험한 바있다. 지난 2008년 7월 어쩌면 1.25 대란과 견줄 수 있을 정도의 확산 위협을 내포한 DNS 캐쉬 포이즌(DNS Cache Poisoning) 취약점이 발표되었고 뒤를 이어 이를 이용한 실제 공격 Exploit 코드들이 다수 공개되었다.

DNS 캐쉬 포이즌 공격은 공격자가 DNS 서버간의 통신 중간에서 올바른 DNS 응답 대신 잘못된 DNS 응답 메시지를 끼워 넣음으로써, DNS 서버의 캐쉬에 잘못된 정보를 삽입하는 공격이다. 한번의 공격 성공으로 인하여, 해당 서버로부터 DNS 정보를 획득하는 다수의 클라이언트 PC들이 잘못된 정보를 응답 받게 되고, 악의적인 사이트 유도를 통해서 개인정보 가로채기, 악성코드 및 거짓정보 유포 등의 다양한 악의적인 행위를 허용할 수 있었다.

실제로 지난 7월 29일 미국의 대형 ISP(Internet Service Provider)인 AT&T사의 DNS 서버가 공격을 받은 것으로 알려졌다. 이미 제품 벤더로부터 해당 취약점에 대한 패치 방안이 발표되었으나, 소스 포트와 Transaction ID가 유추 가능하다는 랜덤성(randomness) 문제는 여전히 해결되지 않은 문제로 남아있기 때문에, 도메인 정보에 대한 신뢰성 유지를 위해 지속적인 노력이 필요할 것이다.

---

[1] Win-Trojan/Gimmiv, Win32/Conficker.worm

무선 네크워크 해킹을 통한 인터넷 금융 사고 발생

최근 무선 AP 기능을 포함하는 유무선 공유기가 보급됨으로써 누구나 손쉽게 무선 네트워크를 구축하고 사용할 있게 되었으나 편리함에 앞서 과연 무선 네트워크이 얼마나 안전한가에 대한 고려도 잊지 말아야 할 것이다. 무선 네트워크에 대한 취약성은 지난 5월에 발생한 국내 은행이 잇따라 무선랜 해킹 사고를 당한 사례를 통해 잘 알 수 있다. 해당 사건의 주범들은 은행 외부 주차장에 차량을 이용하여 은행 내부에 설치된 무선 AP의 신호를 수집하여 획득된 정보를 통해 수차례에 걸친 내부 통신망 침투시도를 하는 과정에서 검거되었다. 무선은 물리적인 매체가 필요치 않아 신호가 수신되는 모든 곳이 해킹의 위험 지대라고 할 수 있다. 보안을 강화하기 위해 WEP, WPA, MAC 인증 등의 보안 기법을 적용시킬 수 있으나 MAC 인증 방식은 AP, 무선 랜카드 정보를 수집함으로써 손쉽게 우회 가능하며, WEP 방식 역시 WEP으로 암호화된 패킷을 다량으로 수집하면 사용된 KEY 값을 알아낼 수 있는 심각한 취약점이 존재한다. WEP 보다 안전하다는 WPA 방식 또한 알려진 공격 툴을 통해서 다량의 패킷 수집을 통하여 복호화가 가능한 취약점이 존재한다.

최근 무선 인터넷 활성화로 인하여 카페나 각종 공공 장소에 구축된 무선 AP나 주거 밀집지역에서 쉽게 발견할 수 있는 보안 기능이 없는 무선 공유기들은 공격자의 흔적을 감추기 위해 해킹의 경유지로 이용되기도 한다. 이 외에도 공개되거나 인증이 취약한 AP에 접속하여 해당 네트워크에 ARP 스푸핑 등의 기법을 이용하여 스팸이나 악성 코드를 유포는 사례도 있다.

따라서, 안전한 무선 네트워크 환경을 위해서는 강화된 암호화, 인증 기능을 설정하고 무엇보다도, 중요한 정보의 경우 되도록 유선 네트워크을 사용하는 것을 권장한다.

2008년 웹사이트 모니터링 동향

2008년 탐지된 침해지/유포지의 수는 2827/624로서 약 4.5개의 침해지가 한 개의 유포지로 연결되어 있음을 확인할 수 있다.

2008년의 웹을 이용한 악성코드의 배포 방법은 크게 두가지로 나눌 수 있다.

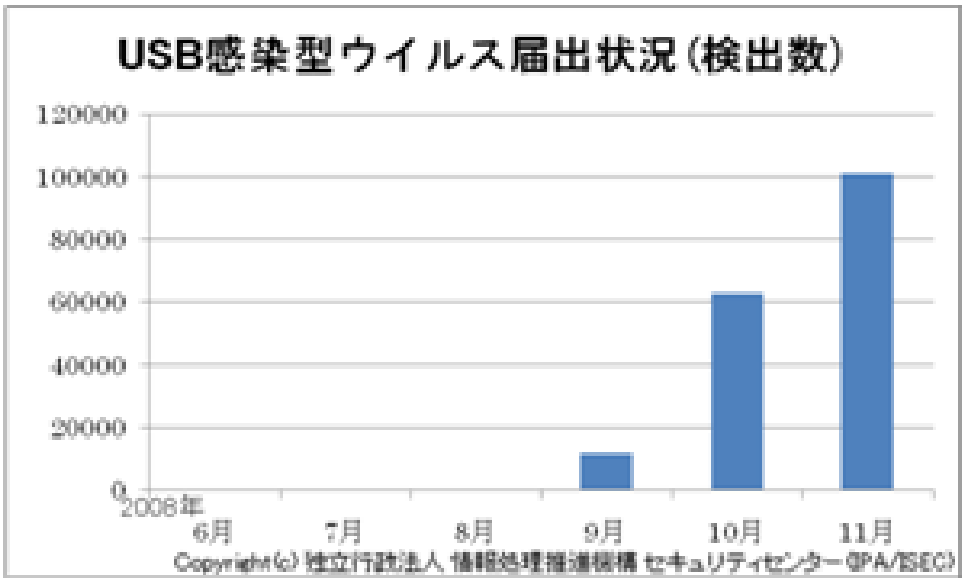
- 브라우저 취약점을 이용한 배포: 가장 최근에 문제가 되었던 MS08-078 취약점을 공격하는 코드가 이에 해당한다. 가장 영향력이 큰 취약점으로 발표가 되는 즉시 배포에 사용된다. 브라우저 내에 존재하는 취약점이기 때문에 특별한 제품을 사용하지 않아도 보안 패치가 적용되지 않은 제품을 사용하거나 Anti Virus 제품을 사용하지 않으면 악성 코드에 감염될 우려가 있다.

- 써드 파티 제품을 이용한 악성코드의 배포: ActiveX나 Flash 등의 취약점을 공격하는 코드가 이에 해당한다. ActiveX 제품의 경우 제품이 대중화된 정도에 따라 그 영향력이 달라진다. 예를 들어, Microsoft, yahoo, real media 등 대형 벤더의 경우, 취약점 공격코드가 취약점 발표 이후 배포되었을 뿐 아니라, 웹 공격코드 생성도구에도 사용되는 등 그 영향력이 매우 컸다. 특히, 플래시 취약점의 경우 국내 피해자가 동시다발적으로 생기기도 하였다.

(5) 일본 4분기 및 연간 악성코드 동향

일본 4분기 동향

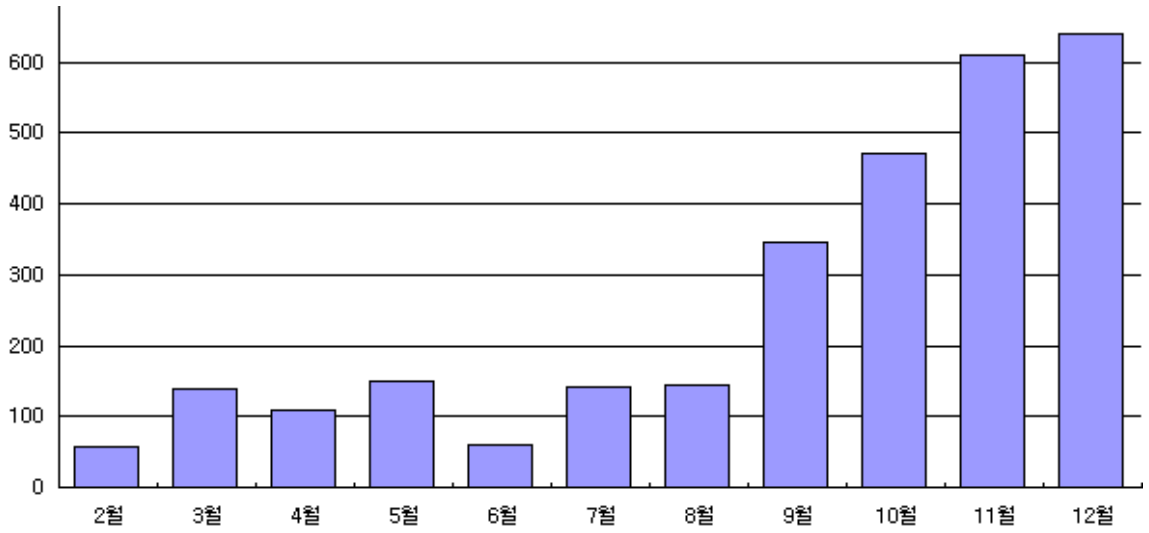
2008년 4분기 일본에서는 오토런(Win32/Autorun)류의 악성코드의 피해가 급증하였고, 윈도우 OS의 보안 취약점을 이용해서 전파되는 컨피커(Win32/Conficker.worm)웜의 피해가 다수 발견되었다.



[그림 2-6] USB 감염형 악성코드 검출 현황 (자료출처: 일본 IPA)

위의 [그림 2-6]은 일본 IPA(http://www.ipa.go.jp)에서 2008년 11월 발표한 악성코드 피해 현황보고서의 내용 중 USB로 전파되는 악성코드 탐지 현황을 보여준다. 9월 이후 USB를 이용한 악성코드의 탐지량이 급격하게 증가하고 있는 것을 알 수 있다.

