안철수연구소에서 발행하는 월간 보안 보고서

ASEC 리포트

2009년 5월호

이달의 보안 이슈

1. 악성코드 – Geno 혹은 Gumblar 악성코드 이슈 2
2. 스파이웨어 – 리워드 프로그램 제작자의 기소 및 Clicker 이슈 5
3. 시큐리티 – IIS의 WebDAV 취약점 주의 요망 9
4. 중국 보안 이슈 – 사이버 머니 갈취범 징역형 및 취약한 PDF 생성기 12

ASEC 칼럼

■ 구름 속 백신 ?! 안랩 스마트 디펜스 15

이달의 통계

1. 악성코드 24
2. 스파이웨어 33
3. 시큐리티 37
4. 사이트가드 40

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 – Geno 혹은 Gumblar 악성코드 이슈

이번 달은 취약한 웹 사이트 방문 시 또는 특정 포털에 대하여 검색 시 악의적인 사이트로 유도 하거나 악성코드를 설치하는 일명 Geno 혹은 Gumblar라는 악성코드가 큰 피해를 일으켰다. 특히 기사화가 되면서 국내외적으로 많은 보도가 있었다. 또한 지난 2월부터 증가하기 시작한 P2P 웜인 Win32/Palevo.worm도 눈에 띄었으며 Mac용 악성코드도 BotNet을 구축하여 활동 한다는 소식도 들려 왔다.

(1) Geno 혹은 Gumblar 악성코드 피해와 Daonol 트로이목마 분석

먼저 Geno라는 이름은 일반적으로 안티 바이러스 업체의 진단명이 아니다. Geno라고 유래가 된 것은 일본의 컴퓨터 판매 사이트인 Geno라는 업체에서 지난 4월 4일경 홈페이지를 통해서 악성코드가 알려지면서 매스컴에 보도가 되었다. 이후 Gumblar라고 알려지기도 하였다. 외국에서는 주로 Gumblar라고 많이 불리어지고 있다. Gumblar라는 이름 역시 악의적인 스크립트에 명시된 gumblar.cn 혹은 martuz.cn에서 유래 되었다.

해당 악성코드는 일반적인 대규모 웹 사이트 공격(SQL 인젝션과 같은)의 파생물로 보인다. 또한 이것은 가장 일반적인 악성코드 전파방식으로 사용되고 있는 Drive-by download 형태의 악성코드라 할 수 있다. 즉, 취약점이 존재하는 웹 브라우저나 응용 프로그램을 통하여 사용자의 의지와 상관 없이 다운로드 및 실행 된다.

악성코드는 PDF와 SWF 취약점으로 감염 될 수 있다. 이번 달 PDF 취약점이 증가한 이유도 해당 악성코드 일정 부분 원인이 있다고 추정해 볼 수 있다. 취약한 PDF 문서가 실행 되면 최종적으로 Win-Trojan/Daonol이라는 악성코드를 설치 한다. Dropper 형태의 EXE 파일을 다운로드 및 실행하며 내부에 있는 DLL 파일을 설치하고 웹 사이트 로그인 정보 등 사용자 개인정보를 탈취 한다. 악성코드 레지스트리에 등록 후 이후 부팅 시마다 동작 하도록 해둔다. 증상에 대한 분석 정보는 다음과 같다.

[파일생성]
랜덤 한 길이와 이름을 갖는 DLL 모듈을 EXE 파일이 실행한 위치와 동일위치에 생성 (예: xltrr.rfs)

[파일수정]
시스템폴더에 존재하는 정상적인 "sqlsodbc.chm" 파일을 손상시킨다.
- C:₩WINDOWS₩system32₩sqlsodbc.chm
해당 파일은 나중에 네트워크 트래픽 정보 및 FTP 사용자 계정에 대한 정보를 유출 시 내용을 임시 저장하는 데이터파일로 활용된다.

[레지스트리 등록]
아래의 레지스트리 값("aux")에 자신이 드랍 한 DLL 모듈의 패스정보를 추가한다.

[HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Drivers32]
"aux"="?:₩..₩xltrr.rfs"
만약 "aux"가 기존에 존재할 경우, 아래와 같이 숫자를 추가하여 새롭게 생성한다.
- "aux1", "aux2" ... "aux:" ...

[DLL 에서 수행하는 작업]
(1) 특정 프로세스 강제종료
- 자신을 로드 한 프로세스의 확장자가 ".com"인 경우 강제종료
(2) 6개 API에 대한 후킹
아래의 API에 대한 주소 값을 얻은 후, 시작 5바이트를 JMP코드로 삽입하여 DLL모듈의 특정 함수로 분기하도록 한다.
- kernel32.CreateProcessW
- ws2_32.WSASend
- ws2_32.WSARecv
- ws2_32.connect
- ws2_32.send
- ws2_32.recv
(2-1) 후킹한 "kernel32.CreateProcessW" API 호출 시 수행하는 작업
A. 아래의 문자열이 존재하는 프로세스 실행 시, DLL 자신을 손상 시킴(1024 bytes의 NULL데이터)

- "gmer"
- "le38"

B. 아래의 문자열이 존재하는 프로세스 실행 시, 강제종료 함.
- .com
- .bat
- .reg
- cmd
- reged

(2-2) 후킹한 네트워크 관련 API 5개를 호출 시 수행하는 작업
A. 전송하는 데이터에 "USER", "PASS"라는 내용이 존재할 경우, 해당 값을 유출 함. (FTP 사용자 계정정보 유출)

B. 접속을 시도하는 사이트 중 아래의 문자열 존재 시 접속을 차단함(1)

- DaonolFix - miekiemoes – bleepingcomputer
– mbam – mcafee - clamav
- prevx

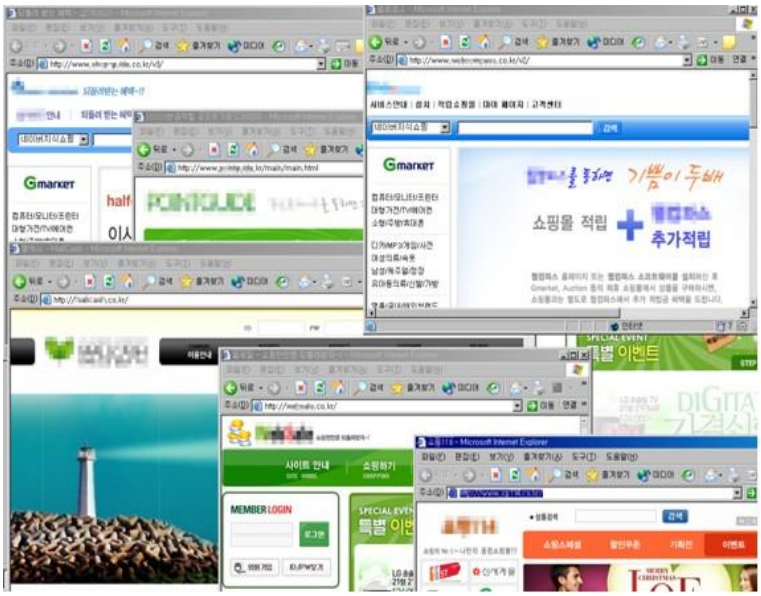
C. 접속을 시도하는 사이트 중 아래의 문자열 존재 시 접속을 차단함(2)
- Adob
- AVG
- AVPU
- CAUp
- COMO

(3) 아래의 파일들에 대한 삭제여부 체크하여 재 생성하는 기능
- DLL 파일
- sqlsodbc.chm
DLL 모듈내부의 Thread 중 하나가 위의 두 파일에 대해 계속적으로 CreateFileA -> CloseHandle 을 반복하여 삭제 시 재 생성하는 기능을 갖는다.

2. 스파이웨어 – 리워드 프로그램 제작자의 기소 및 Clicker 이슈

(1) 리워드 프로그램 제작자의 기소

지난 5월 인터넷 쇼핑몰 방문 경로를 조작해 40여억원의 부당이득을 챙긴 제휴마케팅 업체의 대표 등이 적발되어 불구속 기소되었다. 이들은 주로 무료프로그램의 번들 형식으로 설치되는 리워드 프로그램으로 1년이 넘는 기간 동안 5천여만 대에 자신들의 프로그램을 설치한 뒤 이용자의 쇼핑몰 방문 경로정보를 변조하는 방법으로 인터넷 광고 수수료를 부당 지급받았다고 한다. 특히 한 업체는 수억 원의 이익을 올리고도 고작 1만 2천원만 환급 해 줬다는 점을 미루어 그들이 주장하는 사용자의 동의가 얼마나 형식적이었는지를 보여준다.



[그림 1-1] 수많은 리워드 프로그램 제작사 홈페이지

(2) 온라인 쇼핑몰의 트래픽을 소진시키는 Clicker

분산서비스거부공격(DDOS)는 엄청난 분량의 데이터를 하나의 서버에만 집중적으로 전송함으로써 특정 서버의 정상적인 기능을 방해하는 것을 말한다. 지난 2월 중국의 특정 사이트를 공격하기 위한 스파이웨어가 확인된 후 국내에서도 국내 특정 온라인 쇼핑몰로 많은 트래픽을 발생시켜 정상적인 서비스를 방해하는 Win-Clicker/DDos.36864가 발견되었다. 특정 사이트를 공격하는 프로그램은 주로 대상사이트의 서비스 불능으로 이득을 노릴 수 있는 개인이나 집단에서 범죄집단에 사주해 서비스를 하는 방법이다. 가장 최근의 예로는 지난 3월 국내 모 증권사를 겨냥해 금전을 요구한 후 목적달성을 못하자 직접적인 공격을 한 사건이 있었다. DDOS 툴을 제작해 악성코드와 함께 설치한 후 온라인 쇼핑몰을 공격한다면 소규모

업체로써는 그 방어가 쉽지 않을 것으로 보인다.

(3) 교묘해지는 애드웨어

애드웨어는 그 목적인 광고 역할을 충분히 수행하기 위해 이용자에게 들키지 않고 오랫동안 설치된 상태를 유지하려는 특징이 있다. 최근에는 애드웨어가 노출하는 광고는 더욱더 진짜 같고 일부 언론사에서 배포하는 기사에 포함된 광고가 오히려 애드웨어와 같은 경우가 많이 확인되고 있다.

[그림 1-2] 애드웨어가 노출하는 광고

[그림 1-2]는 국산 Zlob이 설치하는 애드웨어 중 하나인 애드웨어 소프트사이드(Win-Adware/SoftSide.77824)에 의해 노출되는 광고이다. 이 애드웨어는 사용자의 키보드 입력을 감시 해 사용자가 포털 사이트로 접속하는 경우 각 포털 사이트의 색상과 동일한 색상을 사용해 너무 튀지 않는 방법으로 광고를 노출 시켜 애드웨어가 이용자가 애드웨어 설치 사실을 인지할 수 없게 하고 있다.

애드웨어가 정상적인 광고와 유사하게 표현하려는 노력과는 달리 정상적인 광고는 애드웨어가 노출 한 것과 다를 바 없이 사용되고 있다. 최근 한 포털사가 메인 페이지에서 기사를 선택하는 경우 포털사의 뉴스 검색 페이지가 아닌 뉴스제공 언론사의 기사 페이지를 노출 하고 있다. 이렇게 연결된 언론사 사이트는 포털과 비슷하거나 더 많은 광고를 노출 하고 있는데 일부 언론사의 경우 광고가 기사마저 덮고 있어 애드웨어가 노출하는 광고 같은 느낌을 주기도 한다.

[그림 1-3] 기사를 덮고 있는 언론사의 광고

[그림 1-3]은 다양한 방법을 이용하여 광고를 노출하고 있는 언론사의 기사들이다. 이렇게 무분별한 광고 노출은 분명 이들 업체가 수익을 위해 노력한 결과일 것이다. 그러나 이런 자유로운 광고의 노출이 이용자가 스파이웨어의 설치 사실을 인지하는데 어려움이 될 수 있다.

이용자의 PC에 적절한 사용자 동의 없이 스파이웨어가 설치되는 경우 사용자가 그 사실을 빨리 인지하지 못한다면 스파이웨어 제작자는 지속적인 수익을 올리게 될 것이다. 스파이웨어가 노출하는 광고와 각종 사이트의 광고의 구분이 점점 어려워지고 있는 상황에서 이용자

의 인지 없이 방치된 스파이웨어로 인한 문제는 광고 노출로 인한 이용자의 불편 함뿐만 아니라 여러 애드웨어가 동시에 동작하는 경우 발생할 수 있는 오작동 문제로 인한 시스템 성능을 저하시켜 사용자의 인터넷 이용습관과 같은 개인적인 정보마저도 외부로 노출될 수 있기 때문에 위험하다.

인터넷 언론 이용자는 무료로 사용하는 정보에 대한 대가로 광고 노출을 인정하고 있으며, 언론 사이트는 이 점을 십분 활용해 다양한 방법으로 광고를 노출하고 있다. 이런 광고의 다양성이 애드웨어 제작자가 이용자에게 들키지 않고 수익을 올릴 수 있는 손쉬운 길을 제공하고 있는 것이다.

3. 시큐리티 – IIS의 WebDAV 취약점 주의 요망

(1) IIS 의 WebDAV 취약점 발견, 빠른 패치 필요

5월 중순 마이크로소프트사에서는 긴급 패치를 발표하였다. 인터넷 웹 서버로 많이 사용하고 있는 IIS(Internet Information Services)에서 WebDAV를 사용할 경우에 발생하는 것이다. 이 취약점을 이용하여 인증을 우회할 수 있어, 접근제한이 된 페이지에 접근이 가능하고 임의의 파일 업로드 또한 가능해진다. WebDAV(Web-based Distributed Authoring and Versioning)는 HTTP 프로토콜의 확장 판으로 원격의 웹 서버를 통해 협업하여 파일을 수정하거나 관리할 수 있는 기능 등을 제공한다.

이번 취약점은 IIS 웹 서버의 WebDAV 플러그 인에서 발생하는 취약점으로 웹 서버로 전달된 URL 상에 존재하는 유니코드를 정확히 처리하지 못해 발생하는 것이다.

