안철수연구소에서 발행하는 월간 보안 보고서

ASEC 리포트

2009년 7월호

이달의 보안 이슈

1. 악성코드 – DDoS 악성코드의 공격으로 인한 사회적 혼란 2
2. 스파이웨어 – V3를 도용한 가짜 프로그램 등장 5
3. 시큐리티 – 7.7 DDoS 패킷 분석 12
4. 중국 보안 이슈 – 중국에서 제작된 제로데이(Zero-Day) 취약점 생성기 17

ASEC 칼럼

■ 현금 자동 입출금기와 악성코드 22

이달의 통계

1. 악성코드 통계 25
2. 스파이웨어 통계 35
3. 시큐리티 통계 38
4. 사이트가드 통계 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.

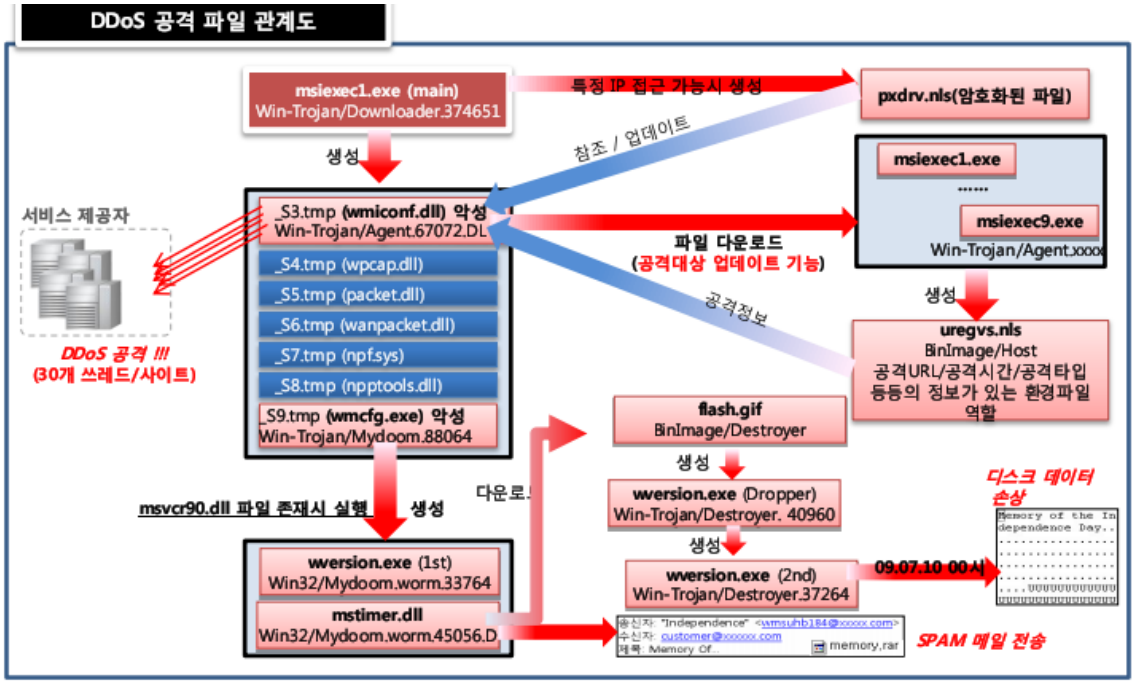
I. 이달의 보안 이슈

1. 악성코드 – DDoS 악성코드의 공격으로 인한 사회적 혼란

7월 초 우리나라는 DDoS (Distribute Denial of Service = 이하 디도스) 공격으로 인하여 정부기관 및 인터넷 뱅킹과 같은 공공 인터넷 웹 서비스에 정상적으로 접근 할 수가 없었다. 이러한 공격은 자신을 유기적으로 동작하며 활동하는 특정 악성코드들에 의해서 발생 하였다. 이 밖에 다른 악성코드로는 스팸 메일을 발송하는 스팸 봇 트로이목마가 여전히 기승을 부렸다. 또한 어도비사의 플래시 플레이어와 아크로벳 리더 각각 제로데이 취약점이 발견, 보고 되기도 하였다.

(1) DDoS 관련 악성코드

7월 초 우리나라와 미국의 공공 웹 서비스를 대상으로 하는 DDoS 공격이 발생 하였다. 이러한 공격은 소위 좀비PC(악성코드에 감염된 PC)라고 불리는 악성코드에 감염된 시스템들이 사용 되었다. 다음은 이번 공격에 사용된 악성코드들의 파일 관계도이다.



[그림1-1] DDoS 공격 파일 관계도

무엇보다도 공격을 수행한 좀비 PC 는 특정일 이후 디스크 0 부터 특정 크기만큼 손상 되어 부팅을 못하게 하는 등 공격자는 치밀한 준비를 한 것으로 보인다. 또한 공격 URL 과 시간, 타입 등이 담겨진 파일은 특정 알고리즘에 의해서 다른 곳으로부터 다운로드 되도록 되

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

어 있기도 하였다. 이러한 과정을 보면 공격자는 오래 전부터 공격 준비를 해왔을 것으로 추정 하고 있다. 이번 일과 관련해서 아직도 많은 시스템들은 안티 바이러스와 같은 최소한의 보안 프로그램도 설치가 되지 않은 것으로 보인다. 안철수연구소 경우 개인 사용자에게는 V3 Lite를 무료로 다운로드 하여 설치 하도록 할 수 있는데 이번 일 이 있은 후에도 설치된 사용자로부터 관련 악성코드의 감염보고를 접수 받을 수 있었다. 이번 일을 계기로 많은 교훈이 있었다고 생각 되지만 한편으로는 컴퓨터를 사용하는 사용자들도 안티 바이러스 제품과 같은 기본적인 보안 프로그램을 사용 할 것을 당부 드린다.

(2) 가짜 백신과 결합한 스팸 봇

스팸 봇이 여전히 기승을 부리는 가운데 이번에는 가짜 백신과 결합하여 함께 발견, 보고 되었다. 이번에 보고된 스팸 봇 역시 커널 모드 쓰레드를 시스템 프로세스에 생성 후 동작 하도록 되어 있다. 특히 가짜 백신과 함께 발견 되는 사례가 많아 두 악성코드는 연관 관계가 있는 것으로 추정 된다. 이 두 악성코드는 허위 API를 호출하는 안티 에뮬레이팅 기법이 동일하고 파일 시작 부분에 사용된 안티 디버깅 기법 두 가지가 [Single Step Exception / INT 2E(SYSENTER)] 역시 동일하다. 요즘 문제가 되고 있는 스팸 봇은 크게 3가지 형태가 있는데 첫 번째는 ndis.sys와 같은 윈도우 시스템 드라이버를 감염 시켜 동작하는 형태가 있다. 두 번째는 독립적인 드라이버 형태가 있다. 세 번째로는 *.EXE 형태의 파일이며 이후 동작은 시스템 쓰레드에 커널 모드 쓰레드를 생성하지 않는다는 것만 빼고는 동일하다. 스팸 봇은 아직 어떤 경로로 감염 되는지 명확하지 않다. 다만 사회공학기법을 이용한 웹 다운로드나 PDF 및 SWF 와 같은 취약점을 이용 할 수도 있다. 따라서 웹에서는 어떤 위험이 도사리고 있을지 모른다. 악성코드 제작자들은 사용자들이 많이 사용하는 응용 프로그램의 취약점을 노린다. 윈도우, 인터넷 익스플로러, MS 오피스 어도비 플래쉬와 아크로벳은 많은 사용자가 사용하며 잠재적으로 위험에 노출 되어 있다고 해도 과언이 아니다. 안티 바이러스 설치 보다 중요한 것은 보안 패치를 꾸준히 업데이트 받는 것이며, 이후 보안 제품으로 인한 있을 지 모른 악성코드 감염에 대비 해야 한다.

(3) 이번 달 제로데이 취약점

제로데이 취약점이란 아직 보안패치가 존재하지 않는 취약점을 말한다. 이번 달 경우 3건의 제로데이 취약점이 보고 되었으며, 해당 취약점을 이용하는 악성코드도 함께 발견 되기도 하였다. 다음과 같다.

- 마이크로소프트 MPEG2TuneRequest 제로데이 취약점 주의
- 마이크로소프트 OFFICE WEB Components(OWC) 제로데이 취약점 주의
- 어도비 플래쉬 플레이어 및 아크로벳 리더 코드 실행 제로데이 취약점

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

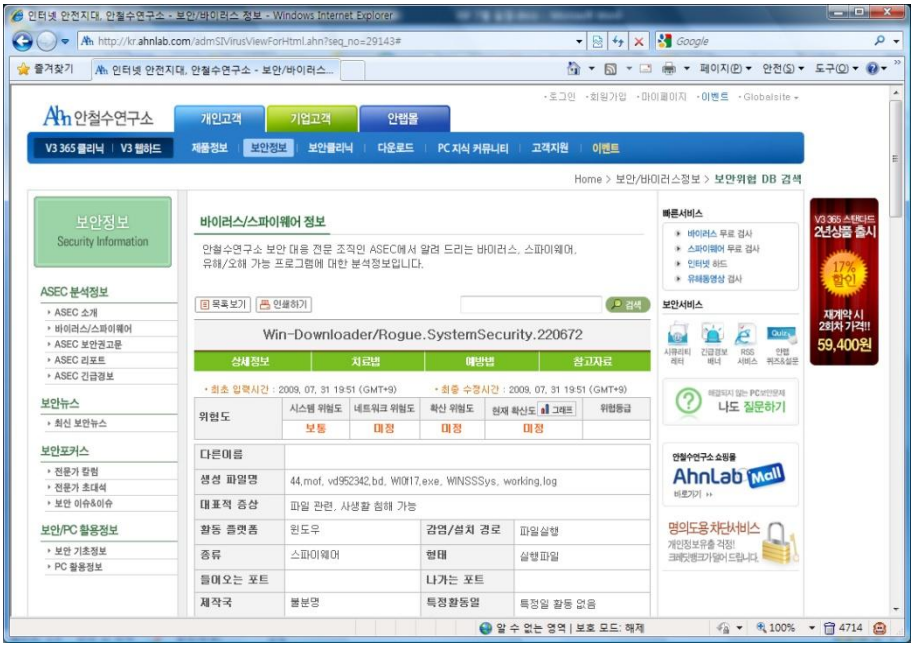
취약점은 일반적으로 악성코드 유포에 사용되는데 특히 제로데이 취약점은 타켓 공격에 집중적으로 사용된다. 이는 아직 보안 패치가 나오지 않았기 때문에 사용자들은 속수무책으로 당할 수 밖에 없게 된다. 보안 패치 적용 전 사용자들이 할 수 있는 방법으로는 각 업체가 공개한 수동 조치 방법을 최대한 적용하며 안티 바이러스와 같은 보안 제품으로 취약점이 존재하는 악의적인 파일을 진단 할 수 있도록 해야 한다.

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

2. 스파이웨어 – V3를 도용한 가짜 프로그램 등장

(1) 가짜 백신 그리고 가짜 V3

컴퓨터를 사용하는 사람이라면 누구나 한번쯤은 악성코드에 감염된 경험이 있을 것이다. 그런데 이러한 사람들 중 대다수는 악성코드가 나쁘다는 정도만 알고 있을 뿐, 자신이 감염된 악성코드가 어떠한 동작을 수행하고 어떠한 증상이 나타나는지, 그리고 그 치료방법은 어떻게 되는지 알지 못한다. 안철수연구소 ASEC에서는 이러한 고객들을 위해 악성코드 분석정보를 AhnLab.com 홈페이지에서 무료로 제공하고 있다. AhnLab.com에서 제공하는 악성코드 분석정보에는 바이러스, 스파이웨어, 유해/오해가능 프로그램에 대한 정보가 제공되며 각각에 대한 증상 및 치료 방법에 대한 정보가 기록되어 있다.



[그림1-2] AhnLab.com 의 ASEC 분석정보 페이지

최근 국내의 가짜 백신들 중에서 AhnLab.com의 분석정보를 자신들의 진단데이터로 도용하는 것들도 있어 문제가 되고 있다. 악성코드 분석정보에는 악성코드가 실행될 경우 생성하는 파일 및 폴더, 레지스트리에 상세한 정보가 포함되어 있는데, 이를 도용하여 진단 데이터로 이용하고 있는 것이다. 흥미로운 것은, 랜덤한 파일/레지스트리 이름 정보까지 그대로 도용하고 그들 홈페이지의 분석정보로 게재하고 있는 것이다. 악성코드 중에는 파일이나 레지스트리 이름을 랜덤한 것으로 생성하는 경우가 있는데, 이 경우 악성코드가 실행될 때마다 다른 이름과 레지스트리 정보를 생성하기 때문에 중복이 일어나는 경우는 거의 없다. 즉, 같은 악성코드의 분석정보를 두 개의 다른 회사에서 작성한다 하더라도 파일이름이나 레지스트리에 대한 정보가 같을 수 없다는 뜻이 된다. 이러한 랜덤한 값들을 진단데이터로 활용할 경우,

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

당연히 진단이 되지 않는다.

[AhnLab.com 홈페이지 악성코드 분석정보]

[폴더 및 파일]

Win-Dropper/BeyondKeylog.4304924가 생성하는 폴더 및 파일은 다음과 같다.

%PFDIR%₩**Eiwnrfwaofjxosg**₩ (폴더)

%PFDIR%₩**Eiwnrfwaofjxosg**₩help.chm

%PFDIR%₩**Eiwnrfwaofjxosg**₩LogW (폴더)

%PFDIR%₩**Eiwnrfwaofjxosg**₩pgkypthyc.exe

%PFDIR%₩**Eiwnrfwaofjxosg**₩unins000.dat

%PFDIR%₩**Eiwnrfwaofjxosg**₩unins000.exe

[레지스트리]

Win-Dropper/BeyondKeylog.4304924가 생성하는 레지스트리는 다음과 같다.

HKCR₩CLSID{28277BE1-769D-0A2A-9CCB-A359A2E717B8}

HKLM₩SOFTWARE₩Microsoft₩Windows₩Current Version₩Uninstall₩**Hsjd9wsdvm_is1**

HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run₩**pgkypthyc**

[스캔OO 홈페이지 분석정보]

Win-Dropper/BeyondKeylog

Program Files **Eiwnrfwaofjxosg**₩help.chm

Program Files **Eiwnrfwaofjxosg**₩LogW

Program Files **Eiwnrfwaofjxosg**₩pgkypthyc.exe

Program Files **Eiwnrfwaofjxosg**₩unins000.dat

Program Files **Eiwnrfwaofjxosg**₩unins000.exe

Program Files **Eiwnrfwaofjxosg**₩

HKEY_CLASSES_ROOT

HKCR₩CLSID{28277BE1-769D-0A2A-9CCB-A359A2E717B8}

HKEY_LOCAL_MACHINE

SOFTWARE₩Microsoft₩Windows₩Current Version₩Uninstall₩**Hsjd9wsdvm_is1**

HKEY_LOCAL_MACHINE

SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run₩**pgkypthyc**

[표1-1] Win-Dropper/BeyondKeylog 분석정보 비교

AhnLab

Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

가짜 백신들 중에는 분석정보를 도용하는 것에 그치지 않고 안철수연구소 제품의 브랜드네임까지 도용하는 것들도 있다. 아래는 Spyzero와 V3 제품의 이름을 도용한 가짜 백신들이다.

