ASEC Report 10월

® ASEC Report

2008. 11.

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

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

I. ASEC Monthly Trend & Issue

(1) 악성코드 – MS08-067 윈도우 보안 취약점을 악용하는 악성코드

이번 달 말에는 윈도우 서버 서비스 취약점(MS 긴급 패치 MS08-067)을 공격하는 악성코드가 제작 발견되었고, 유명 컴퓨터 제조업체의 미니 PC의 하드 디스크에서 악성코드가 발견되었다. 또한 미국의 대표 SNS인 Facebook을 이용하여 전파되는 웜의 변형도 있었으며 국내에서는 온라인 게임 악성코드가 자신을 디버깅하면 MBR 영역을 망가뜨리는 유형이 보고되기도 하였다.

MS08-067 윈도우 보안 취약점을 악용하는 악성코드

해당 취약점은 윈도우 서버 서비스 취약점으로 Server Service가 RPC 요청을 제대로 처리하지 못해서 발생하는 것이다. 해당 서비스는 윈도우 2000, XP, 2003 등의 주요 OS에서 기본적으로 서비스가 되고 있고, 또한 취약점을 이용하여 원격에서 공격이 가능하기 때문에 그 중요도가 '긴급'성을 갖는다. 그러나 일각에서 우려와는 달리 이 취약점을 이용하는 악성코드는 크게 증가하지 못할 것으로 보인다. 이 글을 작성하는 현재 취약점과 악성코드가 보고된 지 9일 정도 흘렀지만 과거 RPC계열의 취약점을 이용하였던 블래스터 웜이나 새서 웜과 같이 해당 취약점을 이용한 악성코드는 쏟아져 나오고 있지 않다.

여기에는 여러 가지 이유가 있겠지만 예전과는 달리 원격에서 윈도우(윈도우 비스타, 2008) 취약점 자체를 공격하는게 과거 보다는 쉽지 않다는데 있다. 윈도우 XP 역시 원격에서의 공격은 원격코드의 실행 보다는 단지 DoS 수준에 머물 것으로 생각된다. 그리고 무엇보다도 이전과 다르게 MS의 발 빠른 패치와 많은 보안 업체들의 대응들도 여기에 한 몫을 하고 있기 때문일 것이다.

유명 컴퓨터 제조사 하드 디스크에서 발견된 악성코드

대표적인 메인보드 및 컴퓨터 제조업체인 Asus가 일본에서 판매하고 있는 Eee PC 라고 불리 우는 미니 PC 하드 디스크에서 악성코드가 발견 되었다. 해당 악성코드는 이와 같은 하드웨어(USB 메모리 스틱과 같은 이동식 디스크 종류)에서 주로 발견, 보고 되는 Autorun 관련 악성코드에 감염된 것으로 밝혀졌다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

[그림 1-1] Asus Eee PC (출처 - www.pcadvisor.co.uk)

올해 들어서 이와 같이 이동식 디스크에 악성코드가 감염된 사례가 종종 발생하고 있는데, 대부분의 경우에 있어 공장에서 해당 하드웨어 대한 초기화 작업(포맷 및 OS 설치 등)에서 주로 감염이 된다. 물론 마스터 작업을 하는 어떤 시스템에 악성코드가 감염된 사실을 몰랐기 때문이고 여기에 백신관련 제품이 설치되지 않았기 때문일 것 이다. 올해 유사 사례를 보면 모두 오래 전에 발견된 악성코드가 이러한 장치들에서 보고되었다. 이는 앞서 언급한 바와 같이 보안에 가장 기본인 안티 바이러스 제품 사용에 소홀하였던 것이 원인이라 할 수 있다.