영향을 받는 소프트웨어는 아래와 같다.

- Microsoft Internet Information Services 5.0
- Microsoft Internet Information Services 5.1
- Microsoft Internet Information Services 6.0

WebDAV를 사용하지 않으면 근본적으로 이 기능을 사용하지 않는 것이 보안적인 면에선 권장한다. IIS 5.X 의 경우는 다음과 같은 방법을 통해 WebDAV의 사용을 중지할 수 있다.

1. 레지스트리 에디터 실행 (Regedit32.exe)
2. 다음 경로의 레지스트리를 찾음
   HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩W3SVC₩Parameters
3. Edit 메뉴에서 Add Value를 하여 다음의 키 값을 생성
   키 이름 : DisableWebDAV
   데이터 타입 : DWORD
   데이터 값 : 1
4. IIS 를 재시작. (IIS 재 시작 전 까지는 반영되지 않음)

이번 취약점은 제로데이 공격으로 패치 발표 이전에 취약점이 공개되었다. 물론 취약점 발표 후 마이크로소프트사에서도 보안 패치를 발표한 만큼, IIS 를 운영하는 사용자라면 보안패치를 적용하거나 WebDAV를 사용하지 않을 것을 권고한다.

(2) DirectShow의 원격코드 실행 취약점 등장.

5월에 WebDAV 제로데이 취약점이 공개되며 마이크로소프트사에서는 급하게 패치를 내 놓았다. 그런데 5월말에 또 다시 MS 사에서는 보안 권고문을 발표했다. 이 취약점은 DirectX에 존재하는 것으로 조작된 퀵타임 미디어 파일을 오픈 하는 경우 임의의 코드가 실행될 수 있다. 영향을 받는 제품은 아래와 같다

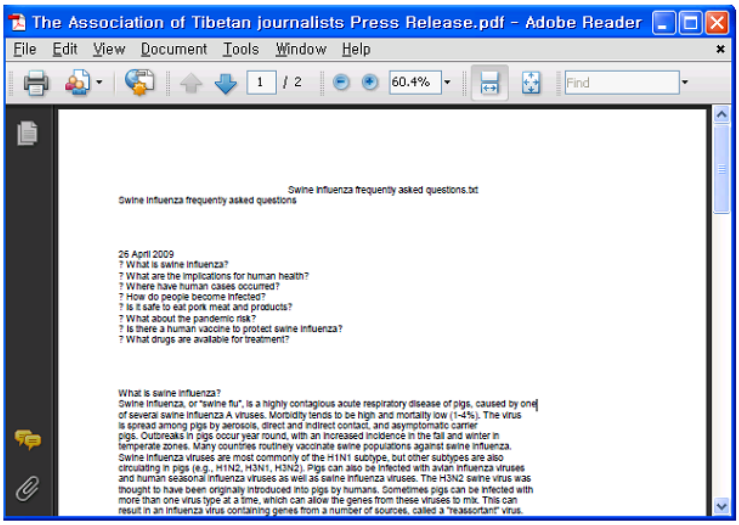
Microsoft DirectX 7.0
Microsoft DirectX 8.1
Microsoft DirectX 9.0

이 문서가 작성되는 시점까지 공식적인 보안패치는 나오지 않았다. 임시적으로 이러한 위협으로부터 보호되기 위해서는 알 수 없는 출처로부터의 퀵타임 파일은 오픈 하지 말고, 다음과 같은 방법을 통해 해당 라이브러리를 제외시킬 수 있다. 단, 이것은 해당 라이브러리와 관련한 동영상 재생에 문제를 줄 수 있으므로 필요에 따라 판단해야 한다.

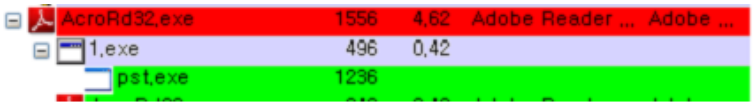
Regsvr32.exe -u %WINDIR%₩system32₩quartz.dll

(3) 신종 인플루엔자 사회공학적 기법 이용 증가 - 도메인 증가, 악성코드 배포

과거 조류 인플루엔자에 이어 멕시코에서 시작된 신종 인플루엔자에 감염된 많은 사람이 나타나며, 전 세계적으로 큰 위협이 되고 있다. 우리나라에서도 20여명이 넘는 감염자가 확인이 되었고, 이웃나라인 일본은 이 보다 훨씬 많은 감염자가 나왔다. 이렇게 사회적 이슈가 발생하면 이를 악용한 사례가 컴퓨터 네트워크 세상으로 까지 들어오고 있다. 악성코드, 스팸, 피싱 등이 해당된다. 이 분위기에 따라 Swine, Mexican, H1N1 키워드를 포함한 새로운 도메인이 우후죽순으로 등록되고 있는 것으로 나타났다. 1천여 개가 넘는 도메인이 존재하는 걸로 알려져 있다. 더불어 신종 인플루엔자의 현 상황을 악용하여 취약점을 이용한 PDF 문서도 확산되고 있어 주의가 필요하다. 다음 그림은 Adobe Acrobat Reader JBIG2 취약점을 이용하여 실행된 모습으로, “The Association of Tibetan journalists Press Release.pdf” 라는 이름으로 파일이 배포되었다.



[그림 1-4] PDF 파일의 내용 – 신종인플루엔자 내용이 담겨있다.



[그림 1-5] PDF 파일을 오픈 한 후 실행된 또 다른 프로세스

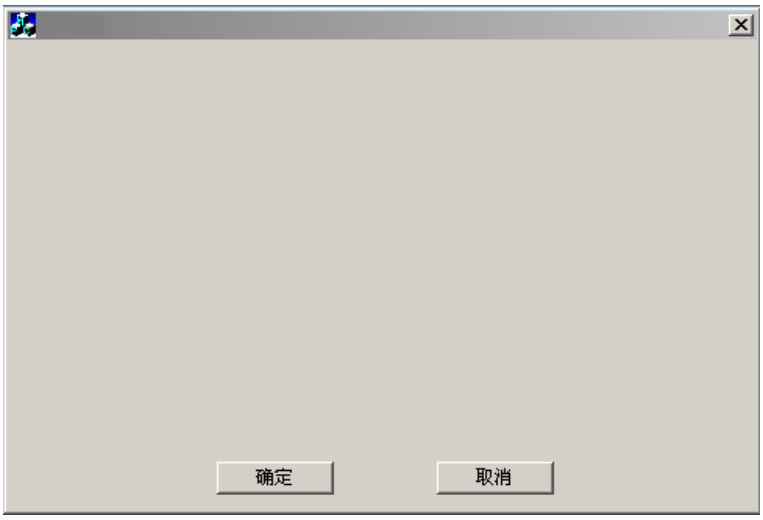
4. 중국 보안 이슈 – 사이버 머니 갈취범 징역형 및 취약한 PDF 생성기

(1) 중국 정부의 사이버 머니 갈취범에 대한 징역형 선고

5월 26일 중국 국영 언론기관인 신화통신을 통해 온라인 게임에서 사용되는 사이버 머니와 게임 아이템을 절도한 혐의로 4명이 구속되는 사건이 발생하였다. 이번에 발생한 사이버 머니와 게임 아이템 절도는 기존에 알려진 온라인 게임의 사용자 정보를 유출하는 악성코드를 이용한 것이 아니라 직접적으로 피해자를 협박해서 갈취 하였다는 점으로 인해 더욱 충격을 주고 있다. 피의자는 친구 3명과 공모하여 인터넷 카페에서 온라인 게임을 즐기고 있는 청소년들을 대상으로 협박과 폭력을 사용하여 구속되기 전까지 총 10만 위엔(한화 약 1천 8백만 원)상당의 온라인 게임에서 사용되는 사이버 머니와 아이템들을 갈취한 혐의로 구속되었다. 현재 피의자와 공범 3명 모두 중국 정부에 의해 벌금형을 선고 받았으며 이 중 1명은 주동적인 범죄 혐의가 인정되어 구속 3년 형의 징역을 선고 받았다. 이번 구속 사건으로 인해 중국 정부는 2월 전국 인민 대표 회의를 통해 개정된 컴퓨터 범죄 관련 형법을 이용해 즉각적인 형법 적용의 태도를 보여준 사례라고 할 수 있다. 그리고 이와 더불어 사이버 범죄가 온라인 상에서만 발생하는 것이 아니라 오프라인 세상에서도 발생 할 수 있다는 점을 보여준 사례라고 할 수 있다.

(2) 중국 언더그라운드에서 제작된 취약한 PDF 생성기

현재 전세계적으로 취약한 PDF 파일이나 마이크로소프트의 오피스 문서를 악용해 악성코드 감염을 시도하는 타겟 공격(Target Attack)이 증가하는 추세를 보이고 있어 이러한 문서 관련 어플리케이션 사용에 대한 많은 주의가 요구되고 있는 실정이다. 이러한 상황에서 이번 5월 중국 언더그라운드에서는 취약한 PDF을 생성 할 수 있는 생성기가 발견되었으며 많은 중국인들에 의해 악의적인 용도로 활용되고 있는 것으로 추정된다. 이번에 발견된 취약한 PDF 생성기는 지난 3월에 제작되어 이미 컴퓨터 보안 및 해킹과 관련된 중국 언더그라운드 웹 사이트에 공개적으로 제공되고 있었다.



[그림 1-6] 취약한 PDF 파일 생성기

해당 생성기는 정상적인 PDF 파일과 공격자가 지정한 악성코드를 결합시켜 어도비 아크로뱃 리더(Adobe Acrobat Reader)에 존재하는 자바스크립트 매소드(JavaScript Method)에 존재하는 원격 파일 실행 취약점을 이용해 공격자의 악성코드를 실행 시킬 수 있는 취약한 PDF 파일을 생성할 수 있도록 해준다. 해당 생성기를 통해 생성된 취약한 PDF 파일이 실행되면 표면적으로는 정상적인 PDF 파일이 실행되지만 컴퓨터 시스템에는 사용자 몰래 백그라운드 프로세스로 공격자가 지정한 악성코드를 실행하게 된다.

중국 언더그라운드에서 제작되는 다양한 취약한 PDF 파일 및 오피스 문서 생성기들은 타겟 공격이 증가 할 수 있게 만드는 원인 중 하나로 볼 수 있다. 그리고 이러한 취약한 문서 파일에 의해 발생되는 타겟 공격을 근본적으로 예방하기 위해서는 결국 해당 어플리케이션에 대해 보안 패치를 충실히 적용하여야만 할 것이다.

(3) 중국 팬톰 시큐리티 팀(Ph4ntom Security Team)의 웹진 발간

5월 초 중국 언더그라운드 보안 연구팀인 팬톰 시큐리티 팀에서 세 번째 보안 웹진을 발표하였다. 팬톰 시큐리티 팀은 중국 내에서 주기적으로 시스템 및 네트워크 보안과 관련된 연구 결과들을 정리하여 웹진 형태로 발표하는 것으로 널리 알려져 있는 팀 중 하나이다. 해당 팀의 연구 결과물을 통해서 현재 중국 언더그라운드에서는 어떠한 공격 기법에 대해서 많은 관심을 가지는지 살펴 볼 수 있는 계기로 삼을 수 있다.

[그림 1-7] 중국 언더그라운드 시큐리티 그룹 Ph4ntom의 보안 웹진

이번 발표된 웹진은 다음과 같은 시스템 보안과 관련된 내용들을 담고 있었다.

1. 0-Day 취약점 검출과 익스플로잇(Exploit) 공개
2. 리눅스 커널에 대한 인라인 후킹(Inline Hook) 기법
3. 자바 스크립트를 이용한 크로스 사이트 스크립트(Cross Site Script)공격 기법
4. 크로스 사이트 스크립트를 통한 윈도우 시스템 권한 획득 기법
5. PHP 어플리케이션을 통한 취약점 공격 기법
6. 웹 어플리케이션의 보안 전략

이번에 발표된 주제들 역시 대부분이 웹 어플리케이션과 크로스 사이트 스크립트 공격 기법에 대한 기술적 내용들이 많았다. 이러한 웹 어플리케이션과 관련된 공격 기법에 대한 연구가 활발하다는 점은 결국 중국 언더그라운드에서도 역시 웹 서버와 웹 사이트에 대한 공격에 많은 관심이 있으며 실제로도 이러한 공격 형태가 많이 증가 할 수도 있다는 사례로 볼 수 있다.

그리고 지난 MS09-002 취약점인 인터넷 익스플로러의 초기화되지 않은 메모리 손상 취약점 (CVE-2009-0075)이 중국의 한 보안 연구팀의 실수로 인해 중국 언더그라운드에 알려지게 되어 악의적인 공격 사례가 다수 발생 하였다. 이러한 점으로 인해 많은 사람들이 사용하는 어플리케이션에 대한 0-Day 취약점 검출 및 익스플로잇(Exploit) 공개 등과 관련 된 사항은 신중하게 다루어져야 된다는 글은 '중국 언더그라운드에서 취약점 발견을 통해 악의적인 공격에 활용하기 보다는 건전한 보안 연구를 중시하자' 라는 새로운 방향 제시라고도 볼 수 있다.

II. ASEC 칼럼

■ 구름 속 백신 ?! 안랩 스마트 디펜스

2009년 6월 1일 안철수연구소는 클라우드 컴퓨팅 개념의 악성코드 대응 기술인 안랩 스마트 디펜스(AhnLab Smart Defense)의 베타 테스트를 시작했다. 이 글에서는 클라우드 컴퓨팅 개념과 이를 백신에 어떻게 접목 시키는가와 이 기술의 장단점에 대해서 알아보았다..