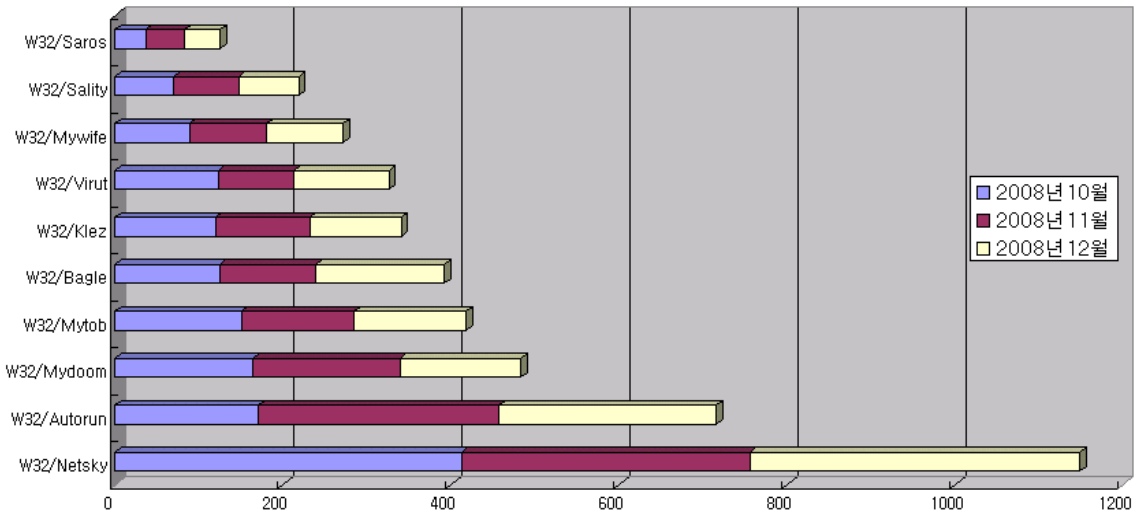
일본 트랜드마이크로사(http://www.trendmicro.co.jp)에서 발표한 악성코드 피해 보고서에서도 오토런 악성코드의 피해 증가 현황을 확인할 수 있다. 보고서에 의하면 2008년 3분기 악성코드 피해는 631건이었으나 4분기의 경우 1,722건으로 전 분기에 비해 세 배 가까이 증가한 것으로 나타났다. 아래의 [그림 2-7]는 매 월 보고된 오토런 악성코드의 피해 현황을 집계한 것으로 9월부터 피해가 급격하게 증가한 것을 알 수 있다.



[그림 2-7] 일본 트랜드마이크로사의 오토런 피해현황 보고

오토런 악성코드가 전 세계적으로 유행하기 시작한 것은 오래 전부터이지만 일본의 경우 올해 상반기까지 메일이나 웹 사이트상의 스크립트 등의 전파경로를 통한 감염 피해가 주로 발생했다. 그러나 최근 일본에서 피해가 급증하는 오토런 악성코드가 자체 전파 기능을 가지고 있는 것을 고려해 보았을 때, USB 메모리와 같은 이동식 저장매체를 통한 악성코드 전파가 일본에서도 보안을 위협하는 주요 요인이 되고 있는 것으로 보인다

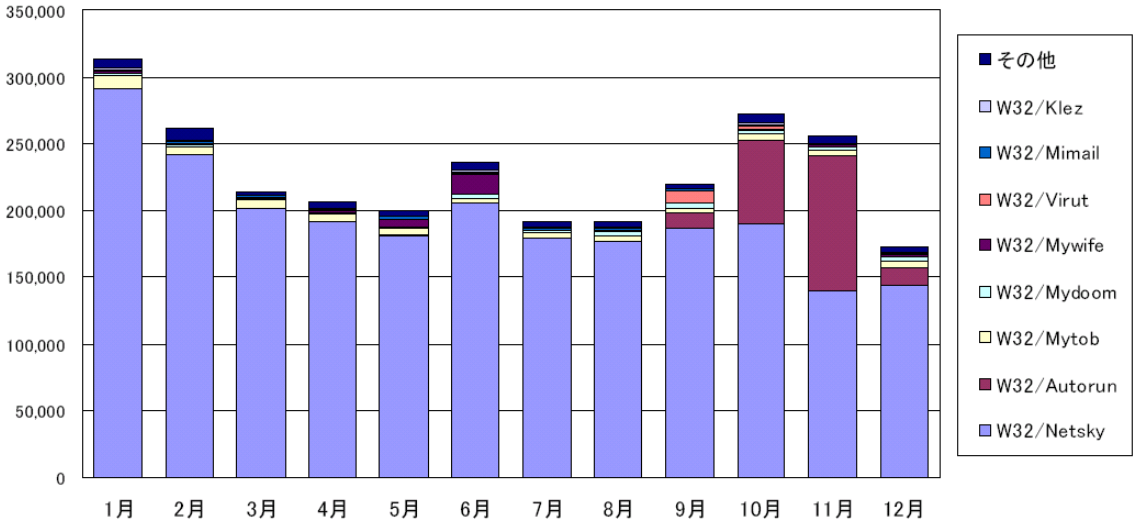
일본 IPA에서 발표한 악성코드 피해 통계에 의하면 2008년 4분기 일본에서 가장 많은 피해가 발생한 악성코드는 넷스카이(Win32/Netsky.worm) 웜이다. [그림2-8]은 4분기에 발생한 악성코드 피해 통계를 집계한 것이다. 넷스카이 웜의 감염 피해가 매우 높게 발생하고 있는 것을 알 수 있다.



[그림 2-8] 2008년 4분기 악성코드 피해 통계 (자료출처: 일본 IPA)

넷스카이 웜 이외에도 마이둠 웜(Win32/Mydoom.worm) 등 이메일 웜의 감염 피해가 여전히 많이 발생하고 있는 것을 알 수 있다. 그러나 오토런이나 바이럿(Win32/Virut) 등 메일이 아닌 다른 매체(전파 수단)를 이용한 악성코드의 피해가 증가하고 있고 이러한 추세는 앞으로도 계속될 것으로 보인다.

아래의 [그림 2-9]는 IPA에서 집계한 월별 악성코드 탐지 통계이다.



[그림 2-9] 악성코드 탐지 통계 (자료출처: 일본 IPA)

10월 이후 넷스카이 웜의 활동량이 많이 감소한 것을 볼 수 있다. 통계에서 주목해야 할 점은 오토런의 활동량이 급증한 것으로, 실제 고객에 미치는 피해가 증가하였을 뿐만 아니라 전파되는 개체 수 또한 매우 많은 것을 알 수 있다. 이러한 증가 현상이 이후로도 계속될 것인지 관심을 가지고 추이를 지켜볼 필요가 있다.

아래의 [표 2-4]는 일본 트랜드마이크로사에서 발표한 월별 악성코드 피해 통계이다. 오토런 악성코드의 감염 피해가 가장 많은 것을 알 수 있다.

2008 년 10 월		2008 년 11 월		2008 년 12 월	
악성코드명	피해량	악성코드명	피해량	악성코드명	피해량
MAL_OTORUN	471	MAL_OTORUN	611	MAL_OTORUN	640
BKDR_AGENT	78	MAL_HIFRM	89	WORM_DOWNAD	123
MAL_HIFRM	78	TROJ_GAMETHIEF	76	BKDR_AGENT	79
TROJ_DLOADER	56	TSPY_ONLINEG	67	MAL_HIFRM	68
TSPY_ONLINEG	52	JS_IFRAME	65	TSPY_ONLINEG	65
WORM_AUTORUN	46	BKDR_AGENT	64	JS_IFRAME	63

TROJ_VUNDO	43	WORM_DOWNAD	60	ADW_BJCFD	55
TROJ_FAKEAV	42	TROJ_VUNDO	55	TROJ_DROPPER	36
TROJ_GAMETHIEF	39	TROJ_DLOADER	44	TROJ_DLOADER	32
JS_IFRAME	25	WORM_AUTORUN	44	TROJ_GAMETHIEF	27

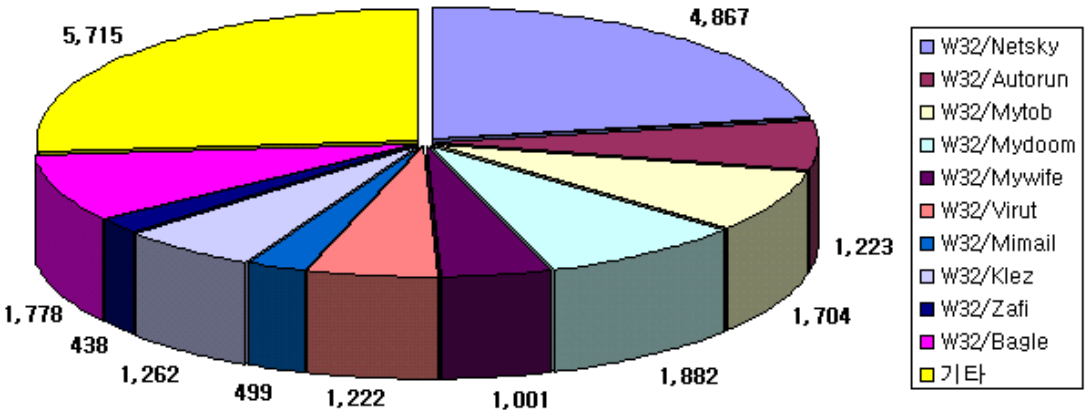
[표 2-4] 일본 트랜드마이크로 월별 감염 피해통계

위의 표에서 주목할 부분은 컨피커 웜(WORM_DOWNAD)의 피해가 10월 최초 발견된 이후 12월에 피해가 급증한 것이다. 컨피커 웜은 윈도우 OS의 MS08-067 보안 취약점을 이용하여 전파되는 악성코드로서 2008년 10월경 취약점이 발표된 이후 몇 가지 유형의 취약점을 이용한 악성코드가 발견되고 있다. 보안 패치를 하지 않은 시스템의 경우 원격에서 직접 감염시킬 수 있는 취약점의 특성을 고려했을 때 이러한 유형의 악성코드들에 의한 피해는 일본에서도 계속 증가할 것으로 보인다.