[그림1-3] 안철수연구소 스파이제로(SpyZero) 이름을 도용한 허위 안티스파이웨어

[그림1-4] 안철수연구소 V3 이름을 도용한 ○○○○○V3 허위 안티스파이웨어

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

AhnLab.com 홈페이지에 공개되어 있는 악성코드 분석정보는 악성코드의 위협으로부터 노출되어 있는 모든 사람들을 위해 공개된 것이며, 안철수연구소 ASEC 연구원들의 노고로 만들어진 지적 재산이다. 이를 도용하는 것은 엄연히 저작권 침해에 해당한다. 가짜 백신은 사용자 동의 없이 설치되어 허위 결과를 표시하여 결제를 유도하고, 다른 악성코드를 설치하는 등의 사기행각을 저지르는 것도 모자라 이제는 저작권 침해까지 하고 있는 것이다. 사용자는 이러한 가짜 백신의 피해를 피하기 위해, 믿을 수 있는 업체에서 제작 또는 배포되는 보안 프로그램만을 설치하는 주의가 필요하다.

(2) 사용자 보안을 위협하는 무료 프로그램들

요즘은 꼭 돈을 주고 프로그램을 구매하지 않더라도, 무료로 배포되는 프로그램을 이용하여 문서 작성부터 동영상 편집까지 다양한 일들을 할 수가 있다. 심지어는 OS(Operating System)까지 무료로 배포되고 있어, 유료 프로그램을 단 하나도 설치하지 않고도 컴퓨터로 하는 거의 모든 작업들을 할 수가 있을 정도다.

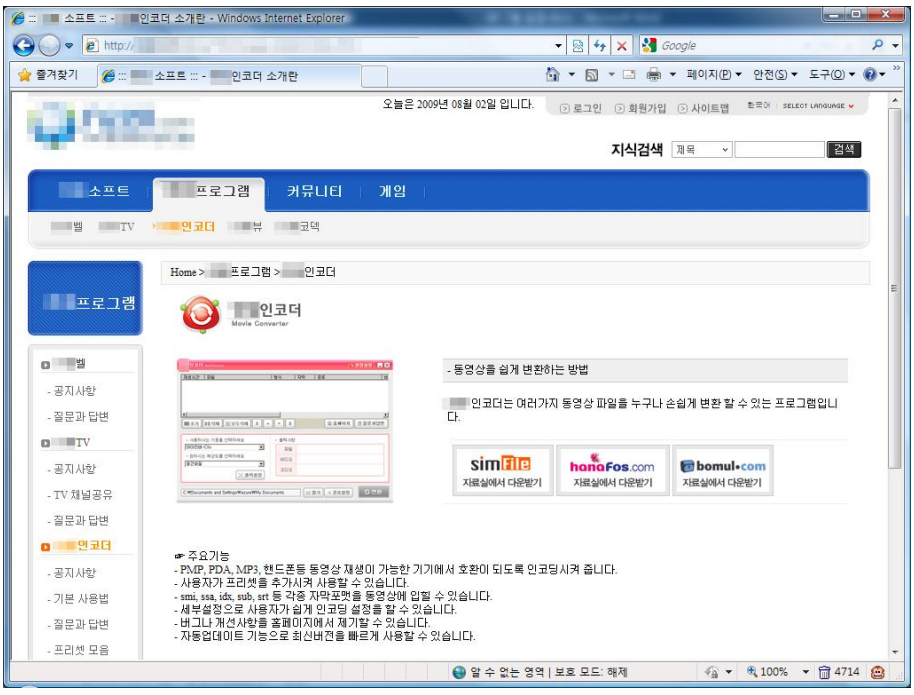
[그림1-5] 다양하고 유용한 무료 프로그램들

그런데 이러한 프로그램들은 대체 어떠한 이유에서 개발되고 또 이러한 프로그램을 개발한 개발자나 개발 업체는 어떻게 수익을 얻는 것인지 한번쯤은 의문을 가져봤을 것이다. 개인이야 다양한 이유가 있을 수 있겠지만, 기업은 어떠할까? 자본주의 사회에서의 기업은 철저하게 영리 추구가 목적인 집단이다. 그런데 이들이 아무런 수익도 없는 무료 프로그램을 배포한다는 것은 이해가 되지 않는 부분이다. 기업에서 무료 프로그램을 배포하는 이유로는 많은

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

것들이 있을 수 있겠지만, 사용자들로부터 후원을 받거나, 공익 실현을 통한 브랜드 가치 상승을 노리거나, 혹은 광고 노출을 이용한 간접 이익을 얻는 것이다. 국내 무료 배포 프로그램들의 경우는, 상당수가 광고 노출을 이용하여 수익을 얻는다. 그런데 최근 그 방법에 있어 다소 문제가 많고, 프로그램이 설치된 사용자의 시스템을 보안 위협으로 노출시키고 있어 문제가 되고 있다. 무료 프로그램이 광고를 통해 수익을 얻는 방법에는 크게 두 가지 정도가 있다. 첫 번째 방법은 프로그램 자체에 광고를 삽입하거나 팝업 광고를 노출하여 클릭을 유도하는 것이다. 프로그램 개발자나 개발업체는 이 때 발생하는 클릭에 대해 광고 업체로부터 수익을 얻는다. 이 방법은 불법 도박 사이트나 성인 광고를 노출하거나 사용자를 귀찮게 하는 것 이외에 사용자 시스템에 큰 문제를 야기하는 경우는 드물다.

두 번째 방법은 무료 프로그램이 설치될 때, 다른 업체의 광고 프로그램을 설치하여 설치당 수익을 얻는 것이다. 대개는 다른 광고 프로그램을 설치하기 전에 사용자 약관을 통해 이를 알리고 적절하게 사용자의 동의를 얻고 설치되지만, 그렇지 않은 경우가 상당수 존재한다. 아래는 다양한 무료프로그램을 제작하여 배포하는 ○○소프트의 홈페이지다. 무료TV 프로그램부터 시작하여 동영상 코덱까지 상당히 다양한 프로그램들을 제작하여 배포하고 있다. 겉으로 보면 상당히 고마운 업체로 보이지만, 실상은 그러하지가 못하다.



[그림1-6] 다양한 무료 프로그램을 제공하는 ○○소프트

○○소프트의 무료 프로그램들은 설치된 사용자의 PC에 스파이웨어(Win-Downloader/ColorSoft.434176.B)를 시스템에 설치하고, 설치된 스파이웨어는 시스템이 재부팅 될 때마다, 서버로부터 다운로드 받을 애드웨어의 목록을 받아와서 사용자 몰래 그것들

AhnLab
Copyright © AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

을 설치한다. ○○소프트에서는 단지 다운로드 목록을 수정하는 것만으로 원하는 어떠한 프로그램도 설치할 수가 있는 것이다. 그것이 설령 악성코드라 할지라도 말이다. 게다가, 시스템에 설치된 ○○소프트의 제품을 제어판의 '프로그램 추가/제거'에서 제거하여도 'Win-Downloader/ColorSoft.434176.B'는 제거되지 않아, 계속해서 다른 애드웨어를 다운로드 하게 되며, 시스템 폴더에 다른 정상 파일들과 같이 들어가 있어, 일반 사용자들이 이를 찾기는 쉽지가 않으며, 설치된 사실조차 알기가 어렵다.

아래 [[표1-2]는 이와 유사한 방법을 사용하는 'Win-Downloader/Sbrowser.364544'의 애드웨어 다운로드 목록(http://up.○○○○○○.org/duplicater_update.php)의 내용이며, 붉은 색으로 표기된 부분이 다운로드 하여 실행할 파일의 URL정보이다.

```
<?xml version="1.0" encoding="euc-kr" ?>
<ORDER>
        <DEFAULT>
                <COUNT>0</COUNT>
        </DEFAULT>
<UPDATE00>
                <TITLE>인터넷 검색 도우미(스폰서)</TITLE>
                <VERSION>20090709</VERSION>
                <SIZE>link</SIZE>
                <RANDOM>100</RANDOM>
                <ENABLE>0</ENABLE>
                <REG>
                        <HKEY>HKLM</HKEY>
                        <KEY>software₩duplicater</KEY>
                        <VALUE>version</VALUE>
                </REG>
                <ROOT>
                        <TYPE>SILENT</TYPE>
                        <PATH>
                                <DOWN/>
                                <LINK/>
                                <SILENT>http:// ○○○.○○○/AFP/Install_sbrows.exe</SILENT>
                        </PATH>
                </ROOT>
                <DESC>
                        <URL>http:// www.○○○.com<URL>
```


AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

```
                </DESC>
                <COUNT>
                        <USE>0</USE>
                        <INSTALL>1</INSTALL>
                        <URL/>
                </COUNT>
        </UPDATE00>
</ORDER>
```

[표1-2] 애드웨어 다운로드 목록

최근 국내 주요 웹사이트가 좀비 PC로부터 DDoS 공격을 받아 큰 문제가 되었다. 그런데 이 DDoS를 공격을 발생하는 악성코드가 국내 파일공유 사이트의 해킹을 통해 전파되었던 것이라고 한다. 이와 마찬가지로 [[표1-2]에서 사용된 서버가 해킹 당하여 다운로드 될 파일을 DDoS 공격을 수행하는 좀비 프로그램으로 교체된다면, 'Win-Downloader/Sbrowser.364544'에 감염된 PC는 모두 좀비 PC가 되어버리는 것이다. 그리고 굳이 서버를 해킹하지 않더라도, 해커들은 다양한 해킹기법들을 이용하여 다운로드 목록을 변경하는 것이 가능하다. 'Win-Downloader/ColorSoft'나 "Win-Downloader/Sbrowser' 뿐만 아니라, 국내 대다수의 애드웨어 다운로더들이 이와 동일한 문제점들을 갖고 있다. 그 중에는 목록을 암호화하여 관리하는 경우도 있으나, 이는 극히 일부에 불과할 뿐이어서 사용자의 시스템의 보안에 큰 위협이 된다. 현재로써는 일반 사용자가 정상 적인 무료 프로그램과 스파이웨어를 설치하는 무료 프로그램을 구분하기는 쉽지가 않다. 따라서 보안 프로그램을 설치하고 실시간 감시 기능을 항상 켜놓는 것이 이와 같은 피해를 막을 수 있는 가장 좋은 방법이 된다. 이와 함께 사용자도 항상 믿을 수 있는 사이트에서 배포되는 무료 프로그램만을 사용하고, 신뢰할 수 있는 제작사에서 제작된 것만을 사용하는 습관을 길러야 할 것이다.

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

3. 시큐리티 – 7.7 DDoS 패킷 분석

(1) 7.7 DDoS 공격 패킷 분석

국내 주요 웹사이트에 대해 7월 7일 DDoS 공격이 발생 하였다. 이번 DDoS 공격 패킷은 무엇이 발생하며, 주요 방어책에 대해서 살펴보기로 한다. 먼저 7.7 DDoS 공격은 TCP, UDP, ICMP 프로토콜을 이용하여, 특정 웹사이트들(멀티 도메인)을 공격하도록 설계 되었는데, 공격 패킷들의 주요 특징은 아래와 같다.

- 감염 PC 에서 극도의 패킷을 유발하지는 않음. 초당 300 개 이내의 패킷으로 데이터 양이 크지 않음
- HTTP 에 임의의 데이터를 전송하는 트래픽이 가장 많이 전송되며, ICMP, UDP 도 10-15% 수준에서 차지함
- HTTP > ICMP > UDP 프로토콜 순서로 트래픽을 많이 발생시킴
- HTTP 가 약 70% 대, ICMP 가 12-20%, UDP는 6-8% 수준에서 발생
- 평균 전체 발생시키는 트래픽은 초당 약 260-300/초, 약 50-65K /초

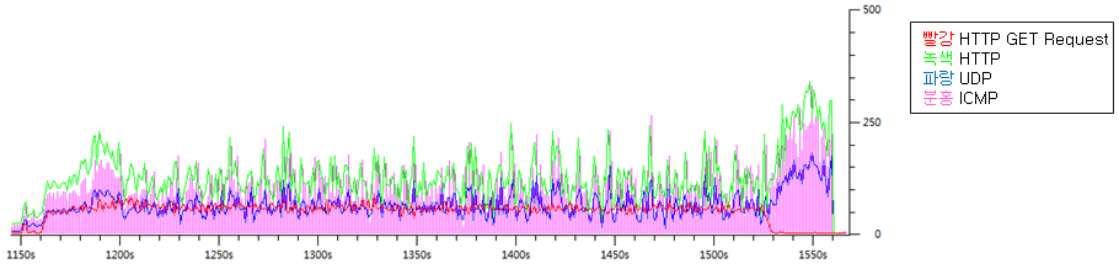
이 중에 문제가 된 것은 역시 GET Flooding 공격을 하는 HTTP 공격과 랜덤 데이터를 TCP 80 포트에 전송하는 공격이 해당된다. 여기서 GET 요청을 하는 HTTP 공격은 초당 약 20개, 12K의 데이터 전송 (출발지IP 위조 없음)하며, 랜덤 데이터를 전송하는 공격은 임의의 4-48byte 데이터를 보내는 패킷을 초당 약 43개, 3.6K의 데이터 전송 (출발지IP 위조)하게 된다.

다음 그림들은 악성코드가 감염된 컴퓨터에서 DDoS 공격을 하는 트래픽을 묘사한 것들이다.

