안철수연구소에서 발행하는 월간 보안 보고서

ASEC 리포트

2009년 8월호

이달의 보안 이슈

ASEC 칼럼

이달의 통계

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

I. 이달의 보안 이슈

1. 악성코드 – Win32/Induc 바이러스 허위 UPS 메일 관련 악성코드

Win32/Induc 바이러스는 개발자를 노리는 바이러스로 알려졌다. 이 바이러스는 백신 업체나 사용자들이 인지하기 훨씬 전부터 감염 되고 있었던 것으로 보인다. 일반 사용자 보다는 델파이 프로그래머를 타겟으로 하는 바이러스로 알려졌다. 사회공학기법은 여전히 악성코드 제작자들로부터 사용되고 있는데 8월에는 허위 UPS 운송메일을 가장하여 악성코드가 링크된 메일이 다수 발견 되고 있다.

(1) 개발자를 노리는 Win32/Induc 바이러스

Win32/Induc 바이러스는 매우 은밀하게 전파 된 것으로 보인다. 안철수 연구소를 비롯한 일부 안티 바이러스 업체는 이 바이러스의 최초 활동은 6월로 추정하고 있다. 이 바이러스는 일반인이 확인 할 수 있는 뚜렷한 감염 증상이 없다. 감염된 파일을 실행하면 델파이가 설치되어 있는지 확인 후 특정한 소스 파일(SysConst.pas)을 감염 시킨다.

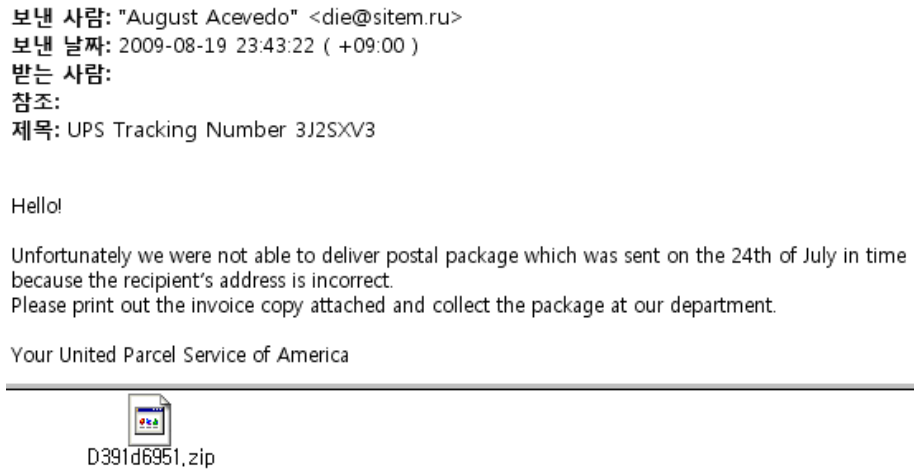
```
FF FF FF 2D-00 00 00 75-73 65 73 20-77 69 6E 64  ÿÿÿ-   uses wind
6F 77 73 3B-20 76 61 72-20 73 63 3A-61 72 72 61  ows; var sc:arra
79 5B 31 2E-2E 32 34 5D-20 6F 66 20-73 74 72 69  y[1..24] of stri
6E 67 3D 28-00 00 00 FF-FF FF FF 50-00 00 00 66  ng=(   ÿÿÿÿP   f
75 6E 63 74-69 6F 6E 20-78 28 73 3A-73 74 72 69  unction x(s:stri
6E 67 29 3A-73 74 72 69-6E 67 3B 76-61 72 20 69  ng):string;var i
3A 69 6E 74-65 67 65 72-3B 62 65 67-69 6E 20 66  :integer;begin f
6F 72 20 69-3A 3D 31 20-74 6F 20 6C-65 6E 67 74  or i:=1 to lengt
68 28 73 29-20 64 6F 20-69 66 20 73-5B 69 5D 00  h(s) do if s[i]
00 00 00 FF-FF FF FF 50-00 00 00 3D-23 33 36 20     ÿÿÿÿP   =#36
74 68 65 6E-20 73 5B 69-5D 3A 3D 23-33 39 3B 72  then s[i]:=#39;r
65 73 75 6C-74 3A 3D 73-3B 65 6E 64-3B 70 72 6F  esult:=s;end;pro
63 65 64 75-72 65 20 72-65 28 73 2C-64 2C 65 3A  cedure re(s,d,e:
73 74 72 69-6E 67 29 3B-76 61 72 20-66 31 2C 66  string);var f1,f
32 3A 74 65-78 74 66 69-6C 65 3B 00-00 00 00 FF  2:textfile;    ÿ
FF FF FF 50-00 00 00 68-3A 63 61 72-64 69 6E 61  ÿÿÿP   h:cardina
6C 3B 66 3A-53 54 41 52-54 55 50 49-4E 46 4F 3B  l;f:STARTUPINFO;
70 3A 50 52-4F 43 45 53-53 5F 49 4E-46 4F 52 4D  p:PROCESS_INFORM
41 54 49 4F-4E 3B 62 3A-62 6F 6F 6C-65 61 6E 3B  ATION;b:boolean;
74 31 2C 74-32 2C 74 33-3A 46 49 4C-45 54 49 4D  t1,t2,t3:FILETIM
45 3B 62 65-67 69 6E 00-00 00 00 FF-FF FF FF 50  E;begin    ÿÿÿÿP
00 00 00 68-3A 3D 43 72-65 61 74 65-46 69 6C 65     h:=CreateFile
28 70 63 68-61 72 28 64-2B 24 62 61-6B 24 29 2C  (pchar(d+$bak$),
```

[그림1-1] SysConst.dcu 에 감염된 Win32/Induc 바이러스 일부

따라서 델파이 프로그래머가 아닌 일반 사용자는 별다른 증상이 없다. 만약 델파이가 설치되어 있는 경우 특정 소스 파일을 감염 시키고 프로그래머가 컴파일을 할 경우 특정한 파일이(SysConst.dcu) 생성 된다. 해당 파일은 정상적인 파일이나 Win32/Induc 에 감염되어 있다. 이후 프로그래머가 새로운 파일을 컴파일 할 때마다 바이러스도 함께 감염된 채로 만들어진다. 해당 바이러스는 일반 사용자의 치료도 중요하지만 무엇보다도 델파이를 이용하여 개발을 하는 개발자들의 치료가 무엇 보다 중요하다. V3는 감염된 SysConst.dcu 파일과 실행파일을 진단/치료하고 있다. 따라서 자신이 델파이 개발자고 감염이 의심된다면 V3 를 이용하여 감염된 시스템을 검사 하도록 한다.

UPS 운송메일로 가장한 악성코드

사회공학기법을 이용한 악성코드는 어제, 오늘의 일이 아니다. 그럴듯한 내용으로 사용자를 속여 메일에 첨부파일이나 링크를 클릭하게 유도한다. 대부분의 사용자가 속지 않을 것이라고 생각되지만 근래의 메일로 확산 되는 악성코드는 대부분 사회공학기법을 이용한다. 국내의 경우 영어로 되어 있는 이런 메일에 좀처럼 속지 않을 수도 있지만 공격자는 자동으로 그리고 대량으로 이러한 메일을 보냄으로 어느 날 호기심으로 클릭 한다면 악성코드에 감염되는 경우가 발생 할 수 있다.



[그림1-2] 악성코드가 첨부된 허위 UPS 운송 메일

첨부된 악성코드는 Win-Trojan/Bredolab 라는 진단명을 가지고 있다. 다음과 같은 증상이 있다. 사용자가 압축을 풀어 실행하면 dummy 로 svchost.exe 를 실행 후 악성코드를 Injection한다. 해당 악성코드는 다운로더 증상을 가지고 있다. 시스템이나 실행된 조건에 따라 Sleep 타임이 8분여가 되면 특정한 호스트로부터 파일을 다운로드 하는데 크게 2가지로 나뉜다.

- 특정 윈도우 시스템 파일(AGP440.SYS)을 감염 시키는 파일
- 가짜 백신을 설치하는 다운로더

감염된 윈도우 시스템 파일은 지금까지 NDIS.SYS, NTFS.SYS 가 있었다. 이후 다른 어떤 시스템 파일도 감염 대상이 될 수 있다. 감염된 파일은 삭제가 아닌 치료를 해야 한다. 정상 파일을 내부에 가지고 있기 때문이다. V3 는 이렇게 감염된 형태는 Win32/Ntfs로 진단/치료하고 있다. 감염된 파일은 스팸 메일을 보내는 증상을 갖는다. 보내는 스팸은 특정 호스트로부터 받아오는 내용에 따라서 달라 질 수 있다.

다음은 악성코드 실행 후 시간 순서에 따른 생성 및 변경된 파일 리스트이다.

svchost.exe	CREATE	C:₩WINDOWS₩Temp₩wpv061251705172.exe ; 다운로드 된 파일
wpv061251705172	CREATE	C:₩WINDOWS₩system32₩sys32_nov.exe ; 파일명 변경
wpv061251705172	CREATE	C:₩Documents and Settings₩사용자 계정명₩sys32_nov.exe ; 자동실행
svchost.exe	CREATE	C:₩DOCUME~1₩GAME-007₩LOCALS~1₩Temp₩BN8.tmp ; 다운로드
svchost.exe	CREATE	C:₩WINDOWS₩system32₩drivers₩agp440.sys ; 감염
svchost.exe	CREATE	C:₩WINDOWS₩system32₩dllcache₩agp440.sys ; 감염
BN8.tmp	CREATE	C:₩WINDOWS₩system32₩dllcache₩figaro.sys ; 생성
BN8.tmp	CREATE	C:₩WINDOWS₩system32₩dllcache₩beep.sys ; 원본파일과 교체
BN8.tmp	CREATE	C:₩WINDOWS₩system32₩drivers₩beep.sys ; 원본파일과 교체
BN8.tmp	CREATE	C:₩WINDOWS₩system32₩braviax.exe ; 가짜 백신 다운로더

[표1-1] Win-Trojan/Bredolab 악성코드 실행 후 대략적인 타임 라인 별 실행파일

이후 시스템은 가짜 백신이 설치되는데 요즘 문제가 많이 되고 있는 PC Antispyware 2010 이다. 해당 가짜 백신은 허위로 진단을 하고 치료를 위해 과금을 하도록 유도하므로 절대로 속아서는 안 된다.

[그림1-3] 가짜 백신 PC Antispyware 2010

이처럼 가볍게 넘겨 호기심으로 실행한 파일이 스팸 메일을 발송하는 좀비 시스템이 되거나 가짜 백신이 설치되어 제대로 시스템을 사용하기 어려운 상황에 처하는 만큼 그럴 듯 하게 만들어져 실행을 해볼 만큼 호기심을 자극하여도 실행하는 우를 범해서는 안 된다.

2. 스파이웨어 – 카페에 글을 도배하는 스파이웨어

(1) 네이버 카페에 글을 도배하는 스파이웨어

최근 국내에서 제작된 스파이웨어로써 유명 포털사이트(네이버) 카페에 글을 도배하는 일명 '네이버 매시버(Naver Massiver)'라는 프로그램이 유행하고 있다. 이 프로그램은 수많은 '도배 프로그램'의 일종이다. 도배 프로그램이란 일정 주기로 게시판, 또는 채팅 창에 글을 올리는 프로그램들을 말하는데, 주로 광고 또는 단순 도배 행위를 위해 이용된다.


네이버 매시버 테스트중(자료 포함)(무제한버전) 2009.08.21
Subject 이 프로그램(도배기[네이버매시버])은 SeiMorTo연구소의 [Plosive]가 제작했습니다. 아래 주소에서 이 도배기(네이버매시버 무제한버전)를 다운받으실 수...
http://cafe.naver.com/[redacted]

도배기 실험해보는중(무제한버전) 2009.08.21
네이버 매시버 실험중(자료 포함)(무제한버전) 이 프로그램(도배기[네이버매시버])은 SeiMorTo연구소의 [Plosive]가 제작했습니다. 아래 주소에서 이 도배기(네이버매시버...
http://cafe.naver.com/[redacted]

[그림 1-4] 네이버 매시버 (Naver Massiver) 를 통해 등록된 글

이번에 발견된 네이버 매시버의 경우 기존의 도배 프로그램과는 많이 차별된 특징을 갖고 있다. 이들은 해외 스파이웨어에서나 볼 수 있었던 기능을 새롭게 도입하였다. 구체적으로는 아래와 같다.