2008년 일본 악성코드 동향

2008년 일본 악성코드 동향에서 가장 이슈가 된 것은 오토런 악성코드의 피해가 급격하게 증가한 것이라고 할 수 있을 것이다. 오토런 악성코드는 올 한해 전 세계적으로 많이 유행한 악성코드이지만 일본의 경우 이러한 유형의 악성코드로 인한 피해가 미약한 편이었다. 그러나 하반기 이후 악성코드의 활동이 급격하게 증가하였고 이러한 상황은 내년에도 계속 될 전망이다.

아래의 [그림 2-10]에서 볼 수 있는 것처럼 전통적인 이메일 웜의 피해가 올 해도 지속적으로 발생한 것이 눈에 띈다. 한국을 비롯하여 대부분의 지역에서 이메일 웜으로 인한 피해가 거의 없는 상태이지만, 일본의 경우에는 점진적인 감소 추세를 보이고 있기는 하지만, 아직까지도 이로 인한 피해가 매우 많이 발생하고 있다.



[그림 2-10] 2008년 악성코드 피해 현황 (자료출처: IPA)

바이럿 바이러스의 피해가 지속적으로 발생하고 있다. 바이럿의 경우 주로 공유폴더나 P2P 프로그램을 이용한 파일 공유 등으로 인해 감염되는데, 악성코드 자체가 가지고 있는 전파 기능이 미약함에도 불구하고 많은 피해가 발생하고 있는 것으로 미루어보아 해당 악성코드로 인한 피해는 당분간 지속될 것으로 보인다.

온라인 게임 계정 탈취를 위한 악성코드의 피해가 지속적으로 발생한 것 또한 올 한해 동안 일본에서 이슈가 되었다. [표 2-5]는 일본 트랜드마이크로사에서 발표한 2008년도 인터넷 위협 리포트의 내용 중 악성코드 감염 피해현황 통계이다. TSPY_ONLINEG나 TROJ_LINEAGE와 같은 온라인 게임 계정을 탈취하기 위한 게임핵의 피해 건수가 작년에 비해 급격하게 늘어난 것을 알 수 있다.

순위	악성코드명	유형	피해건수	전년순위
1위	MAL_OTORUN	기타	2870	NEW
2위	BKDR_AGENT	백도어	818	1위
3위	JS_IFRAME	Java Script	596	NEW
4위	MAL_HIFRM	기타	456	NEW
5위	TROJ_GAMETHIEF	트로이목마	411	NEW
6위	TSPY_ONLINEG	트로이목마	333	권외
7위	TROJ_VUNDO	트로이목마	268	2위
8위	TROJ_LINEAGE	트로이목마	264	권외
9위	TROJ_RENOS	트로이목마	226	권외
10위	TROJ_CABAT	트로이목마	187	NEW

[표 2-5] 2008년 트랜드마이크로 피해 현황 (자료출처: 일본 트랜드마이크로)

피해 통계 순위에 등록된 다른 악성코드들 중에서도 온라인 게임 계정을 유출하는 기능을 포함하고 있는 악성코드들이 많이 존재하는 것으로 미루어보아 게임핵으로 인한 실제 피해는 통계로 집계된 수치를 훨씬 상회할 것으로 추정해 볼 수 있을 것이다.

마지막으로 허위 안티 스파이웨어에 의한 피해가 일본에서도 다수 발생하여 사회적인 이슈가 되었다. AntiVirusXP2008과 같은 허위 안티 스파이웨어의 경우 2008년 하반기 전 세계적으로 많은 피해가 발생하였는데, 일본 또한 이러한 프로그램으로 인한 피해가 다수 발생하였고 외산 프로그램뿐만 아니라 일본에서 제작된 것들 또한 많은 감염 피해를 유발한 것으로 보인다.

(6) 중국 4분기 및 연간 악성코드 동향

2008년 4분기 중국 악성코드 동향

2008년의 마지막 4분기 중국 동향은 기존 악성코드 TOP 10[1]에 포함되어 있던 악성코드들이 순위에서 밀려나고 새로운 악성코드들이 새롭게 TOP 10에 포함되는 현상을 보이고 있다. 그러나 순위에 밀려나는 변화의 크기가 한 계단 정도의 극히 미비한 수준이나 분포 면에서 본다면 비교적 큰 변화가 있었다.

순위	AhnLab V3 진단명	분포
1	Win-Trojan/Obfuscated	75.09%
2	Win-Trojan/Agent	3.60%
2	Win-Trojan/OnlineGameHack	3.60%
4	Win-Trojan/Downloader	2.08%
5	Win-Trojan/Krap	1.48%
6	Dropper/Agent	0.96%
7	Win-Trojan/Autorun	0.96%
8	Dropper/Kgen	0.89%
9	Dropper/OnlineGameHack	0.85%
9	Win-Trojan/Hupigon	0.85%

[표 2-6] 2008년 4분기 ㈜안철수연구소 중국법인 악성코드 TOP 10

지난 3분기에 새롭게 TOP 10에 포함되었던 악성코드가 이번 4분기의 TOP 10에 4 종류가 포함되어있지만 모두 5위 미만의 하위권을 차지하였다. 1위를 차지한 Obfuscated 트로이목마의 경우 2분기에 6위를 차지하고 있었고 3분기에는 순위에서 밀려나 TOP 10에 포함되어 있지 않았었으나, 이번 4분기에서는 75%의 절대 다수를 차지하였다. 그리고, Krap 트로이목마, Autorun 트로이목마 그리고 OnlineGameHack 트로이목마는 2008년 한 해 동안 모두 순위에 포함되지 못하다가 이번 분기 들어 처음으로 TOP 10에 포함되었다.

3 분기와 달리 특이한 사항은 Obfuscated 트로이목마가 전체 분포 면에서 75%를 차지하고 TOP 10에 포함된 다른 악성코드들은 분포 면에서 극히 미비한 점유량을 가지고 있다는 점이다. Obfuscated 트로이목마가 어떠한 특정 트로이목마의 종류를 나타내기 보다는 악성코드의 실행 파일이 특이한 실행 압축 또는 특이한 암호화가 되었을 경우에 분류한 진단명인

[1] 중국 악성코드 동향은 ㈜안철수연구소의 중국법인에서 수집된 악성코드를 기반으로 분석된 결과이다.

것을 감안한다면 이번 분기에서 중국에서 발견된 악성코드들은 기존에 알려진 악성코드 보다는 새롭게 파일 형태를 변경하여 안티 바이러스 소프트웨어의 진단 우회를 위한 시도를 하고 있는 것들이 많은 것으로 추정된다.

2008년 중국 악성코드 동향

2008년에는 비교적 많았던 제로 데이(0-Day) 공격과 SQL 인젝션을 통한 악성코드의 대규모 유포 등 지속적으로 새로운 보안 사고들이 발생하였다.

순위	AhnLab V3 진단명
1	Win-Trojan/Swizzor
2	Win-Trojan/OnlineGameHack
3	Win-Trojan/Obfuscated
4	Win-Trojan/Hupigon
5	Win-Trojan/Agent
6	Win-Trojan/Polycrypt
7	Win-Trojan/Downloader
8	Win-Trojan/KorGameHack
9	Win-Trojan/Dialer
10	Win-Trojan/Klone

[표 2-7] 2008년 AhnLab China 악성코드 TOP 10

[표 2-7]은 2008년 한해 동안 중국에서 발생한 악성코드들을 종합하여 순위별로 정렬한 것으로, 2008년 한 해 동안 중국에서 가장 많이 접수된 악성코드는 Swizzor 트로이목마로서 1분기와 4분기에는 순위에 포함되지 못하였으나 2분기에 압도적으로 많이 발견되었다. 2위와 8위에는 온라인 게임 사용자 정보를 외부로 유출하는 OnlineGameHack 트로이목마와 KorGameHack 트로이목마가 차지하고 있다. OnlineGameHack 트로이목마의 경우에는 2008년 한해 계속해서 순위에 포함될 정도로 중국 내에서 많은 접수가 이루어진 반면 KorGameHack 트로이목마의 경우에는 1분기에 잠시 순위에 포함된 이후에는 포함되지 못하였다. 상반기에는 분석의 지연과 안티 바이러스 소프트웨어의 진단을 회피할 목적으로 실행 파일의 형태가 암호화된 Polycrypt 트로이목마가 많았고, 하반기에는 Obfuscated 트로이목마와 같이 특이한 실행 압축 형태가 많이 발견되었다. 중국의 경우에는 전통적으로 원격제어 형태의 트로이목마가 많이 제작되고 유포되고 있는 것을 4위를 차지한 Hupigon을 통해서 잘 알 수가 있다. 특히 Hupigon 트로이목마의 경우에는 매년 마다 순위에 포함이 될 정도로 많은 변형들이 제작되고 유포되고 있으며 최근에는 중국 언더그라운드에서 안티 바이러스 소프트웨어를 우회하는 상용으로 제작된 별도의 VIP 버전까지 제작되고 있는 실정이다.

2008년에 중국에서 발생하였던 주요 이슈를 살펴보면 아래와 같다.

취약한 웹 사이트 공격

2008년에는 국내를 비롯하여 중국에서도 취약한 웹 사이트에 대한 공격이 많이 발생하였다. 특히 중국발 SQL 인젝션 공격이 활발히 이루어져 전세계적으로 많은 보안 이슈들을 만들었다.

이러한 배경에는 러시아 등의 동구권에서 제작된 웹 익스플로잇 툴킷인 MPack과 FirePack 등이 한 몫 하였으나, 이러한 툴 킷들 역시 2008년 5월에는 모두 중국어로 번역되어 중국 언더그라운드에서 유포되고 있어 웹을 통한 악성코드 유포가 더욱 쉬워지게 되었다. 특히 많은 문제를 야기한 SQL 인젝션 공격의 경우에는 2008년 4월경에 중국 언더그라운드에서 다양한 형태의 SQL 인젝션 공격 툴들이 제작되고 유포되어 SQL 젝션 공격에 대한 기술적인 지식이 충분하지 않더라도 손쉽게 취약한 웹 서버들을 공격할 수 있게 되어 많은 문제를 야기시켰다.