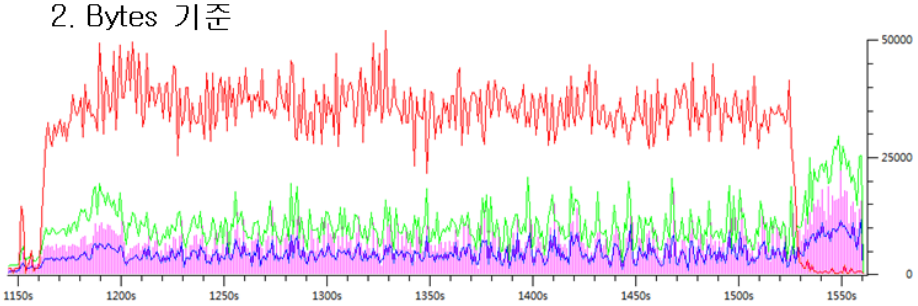
AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

감염 컴퓨터에서 발생시키는 전체 트래픽 현황

1. Packet 기준



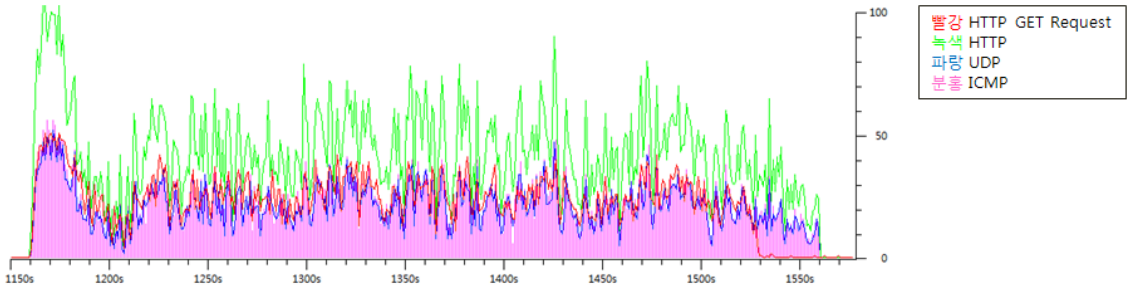
2. Bytes 기준



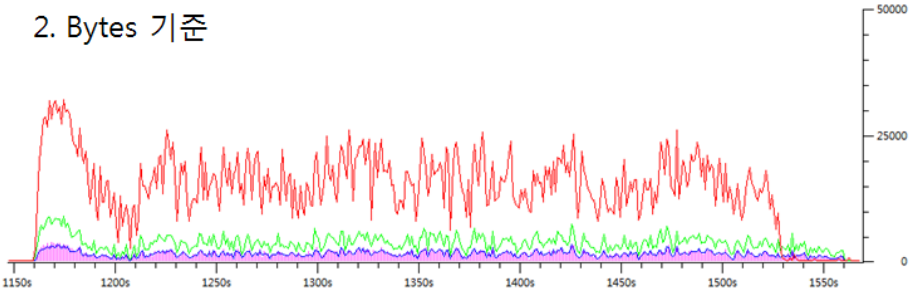
HTTP를 통한 일반 데이터 전송이 가장 높게 나타나며 ICMP 또한 크게 나타나고 있다. UDP 와 HTTP GET Request 는 비슷한 수준을 유지하고 있다. Bytes 기준일 경우는 HTTP GET Request 가 가장 큰 데이터 전송을 보인다.

특정 Target 을 대상으로 한 트래픽 현황

1. Packet 기준



2. Bytes 기준



임의의 페이로드를 포함한 HTTP 트래픽이 가장 크고 HTTP GET reqeust 와 UDP, ICMP 가 비슷한 트래픽 흐름을 보여주고 있다. Bytes 기준에서는 HTTP GET Request 에 보다 많은 데이터가 들어가며 높은 비중을 보이고 있다.

* 이 데이터는 특정 도메인으로 향한 표본을 기준으로 작성된 것이다.

[그림1-7] 감염컴퓨터에서 발생시키는 DDoS 트래픽

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

이번 DDoS 공격들에서 문제가 된 것은 대부분 TCP 80 HTTP 공격이었는데, 트래픽으로 인해 국내 웹사이트들이 지연 또는 마비되는 문제가 발생을 하게 되었다.

그렇다면, 방어 기법에는 어떠한 것들이 존재하는지 살펴보자.
악성코드에서 DDoS 공격은 해당사이트에 접속해서 정상적인 HTTP 요청(GET / HTTP/1.1)을 전달하거나, 랜덤 데이터를 HTTP 서버에 전송하게 되는데, 이 경우 효과적인 방어 기법은 Source Tracking(소스 추적)과 State Limit(접속상태 제한) 이란 방법이 있다.

다음은 PF(Packet Filter)의 Source Tracking 예제이다.

```
pass in on $ext_if proto tcp to $web_server ₩
    port www keep state ₩
    (max 200, source-track rule, max-src-nodes 100, max-src-states 3)

Remote Source 의 접속제한을 최대 3으로 제한 하면서 소스트래킹
```

그 이외 부하를 분산하기 위해서 방화벽 다중화 및 Web Cache Server 도입, 그리고 Load Balancing 등의 방법이 있다. 그러나, 엄청난 트래픽의 DDoS 공격인 경우는 네트워크 앞단에 위치한 라우터(Router)가 트래픽을 버티지 못하여 마비(Hang) 될 가능성이 존재한다.

(2) Adobe PDF & Flash Zero-day 취약점

지난 7월 23일 해외 특정 사이트에서 Adobe 사의 PDF Acrobat Reader 와 플래시 플레이어의 알려지지 않은 제로데이 취약점이 발견되었다.
해당 취약점에 영향을 받는 소프트웨어는 아래와 같다.

- Adobe Acrobat 9.1.2
- Adobe Reader version 9.1.2
- Adobe Flash Player version 9.0.159.0
- Adobe Flash Player version 10.0.22.87

해당 취약점은 공격자가 특정 코드를 실행 시킬 수 있는 취약점들로, PDF 및 Flash 파일 포맷의 특정 오브젝트를 해석하는 과정에서 유효 값 검증을 제대로 하지 않아 발생한다.
해당 취약점을 이용하는 방식은 Flash 파일을 PDF 파일에 삽입하거나 웹 페이지를 통해 호스팅하는 2가지 방법이 이용된다. 아래 그림은 악의적인 flash 파일을 특정 웹 페이지에 삽입하여 공격하는 방식이다.

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

```
<param name="movie" value="    .swf">
<embed src="  .swf" width="550" height="400">
</embed>
</object>
<script language="JavaScript">
var memory;
var nop = unescape("%u0808%u0808");
var spray=decodeURI("abc                    Babcd
d21BBabc                          010abcd5016abcdI
var sss =Array(198,177,                ,141,197,19(
var arr =new Array();
for(var i=0;i<sss.length;i++)
{
arr[i]=String.fromCharCode(sss[i]-80);
}
```

[그림1-8] flash 파일을 특정 웹 페이지에 삽입하여 공격하는 방식

이러한 파일 포맷을 공격하는 방식은 몇 년 전부터 많이 발생하며, 오피스, PDF, 플래쉬, 특정 어플리케이션들이 주요 타겟이 된다. Adobe 사에서는 7월 30일 플래쉬 관련 취약점을 제거하는 보안 패치[1]를 발표하였는데, 인터넷 사용에서 Flash 는 필수임으로, 즉각적인 패치가 요망된다.

(3) ISC Bind Dynamic Update Dos

7월말 일부 ISC Bind(named) 9 버전에서 특정 조작된 Dynamic Update 쿼리를 요청 시에 서비스 거부 취약점이 발견되었다. Dynamic Update 설정이 기본(Default) 설정에서 Off 이긴 하지만 해당 기능을 해제하더라도 영향을 받기 때문에 매우 치명적이다. ISC BIND는 DNS(Domain Name Service)에 대부분 이용이 됨으로, 해당 취약점의 영향이 크다고 볼 수 있다. DNS는 Internet의 구조상 근본이 되는 서비스 임으로, 즉각적인 보안 패치가 필요하다. Dynamic Update 기능은 BIND 8 버전 이후로 지원되며, Zone 파일의 레코드를 동적으로 갱신할 수 있는 기능인데, 일반적으로 Dynamic DNS 업체 또는 Master와 Slave 사이의 통신에서 주로 이용된다.

Dynamic Update 요청은 다음과 같은 구조를 갖는다.

```
+-----------------------------------------------------------+
| Header | Zone | Prerequisite | Update | Additional Data |
+-----------------------------------------------------------+
```

특히, 해당 취약점은 다음 공격 Dynamic Update 요청처럼 prerequisite 섹션에 "ANY" type 레코드를 갖고 적어도 하나 이상의 해당 FQDN의 RRset이 존재하는 경우에 발생한다.

[1] http://www.adobe.com/support/security/bulletins/apsb09-10.html

AhnLab
Copyright © AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

```
-----------------------------------------------------------
 공격 Dynamic Update 요청
-----------------------------------------------------------
;; HEADER SECTION
;; id = 31081
;; qr = 0      opcode = UPDATE      rcode = NOERROR
;; zocount = 0   prcount = 1   upcount = 0   adcount = 0

;; ZONE SECTION (1 record)
;; example.com.   IN        SOA

;; PREREQUISITE SECTION (1 record)
www.example.com. 0         IN        ANY       ; no data
-----------------------------------------------------------
```

해당 공격이 성공하는 경우, BIND Daemon이 Crash 되어 도메인 요청에 대한 정상적인 서비스를 지원할 수 없게 된다. 아래 그림은 실제 공격 시 발생하는 패킷의 일부분이다.

```
⊞ User Datagram Protocol, Src Port: ssdispatch (3430), Dst Port: domain (53)
⊟ Domain Name System (query)
    Transaction ID: 0x72cf
  ⊞ Flags: 0x2800 (Dynamic update)
    Zones: 1
    Prerequisites: 1
    Updates: 0
    Additional RRs: 0
  ⊟ Zone
    ⊟ example.com: type SOA, class IN
        Name: example.com
        Type: SOA (Start of zone of authority)
        Class: IN (0x0001)
  ⊟ Prerequisites
    ⊟ www.example.com: type ANY, class IN
        Name: www.example.com
        Type: ANY (Request for all records)
        Class: IN (0x0001)
        Time to live: 0 time
        Data length: 0
```

[그림1-9] 실제 공격 Dynamic Update 요청

해당 취약점으로 공격 시 Bind 데몬 named가 중지(Denial Of Service) 됨으로 DNS가 마비될 가능성이 있어 매우 위험하다. 보안 패치는 ISC 홈페이지(http://www.isc.org)에서 업데이트 하거나 각 OS 벤더 홈페이지를 이용하여 패치작업을 수행할 수도 있다.

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

4. 중국 보안 이슈 – 중국에서 제작된 제로데이(Zero-Day) 취약점 생성기

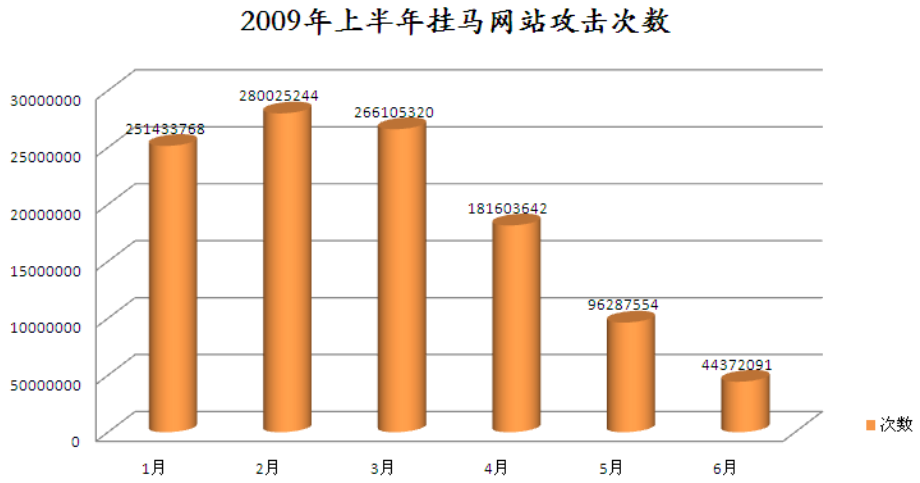
(1) 중국 라이징 상반기 보안 위협 동향 보고서 발표

7월 21일 중국의 보안 업체인 라이징(Rising)에서는 2009년 상반기 동안 발생한 보안 위협 동향들을 정리한 보고서를 발표하였다. 이번에 발표한 보고서는 2009년 상반기 동안 발생한 다양한 보안 위협 이슈들 중에서 악성코드의 주된 감염경로 중 하나인 웹 사이트를 통한 유포에 대한 중국 내에서의 정보가 비교적 상세하게 기술 되어 있었다.

[그림1-10] 2009년 상반기 악성코드 유포 웹 사이트 수치

이번에 발표된 라이징의 보고서에 따르면 2009년 상반기 동안 악성코드 유포에 악용된 웹 페이지는 총 2.9억 개이며 이는 매일 평균 162만 개의 웹 페이지에서 악성코드가 유포되고 있는 것으로 분석하였다. 이를 월별로 나타낸 그래프가 [그림 1-10]과 같으며 악성코드의 유포에 악용된 웹 페이지가 가장 많았던 3월은 총 7천 4백만 개의 웹사이트에서 유포된 것으로 집계 되었으나 2분기인 4월에 접어들어서는 그 수치가 급격하게 줄어들기 시작한 것으로 라이징에서 분석하고 있었다.

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림1-11] 2009년 상반기 웹을 통해 유포된 악성코드 수치]

그리고 악성코드 유포에 악용되는 웹 페이지로 총 11.2억 회에 걸쳐 컴퓨터 사용자들의 접속이 이루어졌으며 이는 매일 평균 622만 명이 웹 사이트를 통한 악성코드 감염의 위험에 노출되었던 것으로 집계되었다고 한다.