(1) 클라우드 컴퓨팅

위키 백과에 따르면 클라우드 컴퓨팅(Cloud Computing)이란 '인터넷 기반(클라우드)의 컴퓨팅 기술을 의미한다.'라고 되어 있다.[1] 또 다른 자료에 따르면 '대용량 데이터베이스를 인터넷 가상 공간에서 분산 처리하고 이 데이터를 데스크톱 PC 등 다양한 단말기에서 불러오거나 가공할 수 있게 하는 환경이라고 한다.'[2]

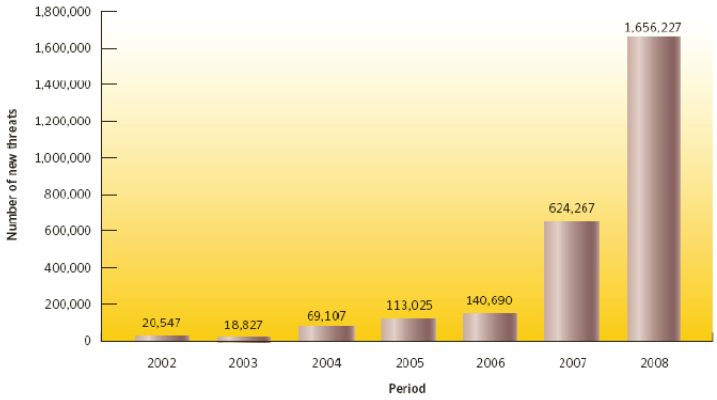
백신 업계에서 인 더 클라우드(In-the-cloud)로 불리는 이 기술은 악성코드 유무를 기존 클라이언트가 아닌 서버에서 판단해 준다. 검사 엔진 및 시그니처가 클라이언트가 아닌 외부에서 이뤄지는 것으로 주요 기능이 사용자가 볼 수 없는 구름 속에서 이뤄진다고 생각하면 된다. 일부 업체에서는 집단지성(Collective Intelligence) 개념을 이용하기도 한다. Collective Intelligence은 집단지성, 집단지능, 집단정보 수집 등으로 번역되고 있으며 '다수의 개체들이 서로 협력하거나 경쟁을 통하여 얻게 된 지적 능력의 결과로 얻어진 집단적 능력을 일컫는 용어'로 정의 된다.

(2) 악성코드 현황과 백신 업체의 대응

연구자나 업체에 따라 전체 악성코드 수는 다르지만 분명한 건 악성코드는 2004년을 기점으로 급격히 증가하고 있다.

1 http://ko.wikipedia.org/wiki/%ED%81%B4%EB%9D%BC%EC%9A%B0%EB%93%9C_%EC%BB%B4%ED%93%A8%ED%8C%85

2 http://blog.ahnlab.com/ahnlab/632



[그림 2-1] 시만텍에서 밝힌 신종 악성코드 수

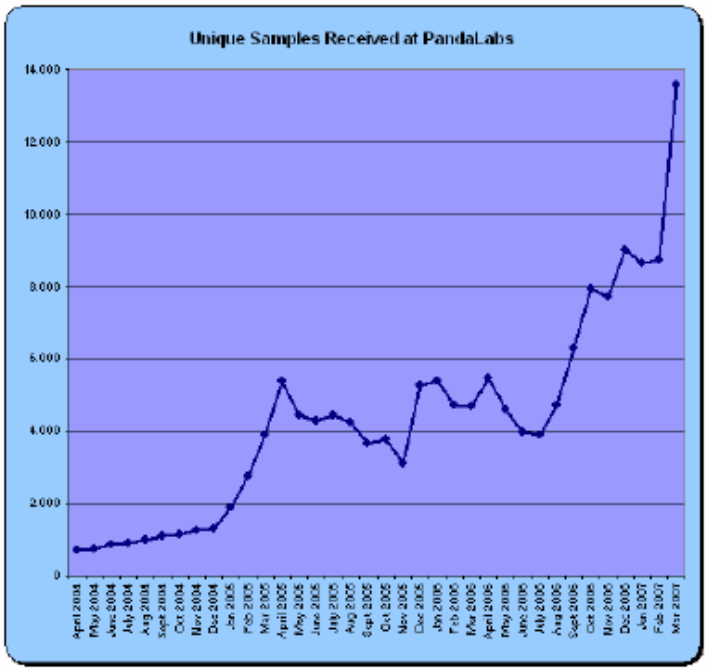
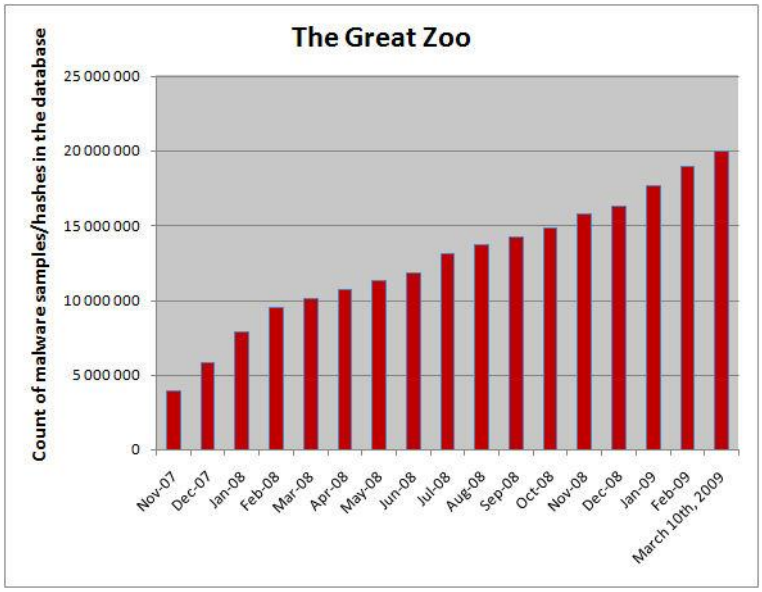


Figure 1: Unique samples received at PandaLabs 2004 to 2007

[그림 2-2] 판다 시큐리티에서 밝힌 접수 악성코드 수



[그림 2-3] 맥아피에서 밝힌 악성코드 수

2009년 6월 현재 하루에 2-3만개씩 악성코드가 발견되고 샘플 접수 – 분석- 시그니처 업데이트 – 테스트 – 배포까지 빨라도 3시간 정도 소요되는 현실상 단순 시그니처 진단법으로는 한계가 있으며 제네릭 진단법(Generic Detection), 휴리스틱 진단법(Heuristic Detection)도 어느 정도 악성코드 수가 수집되고 이를 분석 해 진단 기능을 추가하므로 역시 시간이 걸린다. 이런 대응시간 문제뿐 아니라 악성코드 증가만큼 악성코드의 지문을 담고 있는 백신 프로그램의 시그니처 파일도 비대해지고 있다.

악성코드 수명은 짧은 대신 악성코드 제작자들은 새로운 변형 악성코드를 바로 제작해 새로운 버전으로 대체하고 있다. 또한 과거 사용자들을 놀라게 하기 위해 제작된 악성코드는 파괴적인 활동, 특정적인 증상 등으로 사용자가 쉽게 알아차릴 수 있었지만 최근의 악성코드는 특정 목표를 정해 수백 명 – 수천 명 단위의 적은 시스템에 배포되고 사용자가 알아차릴 수 없게 루트킷 등을 이용해 은밀하게 활동하는 경우가 많다.

이런 악성코드 변화에 판다 시큐리티는 악성코드를 다루는 백신 업계의 변화를 다음과 같이 정리하고 있다.

(가) 첫 번째 세대: 안티 바이러스

시그니처 진단 기반의 안티 바이러스 제품이 탄생했다. 다형성, 도스에서 윈도우 악성코드, 매크로, 스크립트 등에 대한 대처가 추가된다. 악성코드 수가 증가하면서 변형들에 대해 진단하는 제네릭 검사법(Generic detection)과 휴리스틱 검사법(Heuristic detection)이 추가된

다.

(나) 두 번째 세대: 안티 멀웨어

2000년 이후 애드웨어와 사용자가 원하지 않는 프로그램 같은 기존 악성코드와는 또 다른 유형이 등장했다. 고객들의 요구와 안티 스파이웨어 제품이 나오면서 안티 바이러스 제품은 통합적인 안티 멀웨어 제품으로 발견하기 시작했다.

(다) 세 번째 세대: 사전 대응 (Proactive)

악성코드 수가 증가하면서 시그니처 기반의 진단법으로는 대처에 한계가 있어 사전 대응 개념이 도입되었다. 크게 '행동 분석(behavioral analysis)'과 '행동 차단(behavioral blocking)'으로 나뉜다. 행동 분석은 실행되는 프로그램을 감시하면서 위험한 행동에 대해 사용자 동의를 받는다. 행동 차단은 워드, 파워포인트, 엑셀, 엑세스, 아크로뱃 리더, 윈도우 미디어 플레이어 등과 같은 프로그램에서 발생하는 익스플로잇 코드가 실행되는걸 차단하는 역할을 한다.

행위기반에 기초한 특정 행동 차단은 초기 컴퓨터 바이러스가 등장했을 때도 존재했지만 사용자가 일일이 판단 해야 하는 단점이 있어 사용자의 판단을 최소화하는 약간의 시그니처 개념도 포함되어야 한다. 이외 사전 대응을 위해서는 언패킹, 루트킷 진단 등의 기술도 필요로 한다. 사전 대응을 통해 시중에 퍼진 약 80%의 악성코드를 차단할 수 있다는 통계도 있다. 하지만, 행위기반의 사전 대응 방식은 사용자의 판단이 상당부분 개입되어야 하므로 제품을 사용하는 절대 다수인 컴퓨터 지식이 부족한 일반인에게 적용하기에는 무리가 따른다.

(라) 네 번째 세대: 집단지성(Collective Intelligence)

대부분의 사용자들이 보안에 대해서 잘 모르기 때문에 사용자에게 허용 여부를 물어봄으로 초보자가 이용하는데 한계가 있다. 이에 비해 집단 지성은 사용자 시스템에 에이전트를 설치해 생성되는 파일 정보를 수집해 수집된 정보를 바탕으로 허용 여부를 판단한다.

기존의 악성코드 샘플을 보내고 분석하고 시그니처를 업데이트하는데 시간이 오래 걸리는데 이런 문제를 해결하기 위해 집단지성을 이용하면 '자동수집(Automated malware collection)' -> '자동분류(Automated malware classification)' -> '자동제거(Automated malware remediation)'를 자동으로 할 수 있다. 판다 시큐리티는 2007년 이 시스템을 이용해 94.4%의 악성코드를 처리했다고 한다.

클라우드 백신도 이런 집단지성으로 볼 수 있다.

집단 지성은 개별 시스템에는 별도의 시그니처가 필요 없으며 사용자 시스템에서 파일의 지문(해쉬 값)만 얻어 중앙 서버로 전달하고 접수 받지 못한 파일은 중앙으로 보내면 자동적으로 분류가 된다.

이런 집단 지성을 사용하기 위해서는 몇 가지 제한된 조건이 필요하다.

- 서비스 제공 업체에서 정상 파일/악성 파일에 대해 데이터 베이스화 해야 함
- 새로운 악성코드가 집단지성 에이전트가 설치된 시스템에 유입되어야 함
- 형태가 변하지 않는 악성코드로 한정 (바이러스 형태는 진단이 어려움)
- 자동 분석 및 처리가 가능한 샘플

(3) 클라우드 백신

백신 업계의 클라우드 백신 시도는 2007년으로 거슬러 올라간다. 현재까지 클라우드 기술을 이용하는 제품이나 기술은 시만텍, 맥아피, 트렌드, F-시큐어, 판다 시큐리티로 총 5개 사였다.

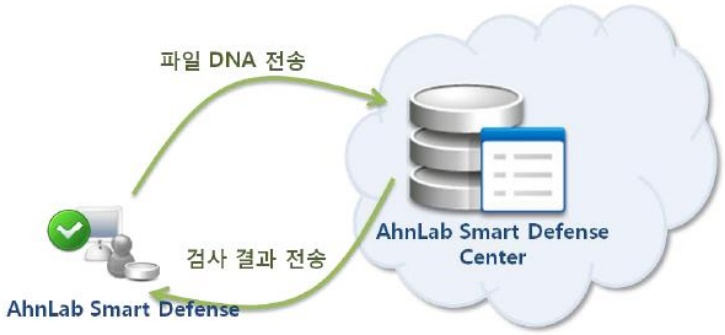
널리 알려진 판다 시큐리티는 집단 지성 에이전트를 400만 개의 센서를 설치해 두었으며 이 시스템은 수 백 만개의 악성코드뿐 아니라 정상 파일에 대한 정보도 담고 있다고 한다. 판다 시큐리티는 액티브스캔 2.0(구 나노스캔)에 해당 기술을 접목 시켰다. 이후 2009년 5월 판다 시큐리티는 자사의 클라우드 백신 베타버전을 출시한다.

[그림 2-4] 판다 클라우드 백신 제품

안철수연구소는 2009년 6월 1일 세계에서 6 번째로 클라우드 기술을 이용한 백신 프로그램을 공개한다.

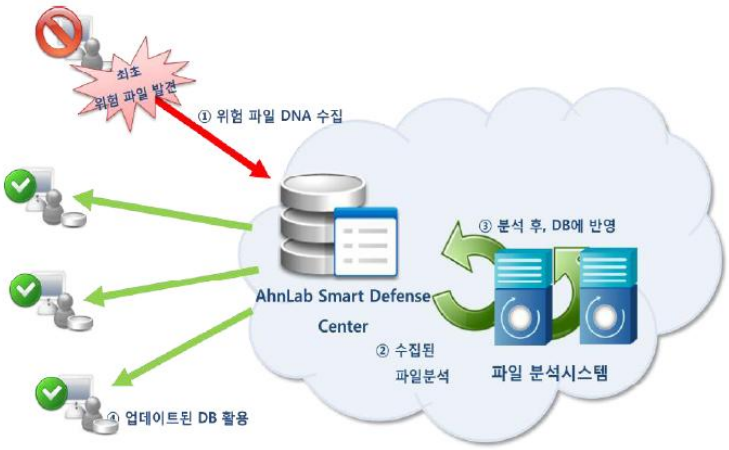
[그림 2-5] 안랩 스마트 디펜스

안랩 스마트 디펜스가 시스템에 존재하는 파일에서 고유의 DNA를 수집해 안랩 스마트 디펜스 센터로 보내 검사 결과를 받는다. 안랩 스마트 디펜스 센터가 구름 역할을 한다.