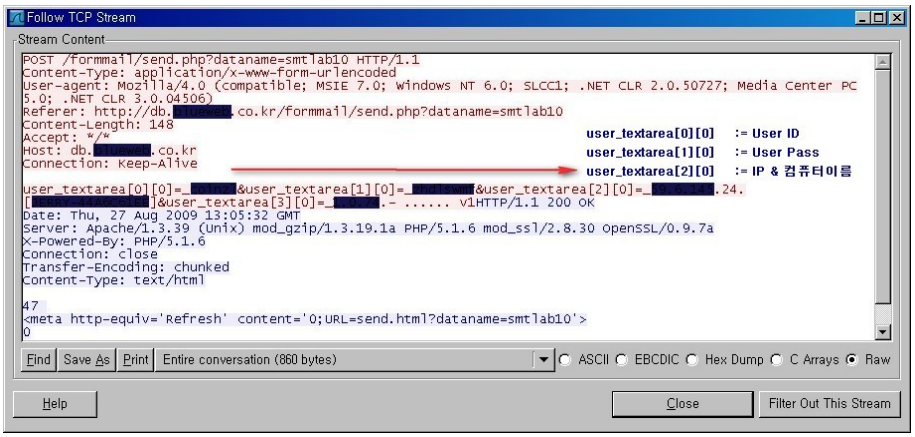
- DNS 초기화 (ipconfig /displaydns)
- 방화벽 비활성화
- beep.sys 드라이버 수정
- netstat.exe, rstrui.exe 교체 (sp2 버전으로 교체됨)
- CCProxy 설정
- 보안 제품 강제 종료 (AY*, AL*, bs*, V3* 로 시작되는 프로세스들을 강제 종료함)

이러한 행위는 네이버 매시버의 초기화 과정에서 수행된다. 보안 제품 및 방화벽에 의한 차단을 막기 위한 AV-Kill 기능 및 보안 설정 변경, 그리고 주요 시스템 파일의 교체 등 기존 국내 스파이웨어에서는 볼 수 없었던 행위들이 확인되었다.

더불어 이 프로그램에는 네이버 계정 수집 기능도 함께 들어가 있다.

[그림 1-5] 네이버 매시버 로그인 화면

프로그램이 구동되면 [그림 1-5]와 같이 로그 인을 위한 계정 입력 화면이 뜬다. 사용자가 계정 정보를 입력하게 되면 네이버로 쿼리를 통해 유효성 여부를 확인한다.



[그림 1-6] 사용자의 계정 정보를 수집하는 모습

사용자 계정이 유효할 경우 위 [그림 1-6]와 같이 사용자의 아이디, 암호, IP, 컴퓨터 이름 등을 서버로 전달한다. 이렇게 수집된 정보가 어떻게 이용되는지 현재로서는 알 수 없으나 '개인 정보의 노출 가능성'은 매우 높다고 볼 수 있다. 암호 자체가 평문(Plain Text)으로 수집되기 때문에 위 서버에 접근할 수 있는 악성코드 제작자라면 임의의 사용자 계정으로 로그인할 수 있으며, 개인 정보를 빼내갈 수도 있다. 중국에서 한국인 개인 정보가 고액으로 거래된다는 것을 보면 충분히 가능성이 있다. 그러므로 호기심으로 네이버 매시버를 이용했던 사용자가 있다면 바로 암호를 변경할 것을 권장한다.

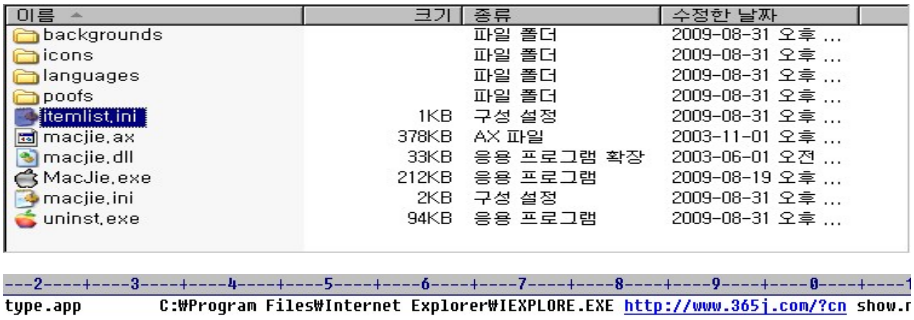
이번 이슈로 소개한 네이버 매시버는 특정 포털 사이트를 대상으로 만들어진 극히 제한적인 악성 프로그램이다. 그래서, 개인이 단순 취미로 제작한 프로그램으로 생각될 수 있다. 더구나 아직 별다른 피해도 보고되고 있지 않아 대수롭지 않게 넘어가도 될 것 같다. 하지만, 국내에서 이용된 적이 거의 없는 스파이웨어 기법들을 이용해 제작되었다는 점과, 사용자 계정을 수집하기 위한 목적이 다분하다는 점에서 그 잠재적인 위험성은 매우 크다고 볼 수 있다.

(2) 다양한 방법으로 시작 페이지를 변경하는 중국 스파이웨어

최근에 중국 악성코드에 의한 시작페이지 변경 문제가 자주 등장하고 있다. 전에는 단순히 '인터넷 등록 정보'의 홈페이지 주소를 변경하는 것들만 문제가 되었으나, 최근에는 등록 정보에 어떤 시작 주소가 설정되더라도 중국 포털 사이트로 이동하는 경우가 종종 있다. 이번 이슈에서는 가볍게 그 사례들을 살펴보도록 한다.

[그림 1-7] Mac OS의 Dock 방식

[그림 1-7]은 최근에 발견된 'Win-Dropper/Macjie.1859149' 에 의해서 설치되는 'Acua Dock' 프로그램으로 간편한 단축 아이콘을 제공하는 기능을 이용해 시작 페이지를 변경하는 사례이다.



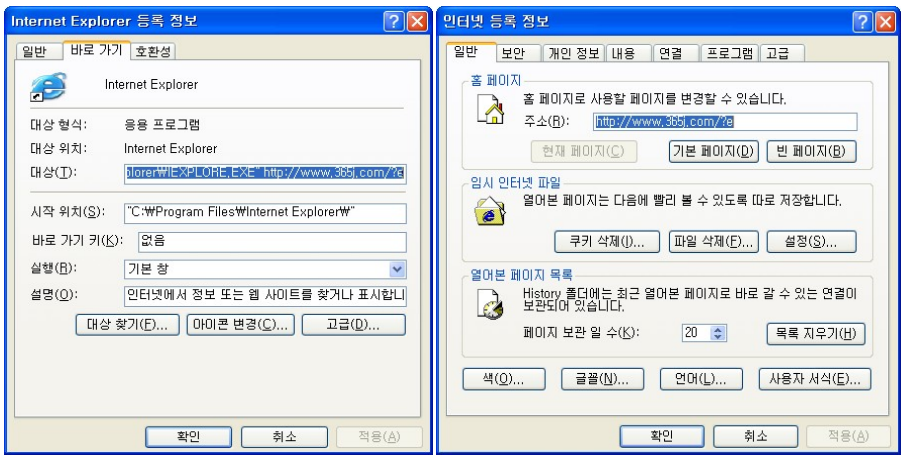
이름	크기	종류	수정한 날짜
backgrounds		파일 폴더	2009-08-31 오후 ...
icons		파일 폴더	2009-08-31 오후 ...
languages		파일 폴더	2009-08-31 오후 ...
poofs		파일 폴더	2009-08-31 오후 ...
itemlist.ini	1KB	구성 설정	2009-08-31 오후 ...
macjie.ax	378KB	AX 파일	2003-11-01 오후 ...
macjie.dll	33KB	응용 프로그램 확장	2003-06-01 오전 ...
MacJie.exe	212KB	응용 프로그램	2009-08-19 오후 ...
macjie.ini	2KB	구성 설정	2009-08-31 오후 ...
uninst.exe	94KB	응용 프로그램	2009-08-31 오후 ...

```
---2----+----3----+----4----+----5----+----6----+----7----+----8----+----9----+----0----+----1
type.app        C:₩Program Files₩Internet Explorer₩IEXPLORE.EXE http://www.365j.com/?cn show.r
```

[그림 1-8] Dock 설정 파일

Dock 은 Mac OS 에서 윈도우의 '빠른 실행'처럼 간편한 실행이 가능하다는 장점 때문에 여러 사용자들이 이용하고 있다. 이 프로그램은 설정 파일을 [그림 1-8]처럼 작성하는 것만으로도 시작페이지를 변경할 수 있는데, 설정 파일의 존재를 잘 모르는 경우 지속적인 피해를 입을 수 있다.

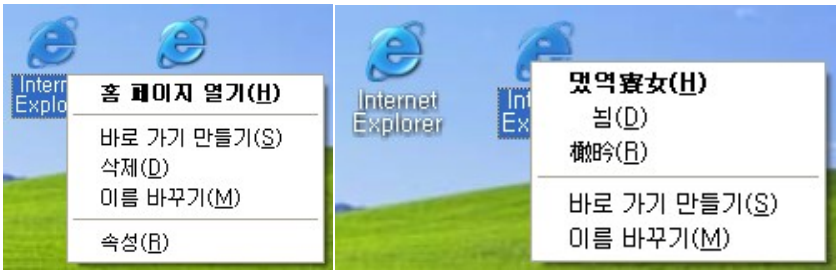
다음으로, 고전적인 방법으로 '인터넷 등록 정보' 의 홈페이지 주소를 변경하는 방식과 '인터넷 바로 가기'의 '대상' 항목에 URL을 입력으로 주는 사례가 있다.



[그림 1-9] 고전적인 시작 페이지 변경

이 경우 속성 페이지를 열어보는 것만으로도 원인 파악 및 해결이 가능하기 때문에 큰 문제가 되지 않는다. 다만, 악성 프로그램이 제대로 치료되지 않는 경우 주기적으로 변경되는 문제가 있을 수 있다.

다음으로는 [그림 1-10]과 같이 바탕 화면에 다중 IE 아이콘을 생성하는 경우와 컨텍스트 메뉴로 제공하는 '홈 페이지 열기' 기능을 이용한 시작페이지 변경 사례가 있다.



[그림 1-10] '홈페이지 열기'를 변경하는 경우

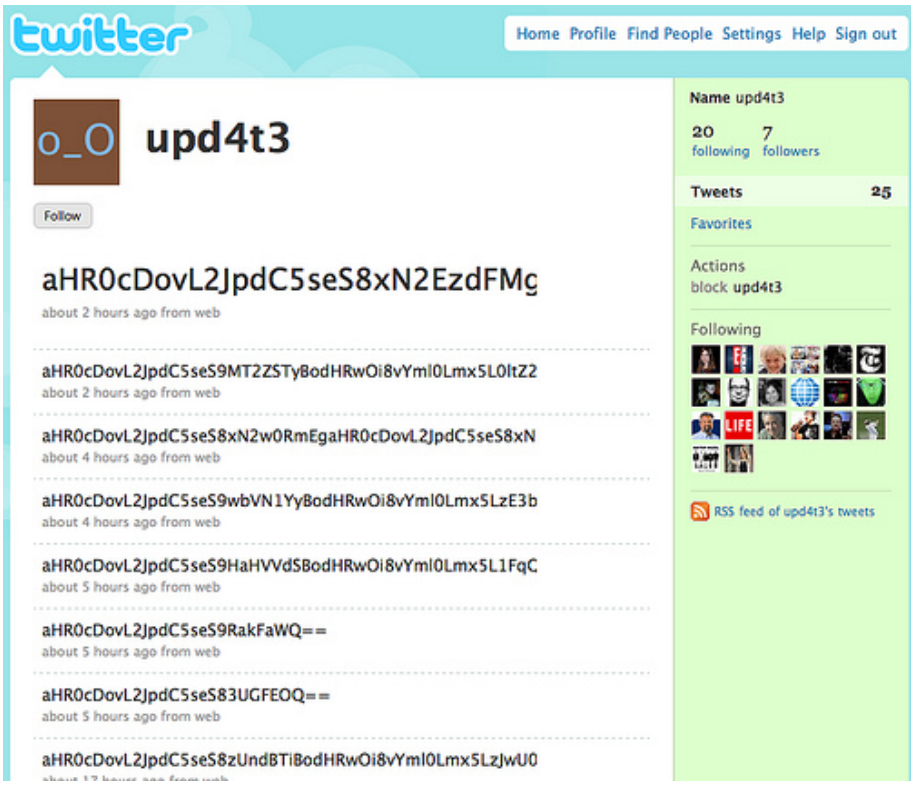
이 사례는 윈도우의 '이전 시작 메뉴' 설정의 경우에 한해서 해당되기 때문에 일부 사용자들에게는 해당되지 않는다.