病毒名称	病毒感染机器台数(MAC)	所占比例
Worm.Win32.Autorun.eyr	20027396	6.24%
Hack.Exploit.Swf.a	8327465	2.59%
Worm.Win32.MS08-067.a	6721821	2.09%
Trojan.DL.Win32.Undef.vt	5375999	1.68%
Trojan.Win32.ECode.ee	5243565	1.63%
Hack.Exploit.Win32.MS08-067.eu	4420574	1.38%
AdWare.Win32.Agent.cdk	4322639	1.35%
Trojan.DL.Win32.Nodef.rn	4080127	1.27%
RootKit.Win32.Undef.bzl	3970165	1.24%
Trojan.DL.Script.JS.Agent.nx	3540249	1.10%

[그림1-12] 2009년 상반기 악성코드 TOP 10

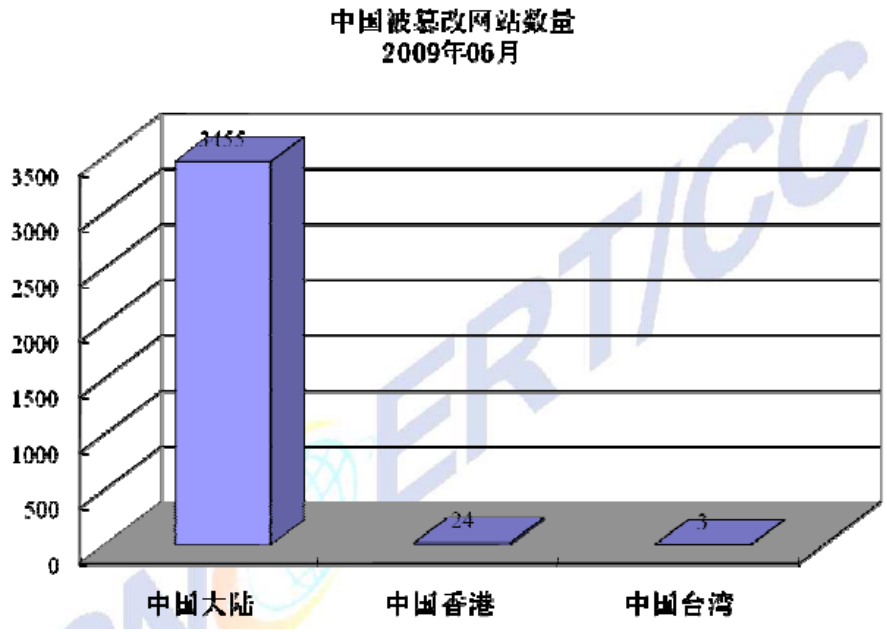
라이징에서 집계한 2009년 상반기 악성코드 TOP 10은 [그림 1-12]과 같으며 1위에는 USB와 같은 외장형 저장 장치를 통해 전파되는 Autorun 웜이 1위를 차지하였다고 한다. 그리고 그 외 운영체제나 일반 소프트웨어의 취약점을 악용하는 악성코드 형태가 3개가 포함되어 있었다. 그 중에는 최근 제로데이(Zero-Day) 취약점의 위협이 발생한 어도비 플래쉬 플레이어(Adobe Flash Player)의 취약점을 악용한 SWF 파일 형태(Hack.Exploit.Swf.a)와 마이크로소프트 윈도우 운영체제의 MS08-067 취약점을 악용하는 악성코드(Worm.Win32.MS08-067와 Hack.Exploit.Win32.MS08-067.eu) 역시 2개가 포함된 점이 특이 사항으로 볼 수 있다. 그 외 2009년 상반기에 발생한 보안 위협 중 라이징에서는 주요 사항으로 2가지를 꼽고 있었다. 그 중 첫 번째가, 7월 6일에 발생한 마이크로소프트 윈도우(Windows) 운영 체제의 BDA 튜닝 모델 MPEG2Tune 요청 관련 취약점을 악용하는 스크립

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

트 악성코드 유포를, 두 번째로는 7월 14일에 발생한 마이크로소프트 오피스에 포함된 웹 컴포넌트(Web Components) 관련 취약점을 악용하는 악성코드 유포이다.

(2) 중국 6월 웹 사이트 위, 변조 보안 사고 동향

중국 대륙의 보안 위협과 사고를 총괄하는 CNCERT/CC에서 7월 23일, 6월 웹 사이트 위·변조 보안 사고 동향 보고서를 발표 하였다.



[그림1-13] 2009년 6월 중국 웹 사이트 위·변조 통계

CNCERT/CC에서 이번에 발표한 보고서에 따르면 중국 대륙은 6월 한 달 동안 총 3455건의 웹 사이트 위·변조 사고가 발생하였으나 5월과 비교하여 399건이 감소한 수치라고 한다. 그리고 홍콩의 경우 6월 총 24건이 발생하였으나 5월과 비교하여 7건이 증가한 수치이며 대만의 경우 지난 5월과 비교하여 1건이 감소한 3건이 발생하였다고 한다. 이번 6월에 발생한 특이 사항으로는 gov.cn 도메인을 가지는 웹 사이트에서 총 161건의 웹 사이트 위·변조 사고가 발생하였으며 이 수치는 지난 5월과 비교하여 130건이나 급격하게 증가한 수치라고 한다.

(3) 바이킹 바이러스 제작자 출소 후 보안 업체 근무 희망

2007년 한국에서도 많은 감염 피해가 있었던 Viking 바이러스 제작자인 중국인 Li Jun은 남은 형기를 마치고 Shenzhen으로 돌아가 보안 업체에 근무 할 예정이라고 한다. Dellboy 바이러스로도 알려진 Li Jun은 2006년에서 2007년도 해당 바이러스 제작으로 총 10만대가 넘

AhnLab
Copyright © AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

는 컴퓨터를 감염으로 인한 피해를 발생시켰으며 해당 바이러스의 소스 코드 판매 등을 통해 총 10,000 위엔(한화 약 180만원)의 금품을 챙겼다고 한다. 이러한 혐의들로 인해 Li Jun은 4년 형을 선고 받고 현재 복역 중에 있으며 약 1년 6개월 정도의 형기가 남았다고 한다. 최근 중국 언론들과의 인터뷰를 통해 Li Jun은 남은 형기를 마친 이후에는 Shenzhen으로 돌아가 컴퓨터 보안 업체에서 근무하기를 희망한다고 하였다. 다른 보안 업체들과 달리 백신 업체로도 알려진 안티 바이러스(Anti-Virus) 업계에서는 관례적으로 악성코드 제작자 또는 제작 이력이 있는 사람 그리고 악성코드만을 전문적으로 수집하는 악성코드 수집가를 채용하지 않는 것이 일반적이다. 이러한 안티 바이러스 업계의 관례적인 면에서 볼 때 Li Jun이 출소 후 어떤 보안 업체를 직장으로 가지게 될지 주목 된다.

(4) 중국에서 제작된 제로데이(Zero-Day) 취약점 생성기

7월에는 6일과 14일과 두 차례에 걸쳐 마이크로소프트(Microsoft)에서 개발한 소프트웨어에서 알려지지 않은 제로데이(Zero-Day) 취약점을 악용한 악성코드가 발견되어 많은 주의를 요구 하였다. 이번에 발견된 취약점들은 마이크로소프트 오피스(Office)에 포함된 웹 컴포넌트(Web Components) 관련 취약점과 윈도우 운영체제에 포함된 다이렉트쇼(DirectShow) MPEG2TuneRequest 취약점이다.

[그림1-14] MS 오피스 웹 컴포넌트 취약점 생성기

[그림1-15] MPEG2TuneRequest 취약점 생성기

이러한 취약점과 이를 악용한 악성코드가 발견된 이 후 중국 언더그라운드에서는 해당 취약점을 악용하는 쉘코드(Shellcode)가 급격하게 공유되고 있었으며 이와 동시 [그림 1-14]와 [그림 1-15]와 해당 취약점들을 악용하는 스크립트 악성코드 생성기들도 발견되었다. 해당 생성기들은 사용자 인터페이스 등으로 미루어 한 명 또는 하나의 그룹에 의해서 제작 되었을 것으로 추정되고 있으며 모두 동일하게 가운데 텍스트 박스에 다른 악성코드 변형들을 다운로드 할 수 있는 웹 사이트 주소를 지정해주고 "생성" 버튼을 클릭하면 자동으로 해당

AhnLab
Copyright © AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

취약점을 악용하는 HTML 파일이 생성된다. 중국 언더그라운드에서 위와 같은 자동화된 형태의 툴이 제작되었다는 것을 통해 더 많은 보안 위협들이 대량으로 양산 될 가능성이 높을 것으로 예측 할 수가 있다.

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

II. ASEC 칼럼

■ 현금 자동 입출금기와 악성코드

현금 자동 입출금기(Automated Teller Machine, ATM)은 직원을 통하지 않고 컴퓨터를 이용해 직접 금융 거래를 할 수 있도록 고안된 기기로 현금 자동 입금 지급기, 현금 인출기, 자동화기기 등으로도 불린다. 현금 자동 입출금기 외에도 병원 장비, 티켓 발권 시스템 등 우리 주변에서 쉽게 볼 수 있는 다양한 자동화기기의 운영체계는 윈도우나 리눅스를 사용하는 경우가 많다. 보통 윈도우 2000이나 윈도우 XP가 사용되므로 윈도우 악성코드가 실행될 수 있고 이들 시스템이 악성코드 제작자의 목표가 될 수 있다. 하지만, 악성코드 제작 의도가 금전적 이득인 된 현재는 현금 자동 입출금기가 악성코드의 목표가 될 수 있다.

[그림2-1] 윈도우를 사용하는 현금 자동 입출금기

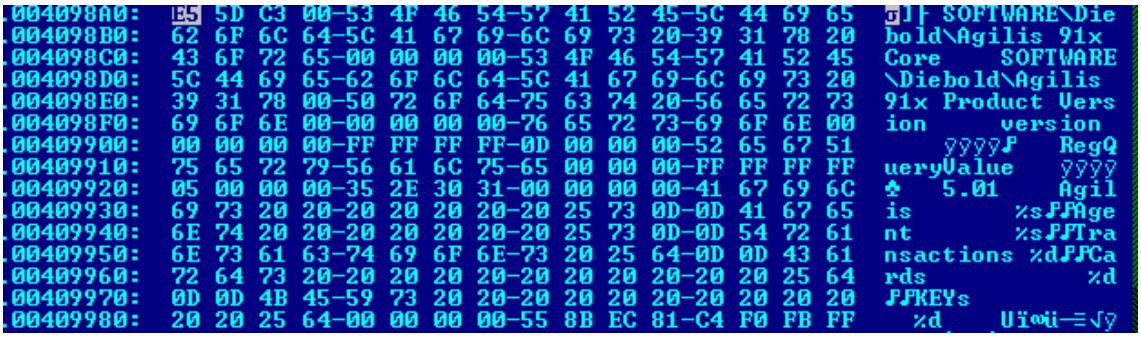
2009년 3월 26일 러시아 일간 니자비스마야 가제타는 은행 현금 자동 입출금기에서 고객 예금을 노리는 새로운 유형의 악성코드가 발견되었다고 보도했다.[1] 이후 4월, 5월에도 이 회사 소프트웨어를 사용하는 현금 자동 입출금기에 설치되어 사용자 정보를 빼가는 악성코드가 발견된다.[2]

V3에서 Win-Trojan/Skimer 시리즈로 진단되며 Win-Trojan/Skimer.57344, Win-Trojan/Skimer.50176, Win-Trojan/Skimer.41984, Win-Trojan/Skimer.81920, Win-Trojan/Skimer.79872 등 여러 변형이 존재한다. 이들 악성코드는 다이볼드(DieBold,

[1] http://www.yonhapnews.co.kr/culture/2009/03/26/0914000000AKR20090326225600080.HTML
[2] http://www.pcworld.com/businesscenter/article/166189/atm_malware_spreading_around_the_world.html

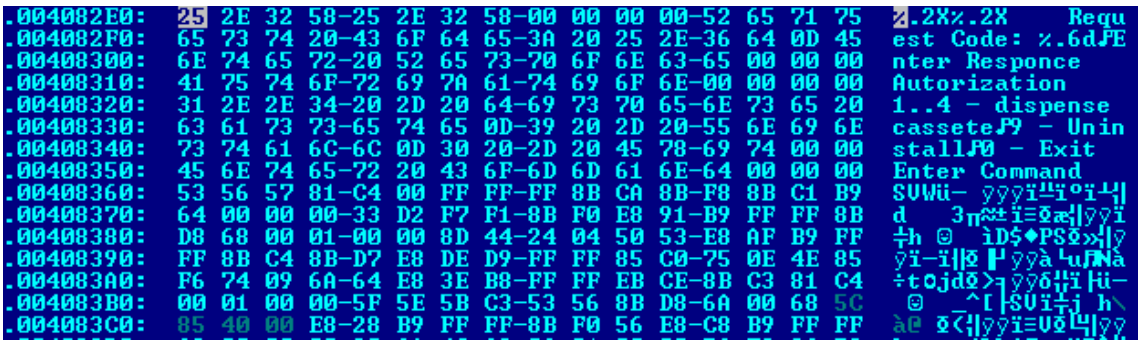
AhnLab
Copyright © AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

http://www.diebold.com/default.htm) 사의 다이볼드 아길스 91x(Diebold Agilis 91x)[1]를 목표로 제작되었다. 현금 자동 입출금기에 설치되어 사용자가 삽입한 카드 정보(magnetic-stripe data)와 카드 비밀번호를 프린트 하거나 파일로 남긴다고 한다. 수집된 정보를 이용해 신용카드 카드 복제 등에 악용될 수 있다고 한다.



[그림2-2] Diebold 사 Agilis 91x가 목표

현금자동입출금기 외부에서 명령을 내릴 수 있다고 한다.



[그림2-3] 외부에서 명령 줄 수 있음

현금 자동 입출금기를 노린 악성코드도 발견되어 충격을 주었지만 한가지 다행인 점은 이런 악성코드가 제작되기 위해서는 시스템을 잘 이해해야 하며 시스템을 관리하는 내부자가 깊게 관여해야 한다. 즉, 내부자 공모가 없다면 어려운 일이다. 이 일은 외국에서 발생했고 국내에서 사용되는 현금 자동 입출금기는 국내 자체적으로 제작된 프로그램이라 아직 이런 공격을 피해 갈 수 있지만 국내에서도 이런 문제가 발생할 가능성은 존재한다. 특히 이번에 발견된 악성코드의 경우 제작 일자가 2007년 6월 25일도 있어 제작된 지 18개월 만에 발견된 것으로 추정된다. 악성코드가 일부 시스템에만 설치되므로 널리 퍼져 빨리 발견되니 다른 악성코드와는 달리 늦게 발견된 것이다. 악성코드가 자동화 기기에 감염될 수 있으므로 이들 시스템에도 백신 프로그램 등의 보안 프로그램이 필요하게 되었다. 하지만, 현금 자동 입출금기의 경우 폐쇄망으로 구성되며 상대적으로 사양이 낮은 경우가 많다. 윈도우 2000 이전에 현금 자동 입출금기에 사용된 것으로 알려진 윈도우 3.1은 2008년 11월 2일에 공식 단

[1] http://www.diebold.com/news/newsdisp.asp?id=2905

AhnLab
Copyright © AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

종되었다고 한다.[1] 또, 단순 백신 프로그램뿐만 아니라 관리자의 부주의나 악의적인 프로그램 설치를 막기 위해 정해진 프로그램만 실행되거나 행동을 할 수 있는 보안 프로그램의 필요성도 대두되었다. 현금 자동 입출금기를 노린 악성코드는 단발성 해프닝으로 끝날 수도 있지만 향후 인터넷과 연동되는 다양한 기기들에 대한 위험성을 알려지는 소중한 기회라고 여겨 진다.