중국내 사회적인 문제를 이용한 보안 위협

중국 내의 여러 사회 문제로 인해 다양한 악성코드와 분산 서비스 거부 공격 등이 다수 발생하였는데, 그 중에서도 가장 많이 이슈화된 것은 중국 북경에서의 올림픽 개최와 티벳의 독립 운동 시위였다. 특히 미국 CNN의 티벳 독립 운동과 관련된 뉴스가 방송되고 난 뒤, 중국내에서는 CNN의 보도가 편파적이라는 이유로 4월에는 대규모의 분산 서비스 거부 공격이 CNN 웹 사이트를 대상으로 발생하게 되었다. 특히 이러한 공격의 배경이 사회적인 이슈라는 점에서 새로운 위협이 다양한 목적을 가질 수 있다는 점을 잘 보여 주었다.

자동화된 공격 툴들로 인한 보안 위협의 증가

2008년에는 다양한 소프트웨어에 대한 취약점이 많이 발견되었고, 이를 악용한 새로운 공격 방법이 등장하는 방식으로 자동화된 공격툴이 다수 제작되었다. 특히 중국의 경우 이러한 과정에 소요되는 시간이 거의 제로데이 공격 수준으로 알려져 있다.

Adobe사의 플래쉬 취약점이 2008년 5월에 알려지면서 취약점을 공격하는 SWF 파일이 대규모로 발견이 되었는데, 이러한 배경에는 바로 자동화된 생성기가 있어 짧은 시간에 다량의 변형들이 대규모로 양산이 되었다. 2008년 6월에는 2007년 극심한 피해를 입혔던 ARP 스푸핑 트로이목마를 자동으로 생성해주는 생성기가 다시 발견되었을 뿐만 아니라 2008년 11월에는 10월에 알려진 “MS08-067 서버 서비스의 취약점으로 인한 원격 코드 실행 문제점

(958644)" 취약점을 자동으로 공격하는 툴까지 발견 되었다. 그리고 2008년 12월에는 인터넷 익스플로러에 존재하는 "MS08-078 포인터 참조 메모리 손상 취약점"이 알려 진지 하루를 넘기지 않고 바로 해당 취약점을 공격하는 스크립트 악성코드 생성기들이 중국 언더그라운드에 유포되고 있었다.

이러한 점은 특정 취약점이 공개되면 중국 언더그라운드에서는 해당 취약점을 자동으로 공격하는 툴이나 악성코드 생성기가 제작될 가능성이 높으며, 이는 바로 대규모의 공격으로 이어진다는 것을 잘 보여준 사례라고 할 수 있다.

규모가 커지고 있는 중국의 사이버 블랙 마켓

비교적 최근에 들어서 알려진 중국의 사이버 블랙 마켓은 러시아의 블랙 마켓과 다르게 온라인 게임과 관련된 아이템 유출을 통한 금전 획득이 가장 큰 비중을 차지하였다. 그러나, 이러한 공격 대상이 온라인 게임 아이템에서 온라인 게임 계정을 생성할 수 있는 개인 정보를 노리는 방향으로 발전하였으며, 이러한 현상은 2008년 5월에 알려진 중국 연변에 위치한 웹 사이트를 통해서 잘 알 수 가 있었다. 특히 해당 웹 사이트에서는 개인 정보에 대한 구체적인 금액이 제시되어 있을 뿐 만이 아니라 온라인 게임 업체의 데이터베이스를 해킹 할 수 있는 해커를 고용한다는 게시물까지 게시되어 청부 해킹까지 공공연히 이루어지고 있다는 것을 알 수가 있었다.

이렇게 개인 정보를 사고 파는 거래뿐 만이 아니라 기업의 웹 사이트를 대상으로 분산 서비스 거부 공격을 통해 금전적인 대가를 받아내기 위해 중국인 해커를 고용하는 사례가 알려졌다. 그리고 특정 목적의 공격을 위해서 다양한 공격 툴들이 사용되었는데 이러한 공격 툴들의 대부분이 중국의 사이버 블랙 마켓에서 일정한 금액만 주어지면 얼마든지 구할 수가 있는 것으로 밝혀졌다.

이러한 사례들을 통해서 중국의 사이버 블랙 마켓은 개인 정보 거래를 바탕으로 시작이 되었지만 지금에 와서는 금전적인 대가를 받는 분산 서비스 거부 공격을 비롯하여 올바르지 못한 목적에 사용하기 위해 주문 제작되는 악성코드 생성기와 공격 툴들까지 그 범위를 확장해 나가고 있는 것을 알 수가 있다.

(7) 세계 연간 동향

이 통계는 각국에 존재하는 주요 백신 업체에서 밝힌 정보를 바탕으로 했기 때문에 해당 업체에는 신고되지 않은 악성코드, 해당 업체에 진단하지 못하는 샘플 혹은 집계 방법에 따라 실제 사용자에게 피해를 입히고 있는 실제 결과와는 다소 다를 수 있다. 2008년에는 단순히 고객 신고나 유입 메일 통계가 아닌 자사 제품으로 진단되는 결과를 집계 내는 방식으로 바꾸면서 실제 사용자 감염 상황을 파악할 수 있게 되는 업체가 증가했으며 년간 통계를 찾을 수 없는 회사도 존재한다. 악성코드가 대량 제작되고 단시간에 퍼지는 양상을 보여 연간 통계 의미가 퇴색된 것도 원인으로 보인다.

루마니아 비트디펜더의 통계에 따르면 2008년 악성코드 통계에서 쿠키를 제외하면 애드웨어나 취약점을 이용하는 악성코드들이 순위를 차지했다. 주로 웹사이트 방문을 통해서 전파되는 트로이목마로 주요 악성코드 전파 경로가 웹사이트 방문이 되면서 넷스카이웜, 나이젬 웜 변형 같이 메일로 전파되는 악성코드가 순위에서 사라진 것으로 보인다.

트렌드사의 통계에 따르면 악성코드 순위에는 USB 플래쉬 메모리 등으로 전파되는 오토런 웜(Autorun worm)이 주요 순위를 차지하고 있다. 대륙별, 국가별로도 USB 플래쉬 메모리를 통해 전파되는 악성코드가 순위에 있었다.

메일로 전파되는 악성코드에 대한 통계는 사용자 감염과는 다소 다른 과거 악성코드가 여전히 활동 중임을 알 수 있다.

슬로바키아 에셋(Eset)사의 2008년 통계에 따르면 1위는 자피 웜(Win32/Zafi.B worm)이다.[1] 2위는 2007년 3위였던 넷스카이 웜 변형, 3위, 5위는 스트레이션 웜이 차지하고 있다. 여전히 메일로 전파되는 웜들이 다수 존재함을 알 수 있다. 에셋사의 통계는 기본적으로 메일을 통해서 파악되며 체코의 포털 사이트인 Seznam (http://www.seznam.cz/)의 메일을 모니터링하고 있기 때문에 체코 내에서 활동하거나 유입되는 악성코드의 통계로 볼 수 있다.

아이슬랜드 프리스크 소프트웨어(Frisk Software)에 따르면 지난 1년간 1위는 압도적으로휴리스틱 진단(Heuristic detection)으로 특정 악성코드는 아니었다. 따라서 실제 악성코드 순위에서 1위는 나이젬 웜 변형(Kapser, Mywife 등)이며 2위는 넷스카이, 마이둠, 마이톱 등의 메일로 전파되는 악성코드들이다.

2008년 세계의 악성코드 동향을 보면 2007년과 마찬가지로 특정 악성코드가 광범위하게 퍼

[1] http://www.virusradar.com/stat_01_current/index_c12m_enu.html

지진 않았다. 이는 악성코드 제작 동기가 실력 과시에서 금전적 이득 목적으로 변화하면서 발생하는 것으로 더 이상 악성코드 제작자는 무작위로 빠른 시간에 널리 퍼뜨리는 것이 아니라 한정되게 목표를 정해 은밀하게 퍼뜨리고 제거에 대비해 새로운 변형으로 교체하는 형태로 바뀌고 있다. 이에 판다시큐리티 2008년 통계에 따르면 악성코드 중 77.49%가 트로이 목마, 16.28%가 애드웨어로 이들 유형이 가장 큰 것을 알 수 있다. 웜은 2.74%이며 바이러스는 기타 통계로 집계되었다. 악성코드 전파 경로도 메일을 통한 전파 방법보다 웹 브라우저 취약점과 USB 플래쉬 메모리 등을 통한 전파 방법이 보편화되고 있다.

2007년 핀란드 F-시큐어(F-Secure)사는 2007년까지 발견된 악성코드는 50만개라고 밝혔고 2008년에도 계속 증가할 것이라고 예상했다. 2008년 스페인 판다시큐리티는 하루에 2만 2천 개의 새로운 악성코드를 접수 받았다고 했다. 다른 업체도 이와 비슷하며 계산해보면 2008년 한해 동안 전세계적으로 악성코드는 800만개 이상 새롭게 발견된 것으로 보인다. 불행히도 2009년에도 문제는 더 심각해져 천 만개 시대가 올지도 모른다.

.

III. 이달의 통계

(1) 악성코드 통계 – 악성코드 증가 추세

12 월순위		악성코드명	건수	비율
1	new	Win-Trojan/Agent.67678	101	31.1%
2	new	Win-Trojan/Agent.8192.PF	40	12.3%
3	new	Win-Trojan/OnlineGameHack.863748	32	9.8%
4	new	Win-Trojan/Downloader.18432.LA	29	8.9%
5	new	Dropper/Changer.214152	27	8.3%
5	new	Win-Trojan/Downloader.14848.GK	27	8.3%
7	new	Win-Trojan/OnlineGameHack.35303	21	6.5%
8	new	Win-Trojan/Agent.43520.FK	18	5.5%
9	new	Win-Trojan/Agent.67678	15	4.6%
9	new	Win-Trojan/OnlineGameHack.19032	15	4.6%
합계			325	

[표 3-1] 2008년 12월 악성코드 피해 Top 10

[표 3-1]은 2008년 12월에 피해 접수가 많이된 Top 10 악성코드들로 이들 악성코드들로 인한 총 피해건수는 325건으로 한 달 접수된 총 피해건 수(4,042건)의 8.04%에 해당하며, 지난 10월 270건(10.0%), 11월 227건(7.4%)과 비교하면 크게 차이가 없다. 전반적으로 Win-Trojan/Downloader와 Win-Trojan/OnlineGameHack류는 크게 다르지 않지만 1위에 랭크된 Win-Trojan/Agent.67678의 피해건 접수가 다소 많았기 때문에 Top 10의 전체 합계가 소폭 상승하였다.