MBR 영역을 손상시키는 악성코드

Win-Trojan/Killmbr.14848은 특정 온라인 게임의 사용자 계정 정보를 탈취하는 트로이목마에서 드랍된다. 해당 악성코드는 특이하게 자신이 디버깅 당하고 있다고 판단되면 더 이상의 분석을 방해 할 목적으로 MBR[1] (Master Boot Record = 이하 MBR)을 손상시킨다. 일반 사용자는 문제가 되지 않을 수 있지만, 해당 악성코드를 분석하려고 디버거를 사용 중 일 때 이 부분을 우회하지 못한다면 분석가 시스템의 MBR 영역이 손상 될 수 있다.

```
Address   Hex dump          Disassembly                          Comment
10001000 r$  64:A1 1800     MOV      EAX, DWORD PTR FS:[18]      Thread  Environment  Block (TEB)
10001006 .   8B40 30        MOV      EAX, DWORD PTR DS:[EAX+30]  Process  Environment  Block(PEB)
10001009 .   0FB640 02      MOVZX    EAX, BYTE PTR DS:[EAX+2]    PEB 의 주소를 얻은 다음
1000100D .   83F8 01        CMP      EAX, 1                      PEB 를 검사하고 PEB + 0x02 위치의
10001010 .v  74 02          JE       SHORT test.10001014         EAX = 1 이라면 디버깅중이라고 판단
10001012 .v  EB 06          JMP      SHORT test.1000101A
10001014 >   E8 F71B000     CALL     test.10002C10
10001019 .   C3             RETN
```

[그림 1-2] IsDebuggerPresent()를 이용한 안티 디버깅

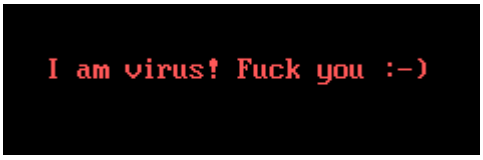
현재 자신의 프로세스가 디버깅 당하고 있다고 판단이 되면 MBR 영역에 특정 데이타를 써

[1] MBR 영역에는 부팅 및 파티션에 대한 중요한 정보가 담겨있다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