[그림 2-6] AhnLab Smart Defense 구상도

새로운 파일의 경우 안랩 스마트 디펜스 센터로 전송되고 파일을 자동 분석해 악성으로 판단되면 즉각 반영해 다른 사용자의 시스템은 보호받게 된다.



[그림 2-7] AhnLab Smart Defense Center

(4) 클라우드 백신의 장단점

클라우드 백신의 장점은 다음과 같다.

(가) 첫째, 진단율 향상

악성코드 뿐 아니라 정상 파일도 미리 데이터베이스화하며 시그니처 기반 뿐 아니라 다양한 진단 방식을 적용할 수 있어 기존 기존 시그니처 기반의 제품보다 향상된 진단율을 볼 수 있다. 안철수연구소에서도 자체 테스트 결과 20% 정도의 진단율 향상 효과가 있었다.

(나) 둘째, PC 리소스 점유율 감소 및 검사속도 향상

시그니처 기반의 백신 프로그램은 설치된 시스템에 모든 정보를 가지고 있어 많은 시스템 자원을 소모한다. 또한, 하나의 파일에 대해서 모든 시그니처와 비교해야 하므로 진단 속도도 느리다. 하지만, 클라우드 백신의 경우 주요 정보는 서버에 보관되며 단지 파일 DNA 정보만 보내면 되므로 적은 시스템 자원을 사용하고 진단 속도가 빠르다.

(다) 셋째, 업데이트 관리 이슈 해결

클라이언트에는 별도의 시그니처 업데이트가 필요 없이 서버에서 시그니처 작업이 진행되면 모든 시스템에 일괄 적용되므로 클라이언트에서 별도의 시그니처 업데이트 작업이 필요 없다.

(라) 넷째, 보다 빠른 대응

많은 클라우드 백신은 알려지지 않은 파일을 수집하는 기능이 있다. 이전에 사용자가 의심스러운 샘플을 찾아 신고해야 하는 번거로움 없이 샘플 처리가 이뤄져 보다 빠른 대응을 할 수 있다.

반면 클라우드 백신의 단점도 존재한다.

(가) 첫째, 네트워크 단절 시 이용 불가

클라우드 백신은 네트워크가 반드시 연결되어 있어야 한다. 폐쇄망의 경우 사용이 제한적인데 이 경우 폐쇄망을 연결하는 컴퓨터에 서버를 두면 해결되지만 네트워크 연결이 아예 단절된 시스템에서는 이용할 수 없다.

(나) 둘째, 서비스 방해

악성코드가 클라우드 백신이 서비스로 통신하는 것만 방해해도 진단을 방해할 수 있다. 단, 이 경우 악성코드가 시스템에 감염되어 있어야 하는 가정이 필요하다. 감염 시 보안 프로그램을 방해하는 기능은 클라이언트에 설치되는 제품에서도 발생하는 문제이다. 네트워크 패킷 위변조를 방지하기 위해 네트워크 패킷 위변조 검증 작업이 필요하다.

(다) 셋째, 미진단 악성코드 존재

현재 나와있는 클라우드 백신은 대체로 파일에서 고유의 값을 추출해 전송한다. 따라서, 파일을 감염시키는 바이러스나 다형성 악성코드의 경우 이런 고유 값을 쉽게 얻을 수 없어 악성 판단이 어렵다. 하지만, 현재 존재하는 악성코드의 80-90%가 형태가 일정한 트로이목마로 클라우드 백신이 기존 제품의 대체가 아닌 약점 보완 측면에서 볼 필요가 있다.

(라) 넷째, 오진 문제

중앙 서버에는 해당 업체에서 수집한 정상 파일 정보와 악성코드 정보를 가지고 있으며 사용자에게 받은 정보를 이 파일에서 추출한 정보와 비교하고 새로운 파일은 자동 분석으로 분류된다. 분류 방법은 각 사의 고유의 방식으로 이뤄지지만 정상 파일이 악성코드로 분류되거나 반대로 악성코드인데 정상 파일로 분류되어 있을 수 있다. 또 클라우드 백신의 경우 시그니처 기반 제품보다 악성 판정이 대체로 느슨한 편이라 오진 확률이 높다.

이외 네트워크 패킷 내용이 해독 당하면 허위 보안 프로그램에서 역으로 이용할 수 있으며

많은 시스템이 사용할 경우 서버에 과부하가 발생할 수 있다.

(5) 향후 전망

클라우드 백신은 장단점이 모두 존재하며 기존 클라이언트 제품을 전부 교체하기는 어려울 것으로 보인다. 하지만, 이들 기술의 적용으로 시그니처 기반 제품과의 상호 보완 및 사전 대응측면에서 큰 역할을 할 것으로 기대된다. 하지만, 클라우드 백신에 대한 회의적인 시각도 존재한다. 2009년 바이러스 블루틴 컨퍼런스(Virus Bulletin Conference)에서는 클라우드 백신이 해결책이 아니라는 발표가 있을 예정이다.[1] 주요 내용은 사전대응(proactive)이 아니며 대응 시간을 좀 더 단축한 것에 불과하며 진단율이 올라간다고 해도 오진이 증가하는 문제점을 지적할 예정이다. 클라우드 백신의 미래는 현재 진행 중이다.

[1] http://www.virusbtn.com/conference/vb2009/abstracts/MorgensternMarx.xml

III. 이달의 통계

1. 악성코드

(1) 5월 악성코드 통계

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

[표 3-1] 2009년 4월 악성코드 피해 Top 10

순위		악성코드명	건수	비율
1	new	Win-Trojan/Bho.372224	17	15.7%
2	new	Win-Trojan/Agent.49664.HR	13	12.0%
3	new	Win-Trojan/Rimecud.39936	12	11.1%
4	new	Win-Trojan/Downloader.22016.HL	10	9.3%
4	new	Win-Trojan/Downloader.18432.LV	10	9.3%
4	new	Win-Trojan/Agent.40448.IX	10	9.3%
5	new	Win-Trojan/Xema.48040	9	8.3%
5	new	Win-Trojan/SpamMailer.39425	9	8.3%
5	new	Win-Trojan/OnlineGameHack.23040.CX	9	8.3%
5	new	Win-Trojan/Downloader.34936	9	8.3%
합계			108	100.0%

[표 3-2] 2009년 5월 악성코드 피해 Top 10

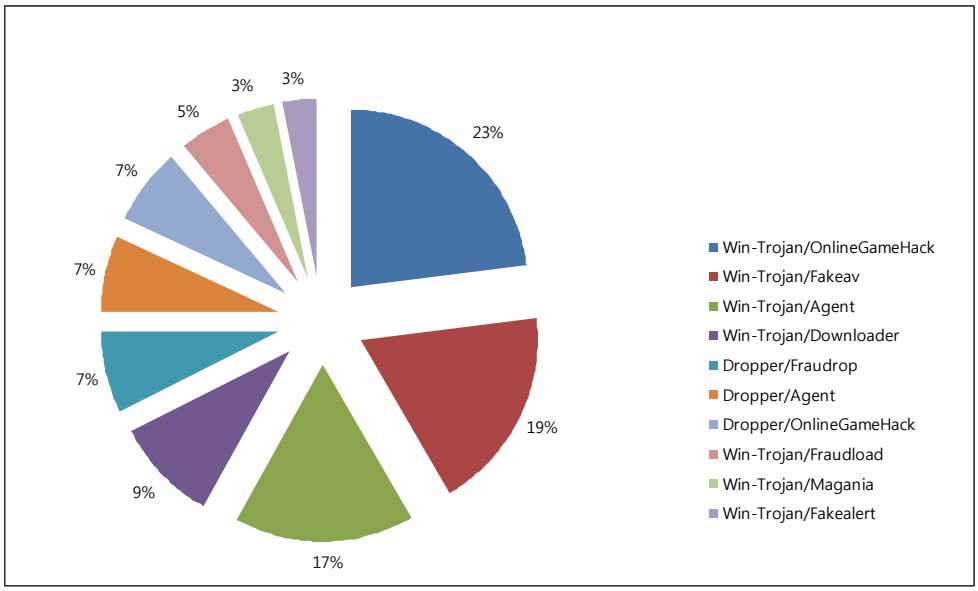
[표 3-1]은 2009년 4월 악성코드 피해 Top 10이며, [표 3-2]는 2009년 5월 악성코드로 인한 피해 Top 10을 나타낸 것이다.

지난달과 비교하여 두드러진 차이점은 트로이목마가 Top 10을 모두 차지했다는 점이다. 또한 악성코드 활동 주기가 짧아짐에 따라 전월과 동일한 진단명은 Top 10에 확인되지 않는다. 특히, 4월에는 드롭퍼가 4개나 Top 10에 포함되어 있었으나 5월에는 드롭퍼가 순위에 들지 못했다. 하지만 아래 대표 진단명에 볼 수 있듯이 드롭퍼가 감소된 것은 아니다. 근래 드롭퍼나 다운로더가 기승을 부리며 IE를 통해 다수의 악성코드를 다운로드 받아 시스템에서 악의적인 기능을 수행한다. 그 중, 'Win-Trojan/Rimecud.39936'의 경우 근래 악성코드가 주로 이용하는 윈도우 휴지통인 Recycler폴더에 악성코드를 생성해두고 자동 시작되도록 서비스에 등록시킨 뒤 IE를 통해 다수의 악성코드를 다운로드 받아 실행시켜 최종적으로 'Malware Doctor'라는 허위 안티 스파이웨어를 설치함으로써 사용자들을 유혹해 결제로까지 유도해 금전적인 목적을 취하고 있다.

아래의 표와 그림은 대표 진단명을 기준으로 변형들을 묶어 통계를 뽑은 것이다. 개별 악성코드 통계보다 전체적인 악성코드 감염 양상을 알 수 있다. 이는 많은 변형의 출현 및 빠른 악성코드 엔진대응으로 개별 악성코드 생명주기가 짧아져서 이를 보강하기 위해 참고 작성된 것이다.

순위		악성코드명	건수	비율
1	↑2	Win-Trojan/OnlineGameHack	568	23.1%
2	↑3	Win-Trojan/Fakeav	457	18.5%
3	↓2	Win-Trojan/Agent	407	16.5%
4	↑2	Win-Trojan/Downloader	232	9.4%
5	↑5	Dropper/Fraudrop	182	7.4%
6	↑3	Dropper/Agent	174	7.1%
7	-	Dropper/OnlineGameHack	170	6.9%
8	↓6	Win-Trojan/Fraudload	115	4.7%
9	new	Win-Trojan/Magania	82	3.3%
10	new	Win-Trojan/Fakealert	77	3.1%
합계			2,464	100.0%

[표 3-3] 2009 5월 악성코드 대표 진단명 Top 10

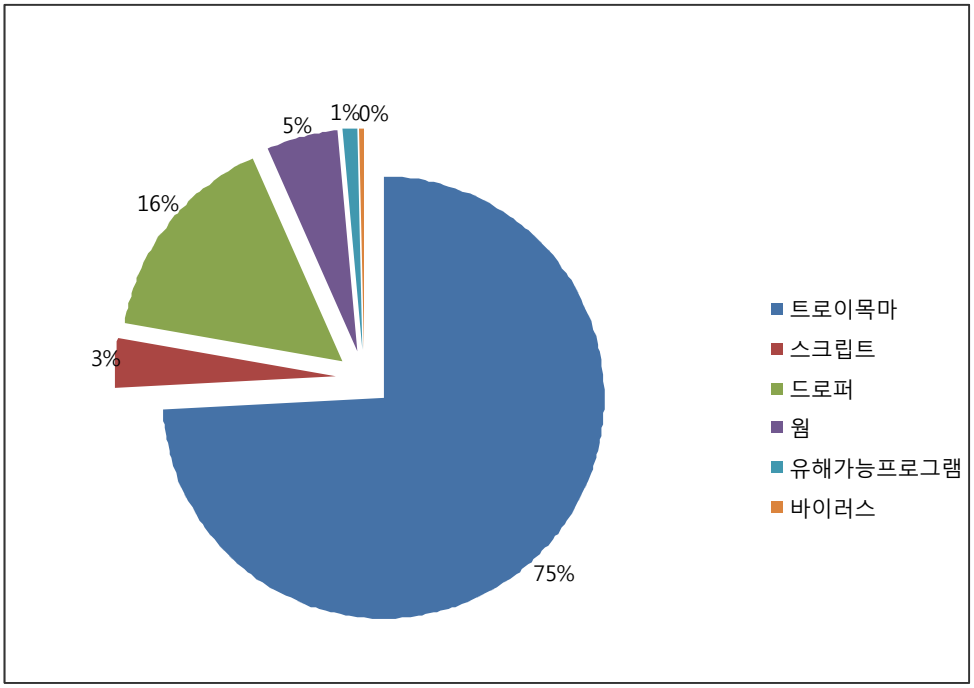


[그림 3-1] 2009년 5월 악성코드 대표 진단명 Top 10

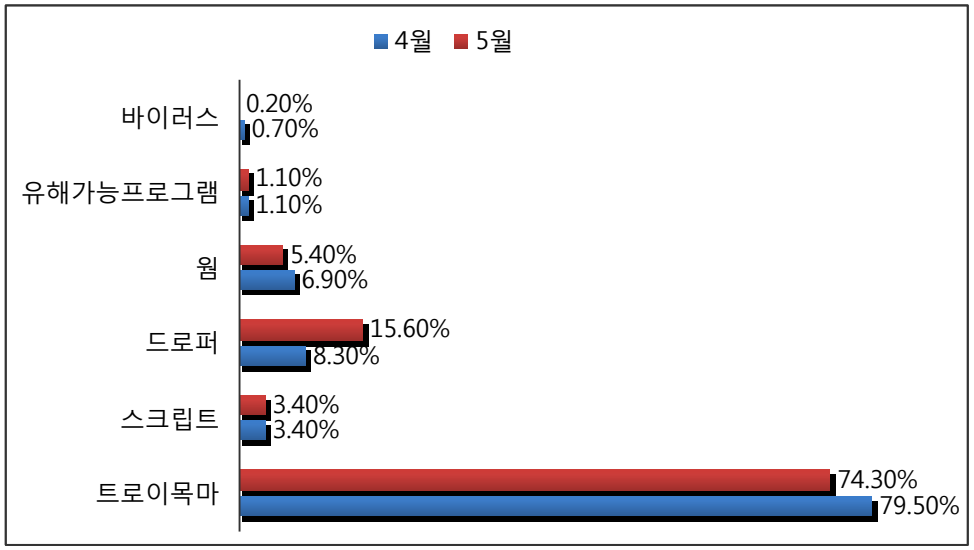
[표 3-3]과 [그림 3-1]은 2009 년 5 월 악성코드의 대표 진단명을 기준으로 유형별 피해 순위 Top 10 을 나타내고 있다.