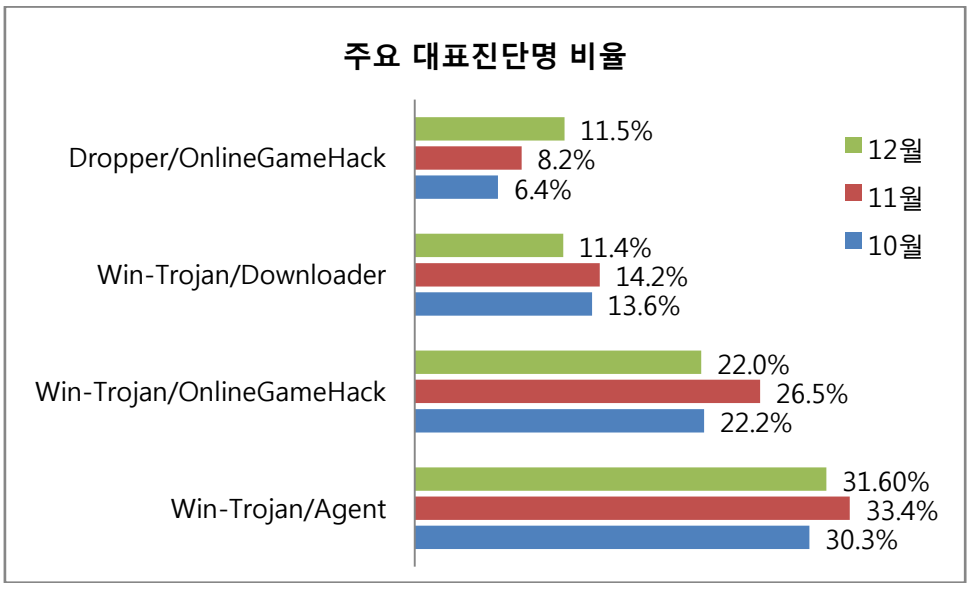
2007년 12월에 이메일로 대량 확산되었던 Win32/Zhelatin.worm류의 악성코드로 인한 신고 신고가 5건으로 예상외로 적어 Top 10에 포함되지 않았다. 이를 바탕으로 추정해보면, 이메일을 통한 악성코드 유포방식이 더 이상 효력을 발휘하지 못하고 있다고 판단된다. 이는 예전과 같이 메일을 여는 것만으로도 악성코드가 실행되는 취약점이 없고, 전반적으로 의심스럽거나 잘 알지 못하는 영문 메일에 대한 위험성을 인터넷 사용자들이 인지하게 된 것으로 보인다.

12 월순위	대표 진단명	건수	%
1	Win-Trojan/Agent	842	31.8%
2	Win-Trojan/OnlineGameHack	588	22.2%
2	Dropper/OnlineGameHack	307	11.6%
4	Win-Trojan/Downloader	303	11.4%
5	Dropper/Agent	150	5.7%
6	Win32/Autorun.worm	124	4.7%
7	Win-Trojan/Xema.variant	107	4.1%
7	Win-Trojan/Sadenav	91	3.4%
9	Win-Trojan/Zlob	82	3.1%
10	JS/Exploit	53	2.0%
합계		2,647	

[표 3-2] 2008년 12월 악성코드 대표진단명 Top 10

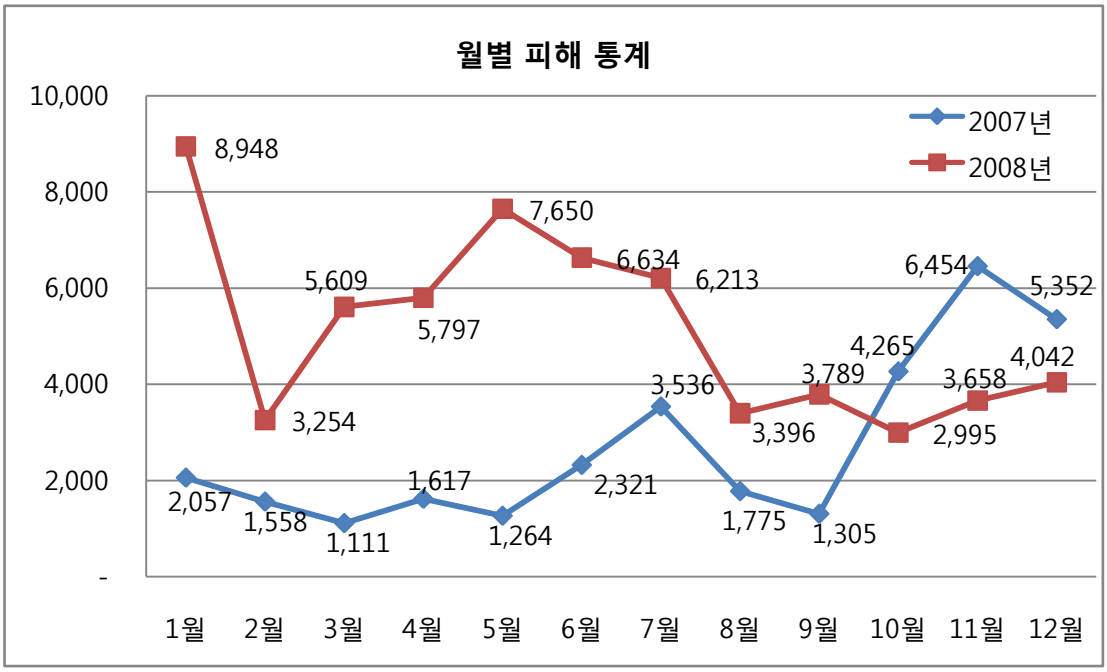
[표 3-2]는 2008년 12월 악성코드의 대표진단명을 기준으로 대표진단명 Top 10 유형별 피해 순위를 나타내고 있다. 유형별 Top 10에 포함된 악성코드 총 피해건수는 2,647으로 11월의 2,299건에 비해 15% 가량 증가하였으며, 한 달간 접수된 총 피해건수(4,042)의 65.5%이다.

12월 대표진단명의 상위에 랭크된 대표진단명의 비율은 다음 [그림 3-1]과 같다.



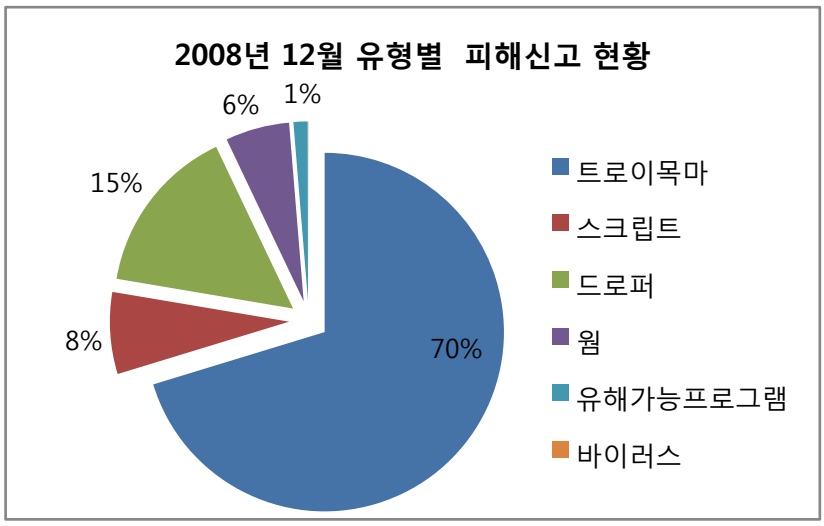
[그림 3-1] 2008년 10월 ~ 12월 주요 대표진단명 비율

월별 피해신고 건수



[그림 3-2] 2007, 2008년 월별 피해신고 건수

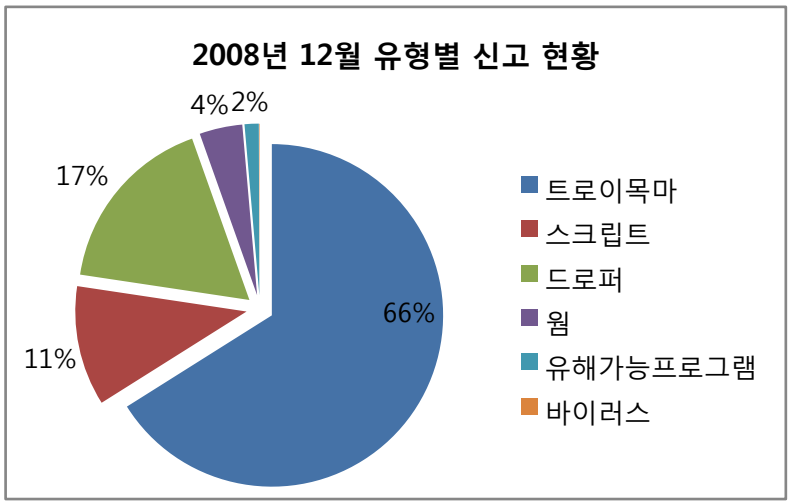
[그림 3-2]는 월별 피해신고 건수를 나타내는 그래프로 12월에는 4,042건의 피해신고가 접수되었다. 2007년과 비교하면 4분기에 접수된 피해신고가 상대적으로 적은 편이지만 2008년 4분기 들어서 지속적으로 피해신고가 증가 추세에 있다.