놓을 부분을 호출한다.

```
0006F69C B8 12 00 CD 10 BD 18 7C B9 18 00 B8 01 13 BB 0C ?.??|?.?■?
0006F6AC 00 BA 1D 0E CD 10 E2 FE 49 20 61 6D 20 76 69 72 .?■?崧I am vir
0006F6BC 75 73 21 20 46 75 63 6B 20 79 6F 75 20 3A 2D 29 us! Fuck you :-)
0006F6CC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```



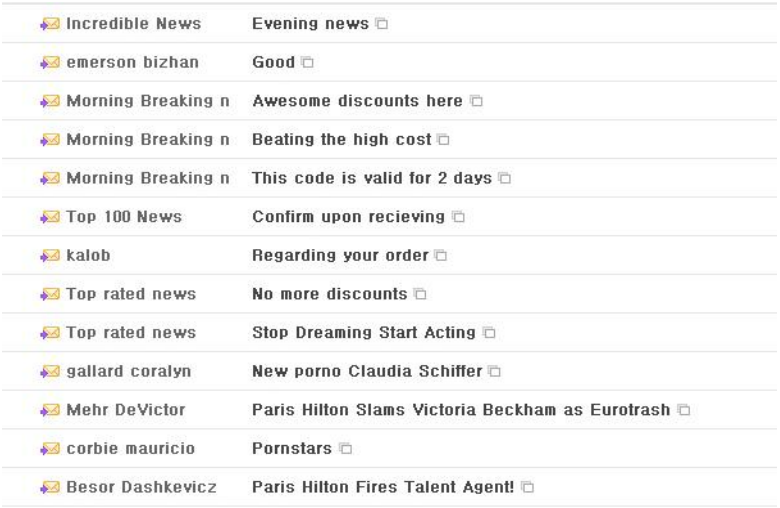
[그림 1-3] MBR 영역에 써놓을 내용과 리부팅시 출력되는 메시지

이와 같은 안티 디버깅은 비교적 간단한 것으로 악성코드를 분석하는 입장에서는 우회하기 쉽다. 또한 이렇게 분석을 방해하거나 지연 시키기 위한 방법은 여러 가지가 있다. 사용자 입장에서는 기존 악성코드들과 다를게 없지만 악성코드를 분석하고 연구하는 입장에서는 꼭 알아야 할 분석 기술 중 하나이다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

(2) 스파이웨어 – 스팸 메일러 피해 증가

최근 해외의 한 보안업체가 27일 발표한 올해 3분기 스팸메일 동향조사에 따르면, 한국이 스팸메일 발송 순위에서 3.8%로 6위를 차지한 것으로 나타났다. 스팸메일 발송 증가의 원인으로는, 스팸 메일러와 스팸 메일러에 감염된 PC의 증가로 추정된다. 최근 다운로더에 의해 여러 스파이웨어와 함께 스팸 메일러가 설치되는 것이 많이 발견되고 있으며, 이로 인한 고객 피해가 증가하고 있는 추세이다. 특히 최근 유행하는 스팸 메일러는 윈도우 기반에서 동작하기 때문에, 윈도우 환경의 사용자가 많고 인터넷 회선 속도 품질이 좋은 한국은 스팸 메일러가 전파되기에 좋은 조건을 갖추고 있다.

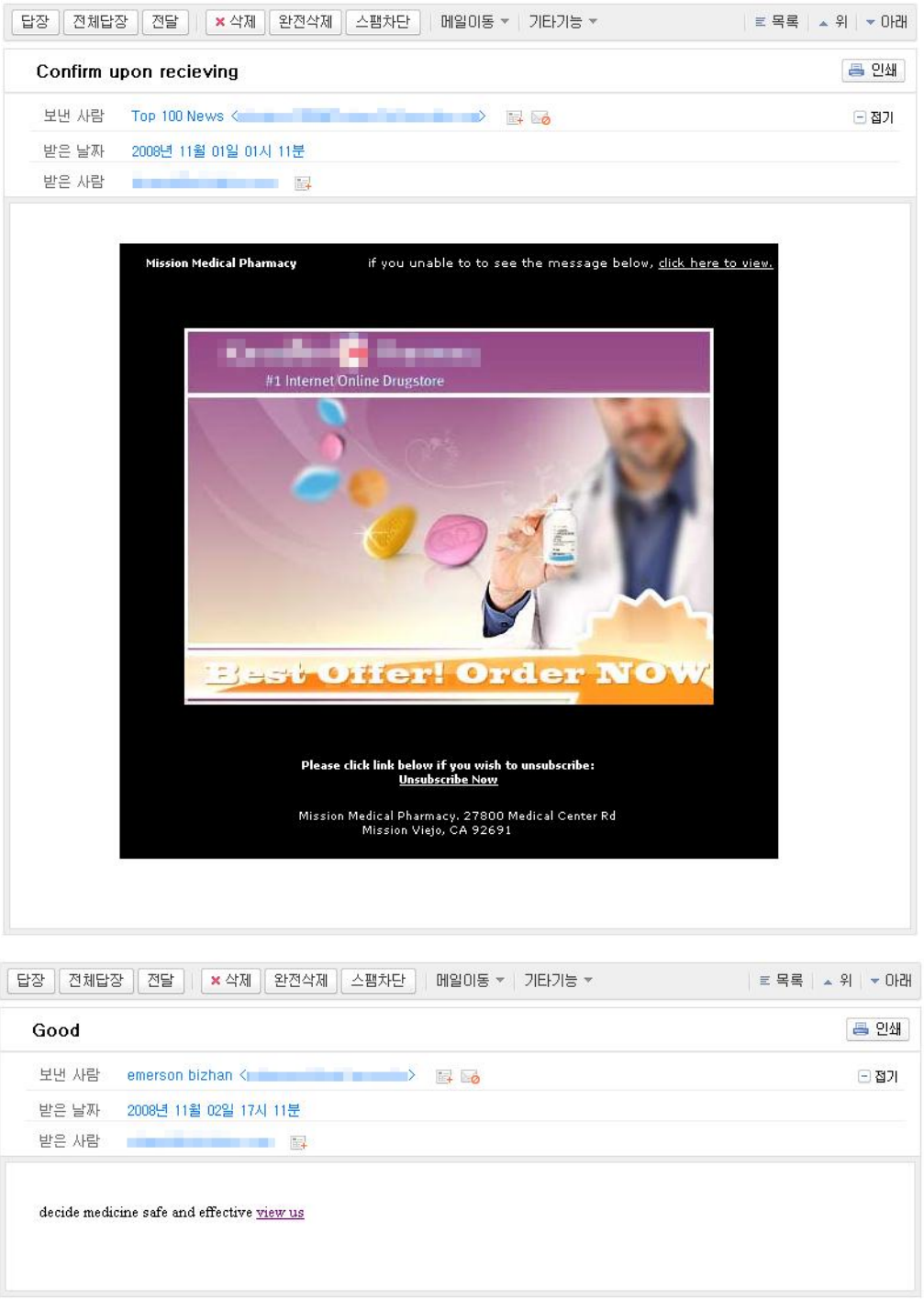


[그림 1-4] 스팸 메일러에 의해 발송된 스팸메일