최근 발견된 중국산 스파이웨어들은 대부분 시작 페이지를 변경하는 특징을 갖고 있는데, 위에 소개한 한가지 사례만 이용하는 것이 아니라, 모든 시작페이지 변경 방식을 동시에 이용한다. 추후 새로운 방식이 발견될 경우 기존 방식에 추가될 것으로 예상된다.

3. 시큐리티 – 7.7 DDoS 패킷 분석

(1) 트위터를 이용하는 봇넷

미국 시각 8월 13일 미국의 네트워크 보안 업체인 아르보(Arbor)는, 소셜 네트워크 서비스(Social Network Service)인 트위터(Twitter)를 이용하여 악성코드에 감염된 좀비(Zombie) 시스템들의 네트워크인 봇넷(Botnet)을 컨트롤하는 명령어를 송신하는 것이 발견되었다고 알렸다.

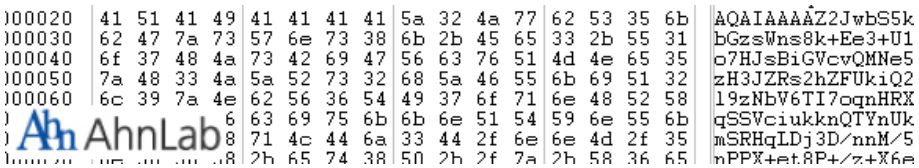


[그림1-11] 봇넷 컨트롤에 사용된 트위터 계정(아르보 제공)

공격자는 명령어들을 베이스64(Base64)로 인코딩하여 자신이 생성한 트위터 계정에 올려두고, 악성코드에 감염된 좀비 시스템들은 해당 트위터 계정에 RSS(Really Simple Syndication) 형태로 접근하여 명령어를 전달 받도록 되어있다.

[그림 1-12] 해당 트위터 계정의 RSS 형태

ASEC에서 분석 당시 송신한 명령으로는 특정 도메인에서 다수의 특정 파일을 다운로드 하는 명령이 존재하였다. 해당 파일들을 다운로드 하여 확인 한 결과 아래 이미지와 같은 베이스64로 인코딩 되어있는 ZIP 압축 파일이었다.



[그림 1-13] base64로 인코딩 되어있는 ZIP 파일

해당 파일들을 디코딩하여 압축을 풀면 UPX로 실행 압축되어 있는 gbpm.exe 파일이 생성된다. 생성된 실행 파일들은 모두 악성코드들로 V3 제품 군에서 다음과 같이 진단한다.

Win-Trojan/Banc.104960
Win-Trojan/Banc.103936
Win-Trojan/Banc.33792
Win-Trojan/Banc.34304
Win-Trojan/Banc.71680
Win-Trojan/Banc.104448

해당 악성코드가 실행되면 DLL 파일 1개를 생성해서 웹 브라우저인 인터넷 익스플로러(Internet Explorer)와 파이어폭스(Firefox)가 특정 금융 관련 웹 사이트에 접속이 이루어지면 사용자가 입력하는 키보드 입력 값을 후킹하는 기능을 수행한다.

ASEC에서 현재까지 분석한 사항들을 종합 해보면 해당 악성코드 제작자는 트위터의 RSS 기능을 이용해 좀비 시스템에 다른 악성코드를 다운로드 하도록 하여 감염을 시도한 것으로 분석 된다. 이러한 봇넷 컨트롤 방식은 기존의 HTTP C&C 봇넷과 유사한 형태지만, 봇넷

컨트롤을 위한 웹 서버를 구축하기 위해 다른 서버를 해킹하지 않고 온라인에서 합법적으로 손쉽게 만들 수 있는 트위터 계정을 이용하였다. 따라서, 앞으로는 트위터 뿐만 아니라 RSS 등과 같이 손쉽게 메시지를 전달 받을 수 있는 형태를 제공하는 다른 SNS 서비스나 블로그 등 온라인 상에서 손쉽게 개설할 수 있는 서비스들을 이용한 봇넷 컨트롤 방식이 나타날 수 있을 것 같다.

관련 링크

1. http://asert.arbornetworks.com/2009/08/twitter-based-botnet-command-channel/

(2) 리눅스 커널 'sock_sendpage()' NULL Pointer Dereference 취약점

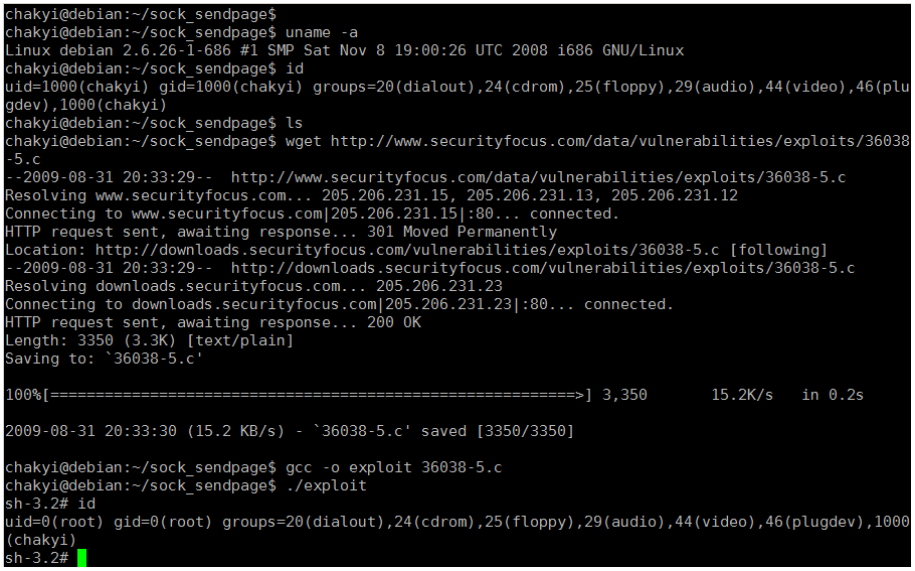
지난 8월 13일 대부분의 리눅스 커널(2.4.37.5 이전, 2.6.31-rc6 이전)에 적용 가능한 심각한 취약점이 발표되었다. 해당 취약점은 sock_sendpage() 함수에서 사용하는 proto_ops 구조체의 초기화가 제대로 진행되지 않은 상태에서 널 포인터를 참조함으로써 발생한다. proto_ops 구조체는 시스템에 영향을 줄 수 있는 여러 가지 함수들의 포인터를 가지고 있기 때문에 해당 취약점을 이용하여 시스템을 재 부팅 시킨다거나 특정한 명령을 실행시킬 수 있으며 일반 사용자가 root 권한을 획득하는 것이 가능하다.


```
        ** There are some cases that we need mprotect due to the dependency matter with SVR4. (howev
er, I did not confirm it yet)
        */
        if(personality(0xffffffff)==PER_SVR4){
                if(mprotect(0x00000000,0x1000,PROT_READ|PROT_WRITE|PROT_EXEC)==-1){
                        perror("[-] mprotect()");
                        return -1;
                }
        }
        else if((zero_page=mmap(0x00000000,0x1000,PROT_READ|PROT_WRITE|PROT_EXEC,MAP_FIXED|MAP_ANONY
MOUS|MAP_PRIVATE,0,0))==MAP_FAILED){
                        perror("[-] mmap()");
                        return -1;
        }
        *(char *)0x00000000=0xff;
        *(char *)0x00000001=0x25;
        *(unsigned long *)0x00000002=(unsigned long)&kernel;
        *(char *)0x00000006=0xc3;

        if((fd_in=open(argv[0],O_RDONLY))==-1){
                perror("[-] open()");
                return -1;
        }
```

[그림 1-14] 공격 코드 일부

현재, 인터넷 상에 해당 취약점을 이용하여 공격을 수행하는 코드(익스플로잇)가 공개되어 있어 누구든지 손쉽게 다운로드 가능한 상태이며, 이 취약점 문제를 해결할 수 있는 패치를 제공하는 운영체제들이 많지 않기 때문에 심각한 문제가 될 수 있다.



[그림 1-15] 공개된 익스플로잇 테스트

다행히도 이번 취약점은 원격에서 수행할 수 없는 로컬 취약점이지만, 로컬상에서는 위와 같이 몇 가지 간단한 명령어를 입력하는 것 만으로도 손쉽게 root 권한을 획득하는 등의 공격을 수행할 수 있다.

이러한 로컬 취약점들은 시스템을 사용하는 일반 사용자가 수행할 수도 있지만 다른 취약점들과 함께 사용한다면 원격에서 임의의 공격자가 사용할 수도 있다. 예를 들면, 웹 서버일 경우 웹 페이지에서 sql injection, 파일 업로드-실행 등의 취약점이 존재한다면 이를 이용하여 웹 서버 데몬의 실행 권한을 획득한 뒤 해당 취약점의 익스플로잇을 이용하여 root 권한을 획득할 수 있다. SSH나 TELNET 등의 서비스도 공격에 사용될 수 있다. 만약 시스템에 취약한 비밀번호를 사용하고 있는 사용자가 있다면 브루트포스 공격(무작위-순차적 대입)에 의해 비밀번호가 확인될 수 있고, 이러한 계정으로 로그인 한 뒤에 로컬 취약점을 공격하는 익스플로잇을 이용할 수도 있다. 게다가, 인증서를 이용하여 로그인 하는 SSH 방식을 사용하는 경우에도 취약한 인증서를 사용함으로써 원격의 공격자에게 로그 인을 허용하게 하는 경우(최근 apache.org 홈페이지도 취약한 인증서를 사용하는 SSH 서비스에 의해 공격 당했음)도 있기 때문에 주의를 해야 한다.

이러한 공격에 대비하기 위해서는 운영체제 커널의 최신 패치와 관련된 서비스들의 취약점 제거, 사용자 계정들의 안전한 패스워드 사용 등의 꾸준한 노력이 필요하다.

관련 링크

1. http://www.securityfocus.com/bid/36038
2. http://www.boannews.com/media/view.asp?idx=17546&kind=0
3. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2692

(3) 꾸준히 발생하는 인터넷뱅킹 해킹 사건

예전부터 끊이지 않고 발생하고 있는 인터넷뱅킹 해킹 사건이 얼마 전에도 발생하였다. 하지만 이번 사건은 보안 프로그램의 문제점도 있었겠지만 피해자들의 안전 불감증도 한 몫 했다. 대부분의 피해자들은 인터넷뱅킹을 편하게 이용하려고 계좌번호, 보안카드 등의 중요한 정보들을 자신들의 이 메일, 웹 하드 등에 올려두었다고 한다. 공격자는, 이 메일 서버를 해킹하거나 이 메일 계정의 허술한 비밀번호를 추측 또는 해당 이 메일로 악성코드를 전송하여 저장되어 있는 중요 정보들을 획득하여 인터넷뱅킹 해킹에 사용하였다 한다.

이러한 인터넷뱅킹 문제점들을 예방하기 위해서 안철수 연구소는 다음과 같은 보안 수칙을 제안하고 있다.

인터넷 뱅킹 보안수칙

1. 공인인증서, 보안카드, 비밀번호 등을 스캔해서 사진파일이나 엑셀파일 형태로 개인 이 메일 계정 또는 인터넷 하드에 저장하지 않는다.
2. 가급적 공인인증서는 PC보다 USB나 외장하드 등 이동저장매체에 보관해서 인터넷 뱅킹 사용시에만 PC에 연결해서 사용한다.
3. 보안카드보다 OTP(One Time Password)나 MOTP(Mobile One Time Password) 등을 사용한다.
4. 은행 인터넷뱅킹 계정이나 포탈 메일 계정 비밀번호 주기적 변경 및 관리한다.
5. 인터넷 금융거래 계정 ID와 비밀번호는 포탈 메일 계정 ID비밀번호와 다르게 사용하고 절대 타인에게 알려주지 않는다.