5월 악성코드 대표 진단명 Top 10을 살펴보면 OnlineGameHack이 여전히 강세를 보이며 전체 약 33.3%(1위, 7위와 9위)의 비율을 차지하고 있다. Downloader의 경우 2단계 상승된 4위를 기록하였으며, 지난달 강세에 이어 FakeAV, Fraudrop, Fraudload, Fakealert 등으로 불리는 허위 안티 스파이웨어류가 전체의 33.7%를 차지하였다. 지난달(46.9%)에 비해 다소 감소된 수치이나 여전히 다양한 변종이 발생되므로 사용자 주의가 필요하다. 이를 예방하기 위해서는 게시판, 자료실, E-mail 등 의심되는 파일은 가급적 실행하지 말고 감염되었다 하더라도 허위 안티 스파이웨어임을 인지하여 백신프로그램을 이용한 진단/치료 및 [바이러스 신고센터]로 신고하여 피해를 줄일 수 있다.

아래의 [그림 3-2]는 2009년 5월 전체 악성코드 유형별 피해신고 건수를 나타내고 있는 그래프이다. 트로이 목마 프로그램은 74.3%로 다른 악성코드보다 월등히 많은 비율을 차지하고 있으며, 드롭퍼와 웜이 각각 15.6%와 5.4%, 그 뒤를 이어 스크립트 3.4%, 유해가능 프로그램이 1.1%를 차지하고 있다. 저번 달과 동일하게 바이러스는 0.2%로 극히 낮은 비율을 유지하고 있다.

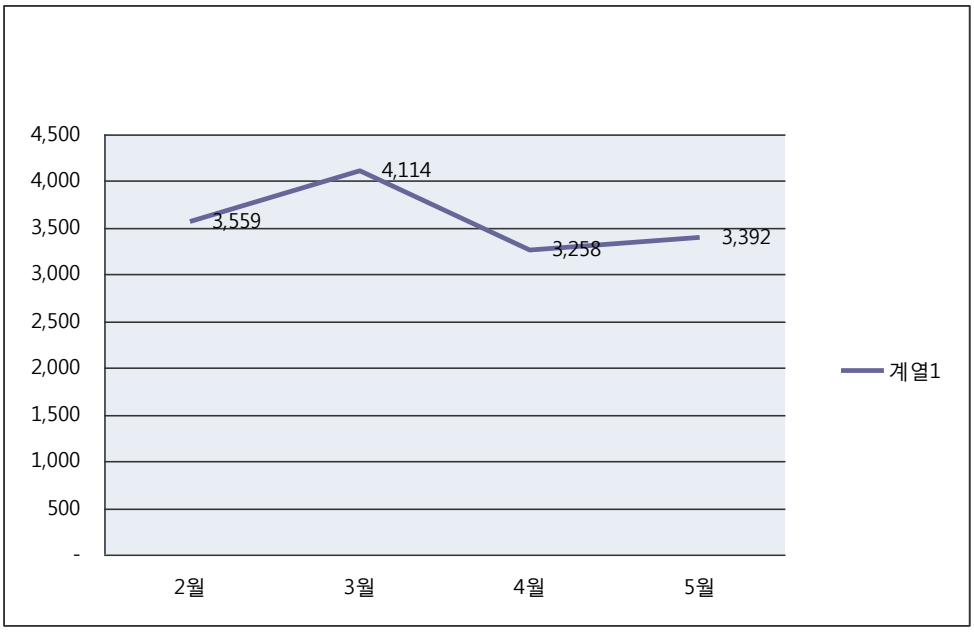


[그림 3-2] 2009년 5월 악성코드 유형별 피해신고 비율



[그림 3-3] 2009년 5월 악성코드 유형별 피해신고 비율 전월 비교

위의 [그림 3-3]은 전월과 비교한 악성코드 유형별 피해신고를 나타낸 것이다. 증가한 것은 드롭퍼의 경우 전월과 비교하여 15.6%가 증가하였으며, 트로이목마는 74.3%로 전월에 비해 5.2%가 다소 줄어들었다. 웜은 5.4%로 전월에 비해 소폭 감소하였으며, 스크립트, 유해가능프로그램과 바이러스는 약간의 수치 차이는 있겠으나 전월과 많은 차이가 없었다.



[그림 3-4] 월별 피해신고 건수

[그림 3-4]는 월별 피해신고 건수를 나타내는 그래프로 2월부터 피해가 증가하였으나 4월부터 엔진에 반영된 샘플수가 전달에 비해 약 2배정도 증가됨에 따라 사전 대응이 높았던 것으로 추정된다. 참고로, 5월에 반영된 엔진은 4월 대비 웜은 4,441개에서 4,140개로 감소, 트로이목마는 98,990개에서 105,878개로 증가하였다.

악성코드의 유형이 점차 은폐형 악성코드 및 최신 취약점을 이용하는 악성코드가 늘어남에 따라 피해를 막기 위해서는 최신 보안패치와 함께 최신 버전의 백신프로그램으로 주기적으로 검사하는 습관이 필요하다.

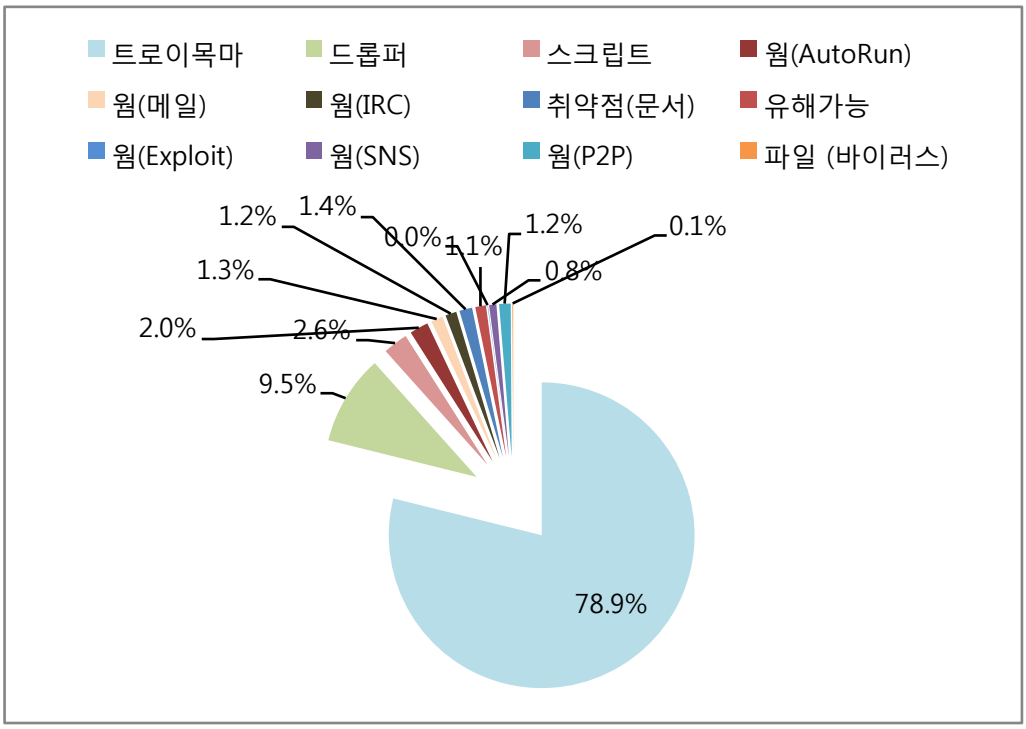
(2) 국내 신종(변형) 악성코드 발견 피해 통계

5월 한 달 동안 접수된 신종(변형) 악성코드의 건수 및 유형은 [표 3-4]과 같다.

월	트로이목마	드롭퍼	스크립트	웜	파일	유해가능	합계
03 월	1385	237	80	151	1	14	1868
04 월	1700	202	92	190	1	24	2209
05 월	1780	211	58	143	2	25	2220

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

이번 달 발견, 보고된 신종 및 변형 악성코드는 전월 대비 큰 차이는 보이지 않는다. 다만 트로이목마와 PDF 취약점을 이용하는 악의적인 PDF 문서가 다수 보고 되었다. 특히 온라인 게임의 사용자 계정을 탈취하는 형태의 악성코드가 전월 대비 큰 폭으로 상승하였다. 반면 보통 해당 악성코드가 발견 되면 동반 상승하였던 스크립트 유형은 오히려 전월 대비 37% 감소 하였다. 웜 유형 또한 전월 대비 25% 감소 하였다. 그러나 올 2월부터 발견되기시작한 P2P 웜인 Win32/Palevo.worm이 새롭게 발견되어 P2P 웜 유형의 상승을 이끌었다.
다음은 이번 달 악성코드 유형을 상세히 분류하였다.



[그림 3-5] 2009년 05월 신종 및 변형 악성코드 유형

이번 달 트로이목마 유형의 특징은 우선 온라인 게임의 사용자 계정정보를 탈취하는 형태의 악성코드가 큰 폭으로 상승한 것이다. 그리고 지난달과 마찬가지로 커널 스팸 메일러인 Win-Trojan/Rustock 변형이 사용자들로부터 자주 보고되는 등 기승을 부렸다. 또한 올해부터 지속적으로 변형이 보고되었던 Win-Trojan/Bagle 경우도 그 수는 작지만 사용자들로부터 다수 보고가 되어 피해문의가 끊이지 않았다.

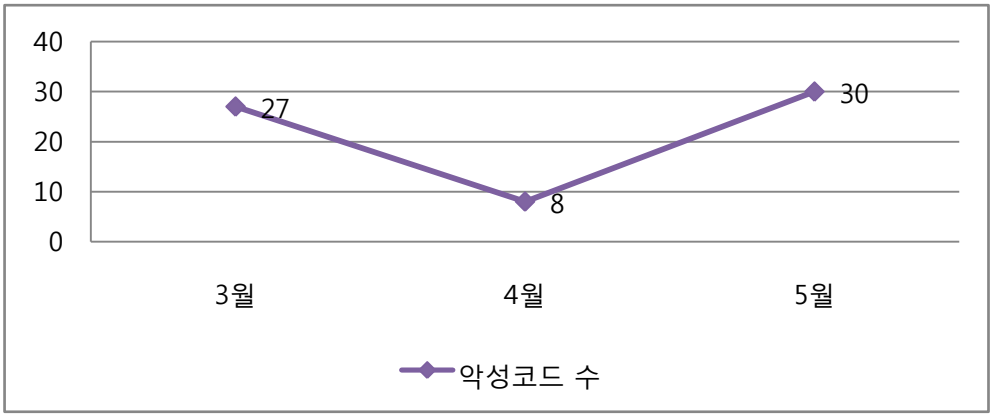
드롭퍼 유형은 소폭 증가 하였지만 그 영향은 미비하다. 역시 온라인 게임의 사용자 계정 정보를 탈취하는 형태가 소폭 증가했으며 그 수는 작지만 국산 메신저로 전파되는 악성코드 변형이 보고되었다. 해당 악성코드는 RARSFX 형태로 되어있고 실행 후 압축이 풀리면서 온라인 게임의 사용자 계정정보를 탈취하는 악성코드를 설치한다. 올해 들어 자주 보고되고 있는 국산 메신저를 통해서 전파되는 악성코드는 앞으로도 악성코드 전파 및 메신저 피싱 등

에 주의가 요구 될 만큼 사용자들의 주의를 기울일 필요가 있다.

스크립트 유형은 37% 감소 하였는데 그 이유는 명확하지 않다. 일반적으로 온라인 게임 관련 악성코드가 증가하면 반대로 상승하는 경향이 강했지만 최근 들어서는 그 논리가 무색할 만큼 다른 양상을 보이고 있다. 현재 대부분의 악성코드 유입 경로가 취약한 웹 브라우저를 이용하여 악의적인 웹 사이트나 취약한 웹 사이트를 방문하면 감염될 정도로 메일을 제치고 대표적인 악성코드 감염 경로가 되어버렸다. 마치 웹은 지뢰밭이란 표현이 사용될 만큼 현재 웹은 그다지 안전하지 못한 공간이 되어버렸다. 불행 중 다행이라면 악성코드 감염에 매우 오래전에 알려진 취약점이 가장 많이 사용되며 최근 취약점은 비교적 잘 사용되지 못한 것을 알 수 있다. 그러나 악성코드 제작자들은 여러가지 취약점을 복합적으로 사용하거나 오래된 취약점과 신규 취약점 역시 복합적으로 사용하기 때문에 다양한 방법으로 사용자 시스템을 공격하려고 한다.

웜 유형은 전월 대비 25% 감소 하였다. 특징으로는 취약점을 이용하여 전파되는 Win32/Conficker (이하 컨피커 웜) 웜 변형이 전월과 다르게 단지 1건만 보고 되었다. 컨피커 웜이 더 이상 왕성한 활동을 하지 않지만 가끔 기존 변형 중에서 Generic 진단을 피하는 형태가 보고 되었을 뿐 새로운 변형이 보고되지 않았다. 반면 Win32/Palevo.worm라고 명명된 P2P 웜은 지난 3월부터 조금씩 보고되기 시작 하더니 이번 달은 전체 악성코드 1.2% 를 차지할 만큼 다수 보고되었다. 해당 웜은 휴지통 폴더에 자신을 복사하며 이동식 디스크에도 자신을 복사하며 잘 알려진 P2P 프로그램의 공유 폴더에 자신의 복사본을 생성한다.