최근 유행하는 스팸 메일러는 불법 사이트 등에서 배포되는 허위 크랙, 해킹된 웹사이트, 악성코드 다운로더, 웜 등의 다양한 방법에 의해 설치되며, 보통 다른 여러 악성코드들과 함께 설치된다. 대부분의 스팸 메일러는 루트킷을 이용하여 사용자나 보안 제품으로부터 자신을 은폐하고 보호하며, 윈도우 서비스로 등록되어 동작하고, UI가 없기 때문에, 사용자는 스팸 메일러에 감염되더라도 그 사실을 알아차리기 어려워 자신도 모르는 사이에 스팸 메일을 발송하는 스팸 메일러가 되어버린다.

스팸 메일러에 의해 발송되는 스팸메일은 그 목적에 따라 광고와 악성코드 전파, 그리고 피싱 등으로 구분되는데. 광고메일의 경우는 쇼핑몰이나 성인사이트 등을 홍보하기 위한 것으로 위험성은 낮은 편이다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



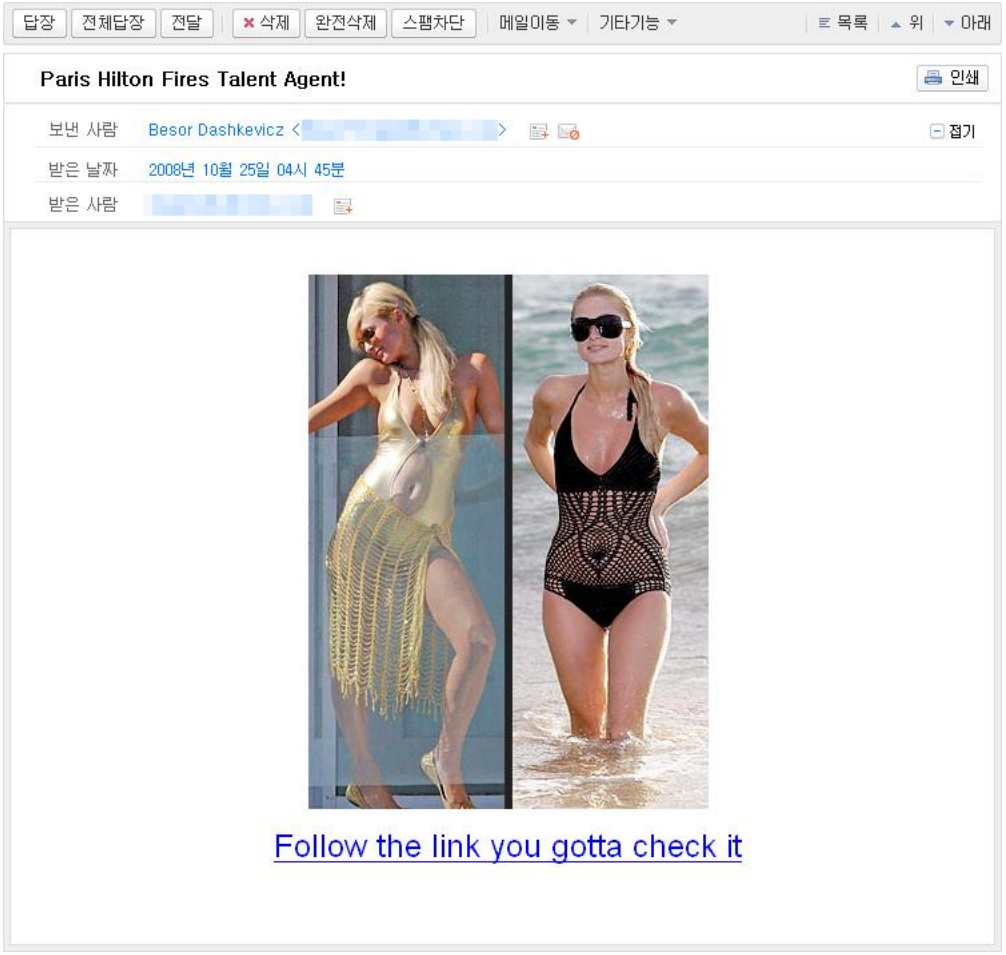
[그림1-5] 스팸 메일러에 의해 발송되는 광고메일

최근 스팸 메일러에 의해 발송되는 스팸메일은 [그림 1-5]와 같은 특정 의약품 광고가 많은데 이 경우, 광고에 삽입된 링크가 중국 웹사이트를 경유하여 이동되는 것으로 보아 중국에서 제작된 스팸 메일러가 많은 것으로 추정된다.

광고가 아닌 악성코드 전파가 목적인 것들은 메일을 수신한 사용자 PC의 보안에 큰 위협을

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

주고, 또 다른 스팸 메일러가 되어 동작할 수 있으므로 그 문제가 심각하다. 보통 악성코드 전파를 위해 발송되는 스팸메일들은 사용자가 메일을 열람하도록 유도하기 위해 주로 [그림 1-6]과 같이 연예인의 사진이나 포르노 등을 이용한다.



[그림 1-6] 악성코드 전파가 목적인 스팸메일

위의 “Follow the link you gotta check it” 링크를 클릭하면 악성코드가 다운로드 된다. 다운로드되는 악성코드는 Win-Downloader/Zlob 종류인 경우가 많으며, 주로 [그림 1-7]과 같은 허위 안티-말웨어 프로그램을 다운로드 한다. 허위 안티-말웨어 프로그램은 사용자에게 허위 진단 결과를 표시하거나 직접 다른 악성코드를 설치하여 진단하는 방식으로 사용자에게 부당한 결제를 요구하는 스파이웨어이다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

[그림 1-7] 스팸메일을 통해 전파되는 허위 안티-스파이웨어