[그림 3-3] 2008년 12월 악성코드 유형별 피해신고 건 수

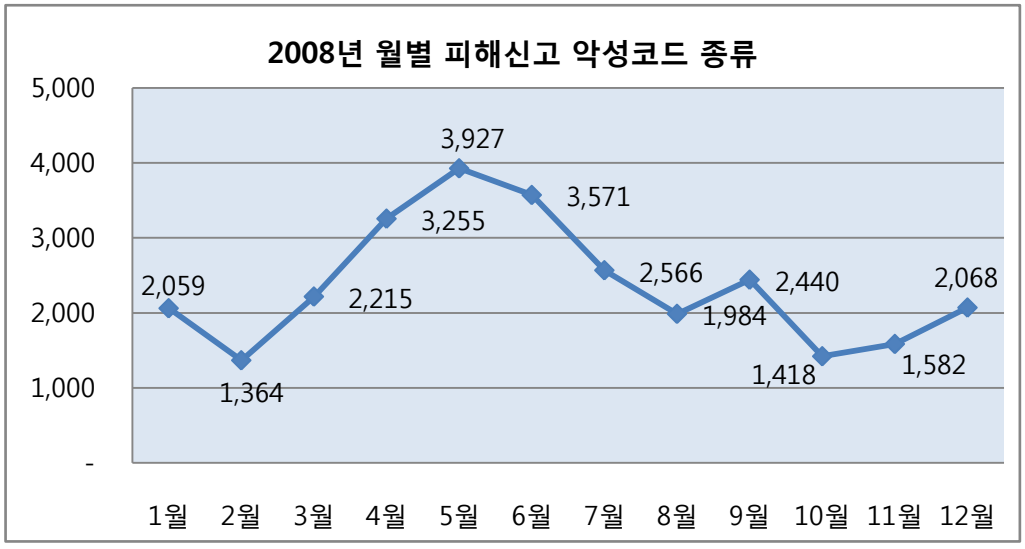
[그림 3-3]은 2008년 12월 전체 악성코드 유형별 피해신고 건 수를 나타내고 있는 그래프이다. Top 10의 유형과 마찬가지로 전체 피해신고 유형에서도 트로이목마 비율이 11월의

77%에 비하여 70%로 하락하였지만, 피해신고 유형의 절대 다수를 차지하고 있다. 드로퍼가 지난달보다 3%증가하였는데, 이는 중국에서 제작되고 있는 악성코드 유포툴이 거의 대부분 드로퍼를 웹사이트에 삽입시키기 때문에 나타나는 현상으로 보이며, 이러한 드로퍼로 인한 피해는 2009년에도 지속될 것으로 예상된다.



[그림 3-4] 2008년 12월 피해 신고된 악성코드의 유형별 현황

[그림 3-4]는 12월 한달 간 접수된 유형별 신고건수로 [그림 3-3]의 유형별 피해신고 건수와 마찬가지로 트로이목마가 66%로 높은 비율을 차지하고 있다. 나머지 스크립트 11%, 웜 4%, 유해가능프로그램이 2%를 차지하고 있으며, 드로퍼의 증가율이 11월 12.8%에서 4.2% 상승한 17%를 기록하고 있다. 그리고 12월은 IE 취약점을 이용한 스크립트류의 악성코드로 인하여 11월에 접수된 126건에 비해 229건으로 81.7% 증가하였다.



[그림 3-5] 2008년 월별 피해신고 악성코드 종류

[그림 3-5]는 2008년 월별로 피해신고가 되는 악성코드의 종류를 나타낸 그래프이다. 월별로 신고되는 [그림 3-2]의 월별 피해신고 건수와 마찬가지로 10월부터 악성코드 종류가 점차 증가하고 있는 것으로 나타났다.

악성코드의 유형이 점차 Rootkit과 같이 은폐형 악성코드로 발전함에 따라 고객의 피해신고 건수뿐만 아니라 악성코드의 종류도 지속적으로 증가할 것으로 예상된다.

국내 신종(변형) 악성코드 발견 피해 통계

12월 한 달 동안 접수된 신종 (변형) 악성코드의 건수 및 유형은 [표 3-3]과 같다.

	웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
10 월	58	899	130	145	3	0	0	0	16	0	1251
11 월	57	1162	197	151	19	0	0	0	6	0	1592
12 월	85	1431	370	263	3	0	0	0	23	0	2175

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

이번 달은 전월 대비 37% 가량의 증가하여 올해 들어 가장 많은 신종 및 변형 악성코드가 보고 되었다. 전체적으로 모든 유형의 악성코드가 증가하였으며, 이는 올 6월 달 각종 취약점들로 인하여 Drive by Downloads[1]형태의 악성코드가 급증했던 6월과 비교하여도 소폭 증가한 것이다.

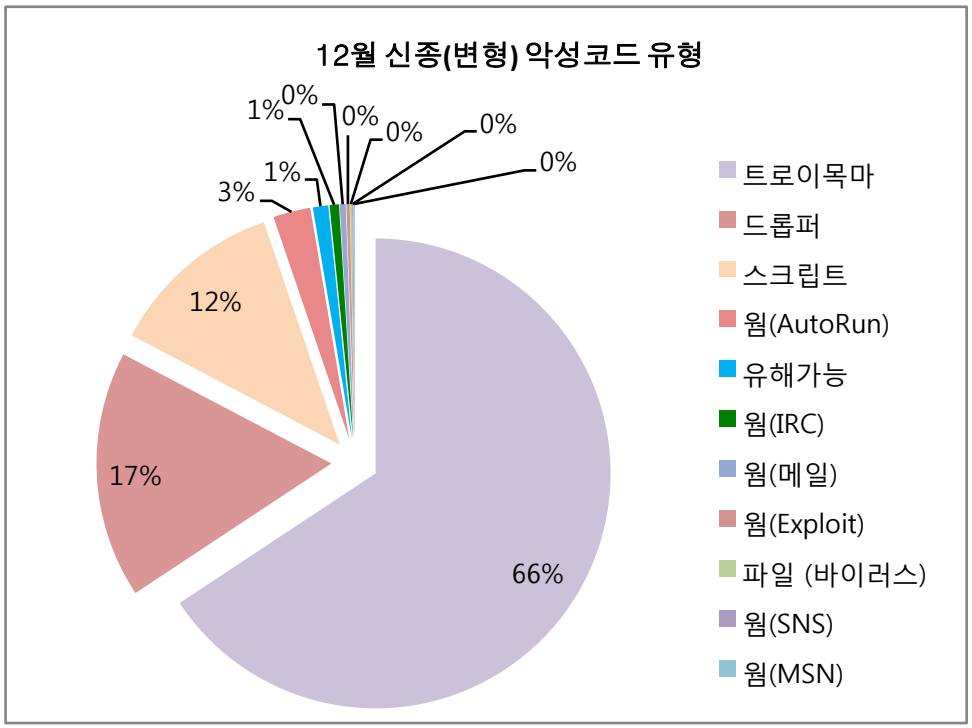
이와 같이 신종 및 변종 악성코드가 증가한 원인을 찾아보면 아래와 같다.

- 국내를 향한 중국 발 해킹과 악성코드 유포를 위한 중간 경유지로 여전히 많은 국내 시스템들이 악용되고 있다는 점.
- 악성코드 제작도구의 자동화와 더불어 도구를 판매하고 공유하면서 일반 사용자들도 범죄에 끌어 들이려고 한다는 점
- 악성코드 제작과 유포 등이 지능적이고 전문화된 집단에서 계속 만들어지고 있는 것으로 추정됨

이와 같은 상황이 계속될 것으로 예상되기 때문에 악성코드의 수는 앞으로도 증가할 것으로 보인다.

다음은 이번 달 악성코드 유형을 상세히 분류 하였다.

[1] (웹 브라우저와 같은 응용 프로그램의 취약점을 이용하여 사용자의 별도의 행동없이 다운로드 되어 자동실행 되는 악성코드 형태)



[그림 3-5] 2008년 12월 신종 및 변형 악성코드 유형

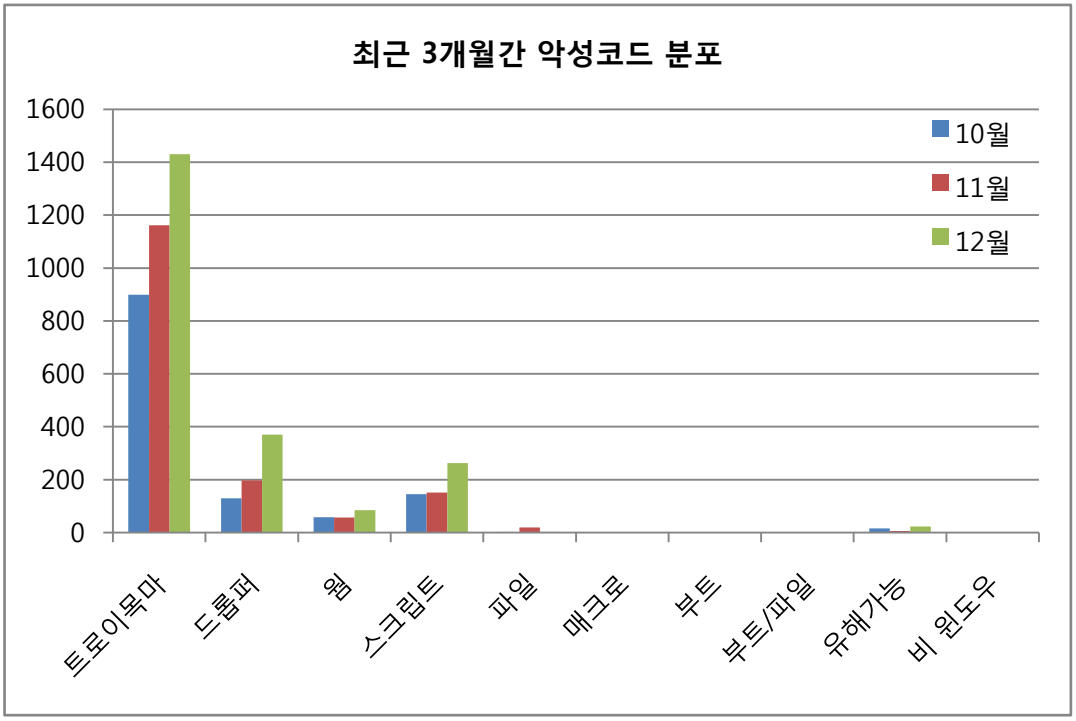
트로이목마 유형은 전월 대비 23% 증가 하였다. 특히 온라인 게임의 사용자 계정 정보를 탈취하는 형태도 급격히 증가하였다. 이번 달 특징적인 트로이목마로 DNS 서버주소를 특정주소로 변경하는 Win-Trojan/DNSChanger가 국내에 12월 초 갑자기 증가하였다. DNS 주소를 변경하는 형태의 트로이목마는 이전에도 존재하였던 형태였으나, 갑자기 국내에서 다수의 고객으로부터 신고되었고, 이후 발견된 변형들에서 은폐기법과 자기보호 기능을 포함하고 있는 것으로 분석되었다. 이는 일반 사용자는 물론 시스템을 잘 아는 전문가들도 해당 악성코드를 처리하는데 쉽지 않았을 것으로 생각 된다.