참고자료

[1] Automated Teller Machine (ATM) Malware Analysis Briefing (http://regmedia.co.uk/2009/06/03/trust_wave_atm_report.pdf)

[2] Data-sniffing trojans burrow into Eastern European ATMs (http://www.theregister.co.uk/2009/06/03/atm_trojans/)

[1] http://gizmodo.com/5077047/windows-3x-discontinued

AhnLab

Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

III. 이달의 통계

1. 악성코드 통계

(1) 7월 악성코드 통계

7 월 순위		악성코드명	건수	비율
1	-	Win-Trojan/Banker.702976.D	24	15.8 %
2	3	Win-Trojan/Netmen.221696.B	21	13.8 %
3	NEW	Dropper/OnlineGameHack.166327	15	9.9 %
3	NEW	Win-Trojan/Downloader.374651	15	9.9 %
5	NEW	Win-Trojan/Agent.33841	14	9.2 %
5	NEW	Win32/Mydoom.worm.45056.D	14	9.2 %
7	NEW	Win-Trojan/Agent.32768.AIK	13	8.6 %
8	NEW	Win-Trojan/Agent.24576.AVD	12	7.9 %
8	NEW	Win-Trojan/Agent.67072.DL	12	7.9 %
8	NEW	Win-Trojan/OnlineGameHack.166567	12	7.9 %
		합계	**152**	**100 %**

[표3-1] 2009년 7월 악성코드 피해 Top 10

6월의 Top 10에서 1위인 Win-Trojan/Banker.702976.D는 7월에도 순위변동 없이 1위를 고수했다. 대표 진단명 기준으로 볼 때 Win-Trojan/Banker계열의 악성코드가 6월 이전까지의 악성코드 피해 Top 10에 랭크 되지 못했던 것을 감안하면 Win-Trojan/Banker가 6, 7월 악성코드 피해 Top 10에서 1위를 차지했다는 것이 특이하다. 보통 고객에게서 접수된 의심파일이 Win-Trojan/Banker로 명명된 경우는 주로 중·남미권 고객들로부터 샘플이 접수된 경우인데 이는 V3제품이 중·남미 권에서 시장 점유율이 높아지고 있기 때문인 것으로 판단된다. 악성코드의 동향이 금전적인 목적을 노린 트로이목마 류로 이동하면서 거의 자취를 감췄던 Win32/Mydoom.worm의 변종이 발견되면서 7월 악성코드 피해 Top 10에서 5위에 랭크 된 것에 주목할 필요가 있다. 이번에 발견된 Win32/Mydoom.worm.45056.D는 메일의 첨부파일로 확산시도 하는 것뿐만 아니라 외국 및 국내 정부기관 및 포털, 보안업체 등 주요 사이트에 DDoS(분산 서비스 거부)공격을 수행하는 악성코드들과도 관련이 있다.

6월의 악성코드 피해 Top 10에서는 Dropper를 포함한 OnlineGameHack 계열의 악성코드가 5종이나 랭크 되어 있었지만 7월의 경우 Win32/Mydoom.worm을 비롯한 DDoS(분산 서비스 거부)공격관련 악성코드들이 고객들로부터 다수 접수되면서 OnlineGameHack 악성코드 2종만이 각각 3위, 8위에 랭크 되었을 뿐 대부분 악성코드 피해 Top 10 순위권 밖으로

AhnLab
Copyright © AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

밀려났다. 악성코드 피해 Top 10을 살펴보면 매월 신규 또는 변종 악성코드로 대체되고 있는데 이는 백신벤더의 신속한 대응으로 인해서 악성코드의 라이프 사이클이 짧아졌고 악성코드 자동 생성기, 공개된 악성코드 소스 활용 등으로 수많은 신·변종 악성코드들이 제작되고 있기 때문이다.

그 밖에 Win-Trojan/Netmen.221696.B는 3단계 상승하여 2위를 차지했고 Win-Trojan/Bho.376832는 7월에 Top 10 순위권 밖으로 밀려났다.

7 월 순위		악성코드명	건수	비율
1	1	Win-Trojan/Agent	479	18.8 %
2	1	Win-Trojan/OnlineGameHack	450	17.6 %
3	NEW	Win32/Virut	395	15.5 %
4	1	Win-Trojan/Downloader	303	11.9 %
5	5	Win-Trojan/Fakeav	269	10.5 %
6	1	Dropper/OnlineGameHack	231	9 %
7	NEW	Win-Trojan/Magania	153	6 %
8	-7	Win-Trojan/Fraudload	99	3.9 %
9	-5	Win32/Autorun	98	3.8 %
10	NEW	Dropper/Agent	77	3 %
합계			**2,554**	**100 %**

[표3-2] 2009 7월 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 파악하는데 목적이 있다.

[표 3-2]를 요약하면 아래와 같이 요약할 수가 있다.

Win-Trojan/OnlineGameHack이 1단계 상승으로 2위 차지
Win-Trojan/Downloader이 1단계 상승으로 4위 차지
Dropper/OnlineGameHack이 1단계 상승으로 6위를 차지
Dropper/Agent가 10위로 대표 진단명 Top 10에 신규 진입
Win-Trojan/Magania가 7위로 대표 진단명 Top 10에 신규 진입
Win32/Virut가 3위로 대표 진단명 Top 10에 신규 진입

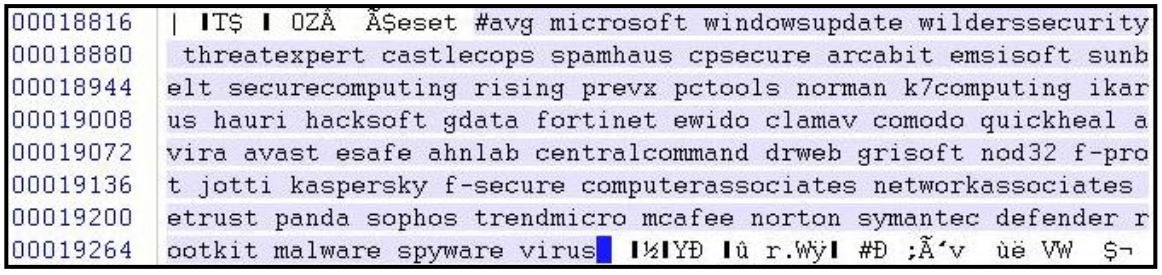
[표 3-2]에서 표기된 악성코드들은 Internet Explorer나 Acrobat Reader같은 응용프로그램의 취약점(0-day 취약점)이 존재할 경우 악성 스크립트와 함께 유포가 되는 특징을 가지고

AhnLab
Copyright © AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

있다. 그리고 대표 진단명 Top 10 순위권 안에는 들지 못 했지만 앞에서 언급한 응용 프로그램의 취약성을 공격하는 악성 스크립트는 V3 진단명 기준으로 JS/Exploit, PDF/Exploit, SWF/Exploit, JS/MPEG2Exp 등이 여러 가지가 있다.

Autorun 웜은 7월에 5단계 하락한 9위를 차지했지만 여전히 고객들로부터 피해가 꾸준히 접수되고 있다. Autorun 웜에는 특정 보안 프로그램들의 파일을 삭제하거나 손상시켜서 실행을 방해하는 AVKiller 기능을 가지고 있다. 사용자가 처리하는 것이 어려울 수도 있다.

Win32/Virut바이러스가 3위에 랭크 되면서 새롭게 Top 10에 진입했다. 보통 바이러스의 라이프 사이클을 고려해 볼 때 소멸되지 않고 꾸준히 변종이 제작되어 유포되는 바이러스는 극히 드물다. 최근에 Win32/Virut.F로 추가된 변종 Win32/Virut바이러스의 경우, 메모리에서 프로세스에 스레드(Thread)형태로 자신의 코드를 주입 및 실행함으로써 치료를 어렵게 만들고 Conficker(Kido)웜과 동일하게 감염된 시스템에서 특정 보안 사이트로 접속하는 것을 방해하는 특징을 가지고 있다. (그림 3-1. 참고)



[그림3-1] Win32/Virut.F의 보안 사이트 차단리스트

FakeAv는 7월에는 5단계 상승하여 5위를 차지하였다. FakeAv의 경우 주로 동영상 재생 프로그램 또는 코덱파일로 위장하고 있거나 메일본문에 포함된 링크를 클릭할 경우 악성스크립트가 다운로드 및 실행되면서 FakeAv를 설치하는 경우인데 사회 공학기법(예를 들면 마이클 잭슨 사망 등 사회적으로 큰 이슈가 될만한 내용으로 위장)를 사용하기 때문에 국내 사용자들도 의심 없이 링크를 클릭하여 감염되는 피해사례가 상당수 보고되고 있는 실정이다.

최근 들어 System Security라 불리는 FakeAv가 다수 고객들로부터 피해사례가 접수되고 있다. 해당 악성코드에 감염되면 윈도우의 중요 프로세스를 제외한 모든 프로세스는 종료하는 기능을 가지고 있다.

wuauclt.exe / wscntfy.exe / winlogon.exe / wininit.exe / nvsvc.exe / lsm.exe / lsass.exe / iexplore.exe / system / svchost.exe / spoolsv.exe / smss.exe / slsvc.exe / services.exe / explorer.exe / ctfmon.exe / csrss.exe / alg.exe

AhnLab
Copyright © AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

아래 그림은 FakeAv가 유포되는 경우의 한 예이다.

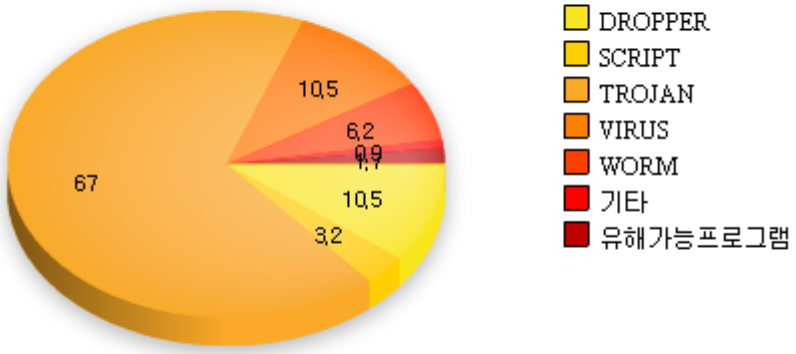
```
To: <geekitus@xxxxxxx>
Date: Thu, 11 Jun 2009 19:55:32 -0600
Message-id: <000d01c9eb00$de6506e0$6400a8c0@evelynmp52>

You have (6) message from TheBat.

Please re-configure your TheBat again.

Download attached setup file and install.
  Attachment: client_update.zip
 Description: Zip archive
```

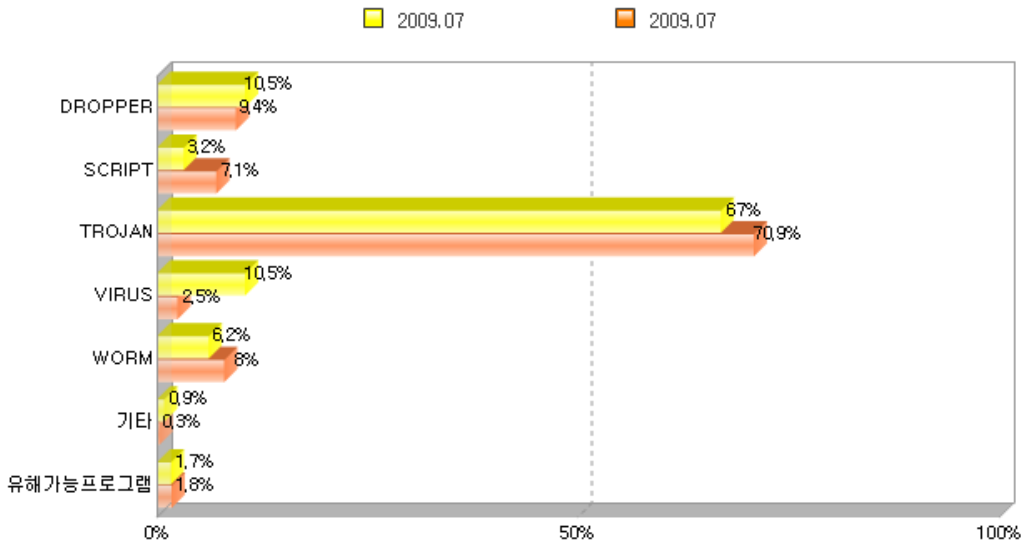
[그림3-2] 메일을 통해서 확산되는 FakeAv 샘플의 예



[그림3-3] 2009년 7월 악성코드 유형별 피해신고 비율

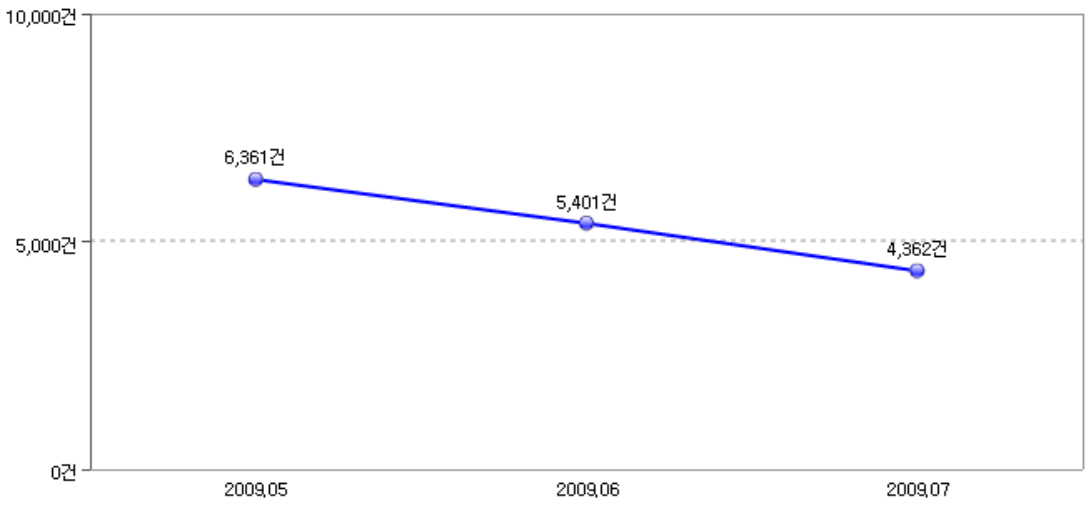
[그림 3-3]은 2009년 7월 전체 악성코드 유형별 피해신고 건수를 나타내고 있는 그래프이며 트로이목마 > 바이러스, 드롭퍼 > 웜 > 스크립트 > 유해가능 프로그램 > 기타 순으로 정리해 볼 수 있다. 보통 바이러스의 경우 10%를 넘는 경우가 없었는데 Win32/Virut의 변종이 꾸준히 발견되면서 7월에는 Trojan 다음에 위치하고 있다.