스팸 메일러가 설치되는 것을 예방하기 위해서는 다른 악성코드 예방법과 마찬가지로 불법 프로그램/크랙 등의 사용을 자제하고, 취약점을 이용한 설치를 막기 위해 항상 최신의 업데이트를 유지해야 하며 반드시 방화벽 및 보안제품을 사용하여야만 한다. 특히 방화벽의 사용은, 스팸 메일러에 의해 발송되는 스팸메일을 차단할 수 있으므로, 스팸 메일러 감염에 의한 2차 피해를 막을 수 있다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

(3) 시큐리티 – 원격 공격이 가능한 MS08-067

10월에 있었던 주요 이슈 중에서 가장 큰 이슈는 10월24일(한국시간)에 발표된 마이크로소프트사의 취약점이라 할 수 있다. 마이크로소프트사의 보안패치 정책은 매월 둘째 화요일에 발표되고 있는데, 이번의 경우 예외적으로 긴급하게 보안패치를 발표하였다. MS08-067 취약점에 대해 좀더 세부적인 내용과 TCP/IP의 새로운 취약점에 대해 알아보도록 하겠다.

MS08-067 서버 서비스 취약점 공개돼, 주의 필요

이번에 발표된 패치는 MS08-067 서버 서비스 취약점으로 올해 벌써 67번째에 해당하는 보안패치이다. 작년의 보안 패치 마지막 번호가 MS07-069인 것을 보면 2008년은 보안 취약점이 전년대비 더욱 증가될 것으로 예상된다. 이번 취약점은 특정 응용프로그램이 아니라 많은 사용자층을 확보하고 있는 윈도우 운영체제에 기본으로 포함되어 있는 서비스가 대상이 되어 공격대상의 범위가 넓다고 볼 수 있다.

이 취약점을 이용하면 공격자는 시스템의 관리자 권한을 획득하여 시스템을 완전히 제어할 수 있게 되어 시스템이 위험에 노출될 수 있다. 공격자는 조작된 RPC 메시지를 인증없이 전송하여 임의의 코드 실행이 가능한데, 이것은 윈도우 서버 서비스가 조작된 RPC 요청을 적절히 처리하지 못해 발생하는 것이다.

RPC는 네트워크 상의 컴퓨터들 사이에 프로그램 서비스를 요청할 수 있는 프로토콜로서 상호운영성을 제공해 준다. 서버 서비스는 RPC를 통해 파일, 프린트 그리고 네트워크 공유를 지원해 다양한 기능을 제공해준다.

서버 서비스는 RPC 인터페이스로 srvsvc 이름의 파이프를 오픈하며, ntsvcs의 이름으로도 사용된다. SRVSVC 인터페이스는 UUID 4b324fc8-1670-01d3-1278-5a47bf6ee188 값이 등록되어 있다. 이 인터페이스를 통해 공유설정, 세션, 파일 오픈 및 기타 서버의 자원 접근이 가능해 지는 것이다. SRVSVC 인터페이스의 RPC 기능으로 사용 가능한 것은 아래와 같다.