4. 중국 보안 이슈 - 중국의 범죄자 양성 교육

(1) 중국의 잘못된 컴퓨터 보안 기술 교육

2월 28일 중국에서는 제 11회 중화인민공화국 전국인민대표회의 상무의원 회의 개최를 통해서 중국 내에서 현재 발생하는 다양한 컴퓨터 관련 범죄에 대해 강력한 처벌을 위한 형법들이 추가 및 개정되었다. 이렇게 중국 정부에서는 형법 개정들을 통해 컴퓨터 관련 범죄에 대해 강력한 대응을 하기 위해 노력하고 있다.

하지만 8월 4일 중국일보(China daily)의 기사에 따르면 아직도 중국 사회에서는 컴퓨터 해킹 기술을 통해 금전적인 이득만을 노리는 잘못된 컴퓨터 보안 기술 교육들이 이루어지고 있다 한다.

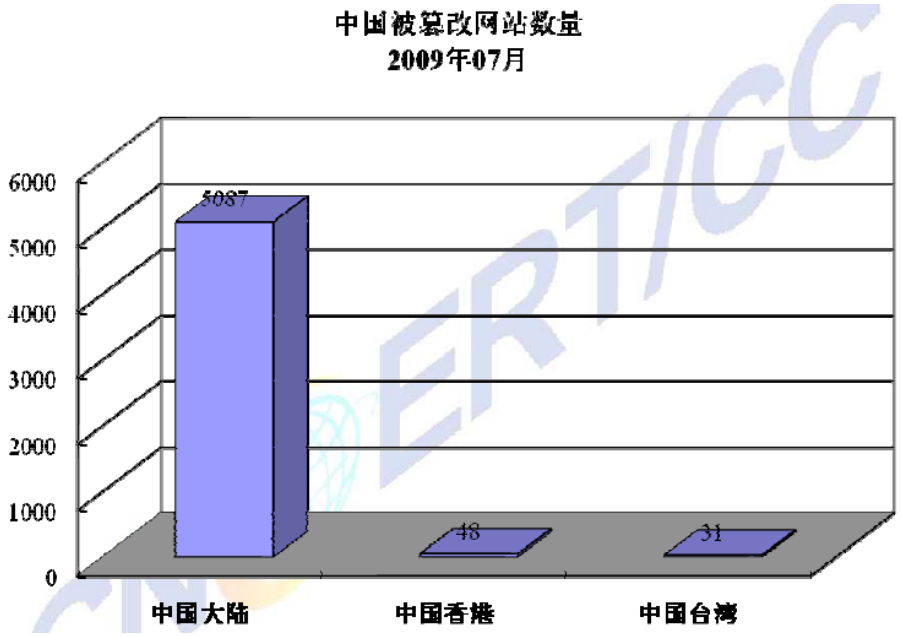
[그림 1-16] 사설 컴퓨터 학원의 수강생 모집 간판

위 이미지는 중국 귀주성 귀주시 Wang Chuan Chang 버스 정류장에 설치되어 있는 해커 양성 교육생을 모집한다는 광고판이다. 이러한 해커 양성 교육을 위한 사설 학원 대부분이 북경에 집중 되어 있으며 중국 전체에서 발생하는 매출이 2억 3천 8백만 위엔(한화 약 428억)에 달한다고 한다. 해당 기사에 따르면 해커를 양성한다는 사설 보안 기술 교육 과정들 대부분이 취약한 컴퓨터 시스템에 대한 공격 기법과 기술들만 가르치고 있으며 이를 배우는 학생들 대부분이 악용하고 있다고 한다. 해당 언론과 인터뷰를 한 상해에서 북경으로 상경한 25세의 Wang은 해당 보안 기술 교육을 배우는 학생들의 목적 대부분이 다른 사람들의 컴퓨터를 몰래 훔쳐보기 위해서거나 컴퓨터 해킹 실력을 과시하기 위해 그리고 다른 사람들의 개인 정보를 금전적인 목적으로 도용하기 위해서라고 한다. 보안 기술 교육을 배우는 학생들

이 그 기술을 잘못된 방법으로 사용한다는 점에서 보안 기술 교육을 강의하는 사설 학원 입장에서는 돈 벌이에만 집중하기 보다는 컴퓨터 시스템 및 보안 기술에 대한 건전한 사용과 관련한 보안 윤리 의식 교육이 먼저 선행되어야 할 것으로 보여진다.

(2) 중국 7월 웹 사이트 위, 변조 보안 사고 동향

중국 대륙의 보안 위협과 사고를 총괄하는 CNCERT/CC에서 8월 18일, 7월 웹 사이트 위 변조 보안 사고 동향 보고서를 발표 하였다.



[그림 1-17] 2009년 7월 중국 웹 사이트 위 변조 통계

CNCERT/CC에서 이번에 발표한 보고서에 따르면 7월 한 달 동안 중국 대륙, 홍콩 및 대만 모두 큰 폭으로 웹 사이트 위 변조 사고가 증가하였다고 한다.

특히 중국 대륙의 경우에는 총 5087건의 웹 사이트 위, 변조 사고가 발생하여 지난 6월과 비교하여 1632건이 증가한 수치를 보였다. 그 외 홍콩의 경우 7월 48건이 발생하여 지난 6월과 비교하여 24건이 증가한 수치이며 대만의 경우 지난 7월과 비교하여 28건이 증가한 31건이 발생하였다고 한다.

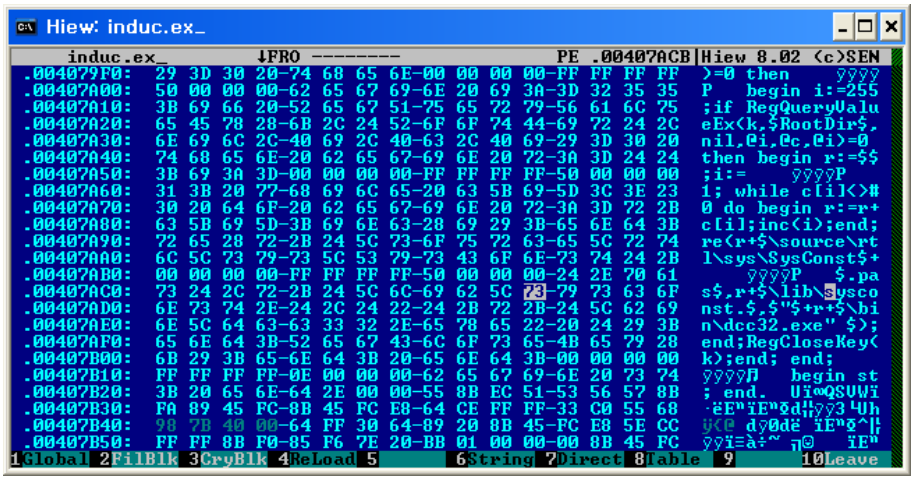
II. ASEC 칼럼

■ Win32/Induc 바이러스가 남긴 과제

2009년 8월 중순 델파이 라이브러리 파일을 변조해 컴파일 되는 파일에 바이러스를 포함되는 Win32/Induc 바이러스가 발견되었다. 백신에 이 바이러스 탐지 기능이 추가되면서 지금까지 잘 사용하던 프로그램이 진단되어 오진 아니냐는 문의가 쏟아졌고 일부 백신에서는 치료 대신 삭제해 버렸다. 또, 감염된 파일을 치료하는 백신도 실행 압축된 파일의 경우 진단 후 삭제해버려 사람들이 혼란이 발생한다. Win32/Induc 바이러스에 대해 알아보고 이 바이러스로 인한 과제를 알아보자.

(1) Win32/Induc 바이러스

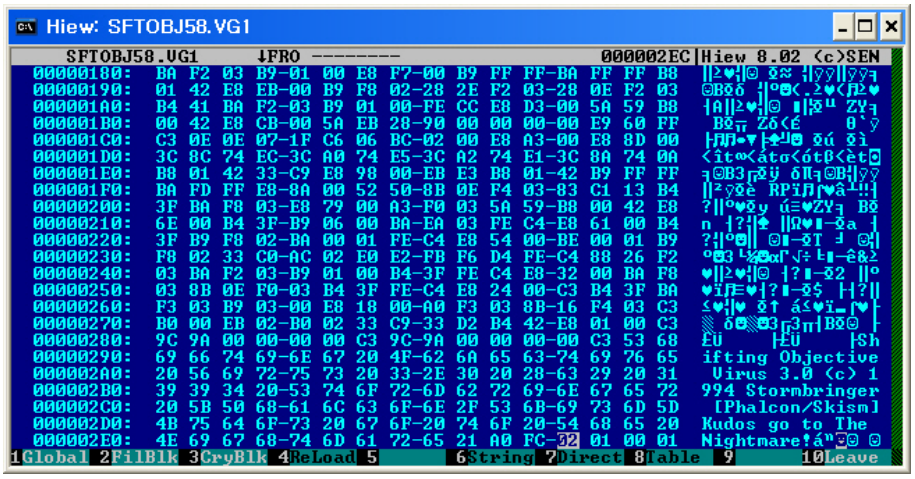
2009년 8월 19일 흔히 델파이 바이러스로도 불리는 Win32/Induc 바이러스가 발견되었다. 발견은 늦게 되었지만 2009년 2월에 제작된 프로그램에서도 발견되어 2009년 초 혹은 그 이전부터 델파이 개발자를 중심으로 은밀하게 퍼진 것으로 보인다. 다른 악성코드에 비해 발견 시기가 늦어 진 건 일반 컴퓨터에서는 별다른 증상이 없고 델파이 개발자만을 대상으로만 활동하기 때문이다. Win32/Induc 바이러스는 델파이가 설치되어 있으면 sysconst.pas에 바이러스 소스코드를 삽입하고 dcc32.exe를 이용해 라이브러리 파일을 생성해서 컴파일 되는 모든 파일에 바이러스 코드를 포함하게 하는 방법을 이용한다.



[그림 2-1] Win32/Induc 바이러스에 감염된 파일

(2) 개발자를 노린 바이러스들

개발자를 노린 바이러스는 예전에도 과거에도 존재했다. 1994년 발견된 ShiftObj 바이러스는 소스코드와 실행코드의 중간 형태인 OBJ 파일을 감염시키는 바이러스이다.



[그림 2-2] ShiftObj 바이러스에 감염된 파일

C나 파스칼(Pascal)의 소스코드에 바이러스 소스코드를 포함시키는 바이러스도 존재한다.


```
Main()
{
    Printf(“Hello world!”);
}
```

[그림 2-3] 원래 소스코드

```
#include “virus.h”
Main()
{
    Printf(“Hello world!”);
    Virus();
}
```

[그림 2-4] 감염 된 소스코드

소스코드를 직접 변조하는 바이러스는 개발자에 의해 쉽게 발견되는 단점이 있다.

Win32/Apparition.96239 바이러스는 바이러스 내에 소스 코드를 포함하고 있고 컴파일러가 설치된 시스템에서 그 소스코드를 일부 변조해 컴파일 해 새로운 변종을 만들어 내는 방식을 이용한다.

이런 개발자를 목표로 한 바이러스는 개념증명 수준으로 일반에 퍼진 경우는 드물어 그 동안 큰 문제가 되지 않았다.

(3) 치료 문제

Win32/Induc 바이러스는 6개월 이상 발견되지 않고 개발자들 사이에 퍼졌고 컴파일 되는 파일들이 바이러스를 포함되어 배포되었다. 감염된 파일을 치료하는 백신도 있었지만 일부 백신은 치료 대신 삭제를 했으며 개발사에서 실행 압축된 형태로 배포한 경우 치료할 수 없어 감염된 파일을 삭제해 문제가 발생했다. 이에 백신 업체가 과잉 대응 한 게 아닌가 하는 논란도 발생한다.

- 델파이 바이러스 '백신' 과잉대응 논란 (디지털데일리, 2009년 8월 23일)
http://www.ddaily.co.kr/news/news_view.php?uid=53343

- 보안뉴스: 변형된 델파이 바이러스 대응책 마련 시급!
http://www.boannews.com/media/view.asp?idx=17550&kind=1

백신 업체에서 해당 바이러스를 진단에서 제외한 것으로 오해할 수 있지만 안철수 연구소의 경우 백신에서 해당 바이러스 진단 기능을 제외하지 않았다. V3의 경우 감염된 파일의 치료를 기본 정책으로 진행하지만 실행 압축 파일의 경우 치료를 못해 삭제하는 문제가 있어 실행 압축되어 있을 때만 진단을 제외했으며 향후 적절한 정책을 진행할 예정이다. 이전에도 실행 압축 안에 바이러스가 감염된 경우가 있었지만 감염된 프로그램의 배포는 제작자의 잘못이고 그 수가 적었기 때문에 삭제를 기본 정책으로 했다.