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림3-4] 2009년 7월 악성코드 유형별 피해신고 비율 전월 비교

위의 [그림 3-4]는 전월과 비교한 악성코드 유형별 피해신고를 나타낸 것이다. 트로이목마는 전월 대비 2.1%정도 감소하였으나 여전히 다른 악성코드에 비해서 월등히 높은 점유율을 보이고 있으며 스크립트, 웜, 유해가능 프로그램 역시 소폭 감소하였지만 전체적인 점유율은 전월과 거의 비슷하다. 여기서도 잘 알 수 있듯이 바이러스 경우 전월 대비 약 5배정도 증가하였는데 그 원인은 앞에서 언급하였기 때문에 여기서는 생략한다.



[그림3-5] 월별 피해신고 건수

ASEC Report 6월호에 포함된 월별 피해신고 건수와는 상이한 수치인데 이는 고객에게 좀더 정확하고 자동화된 정보를 제공하기 위해서 통계산출방식을 변경하였기 때문이다.

AhnLab
Copyright © AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

신 통계산출방식에 따르면 월별 피해신고 건수는 [그림 3-5]처럼 하락세를 나타내고 있지만 현재 사회적으로 이슈가 된 악성코드의 유포방법을 살펴보면 OS에 존재하는 취약점보다는 사용자들 사이에서 널리 사용되는 응용프로그램(Internet Explorer, Acrobat Reader 등 여러 가지)의 취약점을 공격하며 이것이 침해사고가 발생한 웹 사이트와 결합되면서 파급효과가 크다는 것이다. 또한 여기에 사회공학기법, 메신저 쪽지 등 사용자를 유혹하는 다양한 방법이 사용되고 있다.

결론은 현재 사회적으로 이슈가 되고 있는 악성코드들로부터 자신의 시스템을 안전하게 지키기 위해서는 주기적인 보안업데이트 점검 및 설치, 백신엔진을 최신으로 유지하고 주기적으로 검사 및 치료, 의심스러운 메일 또는 쪽지는 열람하지 않는 등의 기본적인 보안수칙을 지켜야 한다.

(2) 국내 신종(변형) 악성코드 발견 피해 통계

7월 한 달 동안 접수된 신종 (변형) 악성코드의 건수 및 유형은 [표3-3]과 같다.

월	트로이목마	드롭퍼	스크립트	웜	파일	유해가능	기타	합계
2009.05	2,842	576	132	288	59	11	5	3,913
2009.06	2,899	324	253	151	104	22	6	3,759
2009.07	2,184	309	93	161	431	17	30	3,225

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

이번 달부터 통계기준을 새롭게 마련하여 이전 달과 수치가 다를 수 있으니 이와 같은 점을 참고 하여야 한다.

이번 달 악성코드는 전월 대비 – 26% 감소 하였다. 전체적으로 모든 악성코드 유형에서 감소가 있었으며, 원인은 명확히 설명하기 어렵다. 많은 감소 수를 보이는 악성코드는 다음과 같다.

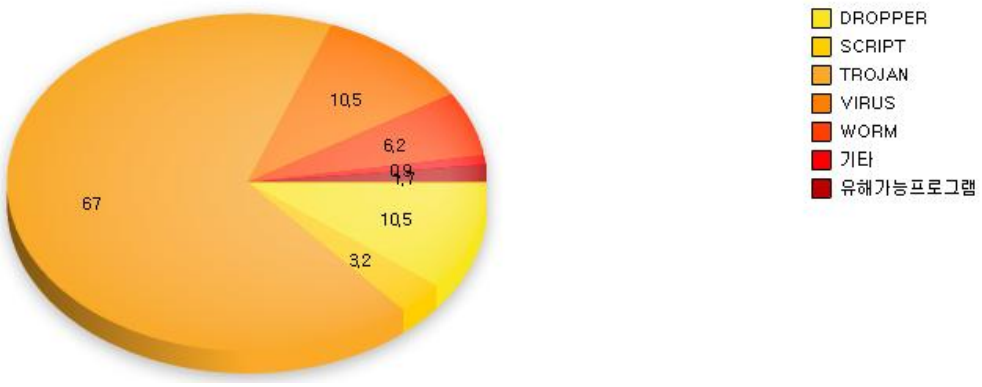
- Win-Trojan/Agent
- Win-Trojan/Hupigon
- Win-Trojan//Infostealer
- Win-Trojan/Injector

위 유형의 악성코드는 모두 평범한 형태의 악성코드로 대부분 국지적으로 발생했다고 사라지고 다시 증가하기도 한다. 이외에도 Win-Trojan/Downlaoder처럼 독립 실행 되지 않고 다른 악성코드들과 유기적으로 결합 되어 있는 악성코드 역시 악성코드의 증가 및 감소에

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

있어서는 뚜렷한 영향을 주지 않는 것들이 대부분 이다. 웜 유형은 대표적으로 Win32/Autorun.worm 유형이 감소 하였다. 그러나 Win- Trojan/Autorun 웜과의 경계가 모호함으로 인하여 해당 악성코드가 감소 했다고 해서 큰 의미를 두지는 않는다.

다음은 이번 달 악성코드 유형을 상세히 분류 하였다.

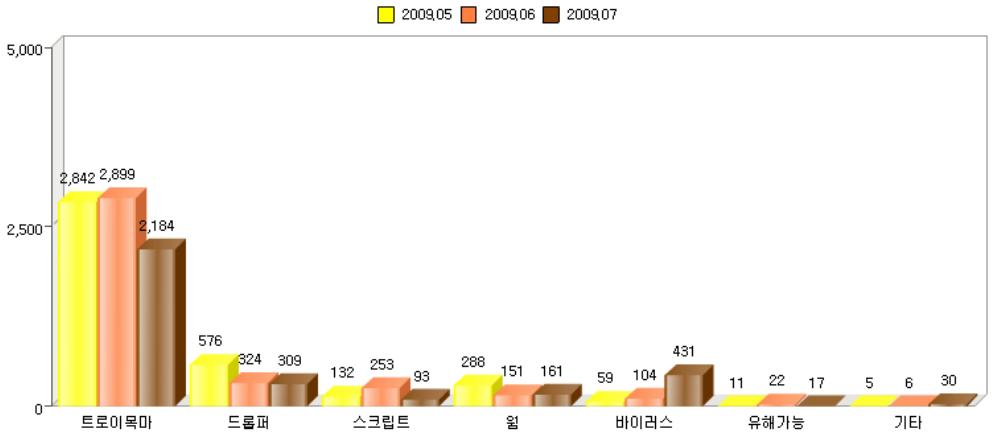


[그림3-6] 2009년 07월 신종 및 변형 악성코드 유형

트로이목마 유형은 전월 대비 20% 감소 하였다. 위에서 언급 했듯이 다수의 악성코드 유형에 있어서 감소가 있었음을 알 수 있었지만 그 원인에 대해서는 명확히 알 수는 없었다. 반면 전월 보다 증가한 악성코드도 있었는데 가짜 백신인 Win-Trojan/Fakeav와 스팸 메일러인 Win-Trojan/SpamBot은 그 변형이 계속 발견 되었다. 이 둘은 연관 관계가 있을 것으로 추정 되는데 사용된 안티 에뮬레이팅 기법이 거의 유사하며 감염된 시스템에서는 동시에 발견된 사례가 많았다. 드롭퍼 유형도 전월 대비 26% 감소 하였다. 스크립트 유형은 14% 감소 하였고, 대부분 자바스크립트 유형이 많이 감소 하였다. 이번 달 발견, 보고된 DirectShow MPEG2TuneRequest 제로데이(0-day) 취약점을 이용하는 악성 스크립트는 국내·외적으로 발견, 보고가 있었지만 큰 피해를 불러 오지는 않았다. 웜 유형은 무려 전월 대비 62% 감소 하였다. 대부분이 Autorun 웜 관련이며 이 유형의 악성코드의 증/감 추세는 명확 하지 않다. 이동식 디스크로 자신을 전파 하도록 하는 방법은 여전히 악성코드 제작자들에게 폭 넓게 사용되고 있다는 반증 정도 이다. 취약점 관련 악성코드는 기존에 알려진 PDF 및 SWF 관련 취약점을 이용하는 형태가 일반적 이였다. 오피스 웹 컨포넌트 관련 제로데이와 어도비 플래쉬 관련 제로데이 등이 보고 되었으며 이와 함께 악성코드도 보고 되었다.

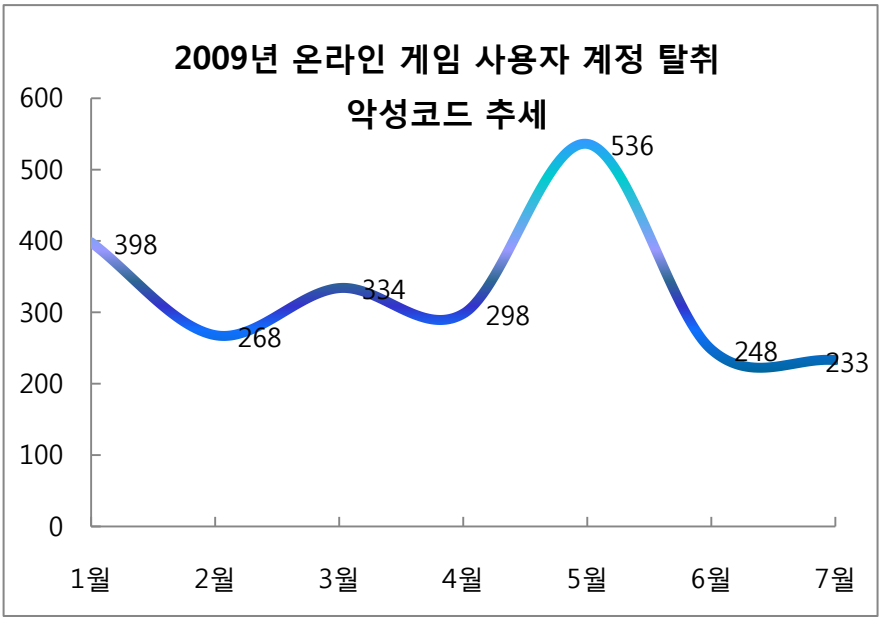
다음은 최근 3개월간 신종 및 변형 악성코드 분포이다.

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림3-7] 2009년 최근 3개월간 악성코드 분포

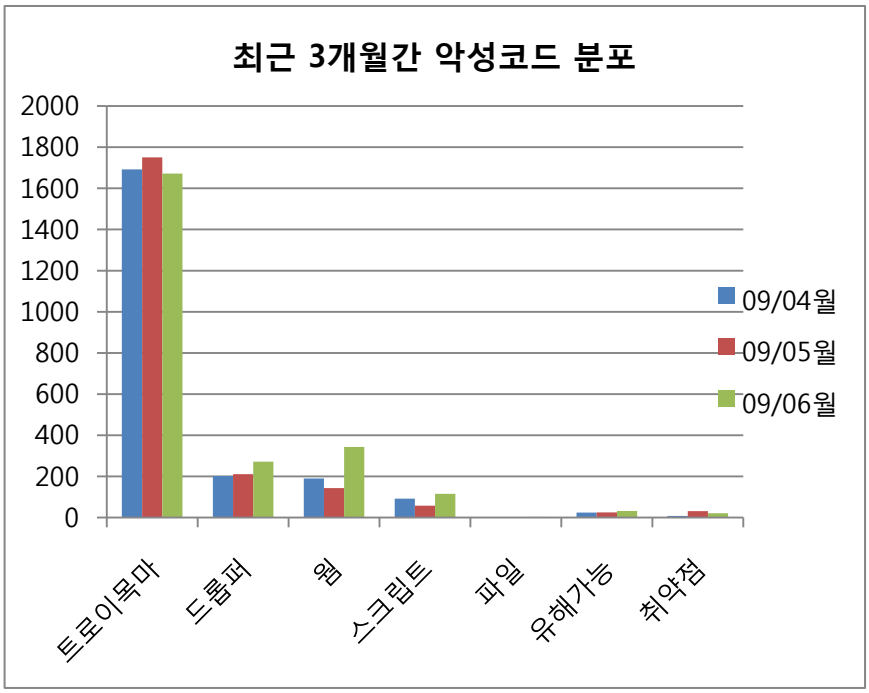
트로이 목마 유형은 최근 3개월간 발견 추세가 하락 하고 있다. 드롭퍼와 웜 유형은 최근 3개월간 소폭 상승 하였지만 7월에 들어서는 전체적으로 하락 했다. 다음은 온라인 게임의 사용자 계정을 탈취하는 악성코드의 추세를 살펴보았다.



[그림3-8] 온라인 게임 사용자 계정 탈취 트로이목마 현황

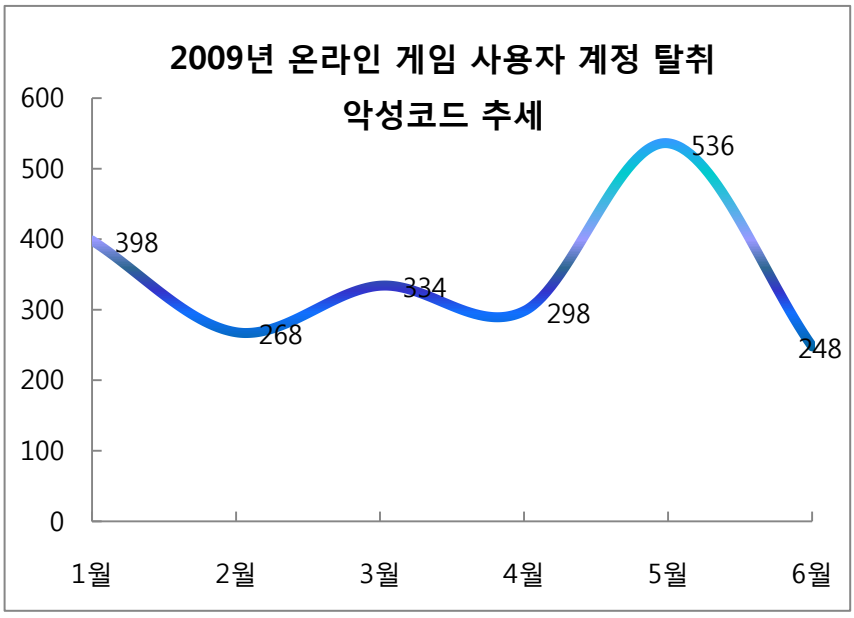
최근 3개월간 해당 악성코드 역시 감소하고 있는 것으로 보인다. 국내에서 발견 되는 유형은 본 보고서를 통해서 언급 했듯이 특정한 custom packer 로 된 유형이 해당 유형 중에서 90% 를 차지 할 정도로 많다. V3 를 비롯한 일부 안티 바이러스 업체에서도 이러한 유형을 Generic 하게 진단 하고 있어 7월은 특히 더 감소 추세가 확연한 것으로 생각 된다.