- NetrFileEnum
- NetrSessionEnum
- NetrShareEnum
- NetrPathCanonicalize
- NetrPathCompare

일반적으로 클라이언트는 서버와 통신하기 위하여 TCP/139, 445번의 SMB(Server Message Block)을 이용한다. RPC를 통해 명령어를 전달하기 전 클라이언트는 서버와 SMB

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

세션을 맺어야 한다. 즉, SRVSVC의 RPC 기능을 호출하기 위해서는 클라이언트는 우선 서버의 SRVSVC 파이프를 오픈하고 바인딩 단계를 거친다. 바인딩 호출이 성공적으로 이뤄지면 클라이언트는 SMB TransactNmPipe 명령어를 이용하여 RPC 메시지를 전달할 수가 있다. 그러나, NETAPI32.DLL에서 처리되는 RPC 기능 중 하나인 NetrPathCanonicalize에 버퍼 오버플로우가 존재하여 임의의 명령어 실행이 가능하다. 공격자는 조작된 RPC 메시지를 전달하여 포인터가 조작된 위치를 가리키도록 하여 명령어가 수행되게 할 수 있다.

* 공격과정 (전형적인 SMB 세션을 통해 공격을 시도하는 과정)

[Attacker] ---------->[Target]

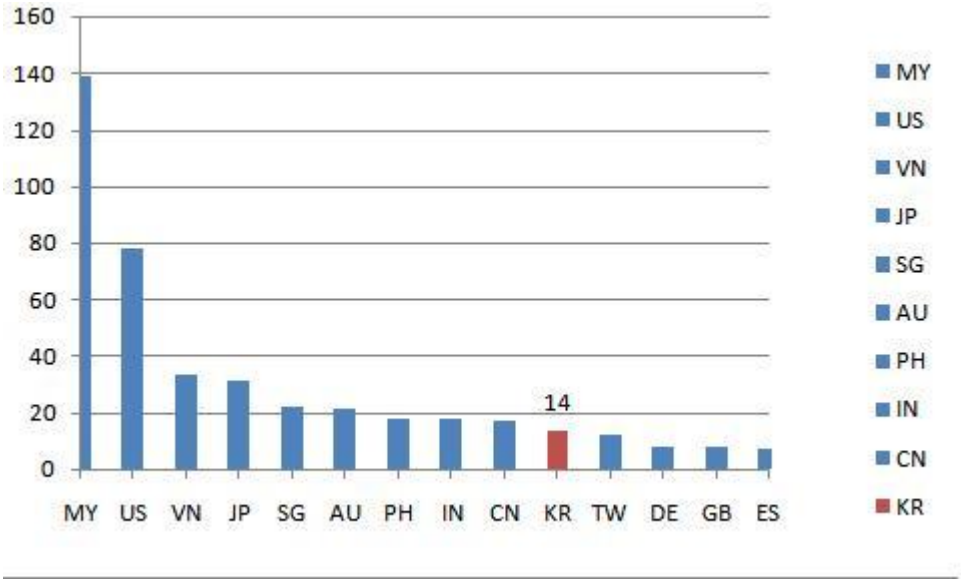
1) **[Attacker]** 공격자는 공격대상 시스템에 SMB 세션 연결을 시도한다.
2) **[Target]** 공격대상 시스템에서는 SMB 세션에 대한 인증
3) **[Attacker]** 공격자는 대상시스템으로 SRVSVC RPC 인터페이스 바인딩
4) **[Target]** 대상 시스템은 바인딩 요청을 허용
5) **[Attacker]** 공격자는 대상시스템으로 조작된 RPC 요청을 전송

이 취약점은 현재 광범위 하게 사용되고 있는 운영체제에 기본으로 사용되고 있는 서비스인 만큼 위험도가 상당히 높다고 볼 수 있으며, 영향을 받는 윈도우를 사용하는 고객은 반드시 패치를 적용할 것을 권고한다. 다만, 한가지 다행인 점은 윈도우 XP SP2, 윈도우 비스타 그리고 윈도우 서버 2008은 방화벽에 의해 기본적으로 해당 인터페이스에 접근이 안되는 것으로 알려져 있다. 그러므로, 공격에 이용되기 위해서는 다음과 같은 상황이 만들어져야 한다.