(4) 백신 업체 정책

델파이 개발자들과 언론을 통해 이런 문제가 제기 되었지만 이런 문제는 기존 백신 업체의 정책 이해도 필요하다.

첫째, 악성코드는 악성코드

예전에 해가 없는 바이러스에 대해 '양성 바이러스'라는 표현을 사용했다. 하지만, 양성 바이러스는 표현은 자칫 해가 없는 바이러스 제작은 괜찮다고 오해 할 수 있어 최근에는 잘 사용되지 않는다. 보안 업체 입장에서는 위험도가 떨어지거나 특정 환경에서만 활동해도 자기 복제 프로그램은 바이러스로 분류해서 악성코드로 진단하고 있다.

둘째, 감염 파일의 치료 혹은 삭제

국내 제품의 경우 바이러스 감염 파일에 대해 치료라는 복구 개념을 사용하고 있지만 일부 해외 제품의 경우 감염된 파일을 삭제하고 재설치를 권장하고 있다.

게다가 이번 바이러스의 경우 정상 파일에 바이러스가 감염 된 게 아니라 개발자가 컴파일러 하면서 생성되므로 감염된 파일을 치료해도 비정상적인 행동을 할 수 있다는 이유로 감염된 파일을 삭제하고 재 컴파일을 권장하는 업체도 존재한다.

다만, 백신 업체가 예측하지 못한 점이라면 델파이로 제작하고 실행 압축 프로그램을 이용해 압축 후 고객에게 제공하는 경우가 많았다는 점이다. 이에 치료 기능을 제공하는 업체도 감염된 파일을 삭제해 그 동안 정상적으로(?) 이용하던 프로그램을 진단하고 삭제해 오진이 아니냐는 문의를 받았다.

국내 업체는 이런 고객들의 불편을 인식하고 실행 압축된 파일은 진단하지 않는 형태로 문제를 해결했지만 바이러스에 감염된 파일의 치료보다는 삭제라는 다른 문화를 가진 제품도 반영될지는 현재까지 알 수 없다.

(5) 남긴 교훈과 과제

이번 악성코드로 백신 업체와 개발자들 간에 몇 가지 교훈과 과제를 안겨주었다.

악성코드의 90% 이상이 단순히 삭제하면 해결되는 트로이목마나 웜이 차지하고 있지만 바이러스에 의한 문제는 계속 발생하고 있어 백신 업체는 바이러스 감염 파일에 대해 삭제에 대해 더 고민할 필요가 생겼다. 특히 이번 바이러스처럼 사용 중에 감염된 파일이 아닌 처음부터 바이러스를 포함한 파일이라면 사용자 입장에서 잘 사용하던 파일이 삭제되어 버려 당혹스러울 수 있다. 감염된 파일을 치료할 수 없을 때 그냥 삭제하는 정책이 아닌 사용자에게 어떤 행동을 할지 물어보는 기능이 요구되는 것이다. 또, 실행 압축 파일 내에 바이러스를 포함한 경우 어떻게 처리해야 하는가 하는 문제도 고민할 필요가 있다.

개발 업체는 개발자 시스템과 빌드 시스템을 분리할 필요가 있다. 백신에서 탐지 되지 않던 새로운 기법을 사용하는 바이러스라고 해도 결국 개발자 시스템에 바이러스가 감염되어 전파되었기 때문에 근본적으로 개발업체의 책임이 존재하며 이는 외부와 차단된 빌드 시스템 구축으로 이어진다.

새로운 기법을 사용하는 악성코드가 등장할 때마다 백신 업체에서는 기존 정책이나 제품의 한계로 어려움을 겪게 되고 이번 Win32/Induc 바이러스도 유사한 경우였지만 고민해 문제

를 해결해야 할 것 이다.

(6) 참고자료

[1] 델파이 개발자를 노린 Induc 바이러스 (http://xcoolcat7.tistory.com/557)
[2] Induc 바이러스 감염 파일 삭제 소동과 고민할 문제 (http://xcoolcat7.tistory.com/560)
[3] 델파이 사태, 새로운 보안 위협의 발견 (디지털데일리, 2009년 8월 24일, http://www.ddaily.co.kr/news/news_view.php?uid=53389)
[4] Eugene Kaspersky, 'Shifting Objectives', Virus Bulletin, March 1994, pp.11-12
[5] Eugene Kaspersky, 'Lock up your Source Code!', Virus Bulletin, June 1994, pp.10-11

III. 이달의 통계

1. 악성코드 통계

(1) 8월 악성코드 통계

순 위		악성코드명	건수	비율
1	-	Win-Trojan/Banker.702976.D	29	28.2 %
2	NEW	Win-Trojan/Downloader.9216.OJ	11	10.7 %
3	NEW	Win32/Induc	9	8.7 %
4	NEW	Win-Appcare/RemoveWGA.49664	8	7.8 %
4	NEW	Win-Trojan/Agent.40605	8	7.8 %
4	NEW	Win-Trojan/Agent.6144.HK	8	7.8 %
4	NEW	Win-Trojan/Fraudload.184393	8	7.8 %
4	NEW	Win-Trojan/Reboot.27526	8	7.8 %
9	NEW	Win-Trojan/Fakeav.26685	7	6.8 %
9	NEW	Win-Trojan/Spambot.11264	7	6.8 %
		합계	**103**	**100 %**

[표 3-1] 2009년 8월 악성코드 피해 Top 10

현재 짧은 시간 내에 수많은 신종 또는 변종 악성코드의 생성 및 소멸 등이 반복되면서 악성코드의 라이프 사이클이 매우 짧아졌고 이로 인해 매월 악성코드 피해 Top 10은 새로운 악성코드 진단명으로 갱신되어 왔다. 그러나 6 / 7 / 8월 3달 동안 Win-Trojan/Banker.702976.D가 1위를 고수했다는 것은 앞에서 언급한 현 악성코드 트렌드에 비춰볼 때 특이하다고 할 수 있지만 이 현상이 현 악성코드 트렌드에 큰 변화는 주지 않을 것으로 보이며 일시적인 것인지 아니면 지속될 것인지에 대해서는 좀 더 모니터링 할 필요가 있다.

바이러스는 타 시스템으로 자체 확산기능은 없기 때문에 Win/Virut을 제외하고는 바이러스류의 악성코드가 월 악성코드 Top 10에 진입하는 것은 매우 드문 일인데 Win32/Induc 바이러스가 8월 악성코드 피해 Top 10에서 3위에 랭크 될 수 있었던 원인을 살펴보면 델파이 개발자의 PC가 Win32/Induc에 감염된 상태에서 델파이로 작성된 소스에 Win32/Induc의 바이러스 코드를 삽입했다. 그리고 감염된 델파이 소스가 컴파일 된 후 인터넷을 통해서 사용자들에게 배포되었기 때문으로 해석될 수 있다. 그나마 다행인 것은 이번 Win32/Induc은 델파이 개발자 PC에 존재하는 델파이 소스에 자신의 바이러스 코드를 삽입할 뿐 일반 사용자의 PC에서 Win32/Induc 바이러스에 감염된 실행파일을 실행하더라도 악의적인 행위는 발생하지 않는다는 점이다.

8월 악성코드 피해 Top 10에서 주목할 것은 4위에 랭크 된 Win-AppCare/RemoveWGA.49664이다. 보통 Win-AppCare는 파일이 정상이면서 악의적인 목적에 사용될 가능성이 있기 때문에 명명된 것으로 전체 진단명을 보면 윈도우의 정품인증을 우회하는데 사용되는 일종의 크랙이나 키젠으로 보여진다. 그리고 Win-AppCare가 4위에 랭크 될 수 있었던 것은 일부 사용자들이 해당 진단명을 가진 파일을 사용해서 정품 윈도우를 불법으로 사용하고 있기 때문인 것으로 추정되며 특정 웹 사이트나 P2P공유 프로그램을 통해서 공유되는 크랙이나 키젠은 본래 목적을 위한 파일도 존재하지만 대부분 악성코드가 상용 프로그램의 크랙 또는 키젠으로 위장한 후 사용자를 현혹하여 악성코드 자신을 다운로드하여 실행하도록 하기 때문에 절대로 다운로드 해서는 안되며 정품 프로그램을 사용해야 한다.

Win-Trojan/Spambot.11264가 8월 악성코드 피해 Top 10에 신규로 진입했고 Win-Trojan/Spambot계열의 악성코드는 악성코드 피해 통계에서 그다지 큰 비중은 차지하고 있지 않으나 꾸준히 피해 신고가 접수되고 있다. 그리고 Win-Trojan/Spambot계열의 악성코드는 감염된 시스템을 좀비 PC로 만든 후 불특정 다수의 사용자에게 스팸 메일을 발송하는데 이 역시 악성코드 제작자 또는 스패너에게 돈벌이 수단으로써 효과적이기 때문이며 이런 현상은 계속될 것이다.

그 외에는 새로운 진단명의 악성코드들이 8월 악성코드 피해 Top 10에 진입하였다.

순 위		악성코드명	건수	비율
1	1	Win-Trojan/OnlineGameHack	470	18.4 %
2	1	Win32/Virut	440	17.2 %
3	-2	Win-Trojan/Agent	421	16.5 %
4	NEW	Win32/IRCBot	356	13.9 %
5	-1	Win-Trojan/Downloader	271	10.6 %
6	NEW	Dropper/Bobax	159	6.2 %
7	NEW	Win-Trojan/Banker	128	5 %
8	2	Dropper/Agent	108	4.2 %
9	NEW	Win-Trojan/Hupigon	105	4.1 %
10	-3	Win-Trojan/Magania	95	3.7 %
합계			2,553	100 %

[표 3-2] 2009 8월 악성코드 대표 진단명 Top 10

[표 3-2]는 대표 진단명을 기준으로 유사 변형들을 묶어 통계를 뽑은 것으로 개별 악성코드에 대한 피해 현황을 설명하고 있는 [표 3-1]보다 좀더 포괄적인 악성코드 감염 현황을 파

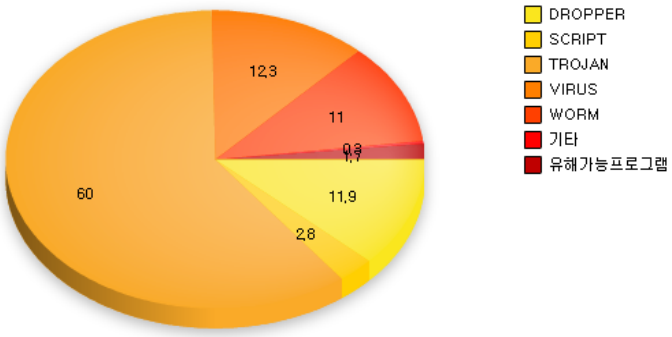
악하는데 목적이 있다.

8월에는 Win32/IRCBot, Dropper/Bobax, Win-Trojan/Banker, Win-Trojan/Banker계열의 악성코드가 악성코드 대표 진단명 Top 10에 신규로 진입하였고 나머지 악성코드들은 전월 대비 소폭 상승하거나 하락 등 변동이 있었지만 대표 진단명의 전체적인 분위기에서 큰 변화는 없었다.

Win32/Virut은 440건의 피해신고가 접수되면서 8월 악성코드 대표진단명 Top 10에서 17.2%를 점유했으며 이로 인해 전월 대비 1 단계 상승으로 2위를 차지했다. 전월과 비교해 볼 때 약 1.7%의 피해신고가 증가한 수치인데 7월에는 기존의 Win32/Virut에 의한 꾸준한 피해신고와 일부 변종이 접수되면서 악성코드 대표 진단명 Top 10에 신규로 진입하면서 3위에 랭크 되었지만 8월에는 추가 변종이 발견되지 않았으며 기존의 Win32/Virut에 의한 피해신고가 꾸준히 접수되었기 때문이다. 현재 Win32/Virut의 전체적인 확산 분위기는 잠시 소강상태이지만 변종의 발견 가능성이 존재하고 기존의 Win32/Virut에 의한 꾸준한 피해신고가 증가할 것인지 하락할 것인지는 좀더 지켜볼 필요가 있다.