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림3-9] 2009년 최근 3개월간 악성코드 분포

이번 달 트로이목마의 상승세는 주춤하였다. 반면 드롭퍼와 웜, 스크립트 유형이 증가하였다. Autorun 유형의 악성코드가 원인이 명확하지 않게 증가한 것도 해당 악성코드 유형들이 증가 하는데 한 몫을 하였다. 다음은 온라인 게임의 사용자 계정을 탈취하는 악성코드의 추세를 살펴보았다.



[그림3-10] 온라인 게임 사용자 계정 탈취 트로이목마 현황

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

이번 달 해당 악성코드는 54% 감소 하였다. 이는 올해 들어 가장 낮은 수치를 보이고 있다. 해당 악성코드가 급격히 감소를 보인 것에 대해서는 명확하지 않다. 다만 스크립트 악성코드 유형 중 인터넷 익스플로러 취약점을 이용한 것이 많지 않았으며 Dropper 역시 해당 악성코드를 Drop 하는 형태가 많지 않았다. 또한 이 유형의 악성코드의 경우 이전에도 언급 했듯이 특정한 custom packer 형태로 만들어진 것이 가장 많은 보고가 이루어진다. 해당 유형은 전체 온라인 게임 악성코드의 대부분을 차지 한다. 비록 그 수치가 전월 대비 줄었다고 해도 해당 악성코드는 사용자로부터 많은 보고가 들어오는 형태로 그 수가 줄었다고 안심할 수는 없다.

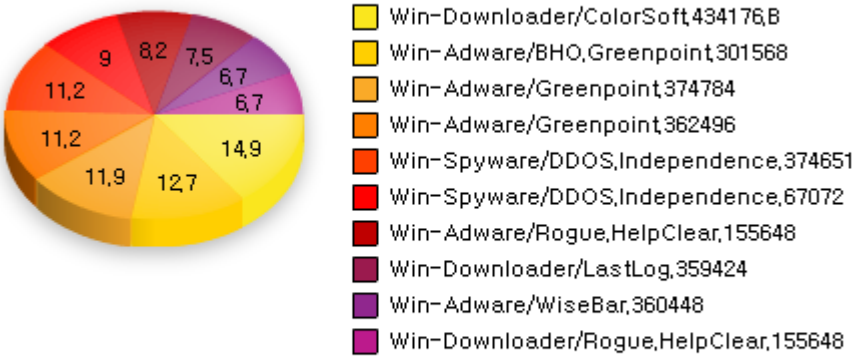
AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

2. 스파이웨어 통계

(1) 7월 스파이웨어 피해 통계

순위		스파이웨어 명	건수	비율
1	NEW	Win-Downloader/ColorSoft.434176.B	20	14.9 %
2	NEW	Win-Adware/BHO.Greenpoint.301568	17	12.7 %
3	NEW	Win-Adware/Greenpoint.374784	16	11.9 %
4	NEW	Win-Adware/Greenpoint.362496	15	11.2 %
5	NEW	Win-Spyware/DDOS.Independence.374651	15	11.2 %
6	NEW	Win-Spyware/DDOS.Independence.67072	12	9 %
7	NEW	Win-Adware/Rogue.HelpClear.155648	11	8.2 %
8	NEW	Win-Downloader/LastLog.359424	10	7.5 %
9	NEW	Win-Adware/WiseBar.360448	9	6.7 %
10	-6	Win-Downloader/Rogue.HelpClear.155648	9	6.7 %
합계			134	100%

[표3-4] 2009년 7월 스파이웨어 피해 Top 10



[그림3-11] 2009년 7월 스파이웨어 피해 Top 10

2009년 7월 스파이웨어 피해 Top10에서는 다운로드 컬러소프트(Win-Downloader/ColorSoft.43417.B)가 가장 많은 피해를 입힌 것으로 나타났다. 다운로드 컬러소프트는 국내 소프트웨어업체에서 제작하고 무료로 배포하는 무료TV 청취프로그램에 의해 설치가 된다. 특히 다운로드 컬러소프트의 제작사는 지난 상반기 많은 피해신고가 확인된 아

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

이쇼우(Win-Adware/IEShow)를 제작한 업체와 동일한 업체로 추정된다. 다운로더 컬러소프트는 사용자 몰래 업데이트 서버에서 프로그램 목록을 다운로드 받아 사용자의 시스템에 설치를 하는 기능을 가지고 있다. 컬러소프트에 의해 설치되는 프로그램은 사용자의 인터넷 검색정보를 감시해 특정 키워드가 검색될 때 주소표시줄에 광고를 노출하는 키워드 광고 프로그램으로 확인되었다. 2,3,4위에 이름을 올린 그린포인트는 적절한 사용자 동의 없이 사용자의 시스템에 설치되는 리워드 프로그램이다.

순위		대표진단명	건수	비율
1	1	Win-Downloader/Zlob	173	32.6 %
2	7	Win-Dropper/Rogue.FakeAV	103	19.4 %
3	NEW	Win-Adware/BestLink	37	7 %
4	NEW	Win-Adware/Greenpoint	34	6.4 %
5	-	Win-Adware/IEShow	33	6.2 %
6	NEW	Win-Downloader/ColorSoft	31	5.8 %
7	NEW	Win-Spyware/DDOS	27	5.1 %
8	-7	Win-Downloader/Rogue.FakeAV	25	4.7 %
9	NEW	Win-Spyware/PWS.OnlineGame	25	4.7 %
10	-7	Win-Adware/Asdfware	21	4 %
합계			530	100%

[표3-5] 7월 대표진단명에 의한 스파이웨어 피해 Top10

[표 3-5]은 변형을 고려하지 않은 대표 진단명을 기준으로 한 피해 건수이다. 6월에는 총 피해건수가 530건으로 지난 6월의 3612에 비해 큰 폭으로 줄었다. 지난달에 이어 가장 많은 피해신고가 접수된 스파이웨어는 다운로더 즐롭(Win-Downloader/Zlob)이다. 다운로더 즐롭의 피해신고가 큰 폭으로 감소했다. 즐롭은 배포사이트에서 실시간으로 변형을 한다. 지난 7월에는 즐롭 배포사이트가 크게 감소했으며, 이 것은 전체적인 피해신고 감소에 큰 영향을 주었다.

2009년 7월 유형별 스파이웨어 피해 현황은 [표 3-6]과 같다.

구분	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
5월	145	222	89	2736	0	8	0	1	0	3021
6월	101	286	74	3647	1	12	2	1	0	4124
7월	156	420	172	406	0	26	4	4	0	1188

[표3-6] 2009년 7월 유형별 스파이웨어 피해 건수

조금씩 줄어들던 스파이웨어와 애드웨어의 피해는 큰 폭으로 증가한 반면 다운로더의 피해

AhnLab
Copyright © AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

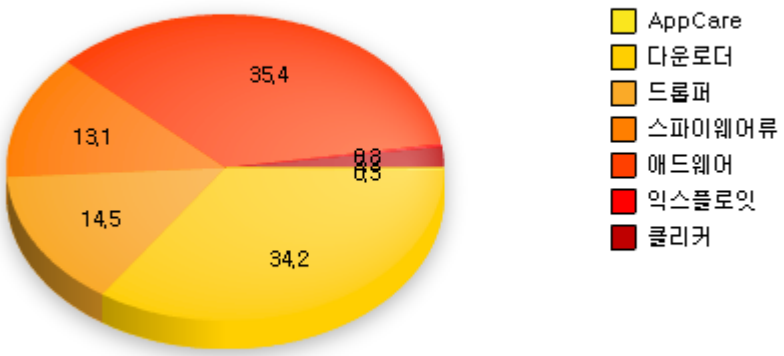
건수는 지난달의 1/9 수준으로 감소했다. 다운로더의 피해건수가 감소한 것은 외산 가짜 백신을 설치 배포하는 사이트가 많이 줄어든 것이 원인이다.

(2) 7월 스파이웨어 발견 현황

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

구분	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
5월	77	177	66	1828	0	5	0	0	0	**2093**
6월	68	122	58	2739	0	8	2	1	0	**2998**
7월	**116**	**187**	**143**	**273**	**0**	**20**	**3**	**0**	**0**	**742**

[표3-7] 2009년 7월 유형별 신종(변형) 스파이웨어 발견 현황



[그림3-12] 2009년 7월 발견된 스파이웨어 프로그램 비율

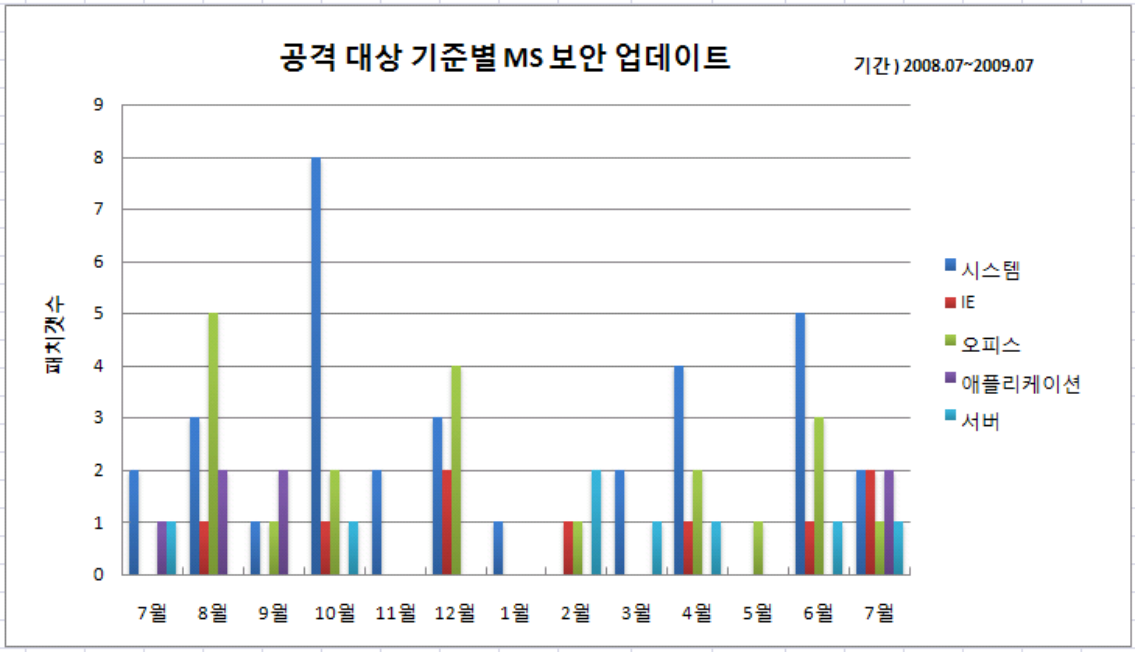
지난달 다운로더의 피해가 신고의 대부분을 차지했던 반면 7월에는 애드웨어에 의한 피해신고가 큰 폭으로 증가했다. 신고가 접수된 애드웨어는 대부분 국산프로그램으로 국산 애드웨어의 피해가 다시 증가하는 것으로 풀이할 수 있다.

AhnLab
Copyright © AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

3. 시큐리티 통계

(1) 7월 마이크로소프트 보안 업데이트 현황

마이크로소프트사로부터 발표된 이달 보안 업데이트는 총 8건으로 긴급(Critical) 4건, 중요(Important) 3건, 보통(Moderate) 1건이다.



[그림3-13] 7월 MS 보안 업데이트 현황

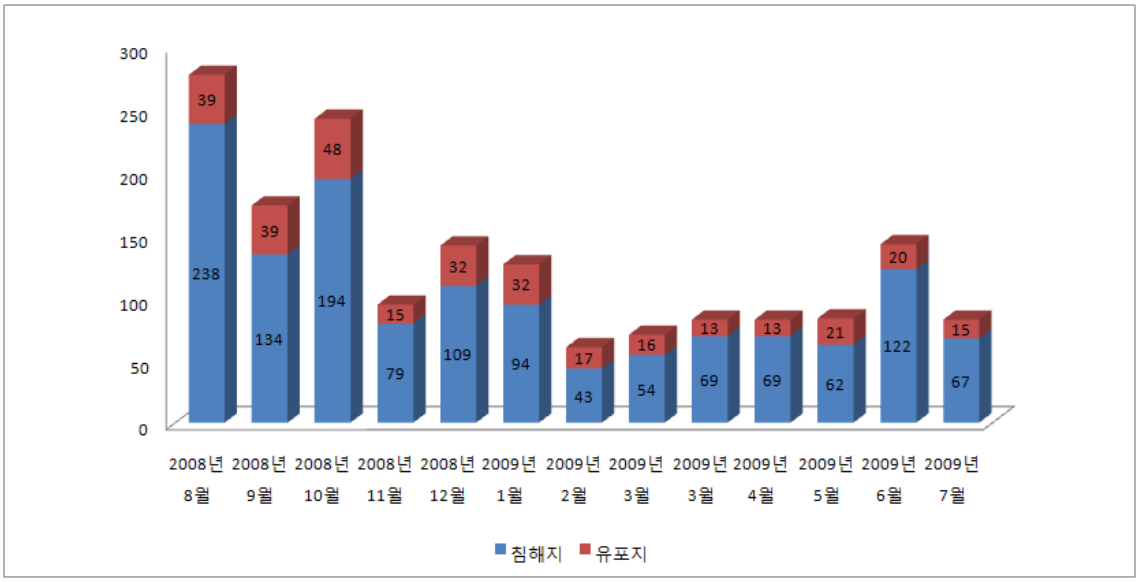
위험도	취약점	PoC
긴급	(MS09-028) Microsoft DirectShow의 취약점으로 인한 원격 코드 실행 문제점	유

[표3-8] 2009년 07월 주요 MS 보안 업데이트

이 달에는 7월 초경에 제로데이 취약점으로 알려진 웹 서버인 DirectX 의 MPEG2Tune의 취약점을 보완하는 보안 업데이트가 포함되어 있다. 현재 Internet Explorer 를 이용하여 해당 취약점을 통해 악성코드가 유포됨으로 일반 사용자들은 반드시 보안 패치를 하여야 한다. 7월 13일경에 발표된 Microsoft Office Web Component 에 해당하는 패치가 아직 발표되지 않았는데, 해당 취약점은 악의적으로 이용이 가능함으로 주의가 필요하다.