드롭퍼 유형은 당연히 온라인 게임 트로이목마를 설치하는 형태가 가장 많은 수를 차지하였다. 이러한 드롭퍼의 실행 후 증상은 기존과 크게 다르지는 않았지만, 특이한 점이라면 일부 안티 바이러스 제품에서 사용하는 진단 방법 중 파일의 실행압축 여부 또는 파일 내 특정 문자열을 찾아서 검사하는 진단 방법을 회피할 목적으로 실행압축이 안된 형태가 많이 발견되고 있다.

스크립트 유형은 Drive by Download 형태의 악성코드를 실행하기 위한 목적으로 제작되어 수 많은 변형이 발견되었다. 대부분의 스크립트 악성코드는 크게 VBS 웜 유형과 웹 브라우저의 취약점을 가진 Exploit 형태로 구분 된다고 해도 과언이 아니며, 특히 12월 초에는 인터넷 익스플로러에 대한 XML 관련 제로데이 취약점이 알려져 관련 스크립트 악성코드가 다수 보고 되었다.

유해가능 프로그램 유형에서는 주로 취약점 점검 및 패킷 스니핑 도구류가 주로 발견되고 있으며, 웜 유형으로는 일반적인 유형 이외에 MS08-067(서버 서비스 취약점) 취약점을 이용하여 전파되는 Win32/Conficker.worm 변형이 12월중 다수의 변형이 보고 되었다. 파일 바이러스 유형에서는 잘 알려진 Win32/Dellboy 변형 바이러스가 보고 되었다.

다음은 최근 3개월간 악성코드 분포이다.

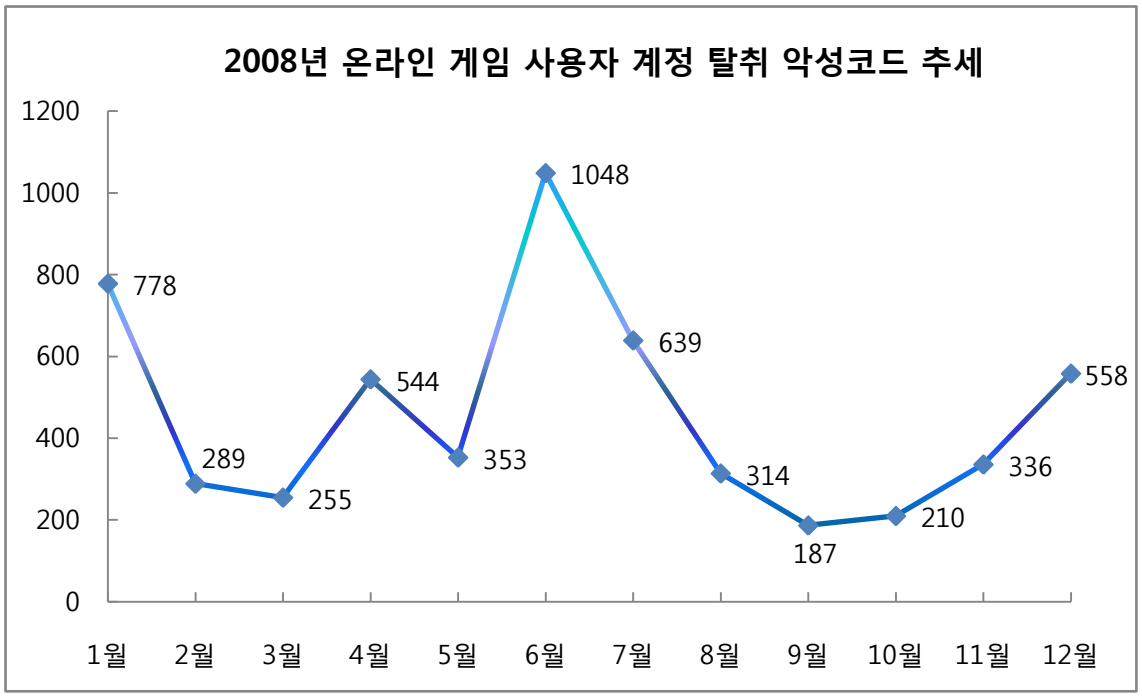


[그림 3-6] 2008년 최근 3개월간 악성코드 분포

최근 3개월간 악성코드는 꾸준히 상승을 하고 있는 것을 알 수가 있다. 정확한 원인을 알 수는 없지만 이는 웹 애플리케이션 공격의 증가에 따라 기인한 것으로 보이고, 주로 사용되는 공격으로 다음과 같은 것이 있다.

- Cross-site Scripting
- SQL Injection
- Drive-by Downloads

다음은 트로이목마 및 드롭퍼의 전체 비중에서 상당한 비율을 차지 하는 온라인 게임의 사용자 계정을 탈취하는 트로이목마의 추세를 살펴보았다.



[그림 3-7] 온라인 게임 사용자 계정 탈취 트로이목마 현황

2008년 하반기에 이러한 유형의 트로이목마가 60% 이상 급증하고 있다. 새로운 유형의 등장이나, 진단하기 어렵거나 또는 진단되지 않는 유형이 나온 것도 아니다. 추정되는 원인은 악성코드 제작에 사용되는 도구가 다수 제작되고 있고, 이러한 도구들을 이용하여 일반인들도 악성코드 제작이 가능한 환경이 구축된 것과 대상이 되는 온라인 게임이 초창기에는 국산 온라인 게임만을 노리는 형태에서 근래에는 국내에 소개 되지 않은 대만 및 중국산 온라인 게임들도 대상으로 하기 때문으로 분석된다.

(2) 스파이웨어 통계 – 무료 소프트웨어 설치시 주의 필요

순위		스파이웨어 명	건수	비율
1	New	Win-Downloader/Gaongil.385536	15	17.6%
2	New	Win-Adware/BHO.PointGuide.244736	13	15.3%
3	New	Win-Downloader/Kwsearch.225280	11	12.9%
4	↑ 4	Win-Adware/PointGuide.207872	9	10.6%
5	New	Win-Spyware/StartPage.Zhaoy.50688	7	8.2%
6	New	Win-Adware/PointGuide.230400	7	8.2%
7	New	Win-Downloader/PlgEvent.503808	6	7.1%
8	New	Win-Adware/JUser.628224	6	7.1%
9	New	Win-Spyware/Flux.16384	6	7.1%
10	↓ 1	Win-Adware/BHO.PointGuide.323072	5	5.9%
합계			85	

[표 3-4] 2008년 12월 스파이웨어 피해 Top 10

2008년 12월 스파이웨어 피해 상위 Top10의 대부분은 애드웨어 포인트가이드(Win-Adware/BHO.PointGuide)를 비롯한 국내에서 제작된 스파이웨어가 대부분이다. 애드웨어 포인트가이드는 팝업광고에 포함된 ActiveX로 배포되는 리워드(적립금)제공 프로그램으로 지난 11월에 최초 발견되어 지난달에 이어 12월에도 많은 피해를 입혔다. 일반적으로 설치와 배포에 ActiveX를 이용하는 스파이웨어는 피해 규모가 크고 단기간에 집중되는 경향을 보이는데 애드웨어 포인트가이드 또한 이러한 특징을 잘 보여준다. 2007년 말에 개정된 정부의 스파이웨어 기준에 따라 불특정 웹사이트에서 ActiveX를 이용하여 배포되는 프로그램을 스파이웨어로 분류함에 따라 최근에는 국내에서 제작되는 스파이웨어의 대부분은 무료 게임, 음악 프로그램의 번들로 설치된다. 설치과정에서 형식적인 사용자 동의를 받지만 프로그램 설명이 충분하지 않으며, 소프트웨어 사용 약관에 포함되지 않은 동작을 하는 경우가 많으므로 인터넷에서 흔히 접할 수 있는 무료 소프트웨어를 설치할 때는 주의가 필요하다.

순위	대표진단명	건수	비율
1	Win-Downloader/Zlob	260	38%
2	Win-Adware/CashBack	91	13%
3	Win-Spyware/Crypter	70	10%
4	Win-Spyware/Zlob	62	9%
5	Win-Dropper/Zlob	59	9%
6	Win-Adware/Kwsearch	52	8%
7	Win-Downloader/Kwsearch	24	4%
8	Win-Dropper/AdRotator	24	4%

9	Win-Adware/BHO.PointGuide	22	3%
10	Win-Adware/PointGuide	21	3%
		685	100%

[표 3-5] 12월 대표진단명에 의한 스파이웨어 피해 Top10

[표 3-5]는 변형을 고려하지 않은 대표진단명에 의한 피해 자료이다. 대표진단명에 의한 스파이웨어 피해 상위 Top10은 전체 피해신고 건수 1,372건의 약 절반인 685건을 차지하며, 그 중에서도 약 40%가량이 성인사이트에서 코덱으로 위장하여 배포되는 스파이웨어 즐롭(Win-Spyware/Zlob) 변형으로 스파이웨어 즐롭의 피해가 지속적으로 발생하고 있는 것을 확인할 수 있다. 2위의 애드웨어 캐쉬백(Win-Adware/CashBack)은 국내에서 제작되어 지난 2008년 6월 발견되었으며, 현재까지 꾸준하게 변형이 발견되고 있으며, 애드웨어 포인트가이드 또한 많은 피해를 입혔다.