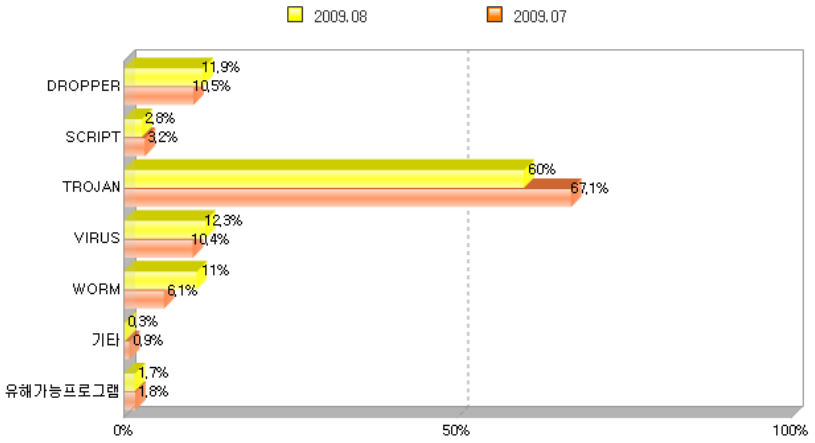
8월에는 Win-Trojan/OnlineGameHack이 1 단계 상승으로 1위를, Win-Trojan/Magania가 3 단계 하락한 10위를 그리고 Dropper/OnlineGameHack이 전월 대비 순위권 밖으로 밀려나긴 했지만 해당 악성코드들은 진단명에 차이가 있을 뿐 동일한 목적을 가지고 있다. 8월에 게임핵 악성코드류가 1위를 차지한 이유는 잠시 소강상태를 보였던 ARP Spoofing을 통한 게임핵 악성코드 유포사례가 일부 접수됐으며 자체적으로 운영하고 있는 Active Honeypot을 통해서 해킹된 웹 사이트를 경유하여 유포되는 게임핵 악성코드를 수시로 수집 및 엔진에 반영한 것도 영향을 준 것으로 보인다.

Win32/IRCBot이 13.9%를 점유하면서 4위에 랭크 되었는데 현 악성코드 트렌드가 국지성, 금전적인 이득 목적을 지향하고 있다는 것을 감안할 때 기존의 악성코드 피해건수 집계에서 Win32/IRCBot의 피해건수가 주는 의미는 크지 않았으나 8월 악성코드 대표 진단명 Top 10에 신규 진입 및 4위에 랭크 되었다는 것은 특이하다고 할 수 있다. 이 현상 Win32/Virut과 더불어 일시적인 것인지 아니면 다음 달에도 Top 10에 랭크 될 것인지에 대해서는 좀더 지켜볼 필요가 있다.



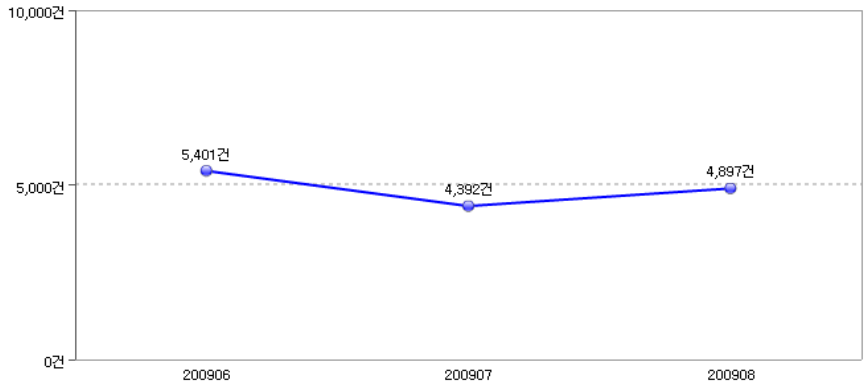
[그림 3-1] 2009년 8월 악성코드 유형별 피해신고 비율

[그림 3-2]는 2009년 8월 전체 악성코드 유형별 피해신고 건수를 나타내고 있는 그래프인데 전월과 동일하게 트로이목마 > 바이러스, 드롭퍼 > 웜 > 스크립트 > 유해가능 프로그램 > 기타 순으로 정리해 볼 수 있다.



[그림 3-2] 2009년 7/8월 악성코드 유형별 피해신고 비율 전월 비교

8월 악성코드 유형별 피해신고 비율도 전월과 유사하게 특정 악성코드 유형에서 눈에 띄게 큰 폭으로 증가했거나 감소한 현상은 없었으며 최대 8%이내에서 상승이나 감소가 있었다. 7월까지 악성코드 유형별 피해신고에서 바이러스의 경우 최대 약 10%를 넘지는 않았지만 8월에 약 1.8% 소폭 상승하면서 처음으로 10%를 넘어서 12.3%를 점유했는데 원인은 앞에서 언급한 것처럼 꾸준한 Win32/Virut계열의 바이러스에 의한 피해신고 접수와 Win32/Induc의 피해신고가 겹친 것으로 볼 수 있다. 또한 웜의 경우도 마찬가지로 8월에 약 5%가 증가한 12.3%의 점유율을 보이고 있는데 정확한 원인은 파악이 불가능하다. 그 외 악성코드 유형에서 별다른 특이사항은 발견되지 않았다.



[그림 3-3] 월별 피해신고 건수

월별 피해건수는 8월에 다시 증가했는데 증가 원인은 앞에서 여러 번 언급했기 때문에 생략하도록 한다.

이번 Win32/Induc과 관련해서 한가지 짚고 넘어가야 할 것이 있다. Win32/Induc에 대해서 아무런 증상이 없는데 백신업체에서 과잉 대응한 것이 아니냐는 논란이 있었다. 백신업체에서는 파일의 원래 제작목적과 상반되는 코드가 존재하고 해당 코드가 실행되어 악의적인 행위를 한다면 당연히 진단해야 하며 설사 아무런 증상이 발생하지 않더라도 분석 후 악성으로 판단되면 진단 및 치료하는 것이 원칙이라는 것을 알아야 한다.

이번 Win32/Induc이 단순히 델파이 소스에 자신의 코드를 삽입하는 것 외에는 별다른 증상은 없어서 그나마 다행이었지만 만약 Win32/Virut처럼 순수 악의적인 목적을 가진 바이러스였다는 가정하에 컴파일 된 파일이 감염된 채로 인터넷을 통해서 일반 사용자들의 PC에 배포되었을 것이고 해당 파일이 실행되면서 저번 7.7 DDoS 악성코드와 유사한 악성코드를 추가로 일반 사용자들 PC에 다운로드 하여 실행되었다면 피해는 상당히 켰을 것이고 이로 인해 다시 한번 혼란에 빠질 수도 있었다.

이번 Win32/Induc의 경우를 볼 때 개발자 입장에서 코딩하는 것도 중요하지만 어떻게 하면 좀더 안전하게 코딩하고 배포할 수 있는지에 대해서 진지하게 생각해 볼 필요가 있다.

(2) 국내 신종(변형) 악성코드 발견 피해 통계

8월 한 달 동안 접수된 신종 (변형) 악성코드의 건수 및 유형은 [표3-3] 과 같다.

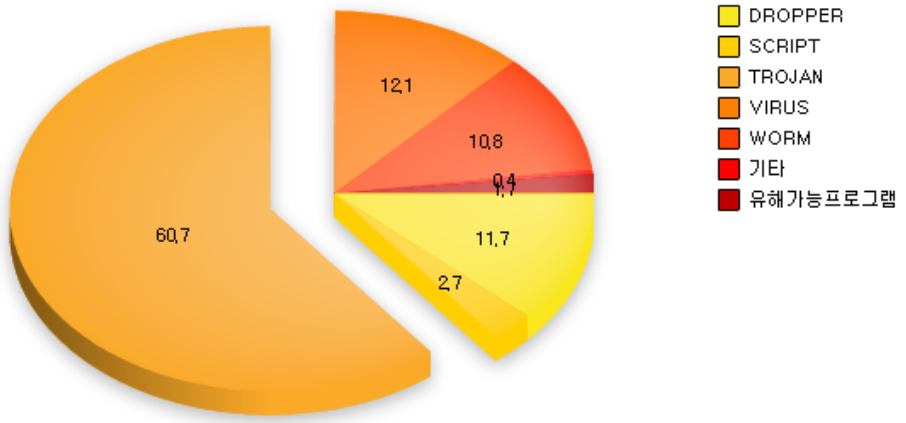
월	트로이목마	드롭퍼	스크립트	웜	파일	유해가능	기타	합계
2009.06	2,899	324	253	151	104	22	6	3,759
2009.07	2,214	309	93	161	431	20	30	3,258
2009.08	1,989	275	88	87	208	6	5	2,658

[표3-3] 2009년 최근 3개월 간 유형별 신종 (변형) 악성코드 발견 현황

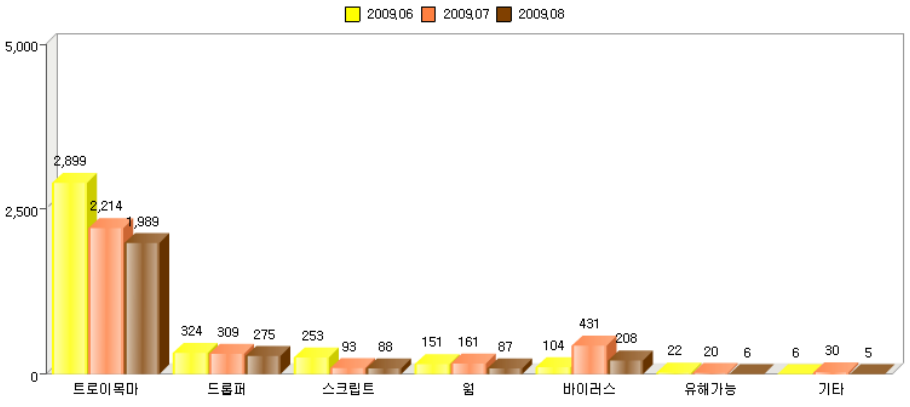
이번 달 악성코드는 전월 대비 18% 감소 하였다. 전월과 마찬가지로 대부분의 악성코드 유형에서 감소 추세가 있었다. 트로이목마는 전월 대비 10% 감소가 있었다. 대부분의 악성코드가 3개월 연속 감소추세에 있지만 감소추세임을 간과 해서는 안 된다. 여전히 작년 동기와 비교하면 악성코드는 왕성한 활동을 보이고 있다.

다음은 이번 달 악성코드 유형을 분류 하였다.

트로이목마가 전체의 60.7% 를 차지 하고 이어서 드롭퍼 및 스크립트 악성코드 유형으로 분포 되어 있다.



[그림3-4] 2009년 08월 신종 및 변형 악성코드 유형



[그림3-5] 최근 3개월간 신종 및 변형 악성코드 분포

가장 많은 유형을 차지하는 트로이목마 유형은 최근 감소 추세가 뚜렷한 것을 알 수가 있다. 감소의 원인은 명확하지 않지만 다음날 이러한 원인에 대해서 다각도로 검토 해볼 수 있는

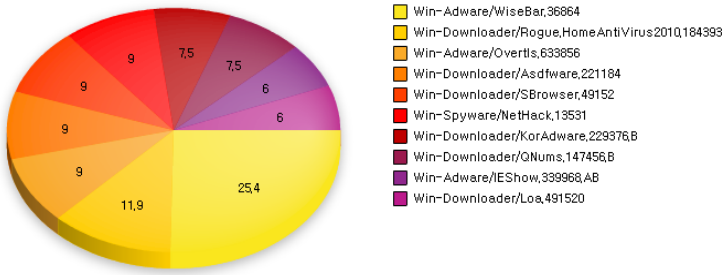
자료가 나올 것으로 기대해본다. 최근 안철수 연구소는 개인 사용자 상용 제품에 클라우드 기반 기술의 안랩 스마트 디펜스 엔진을 탑재 했다. 이러한 노력의 일환으로 안철수 연구소로 접수되는 신규 악성코드가 감소 할 수도 있는데 이러한 부분은 다음 달에 조사하여 정리하도록 하겠다.