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

(2) 2009년 6월 웹 침해사고 및 악성코드 배포 현황



[그림3-14] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

2009년 7월 악성 코드를 위해 침해된 웹사이트의 수와 악성 코드 유포지의 수는 67/15로 2009년 6월의 122/20과 비교하여 유포지의 수는 변화가 없었지만 침해지의 수는 큰 폭으로 감소하였다. 2009년 웹 공격 코드의 특징은 PDF나 오피스 또는 플래쉬 등의 취약점을 공격하는 코드가 많아 졌다는 것이다.


```
PDF = new Array('AcroPDF.PDF', 'PDF.PdfCtrl');
for(i in PDF)
{
        obj = new ActiveXObject(PDF[i]);
        ...
```

[그림3-15] 공격코드

[그림3-15]의 코드는 다음과 같은 문서의 취약점을 공격한다.

```
AcroPDF.PDF
PDF.PdfCtrl
ShockwaveFlash.ShockwaveFlash
```

이러한 공격으로부터 사용자의 시스템을 방어하기 위해서는 항상 사용제품의 보안 상태를 최신으로 유지하고, 최신 상태의 안티바이러스 제품을 사용해야 한다.

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

4. 사이트가드 통계

(1) 2009년 7월 웹 사이트 보안 요약

구분	건수
악성코드 발견 건수	219,383
악성코드 유형	827
악성코드가 발견된 도메인	772
악성코드가 발견된 URL	8,860

[표3-9] 7월 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 3-9]는 2009년 7월 한달 동안 웹 사이트를 통해 발견된 악성코드 동향을 요약해서 보여주고 있다.

사이트가드의 집계에 따르면 7월 한달 동안 악성코드는 827종 219,383건 발견되었으며, 악성코드가 발견된 도메인은 781건, 악성코드가 발견된 URL은 8,860건으로 지난 6월의 급격한 증가와 달리 전반적으로 감소하였다. 악성코드 발견건수 219,383건은 6월 682,795건에 비해 1/3 수준으로 감소한 수치이다. 이는 2009년 6월 도메인수가 엄청난 수치였음을 다시 한번 알 수 있었으며, 7월은 지난 5월에 비해 약 20% 정도 증가하였다.

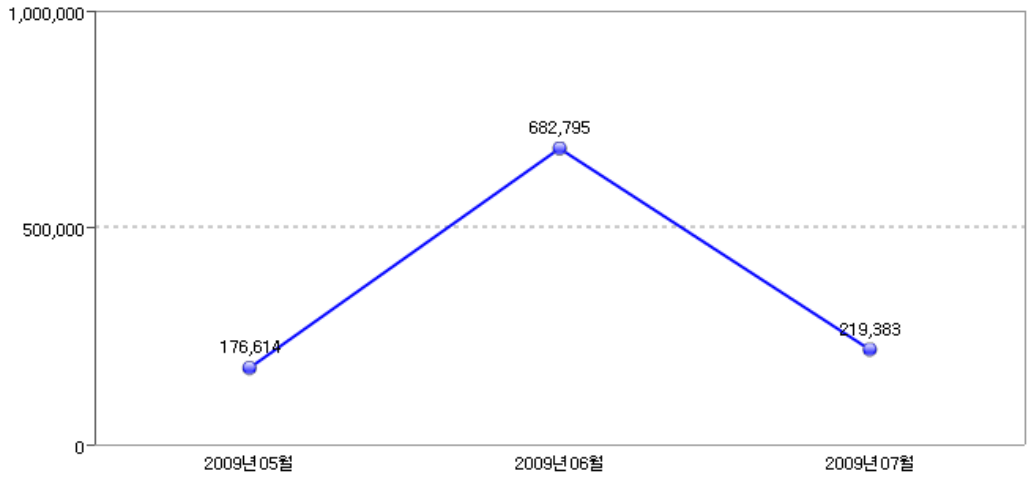
세부내용을 보면 다음과 같다.

[1] www.siteguard.co.kr

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

(2) 악성코드 월간 통계

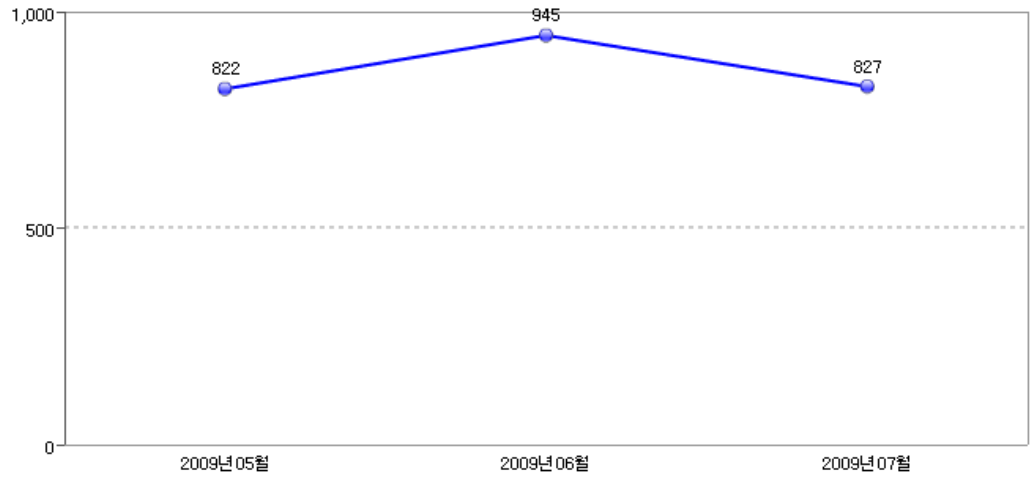
가) 악성코드 발견건수



[그림3-16] 월별 악성코드 발견건수

[그림 3-16]은 최근 3개월인, 2009년 5월부터 2009년 7월까지의 악성코드 발견 건수의 추이를 나타내는 그래프로 7월 악성코드 발견 건수는 219,383건으로 지난달에 비해 약 1/3로 감소 하였다.

나) 악성코드 유형



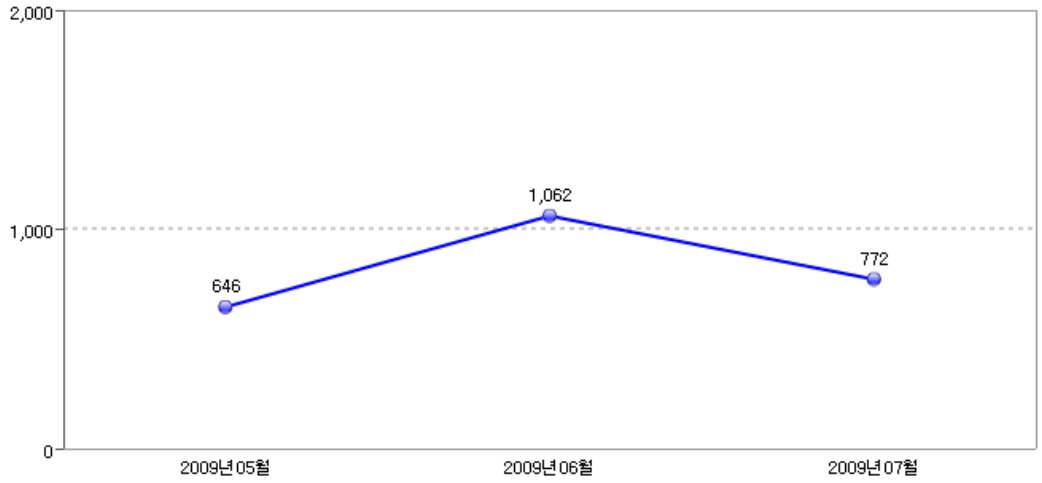
[그림3-17] 월별 악성코드 유형

[그림 3-17]은 최근 3개월간 발견된 악성코드의 유형을 나타내는 그래프로 7월에는 827종

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

으로 지난 6월에 비해 다소 감소하였다.

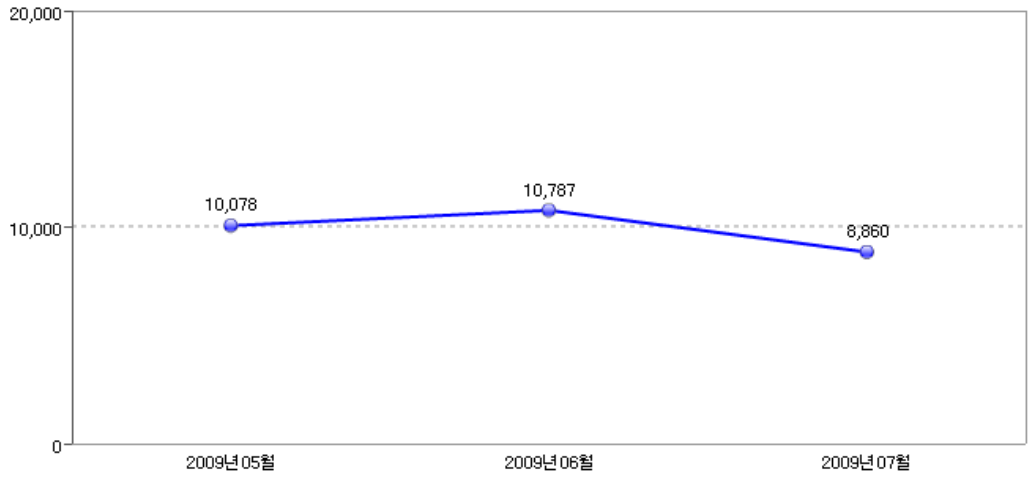
다) 악성코드가 발견된 도메인



[그림3-18] 월별 악성코드가 발견된 도메인

[그림 3-18]은 최근 3개월간 악성코드가 발견된 도메인 수의 변화 추이를 나타내는 그래프로 6월 악성코드가 발견된 도메인은 772개로 전월에 비해 감소하였다.

라) 악성코드가 발견된 URL



[그림3-19] 월별 악성코드가 발견된 URL

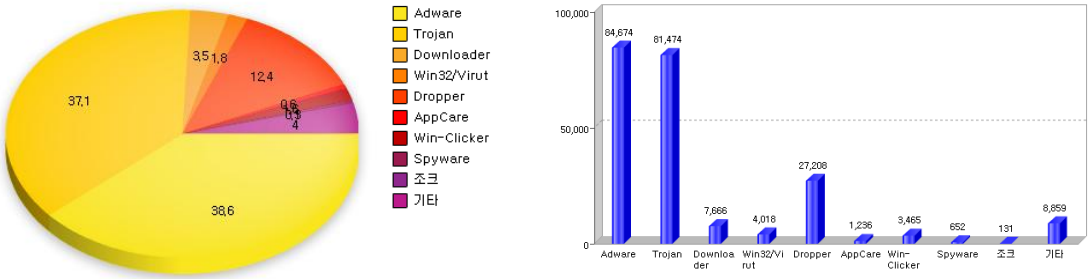
[그림 3-19]는 최근 3개월간 악성코드가 발견된 URL 수의 변화 추이를 나타내는 그래프로 7월 악성코드가 발견된 URL 수는 8,860개로 전월에 비해 다소 감소하였다.

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

(3) 유형별 악성코드 배포 수

유형	건수	비율
Adware	84,674	38.6%
Trojan	81,474	37.1%
Downloader	7,666	3.5%
Win32/Virut	4,018	1.8%
Dropper	27,208	12.4%
AppCare	1,236	0.6%
Win-Clicker	3,465	1.6%
Spyware	652	0.3%
Joke	131	0.1%
기타	8,859	4%
합계	219,383	100%

[표3-10] 유형별 악성코드 배포 수



[그림3-20] 유형별 악성코드 분포

[표 3-10]과 [그림 3-20]은 7월 한달 동안 발견된 악성코드를 유형별로 구분하여 발견 건수와 해당 비율(%)를 보여주고 있다.

7월 한달 동안 총 219,383개의 악성코드가 발견되었으며 이중 Adware류가 84,674개로 6월에 이어서 1위를 고수하였다. Trojan류는 81,474개로 2위를 차지하였으며, 3위는 Downloader류가 7,666개로 3위를 차지하였다.

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

(4) 악성코드 배포 순위

순 위		악성코드명	건수	비율
1	2	Win-Trojan/Xema.variant	53084	35 %
2	5	Win-Adware/Shortcut.InlivePlayerActiveX.234	43426	28.6 %
3	NEW	Win-Dropper/WiseBar.440832	18665	12.3 %
4	2	Win-Adware/Shortcut.IconJoy.642048	7167	4.7 %
5	NEW	Win-Adware/Shortcut.INBEE.iomeet.267270	6507	4.3 %
6	NEW	Win-Trojan/StartPage.505344	6007	4 %
7	NEW	Win-Adware/BHO.HiMyCar.237568	4704	3.1 %
8	NEW	Win-Trojan/Shutdowner.241664.B	4372	2.9 %
9	NEW	Win-Downloader/Rogue.PCPlus.402944.B	4131	2.7 %
10	NEW	Win32/Parite	3785	2.5 %
합계			151848	100 %

[표3-11] 유형별 악성코드 배포 Top 10

[표 3-11]는 3월 한달 동안 웹 사이트에서 사이트가드를 통해 확인된 악성코드 배포 Top 10을 보여주고 있다. Top 10에 포함된 악성코드들의 총 배포건수는 528,413건으로 6월 한 달 총 배포건수 682,795건의 약 77%에 해당된다. '[표3-11] 유형별 악성코드 배포 Top10'에서 알 수 있듯이 Top10의 대부분은 Adware류와 Trojan류가 차지 하였다.

특이한 점은 7월에는 Top 10에 신규로 진입한 악성코드가 7건이나 되었다. 6월에 3건 이었던 것에 비하면 7월은 많은 변동이 있었다는 것을 알 수 있다.

요컨대, 2009년 4월부터 시작된 악성코드의 증가세는 6월에 정점을 찍고 7월에는 감소하였다. 이는 7월에는 급격한 확산을 보이는 악성코드가 6월에 비해서는 적었던 것이 하나의 이유로 보인다. 하지만, 6월은 특이할 정도로 악성코드의 유포가 급격한 달이었으며, 7월은 6월에 비해서는 악성코드의 확산이 적을 뿐이지 지난 4월부터 시작한 악성코드 유포의 증가세는 계속 지속되고 있다. 따라서, 기업 보안관리자는 사이트가드와 같은 웹 보안 서비스를 이용하여 자사의 사이트에 대한 정기적인 점검을 통해 고객의 피해를 방지하는 최소한의 노력이 필요한 시점이다.

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

ASEC REPORT 작성을 위하여 다음과 같은 분들께서 수고하셨습니다.

2009년 7월호

편집장	선임 연구원	허 종 오
집필진	선임 연구원	정 진 성
	선임 연구원	차 민 석
	선임 연구원	이 정 형
	선임 연구원	심 선 영
	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
	주임 연구원	주 설 우
감 수	상 무	조 시 행
참여연구원		ASEC 연구원분들
		SiteGuard 연구원분들

AhnLab
Copyright ⓒ AhnLab, Inc. All rights reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.