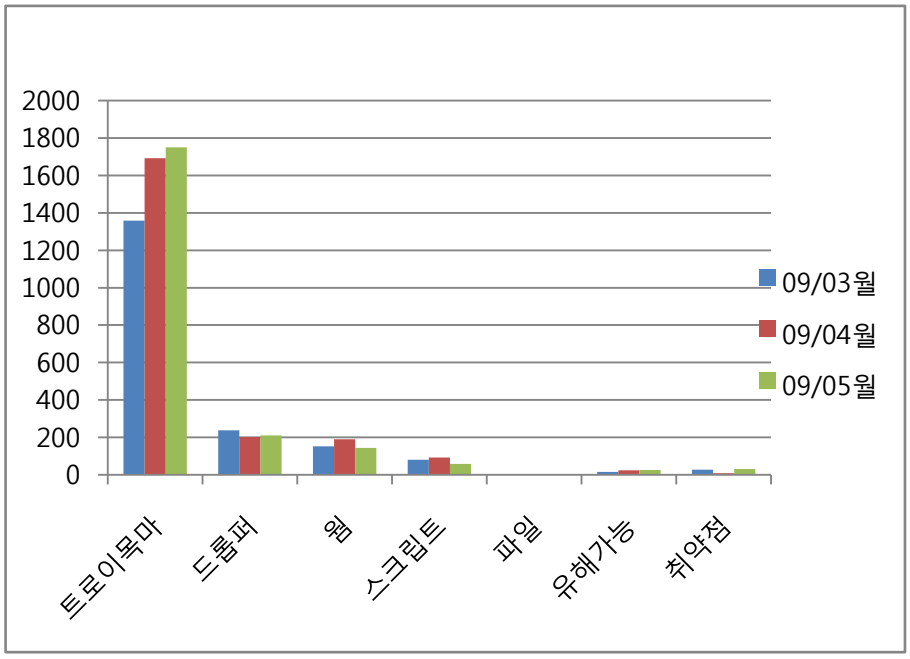
취약점 유형의 악성코드의 경우 이번 달 PDF와 SWF 취약점을 악용한 형태가 주를 이룬다. 이 둘 파일의 취약점은 모두 기존에 알려진 형태이다. 알려진 취약점을 이용하는 악의적인 문서가 자주 보고 되고 있다면 아직까지도 보안 패치를 적용하지 않는 사용자들이 많이 있다라는 것을 보여준다. 다음은 최근 3개월간 취약점이 포함된 문서의 현황이다.



[그림 3-6] 2009년 최근 3개월간 취약점 문서 현황

전월의 경우 3월 대비 적은 수가 발견 되었지만 이번 달 경우 다시 3월 대비 정도로 상승하였다. 작년 말부터 PDF 취약을 이용한 악성코드가 증가하고 있으므로 이러한 추세는 앞으로도 이어질 전망이다. 참고로 PDF 취약점의 경우 내부에 자바 스크립트가 포함되어 있으며 PDF 뷰어의 기능에서 자바 스크립트를 자동으로 실행되도록 하는 기능이 기본값이므로 이 옵션만 비활성화함으로써 취약한 문서 내 악성코드의 실행을 막을 수 있는 임시방편이 있기도 하다. 그러나 근본적으로는 취약점을 패치하는 것이며 웹, 메일, 메신저 등으로 받은 문서 파일에 대해서는 주의를 기울여야 한다.

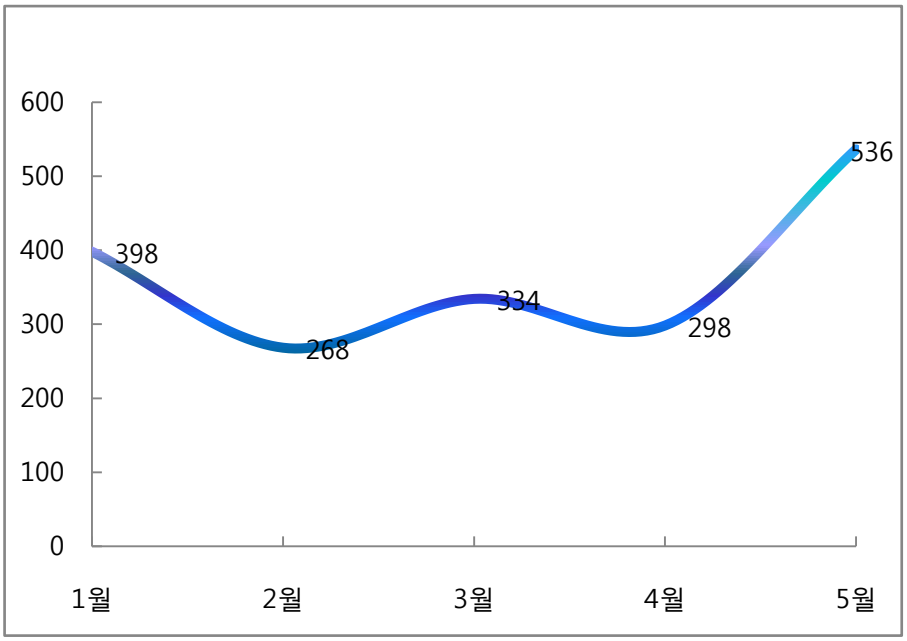
다음은 최근 3개월간 신종 및 변형 악성코드 분포이다.



[그림 3-7] 2009년 최근 3개월간 악성코드 분포

이번 달 경우 최근 3개월간을 통틀어 가장 많은 악성코드가 보고 되었다. 트로이목마와 드롭퍼 그리고 취약점 관련 문서파일이 전월 대비 소폭 증가 하였다. 웜 유형은 전월 대비 감소하였으나 특정 P2P 웜이 다수 발견되기도 하였다. 스크립트 유형은 줄었지만 이와 연관이 깊은 온라인 게임의 사용자 계정정보를 탈취하는 악성코드의 경우 전월 대비 증가함을 알 수 있었다. 트로이목마 유형 중에서는 스팸 메일러가 일반 사용자들에게 큰 피해를 주었으며 대부분 다수의 악성코드를 설치하여 다른 악성코드들과 중복 감염되어 있는 형태로 발견 되었다. 실행 파일을 감염시키는 바이러스의 경우 기존의 Win32/Kashu.B와 Win32/Virut.F 변형이 보고 되었다.

다음은 온라인 게임의 사용자 계정을 탈취하는 악성코드의 추세를 살펴보았다.



[그림 3-8] 온라인 게임 사용자 계정 탈취 트로이목마 현황

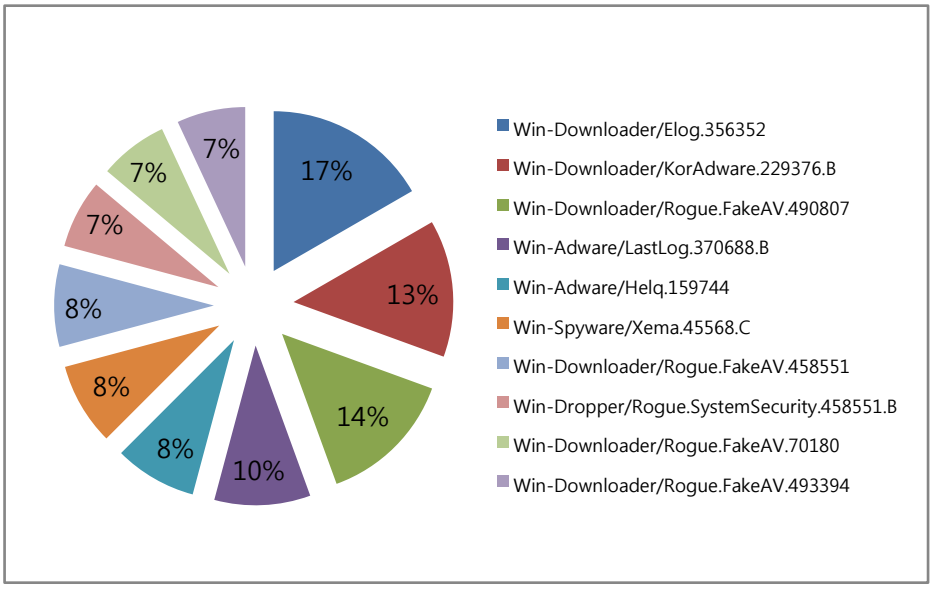
이번 달 해당 악성코드는 전월 대비 80% 가까운 증가율을 보이고 있다. 이 악성코드가 급격히 증가한 원인에 대해서는 명확하지 않다. 분명한 것은 해당 악성코드의 외형과 내형은 지금까지의 형태와 별반 다르지 않다는 것이다. 어떠한 경로로 사용자로부터 많은 수가 보고되었는지에 대한 의문은 남는다. 웹 이외에는 메신저를 통한 감염이라던가 일부 악성코드의 경우 자체 업데이트 및 다운로드 기능을 이용하기도 한다. 따라서 다른 온라인 게임핵을 설치하면서 시스템에 다수의 악성코드가 감염된 경우도 예상해 볼 수 있겠다.

2. 스파이웨어

(1) 5월 스파이웨어 통계

순위		스파이웨어 명	건수	비율
1	New	Win-Downloader/Elog.356352	12	17%
2	New	Win-Downloader/KorAdware.229376.B	10	14%
3	New	Win-Downloader/Rogue.FakeAV.490807	10	14%
4	New	Win-Adware/LastLog.370688.B	7	10%
5	New	Win-Adware/Helq.159744	6	8%
6	New	Win-Spyware/Xema.45568.C	6	8%
7	New	Win-Downloader/Rogue.FakeAV.458551	6	8%
8	New	Win-Dropper/Rogue.SystemSecurity.458551.B	5	7%
9	New	Win-Downloader/Rogue.FakeAV.70180	5	7%
10	New	Win-Downloader/Rogue.FakeAV.493394	5	7%
합계			72	100%

[표 3-5] 2009년 5월 스파이웨어 피해 Top 10



[그림 3-9] 2009년 5월 스파이웨어 피해 Top 10

2009년 5월 스파이웨어 피해 Top 10에서는 다운로더 이로그(Win-Downloader/Elog), 다운로더 코애드웨어(Win-Downloader/KorAdware)와 같은 국산 애드웨어로 인한 피해가 증가

한 것으로 나타났다. 다운로더 코애드웨어의 최초 전파방법은 정확하게 밝혀지지 않았으나, 사용자의 정상적인 동의없이 번들 프로그램을 함께 설치하는 국산 무료소프트웨어 설치 시 함께 설치되는 것으로 추정된다. 다운로더 코애드웨어가 사용자의 시스템에 설치되면, 웹사이트에서 설치목록을 다운로드 받아 시스템에 설치할 수 있기 때문에 많은 종류의 애드웨어가 설치될 수 있다. 이렇게 설치되는 애드웨어는 수시로 사용자의 키워드를 감시해 관련 광고를 노출하거나 대형 포털 사이트의 광고와 유사한 방법으로 광고를 노출한다. 이러한 광고로 인해 사용자의 불편이 증가할 수 있으며, 인터넷 익스플로러의 비정상 종료 등의 문제점이 발생할 수 있다.

순위	대표 진단명	건수	비율
1	Win-Downloader/Rogue.FakeAV	1648	59%
2	Win-Downloader/FakeAlert.RogueAnti	775	28%
3	Win-Downloader/Rogue.SystemSecurity	206	7%
4	Win-Spyware/Crypter	47	2%
5	Win-Spyware/Xema	21	1%
6	Win-Adware/BestLink	18	1%
7	Win-Adware/IEShow	17	1%
8	Win-Adware/Rogue.FakeAV	16	1%
9	Win-Downloader/KorAdware	15	1%
10	Win-Downloader/Elog	12	0%
합계		**2775**	**100%**

[표 3-6] 5월 대표 진단명에 의한 스파이웨어 피해 Top 10

[표 3-6]은 변형을 고려하지 않은 대표 진단명을 기준으로 한 피해 건수이다. 5월 역시 지난 4월과 유사하게 1648건의 피해신고가 접수된 다운로드 로그 페이크에이브이(Win-Downloader/Rogue.FakeAV)가 가장 많이 접수되었다. 가짜백신 설치를 유도하는 페이크에이브이의 변형은 하루에서 수백 건이 생성되고 있으며, 이러한 추세는 당분간 지속될 것으로 보인다. 6, 7, 9, 10위로 등록된 애드웨어는 모두 국산 애드웨어로 대표 진단명을 기준으로 한 피해 건수에서도 국산 애드웨어 피해의 증가를 확인할 수 있다.

2009년 5월 유형별 스파이웨어 피해 현황은 [표 3-7]과 같다.