2. 스파이웨어 통계

(1) 8월 스파이웨어 피해 현황

순위		스파이웨어 명	건수	비율
1	NEW	Win-Adware/WiseBar.36864	17	25.4 %
2	NEW	Win-Downloader/Rogue.HomeAntiVirus2010.184393	8	11.9 %
3	NEW	Win-Adware/Overtls.633856	6	9 %
4	NEW	Win-Downloader/Asdfware.221184	6	9 %
4	NEW	Win-Downloader/SBrowser.49152	6	9 %
4	NEW	Win-Spyware/NetHack.13531	6	9 %
4	NEW	Win-Downloader/KorAdware.229376.B	5	7.5 %
4	NEW	Win-Downloader/QNums.147456.B	5	7.5 %
4	NEW	Win-Adware/IEShow.339968.AB	4	6 %
10	NEW	Win-Downloader/Loa.491520	4	6 %
합계			67	100%

[표 3-4] 2009년 8월 스파이웨어 피해 Top 10



[그림 3-6] 2009년 8월 스파이웨어 피해 Top 10

2009년 8월 에는 애드웨어 와이즈바(Win-Adware/WiseBar.36864)가 가장 많은 피해를 입힌 것으로 나타났다. 애드웨어 와이즈바는 국내에서 제작된 키워드 검색프로그램으로 IE의 플러그인 형태로 동작하며 사용자의 검색 키보드 입력에 대한 광고를 노출하는 애드웨어다. 사용자 동의 없이 여러가지 광고성 프로그램을 설치하는 것으로 알려진 다운로더 에이디에스에프웨어(Win-Downloader/Asdfware.221184)가 피해 Top10에 등록되었다. 다운로더 에

이디에스에프웨어는 주로 국내 고전게임 사이트를 통해 배포되고 있다.

순위		대표진단명	건수	비율
1	7	Win-Downloader/Rogue.FakeAV	246	27.4 %
2	-	Win-Dropper/Rogue.FakeAV	238	26.5 %
3	-2	Win-Downloader/Zlob	197	21.9 %
4	NEW	Win-Spyware/Crypter	65	7.2 %
5	NEW	Win-Dropper/Rogue.SystemSecurity	31	3.4 %
5	NEW	Win-Dropper/Rogue.TotalSecurity2009	30	3.3 %
7	-3	Win-Adware/IEShow	23	2.6 %
8	NEW	Win-Adware/WiseBar	19	2.1 %
9	NEW	Win-Downloader/Asdfware	14	1.6 %
10	NEW	Win-Adware/Overtls	12	1.3 %
합계			**899**	**100%**

[표 3-5] 8월 대표진단명에 의한 스파이웨어 피해 Top10

[표 3-5]은 변형을 고려하지 않은 대표 진단명을 기준으로 한 피해 건수이다. 외산 가짜 백신을 설치하는 다운로더 즐롭(Win-Downloader/Zlob)과 스파이웨어크립터(Win-Spyware/Crypter)에 의한 피해가 계속해서 큰 비중을 차지하고 있으며, 이들 스파이웨어가 설치하는 것으로 알려진 외산 가짜 백신인 시스템시큐리티와(Win-Dropper/Rogue.SystemSecurity) 토탈시큐리티2009(WinDropper/Rogue.TotalSecurity2009)이 그 뒤를 이었다. 7위부터 10위까지의 애드웨어는 국내에서 제작된 애드웨어로 확인되었다.

2009년 8월 유형별 스파이웨어 피해 현황은 [표 3-6]과 같다.

구분	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
6월	108	350	77	3,709	0	12	2	2	0	4,260
7월	156	426	172	412	0	26	4	4	0	1,200
8월	**170**	**207**	**347**	**596**	**0**	**6**	**0**	**3**	**0**	**1,330**

[표 3-6] 2009년 8월 유형별 스파이웨어 피해 건수

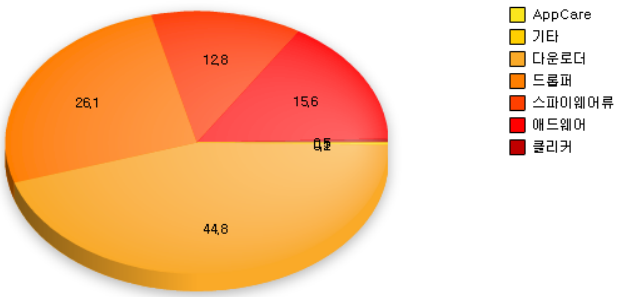
상반기 계속해서 변형을 생산하며 스파이웨어 감염피해의 대부분을 차지하던 다운로더류의 피해건수는 7월을 기점으로 대폭 감소했다. 다운로더류의 피해는 지난달에 비해 소폭 증가했으나, 애드웨어의 피해건수는 감소했다.

(2) 8월 스파이웨어 발견 현황

8월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 3-7], [그림 3-7]와 같다.

구분	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
6월	68	130	57	2,712	0	10	2	0	0	2,979
7월	116	190	143	279	0	20	3	0	0	751
8월	**116**	**92**	**312**	**453**	**0**	**5**	**0**	**0**	**0**	**978**

[표 3-7] 2009년 8월 유형별 신종(변형) 스파이웨어 발견 현황



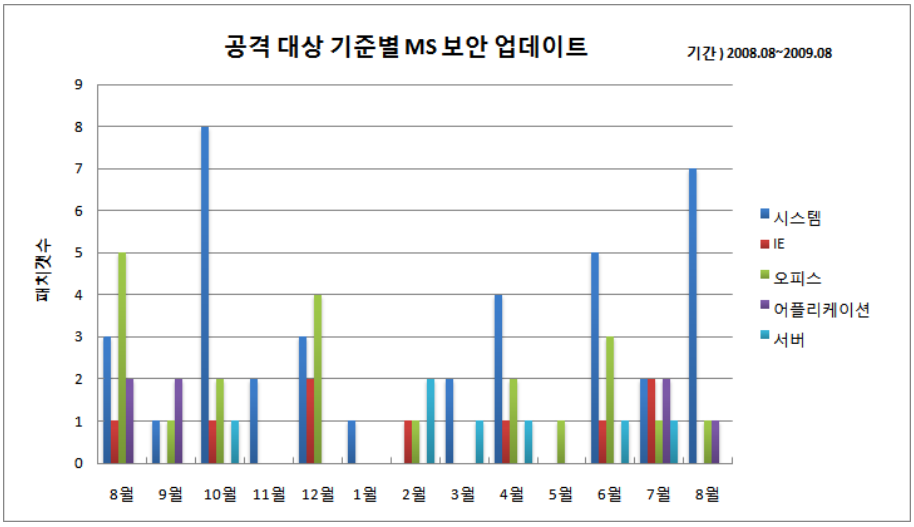
[그림 3-7] 2009년 8월 발견된 스파이웨어 프로그램 비율

상반기 가장 많은 피해신고가 접수된 다운로더류는 7월부터 피해신고가 감소하기 시작했다. 8월에는 소폭 증가했으나 그 수는 상반기에 비해 미미하다. 8월에는 드로퍼류가 많이 발견되었다. 8월에 진단 추가된 드로퍼류 중 대부분이 외산 가짜 백신을 설치하는 기능을 하는 스파이웨어였다. 하반기에는 가짜 백신을 설치하는 드로퍼류의 증가와 함께 외산 가짜 백신의 피해증가가 우려된다.

3. 시큐리티 통계

(1) 8월 마이크로소프트 보안 업데이트 현황

마이크로소프트사로부터 발표된 이달 보안 업데이트는 총 9건으로 긴급(Critical) 5건, 중요(Important) 4건이다.



[그림 3-8] 8월 MS 보안 업데이트 현황

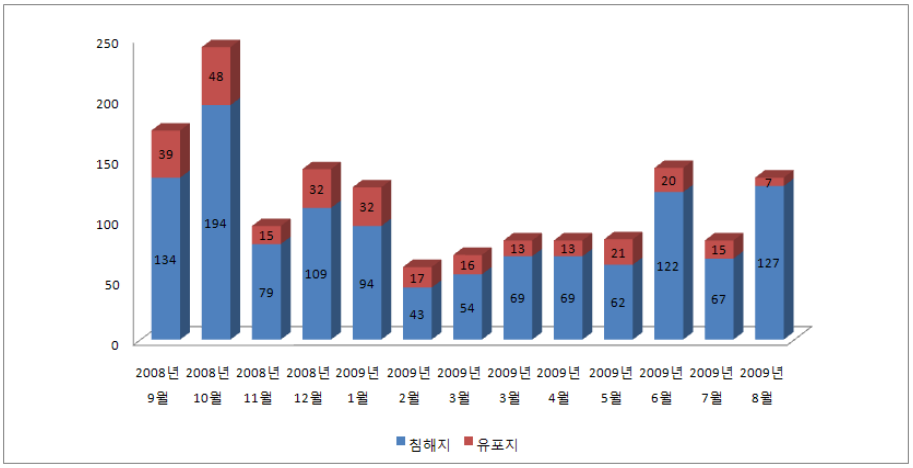
위험도	취약점	PoC
긴급	(MS09-039) MS WINS 취약점으로 인한 원격 코드 실행 문제점	유
긴급	(MS09-043) MS Office Web Component 취약점으로 인한 원격 코드 실행 문제점	유
긴급	(MS09-044) MS Remote Desktop Connection 취약점으로 인한 원격 코드 실행 문제점	유

[표 3-8] 2009년 08월 주요 MS 보안 업데이트

이 달에는 지난 7월에 발표된 Microsoft Office Web Component 취약점에 관련된 패치가 발표되었으므로 반드시 해당 보안 패치를 진행하여야 한다. 또한, MS WINS와 MS Remote Desktop Connection 취약점은 원격으로 코드를 실행할 수 있는 문제를 가지고 있기 때문에 패치가 적용되지 않았을 경우 심각한 문제를 일으킬 수 있다.

(2) 2009년 8월 웹 침해사고 및 악성코드 배포 현황

2009년 8월 웹 침해사고 및 악성코드 배포 현황



[그림 3-9] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

2009년 8월 악성 코드를 위해 침해된 웹사이트의 수와 악성 코드 유포지의 수는 127/7 2009년 7월의 67/15와 비교하여 유포지의 수는 소폭 감소하였고 침해지의 수는 큰 폭으로 증가하였다. 예전에는 침해된 사이트의 HTML 코드 내에 쉘코드 등을 삽입하여 배포하였으나, 요즈음에는 쿠키정보를 공격자에게 전송하는 코드 역시 삽입되어 있다.

다음 코드는 실제 공격 코드의 일부이다.

```
{var endstr=document.cookie.indexOf(";",iz);if(endstr==-1)
….
{var arg=name+ "=";var alen=arg.length;var clen=document.cookie.length;var i=0;var
```

[그림 3-10] 쿠키를 전송하는 공격코드

위와 같은 코드가 실행 되면 asp&location=http%3a//203.,,,, 20windows%20nt%205.1%3b%20sv1%29와 같은 정보가 전송된다. 이러한 공격으로부터 사용자의 시스템을 방어하기 위해서는 항상 사용제품의 보안 상태를 최신으로 유지하고, 최신 상태의 안티 바이러스 제품을 사용해야 한다.

4. 사이트가드 통계

(1) 2009년 8월 웹 사이트 보안 요약

구분	건수
악성코드 발견 건수	302,814
악성코드 유형	926
악성코드가 발견된 도메인	853
악성코드가 발견된 URL	6,381

[표3-9] 8월 웹 사이트 보안 요약

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

[표 3-9]는 2009년 8월 한달 동안 웹 사이트를 통해 발견된 악성코드 동향을 요약해서 보여주고 있다.