2008년 12월 유형별 스파이웨어 피해 현황은 [표 3-6]과 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
10월	274	235	139	452	0	40	0	2	0	**1142**
11월	417	342	191	492	0	39	0	5	0	**1486**
12월	291	437	193	419	3	22	3	4	0	**1372**

[표 3-6] 2008년 12월 유형별 스파이웨어 피해 건수

[표 3-6]은 2008년 12월 유형별 스파이웨어 피해 현황이다. 11월까지 증가세를 이어오던 스파이웨어 피해신고 건수가 12월에는 다소 감소하였다.

12월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 3-7]과 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
10월	180	138	90	345	0	29	0	2	0	**784**
11월	194	165	120	314	0	26	0	2	0	**821**
12월	202	269	132	235	2	19	2	3	0	**882**

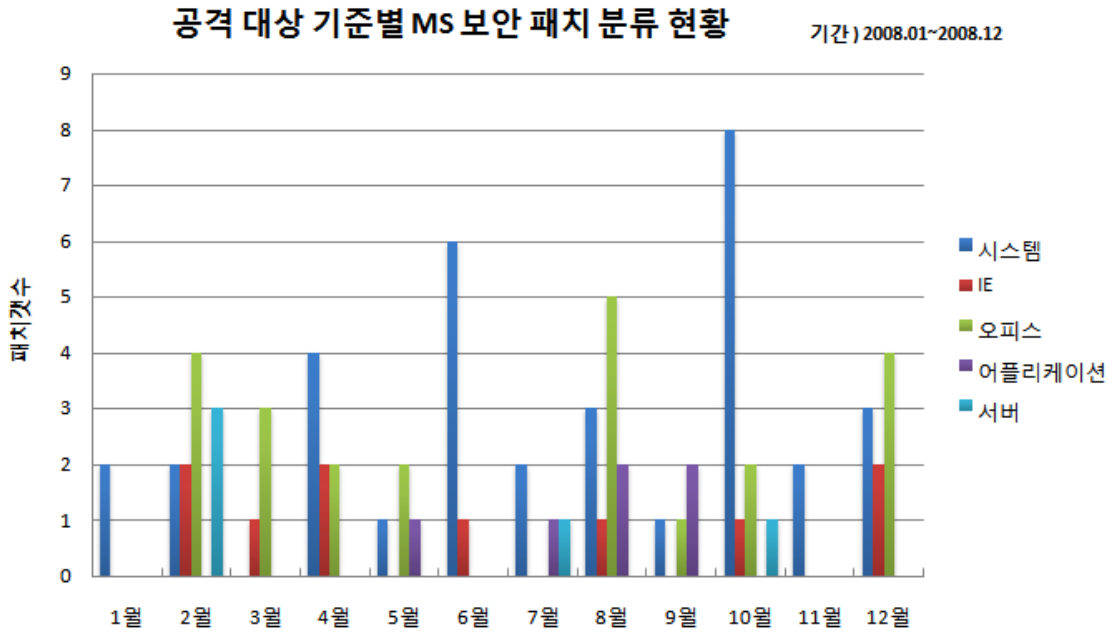
[표 3-7] 2008년 12월 유형별 신종(변형) 스파이웨어 발견 현황

[표 3-7]은 2008년 12월 발견된 신종 및 변형 스파이웨어 통계를 보여준다. 12월 스파이웨어 피해신고 건수는 감소하였으나 변형 스파이웨어 모니터링 강화에 따라 신종 및 변형 스파이웨어의 수는 지난 달 보다 다소 증가하였다. 피해신고와 마찬가지로 신종 및 변형 애드웨어가 많이 발견되었다.

(3) 시큐리티 통계 – IE 긴급 패치

2008년 12월에 마이크로소프트사에서 발표한 보안 업데이트는 총 9건으로 긴급(Critical) 7건, 중요(Important) 2건이다. 그 중에서도 인터넷익스플로러 7에서 발생하는 XML 제로데이 취약점이 큰 이슈가 되었고, 이에 해당하는 MS08-078 긴급 보안업데이트(Out-of-Band)가 발표되기도 하였다.

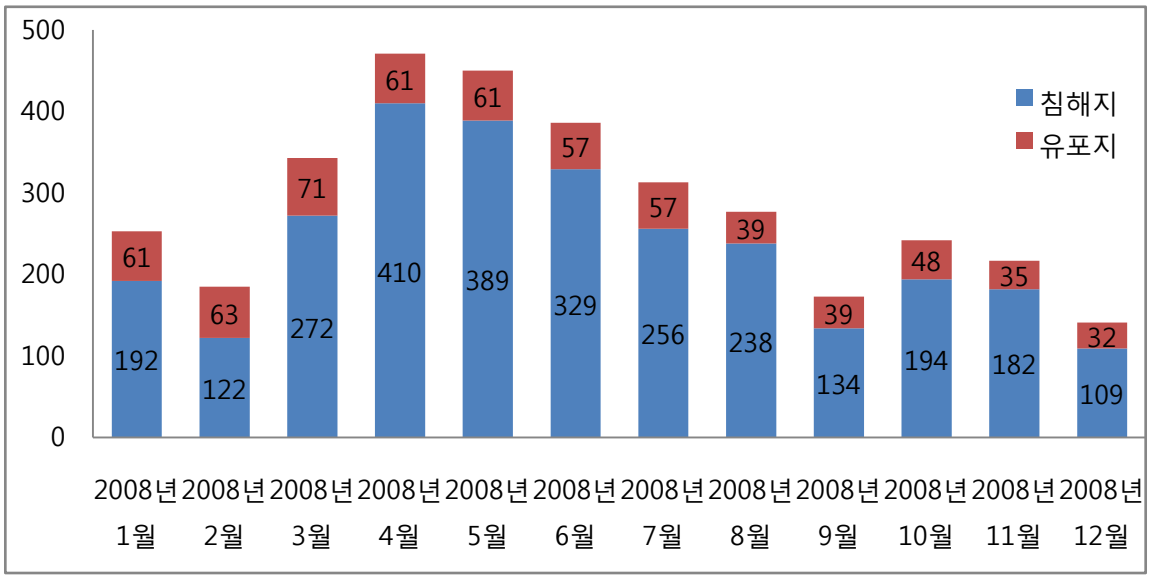
최근 MS SQL 서버 상에서 코드 실행 취약점이 추가로 보고되었고, 해당 취약점과 MD5 관련 이슈에 해당하는 2건의 마이크로소프트 보안 권고문(Security Advisories)이 발표되었다. 특히, MS SQL 서버 상의 취약점은 해당 취약점을 악용할 수 있는 공격코드(PoC)가 웹을 통해 공개되었음에도 불구하고, 아직까지 이에 대한 보안 패치가 발표되지 않은 제로데이 취약점으로 남아있다. 2008년을 마감하는 12월에 유난히 제로데이 공격에 대한 이슈가 끊이지 않고 있어 어느 때보다도 취약점 보안에 대한 중요성을 생각하게 하는 달이다. 사용자 시스템을 보호하기 위한 많은 좋은 솔루션들이 제공되고 있으나, 일차적으로 정기적인 보안 업데이트의 생활화가 사용자 PC를 가장 안전하게 보호할 수 있는 최상의 방법이 될 것이다.



위험도	취약점	PoC
긴급	(MS08-078) Internet Explorer 누적 보안 업데이트	유
긴급	(MS08-076) Windows Media Components의 취약점으로 인한 원격 코드 실행 문제점	유
긴급	(MS08-070)Visual Basic 6.0 런타임 확장 파일(ActiveX 컨트롤)의 취약점으로 인한 원격 코드 실행 문제점	유

[표 3-8] 2008년 12월 발표된 주요 MS 보안 패치

2008년 12월 웹 침해사고 현황



[그림 3-8] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

2008년 12월의 웹 사이트 경유지/유포지 수는 109/32로 지난 달의 182/35에 비해 늘어났다. 이 달에는 MS07-017 취약점을 이용한 배포가 현저하게 줄었으며, MS08-041 Microsoft Access Snapshot Viewer 취약점을 이용해 악성코드 배포를 시도한 사례가 종종 발견되고 있다. 이번 달도 다른 달과 크게 다른 점이 없었으나, 한 가지 주목할 점으로 한때 제로데이로 악명을 떨쳤던 MS08-078 XML 취약점을 이용한 악성코드의 배포가 탐지된 점을 들 수 있다.

MS08-078 취약점의 경우, 그 심각성이 언론에 대대적으로 보도된 것과는 달리 그 영향력이 예상보다 작았다. 109개의 침해지 중 단지 7개만이 MS08-078 취약점을 이용해 배포되었다. 하지만, 써드 파티의 제품이 아니라 마이크로소프트 제품의 취약점이라는 점과 브라우저 취약점이라는 점들을 고려하면 그 영향은 무시할 수가 없다. 따라서, 사용자들은 항상 브라우저와 관계된 모든 어플리케이션의 보안 업데이트를 꼼꼼히 챙겨야 한다.

```
for (var i = 0; i < le7; i++) { if ((new Date().getT
ds){      break;    }}} function spray(sc) { var wkbn
0a0a; var wkbnwvojsqweyvwgabdlieyqfbygrgz=unescape; v
bnwvojsqweyvwgabdlieyqfbygrgz(sc); var heapBlockSize
 = asdfkj129312asdfasd.length * 2; var szlong = heapB
8); var retVal = wkbnwvojsqweyvwgabdlieyqfbygrgz("%u0
mpleValue(retVal,szlong);    aaablk = (wkbnwvojsqweyv
ockSize;    zzchuck = new Array();    for (i=0;i<aaab
= retVal + asdfkj129312asdfasd; } }   function getSam
  while(retVal.length*2<szlong) {         retVal += r
.substring(0,szlong/2); return retVal; } var ai="%u";
```

[그림 3-9] MS08-078 취약점 공격 코드 일부