구분	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
3월	243	248	105	185	2	8	4	0	0	**795**
4월	275	230	104	2171	0	47	3	0	0	**2830**

5월	145	222	89	2736	0	8	0	1	0	3021

[표 3-7] 2009년 5월 유형별 스파이웨어 피해 건수

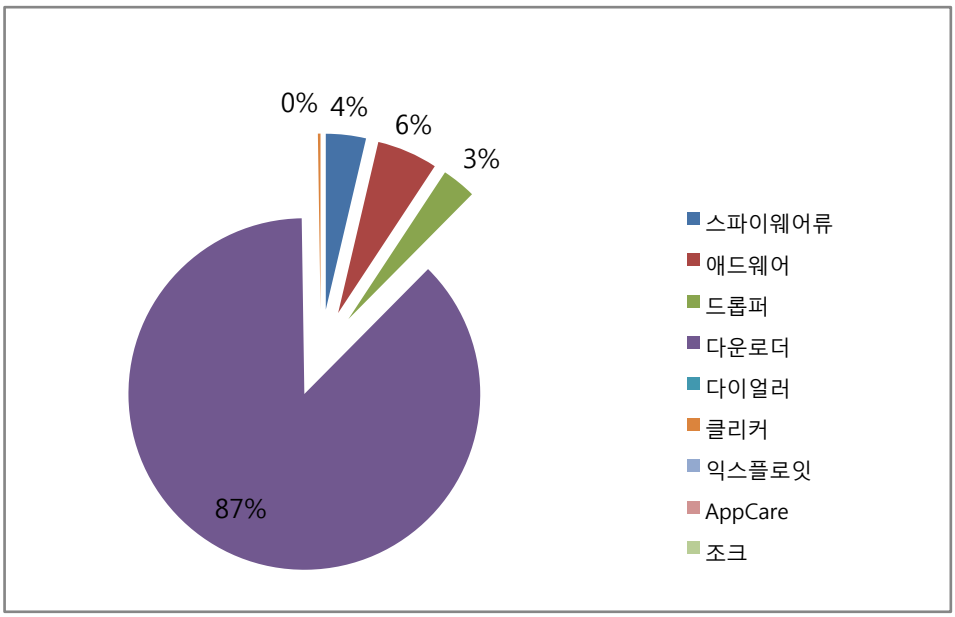
2009년 5월 역시 다운로더의 피해가 전월에 이어 가장 많은 피해를 입힌 것으로 나타났으며, 전월 비 600건 이상 증가 했다. 가짜백신을 배포하는 사이트에서 사이트주소와 타임스탬프 등을 이용해 MD5를 변경하는 다운로더의 피해 증가는 당분간 계속 될 것으로 보인다.

(2) 5월 스파이웨어 발견 현황

5월 한 달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 3-8], [그림 3-10]과 같다.

구분	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
3월	184	139	60	143	2	6	4	0	0	538
4월	199	120	68	1948	0	30	2	0	0	2367
5월	77	177	66	1828	0	5	0	0	0	2093

[표 3-8] 2009년 5월 유형별 신종(변형) 스파이웨어 발견 현황



[그림 3-10] 2009년 5월 발견 된 스파이웨어 프로그램 비율

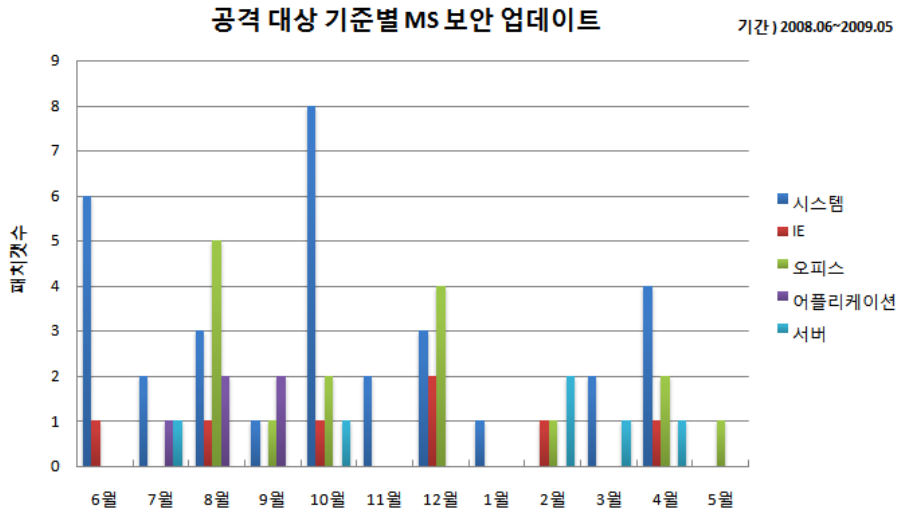
지난 4월에 이어 5월에도 가짜백신을 설치하는 다운로더 신고가 계속되고 있으며, 전체 신종(변형) 발견건수에서 차지하는 비율도 가장 높다. 이러한 외산 다운로더의 경우 하나의 배포 사이트에서도 수많은 변형을 배포하는 경우가 너무나도 많기 때문에 신종 및 변종의 수가 절대적으로 많다.

스파이웨어류의 경우 지난 3, 4월에 비해 대폭 감소했다. 그러나, 애드웨어의 경우 5월에는 국내에서 제작되어 광고를 노출하는 애드웨어의 피해신고가 큰 폭으로 증가했다.

3. 시큐리티

(1) 5월 마이크로소프트 보안 업데이트 현황

마이크로소프트사는 5월에 긴급(Critical) 1건의 보안 업데이트를 발표하였다.



[그림 3-11] 5월 MS 보안 업데이트 현황

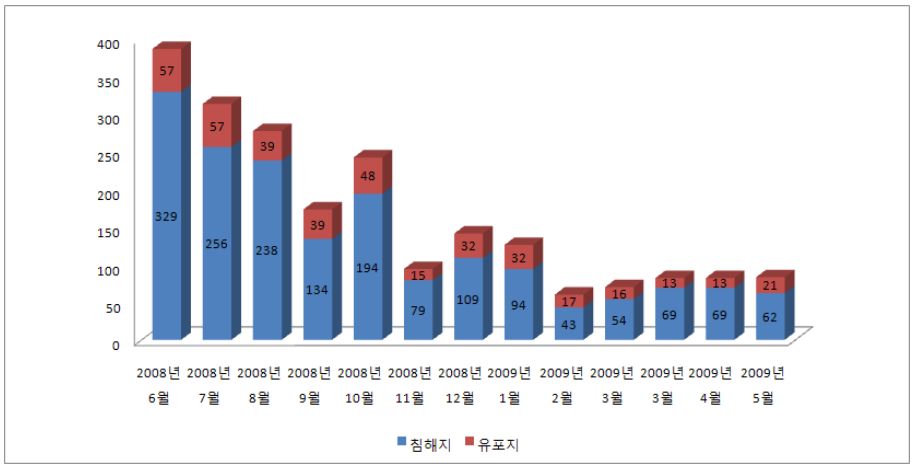
위험도	취약점	PoC
긴급	(MS09-017) Microsoft Office Powerpoint의 취약점으로 인한 원격코드 실행 문제점	유

[표 3-9] 2009년 05월 주요 MS 보안 업데이트

이번 5월은 다른 달과 달리 상당히 적은 패치가 나왔다. 마이크로소프트사에서는 MS09-017 패치 1건만을 내 놓았는데, 파워포인트의 취약점을 해결한 패치이다. 임의로 조작된 파워포인트 파일을 오픈 할 경우 명령어가 실행될 수 있어 위험하다. 이 취약점은 0-day 취약점인 만큼 주의가 필요하고, 이전부터 오피스의 취약점을 이용한 악성코드가 계속 발견되고 있는 점을 비춰봤을 때 파워포인트를 사용하는 사용자라면 꼭 패치를 적용할 것을 권고한다.

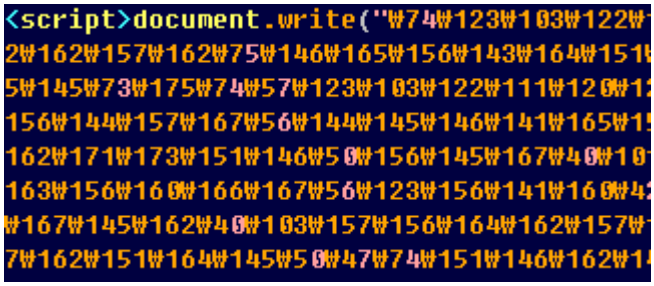
이외 5월 중순경 웹 서버인 IIS(Internet Information Services)의 WebDAV 취약점이 보고되었는데, 이것 또한 제로데이 취약점으로 취약점에 대한 세부정보가 먼저 공개되어 있어 주의를 기울여야 한다. WebDAV 취약점에 대한 자세한 이야기는 ASEC리포트 이번 호(5월호)의 이달의 보안이슈 - 시큐리티 부분을 참고하길 바란다.

(2) 2009년 5월 웹 침해사고 및 악성코드 배포 현황



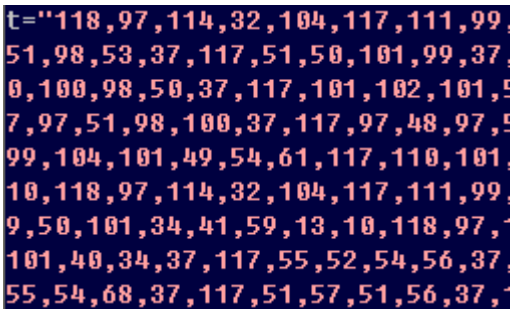
[그림 3-12] 악성코드 배포를 위해 침해된 사이트 수 / 배포지 수

2009년 5월 악성코드를 위해 침해된 웹사이트의 수와 악성코드 유포지의 수는 62/21로 2009년 4월과 비교하여 침해지는 감소하였고 유포지는 증가하였다. 특별히 브라우저와 관련된 어플리케이션의 취약점 발표가 없었던 것을 감안하면 이와 같은 추세는 계속될 것으로 보인다. 웹을 이용하여 배포되는 악성코드는 갈수록 그 패턴이 지능화되고 있다. 또한 힙스프레이 기법을 통해 브라우저의 리소스를 소비하게 하는 여러 개의 취약점을 동시에 공격하는 등 공격의 정도가 갈수록 심해지고 있다. 다음 그림은 특정 공격페이지의 시작 페이지이다.



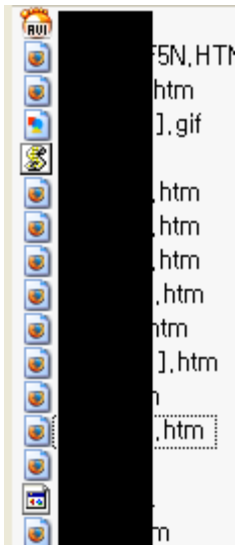
[그림 3-13] 시작 페이지

이 페이지에 접속하면 브라우저는 다음과 같은 취약점 공격코드가 담긴 파일을 추가로 다운로드하며 취약점 공격코드가 실행된다. 이러한 파일 역시 다음과 같이 암호화되어 있다.



[그림 3-14] 암호화된 페이지

이 공격코드는 힙스프레이 기법을 사용하여 사용자 시스템의 자원을 낭비하게 하여 공격이 성공하지 않더라도 과도한 자원을 사용하여 사용자에게 큰 불편을 미친다.



[그림 3-15] 다운로드 받는 파일

따라서 사용자가 이러한 공격코드로부터 피해를 방지하기 위해 항상 보안 패치의 상태를 최신으로 유지하고, 안티 바이러스 프로그램을 사용하여 혹시나 모를 악성코드의 피해로부터 자신의 시스템을 보호해야 한다.

4. 사이트가드

(1) 2009년 5월 웹 사이트 보안 요약

구분	건수
악성코드 발견 건수	176,614
악성코드 유형	822
악성코드가 발견된 도메인	646
악성코드가 발견된 URL	10,078

[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 5월 한달 동안 웹 사이트를 통해 발견된 악성코드 동향을 요약해서 보여주고 있다.

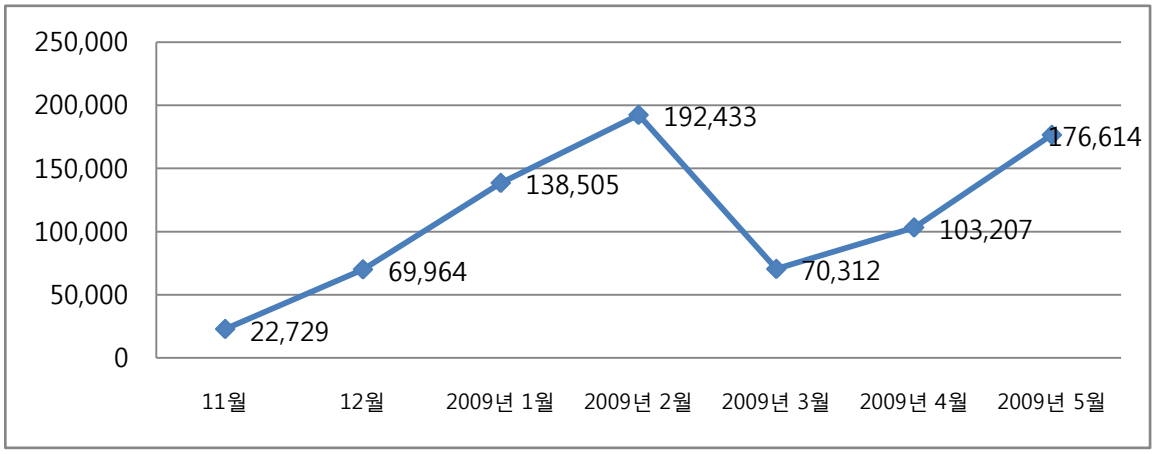
사이트가드의 집계에 따르면 5월 한달 동안 악성코드는 176,614건 발견되었으며, 악성코드 유형은 822종, 악성코드가 발견된 도메인은 646건, 악성코드가 발견된 URL은 10,078건으로 전반적으로 증가세를 보였다. 이는 전반적으로 악성코드의 위협이 증가한 것보다는 사이트 가드의 악성코드 검증/갱신서버의 알고리즘이 개선되어 전체적으로 악성코드에 대한 탐지 기능이 강화되었기 때문이다.

세부내용을 보면 다음과 같다.