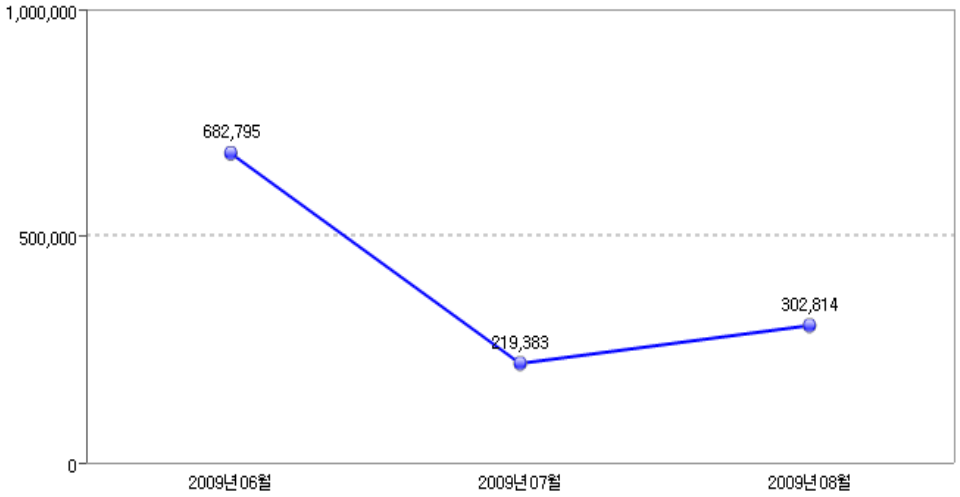
사이트가드의 집계에 따르면 8월 한달 동안 악성코드는 926종 302,814건 발견되었으며, 악성코드가 발견된 도메인은 853건, 악성코드가 발견된 URL은 6,381건으로 발견된 URL 건수만 제외하고 모두 지난 6월보다 증가 하였다. 악성코드 발견건수 302,814건은 6월 302,814건에 비해 38% 수준 증가한 수치이다. 또한, 악성코드 유형은 지난달 보다 12% 증가하였으며, 악성코드가 발견된 도메인은 10%가 증가하였다. 하지만, 악성코드가 발견된 URL은 지난달보다 28%가 감소하였다. 이는 웹 사이트를 이용하여 악성코드를 배포하는 방식이 하나의 도메인에 여러 URL을 이용하였던 추세에서, 이제는 여러 도메인을 사용하는 추세로 변화고 있는 것으로 추정된다.

8월 사이트가드 통계를 기반으로 한 분석결과는 다음과 같다.

[1] www.siteguard.co.kr

(2) 악성코드 월간 통계

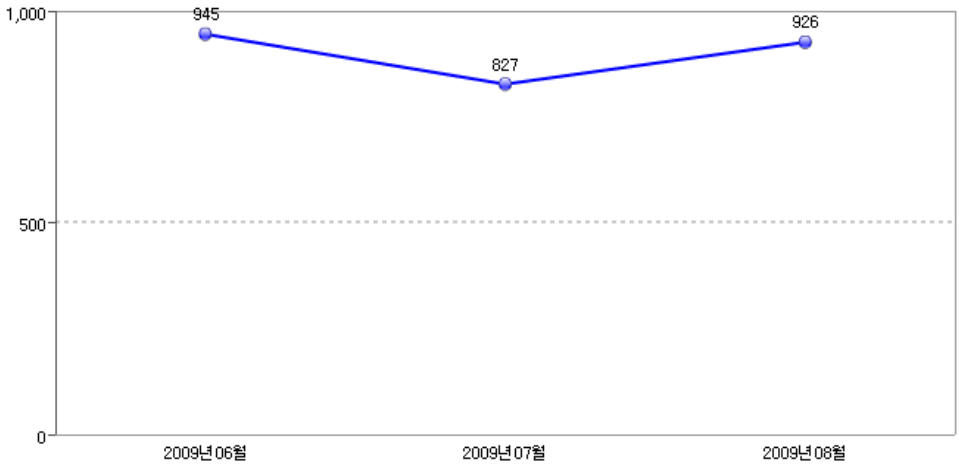
가) 악성코드 발견건수



[그림3-11] 월별 악성코드 발견건수

[그림 3-11]은 최근 3개월인, 2009년 6월부터 2009년 8월까지의 악성코드 발견 건수의 추이를 나타내는 그래프로 8월 악성코드 발견 건수는 302,814건으로 지난달의 급격한 감소세를 벗어나 38% 증가하였다.

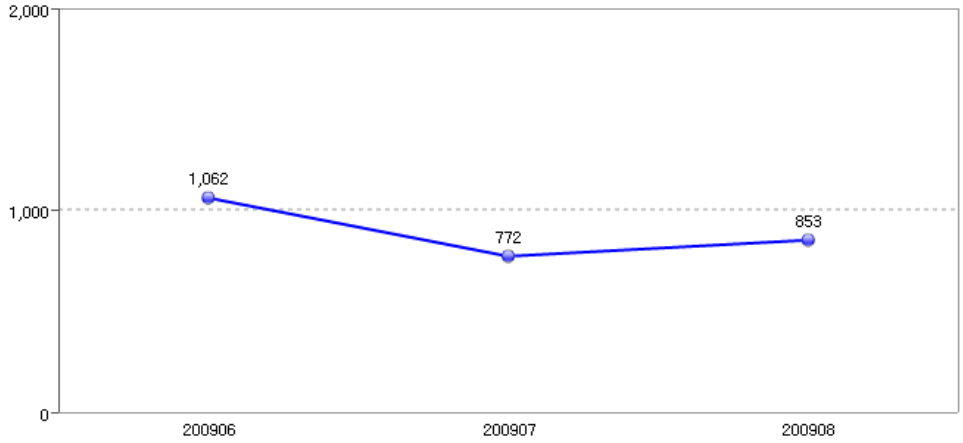
나) 악성코드 유형



[그림3-12] 월별 악성코드 유형

[그림 3-12]은 최근 3개월간 발견된 악성코드의 유형을 나타내는 그래프로 8월에는 926종으로 지난 7월에 비해 소폭 증가하였다.

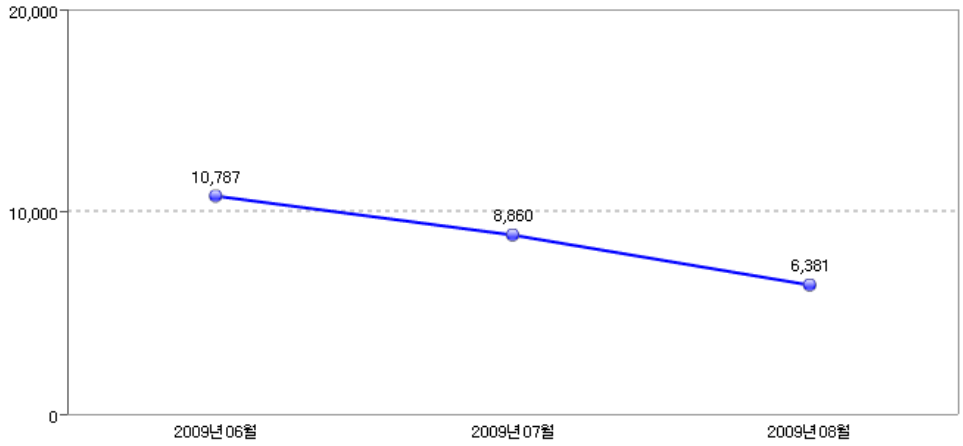
다) 악성코드가 발견된 도메인



[그림3-13] 월별 악성코드가 발견된 도메인

[그림 3-13]은 최근 3개월간 악성코드가 발견된 도메인 수의 변화 추이를 나타내는 그래프로 8월 악성코드가 발견된 도메인은 853개로 전월에 비해 소폭 증가하였다.

라) 악성코드가 발견된 URL



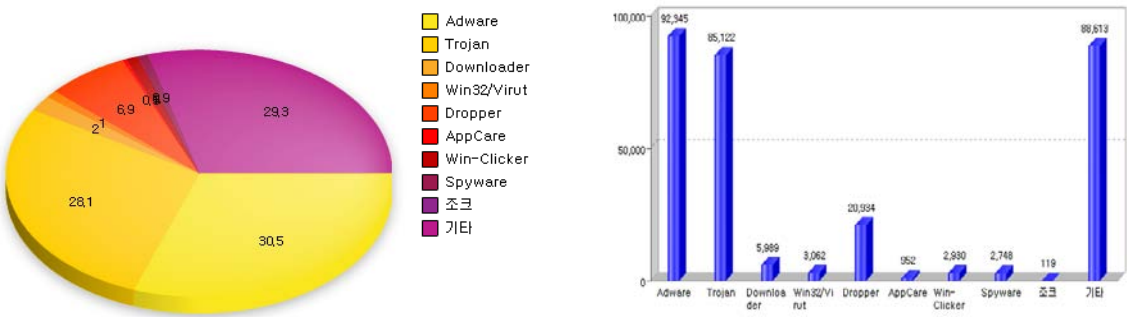
[그림3-14] 월별 악성코드가 발견된 URL

[그림 3-14]는 최근 3개월간 악성코드가 발견된 URL 수의 변화 추이를 나타내는 그래프로 8월 악성코드가 발견된 URL 수는 6,381개로 전월에 비해 28% 감소하였다.

(3) 유형별 악성코드 배포 수

유형	건수	비율
Adware	92,345	30.5 %
Trojan	85,122	28.1 %
Downloader	5,989	2 %
Win32/Virut	3,062	1 %
Dropper	20,934	6.9 %
AppCare	952	0.3 %
Win-Clicker	2,930	1 %
Spyware	2,748	0.9 %
조크	119	0 %
기타	88,613	29.3 %
합계	302,814	100 %

[표3-10] 유형별 악성코드 배포 수



[그림3-15] 유형별 악성코드 분포

[표 3-10]과 [그림 3-15]은 8 한달 동안 발견된 악성코드를 유형별로 구분하여 발견 건수와 해당 비율(%)를 보여주고 있다.

8월 한달 동안 총 302,814개의 악성코드가 발견되었으며 이중 Adware류가 92,345개로 7월에 이어서 1위를 고수하였다. Trojan류는 85,122개로 2위를 차지하였으며, 3위는 Dropper류가 20,934개로 3위를 차지하였다.

(4) 악성코드 배포 순위

순 위		악성코드명	건수	비율
1	NEW	Win32/Induc	76,275	33 %
2	-	Win-Adware/Shortcut.InlivePlayerActiveX.234	46,724	20.2 %
3	-2	Win-Trojan/Xema.variant	45,670	19.7 %
4	NEW	Win-Trojan/Hupigon.22016.AA	16,838	7.3 %
5	NEW	Win-Dropper/KorZlob.5291388	12,991	5.6 %
6	-2	Win-Adware/Shortcut.IconJoy.642048	7,549	3.3 %
7	-2	Win-Adware/Shortcut.INBEE.iomeet.267270	7,025	3 %
8	-1	Win-Adware/BHO.HiMyCar.237568	6,912	3 %
9	-3	Win-Trojan/StartPage.505344	6,403	2.8 %
10	-	Win32/Parite	4,900	2.1 %
합계			231,287	100 %

[표3-11] 유형별 악성코드 배포 Top 10

[표 3-11]는 8월 한달 동안 웹 사이트에서 사이트가드를 통해 확인된 악성코드 배포 Top 10을 보여주고 있다. Top 10에 포함된 악성코드들의 총 배포건수는 231,287건으로 8월 한 달 총 배포건수 302,814건의 약 76%에 해당된다. '[표3-11]유형별 악성코드 배포 Top10'에서 알 수 있듯이 Top10의 대부분은 Adware류와 Trojan류가 차지 하였다.

특이한 점은 델파이 개발자를 타겟으로 제작된 Win32/Induc이 악성코드 Top1에 올랐다는 것이다. 이 점은 개발단계에서부터 악성코드 검사 확인이 얼마나 중요한지를 알리는 좋은 사례이며, 앞으로 개발자부터 악성코드의 위협에 대한 인식과 예방조치가 앞장서는 계기가 되길 바란다.

요컨대, 2009년 4월부터 시작된 악성코드의 증가세는 6월에 정점을 찍고 7월에는 감소하였으나, 다시 8월부터 증가추세를 보이고 있다. 앞으로도 매월 악성코드 배포건수는 증가세와 감소세가 반복되겠지만, 전반적으로는 지속적으로 악성코드는 증가할 것이다. 특히 웹사이트를 통한 악성코드 배포가 효과적인 측면에서 여타의 배포방식보다 높기 때문에, 기업 보안관리자는 사이트가드와 같은 웹 보안 서비스를 이용하여 계속적인 자사 사이트에 대한 관리가 필요할 것이다.

ASEC REPORT 작성을 위하여 다음과 같은 분들께서 수고하셨습니다.

2009년 8월호

편집장	선임 연구원	허 종 오
집필진	선임 연구원	정 진 성
	선임 연구원	차 민 석
	선임 연구원	허 종 오
	주임 연구원	장 영 준
	주임 연구원	강 동 현
	주임 연구원	안 창 용
	주임 연구원	김 민 성
	연 구 원	김 용 구
	연 구 원	하 동 주
감 수	상 무	조 시 행
참여연구원		ASEC 연구원분들
		SiteGuard 연구원분들