[1] www.siteguard.co.kr

(2) 악성코드 월간 통계

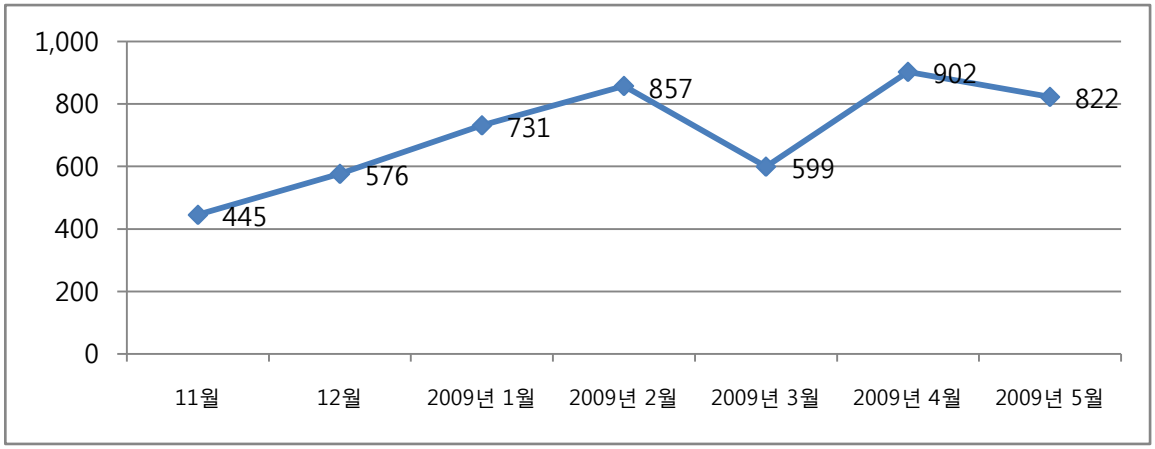
가) 악성코드 발견 건수



[그림 3-16] 월별 악성코드 발견 건수

[그림 3-16]는 최근 7개월간(2008년 11월부터 2009년 5월까지)의 악성코드 발견 건수의 추이를 나타내는 그래프로 5월 악성코드 발견 건수는 176,614건으로 지난달에 비해 약 58%의 급격한 증가세를 보였다.

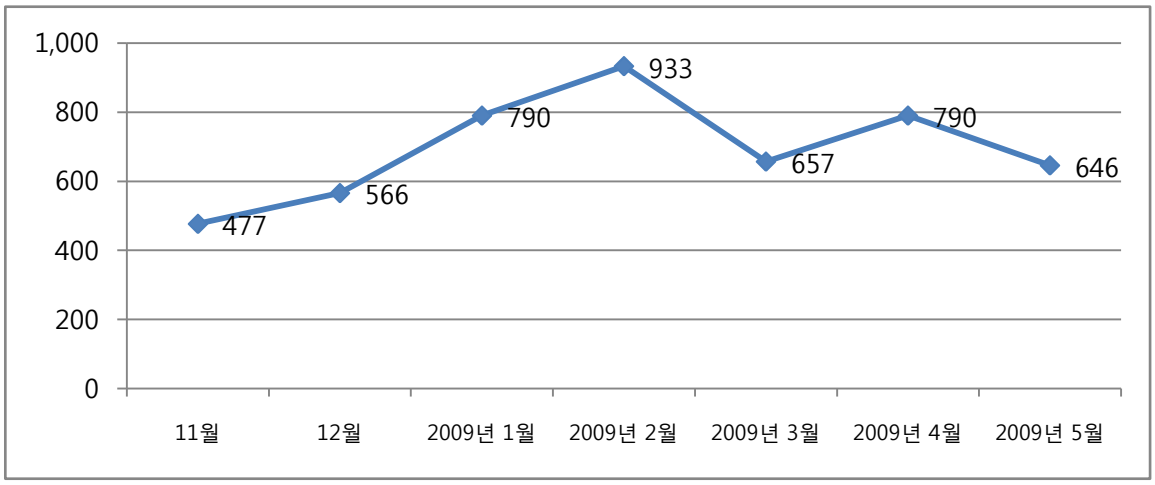
나) 악성코드 유형



[그림 3-17] 월별 악성코드 유형

[그림 3-17]는 최근 7개월간 발견된 악성코드의 유형을 나타내는 그래프로 역시 지난 달의 902건에 비해 약 9%가 감소한 822건으로 확인되었다. 이는 웹 상에서 전파되는 악성코드들이 유형의 큰 변화 없이 기존의 Trojan류 악성코드 위주로 확산되는 동향이 반영된 것이다.

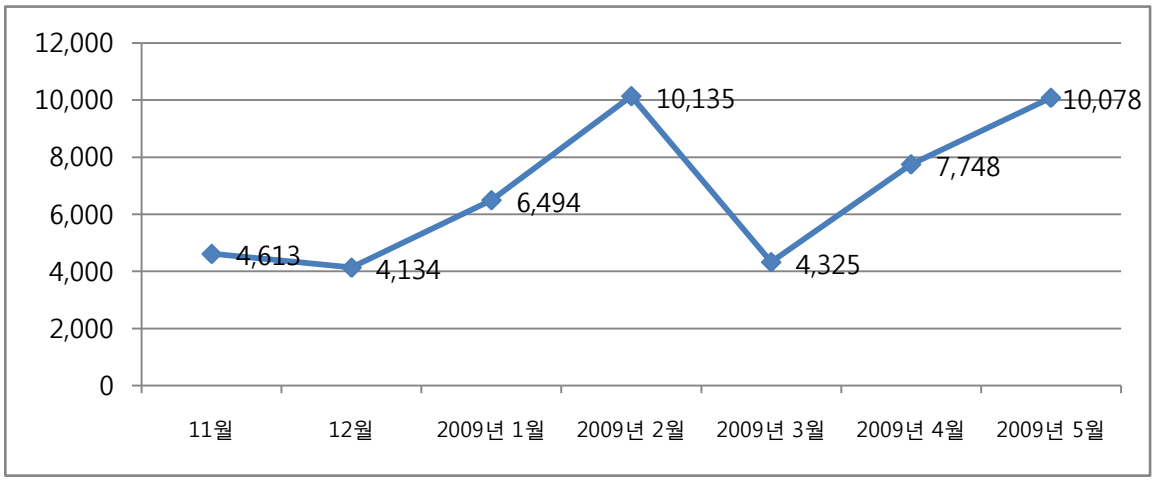
다) 악성코드가 발견된 도메인



[그림 3-18] 월별 악성코드가 발견된 도메인

[그림 3-18]는 최근 7개월간 악성코드가 발견된 도메인 수의 변화 추이를 나타내는 그래프로 5월 악성코드가 발견된 도메인은 646개로 전월에 비해 약 19% 감소하였다.

라) 악성코드가 발견된 URL

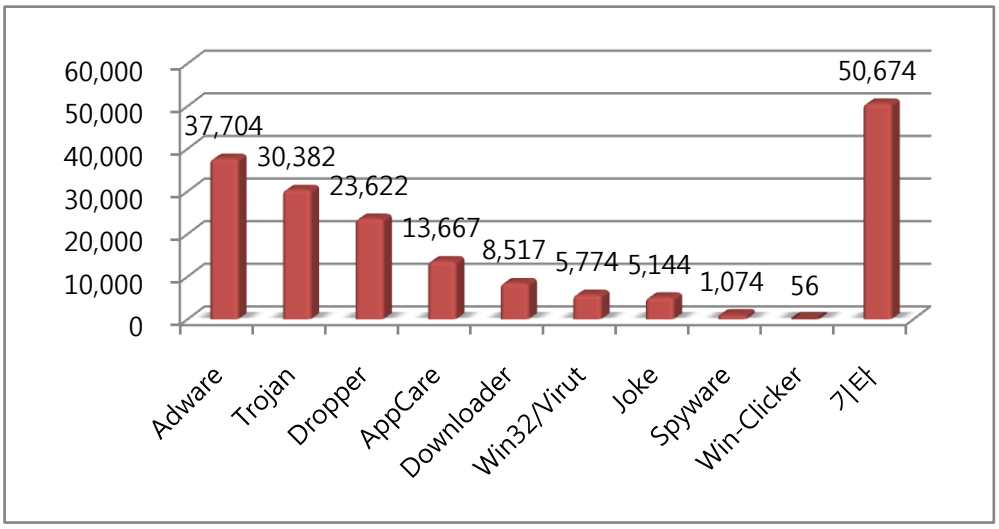


[그림 3-19] 월별 악성코드가 발견된 URL

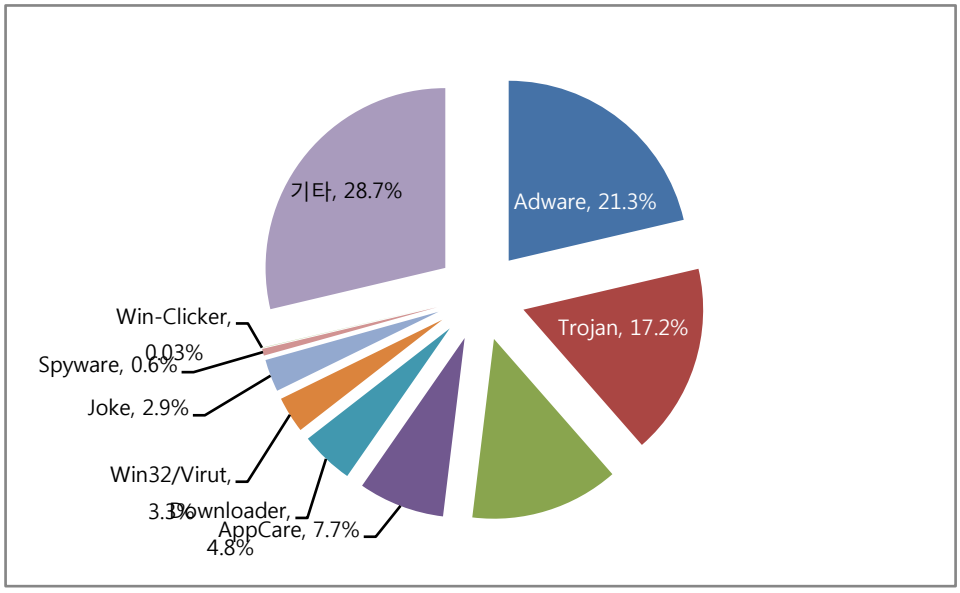
[그림 3-19]은 최근 7개월간 악성코드가 발견된 URL 수의 변화 추이를 나타내는 그래프로 5월 악성코드가 발견된 URL 수는 10,078개로 전월에 비해 30% 증가하였다. 이는 사이트가드의 악성코드 검증/갱신서버의 알고리즘 중에서 악성코드가 발견된 URL의 존재여부를 검증하는 Parser 기능이 강화되어 URL의 탐지기능이 강화되었기 때문이다.

(3) 유형별 악성코드 배포 수

유형	건수	비율
Adware	37,704	21.3%
Trojan	30,382	17.2%
Dropper	23,622	13.4%
AppCare	13,667	7.7%
Downloader	8,517	4.8%
Win32/Virut	5,774	3.3%
Joke	5,144	2.9%
Spyware	1,074	0.6%
Win-Clicker	56	0.03%
기타	50,674	28.7%
합계	176,614	100.0%



[표 3-11] 유형별 악성코드 배포 수



[그림 3-20] 유형별 악성코드 분포

[표 3-11]과 [그림 3-20]은 5월 한달 동안 발견된 악성코드를 유형별로 구분하여 발견 건수와 해당 비율(%)를 보여주고 있다.

5월 한달 동안 총 176,614개의 악성코드가 발견되었으며 이중 Adware류가 37,704개로 지난달 2위에서 1위로 한 단계 상승하였다. 뒤를 이어 Trojan류가 30,382개로 2위를 차지하였다. 그 다음으로는 Dropper류가 23,622개로 3위를 차지하였다. 상위 1~4위까지는 지난달과 변화 없이 Trojan류, Adware류, AppCare류, Dropper류 등이 계속적으로 상위권을 차지하고 있으며, 이러한 변화는 지난 1/4분기부터 지속되는 트렌드로써, 인터넷 사용자의 개인정보 및 금융정보를 탈취/사용하기 위해 제작된 악성코드들이 웹상에 자리를 잡은 것이 이유이며, 앞으로도 이러한 트렌드는 유지될 것으로 보인다.

(4) 악성코드 배포 순위

순위		악성코드명	건수	비율
1	new	JS/Exception.Exploit	31584	27%
2	new	Win-Adware/GSidebar.145920	31519	26%
3	new	Win-Dropper/BoomWhale.87077115	15785	13%
4	new	TextImage/Viking	9300	8%
5	↑1	Win-Trojan/Xema.variant	8799	7%
6	↓2	Win-AppCare/WinKeygen.94208	5241	4%

7	↑1	Win-Joke/Stressreducer.1286147	4932	4%
8	↓3	Win-AppCare/WinKeyfinder.542720	4878	4%
9	↓2	Packed/Upack	4187	4%
10	new	Dropper/Agent.87552.G	2900	2%
합계			**119,125**	**100%**

[표 3-12] 유형별 악성코드 배포 Top 10

[표 3-12]는 5월 한달 동안 웹 사이트에서 사이트가드를 통해 확인된 악성코드 배포 Top 10을 보여주고 있다. Top 10에 포함된 악성코드들의 총 배포건수는 119,125건으로 5월 한 달 총 배포건수 176,614건의 약 67%에 해당되며, 지난달의 60%보다 증가하였다. 특이한 점은 지금까지 Top10에 등장한 적이 없는 악성코드가 1위부터 4위까지를 차지한 점이다. 특히 사용자 동의를 구하지 않고 실행되는 Java Script나 ActiveX Component를 진단하는 JS/Exception.Exploit과 애드웨어인 Win-Adware/GSidebar.145920가 전체 Top10의 53%를 차지한다는 것이다. 이는 지금까지 상대적으로 탐지가 어려웠던 URL에 있었던 악성코드들이 사이트가드의 알고리즘 개선으로 탐지가 되면서 자연스럽게 해당 악성코드들이 Top10에 진입한 것으로 보인다.

요컨대, 이번 달 역시 전반적인 악성코드의 증가세가 지속된 한 달이었다. 앞으로는 사이트가드의 지속적인 기능 개선과 방학기간으로 인한 Script Kids들의 활동력 증가와 맞물려, 악성코드의 증가추세는 지속될 것으로 보인다.

ASEC REPORT 작성을 위하여 다음과 같은 분들께서 수고하셨습니다.

2009년 5월호

편집장	선임 연구원	허 종 오
집필진	선임 연구원	정 관 진
	선임 연구원	차 민 석
	선임 연구원	정 진 성
	선임 연구원	허 종 오
	주임 연구원	장 영 준
	주임 연구원	강 동 현
	주임 연구원	임 채 영
	주임 연구원	김 민 성
감 수	상 무	조 시 행
참여연구원		ASEC 연구원분들
		SiteGuard 연구원분들