1. 방화벽이 중지되어 있어야 함
2. 방화벽이 허용되어 있으나, 파일/프린터 공유가 허용되어 있는 경우

최근 발견된 해당 취약점을 내포하고 있는 악성코드는 시스템 감염 시 일부 도메인에 접근하여 감염된 시스템의 정보를 남기도록 설계되어 있었다. 아래 그래프는 해당 도메인으로부터 수집된 로그 정보로부터 IP 정보를 기반으로 국가별 분포를 살펴본 결과이다. 이는 일부 도메인으로부터 수집된 단편적인 정보이기 때문에 전체를 의미하는 정보로 규정지을 수는 없으나, 많은 국가의 시스템들이 해당 악성코드에 감염되었으며 우리나라(KR) 또한 해당 악성코드 감염 사례가 발견되었다는 점을 확인할 수 있다.

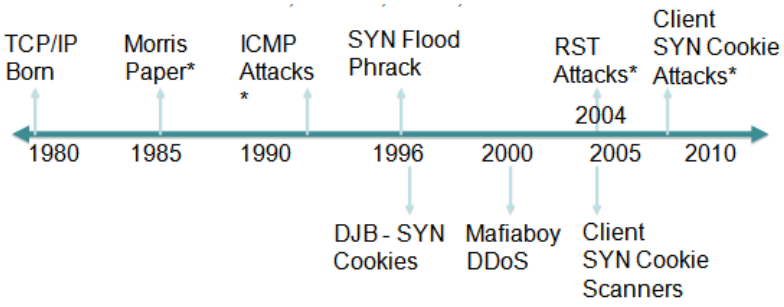
Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림 1-8] 감염 호스트 지역 분포(일부 감염 호스트 로깅 사이트로부터)

Sockstress 라 불리는 TCP 프로토콜 취약점

10월 초 헬싱키에서 열린 T2 컨퍼런스(http://www.t2.fi)에서 TCP/IP의 스택에 존재하는 취약점이 공식적으로 공개되었다. 이번 취약점은 TCP/IP 프로토콜 스택을 사용하는 경우라면 모두 해당이 되고, 발표자는 취약점을 통해 서비스거부(DoS) 상태가 발생될 수 있다고 주장하였다.



[그림 1-9] TCP/IP DoS 공격 기술 흐름[1]

TCP/IP라는 프로토콜 특성 상 인터넷의 기반이 되고 있어 자세한 정보는 공개되지 않고 있다. 우선 현재 이 문제를 해결하기 위하여 업체 및 CERT와도 협의가 진행 중이며 취약점의 자세한 기술적 배경은 2009년쯤에 공개하겠다고 한다. 알려진 바에 의하면, 이 공격은 5분만에 시스템을 다운시킬 수 있으며 실제 T2 컨퍼런스에서 데모를 통해 확인되었다고 한다.

[1] 출처 : Outpost24 의 "Introduction to SockStress 발표자료 중"

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

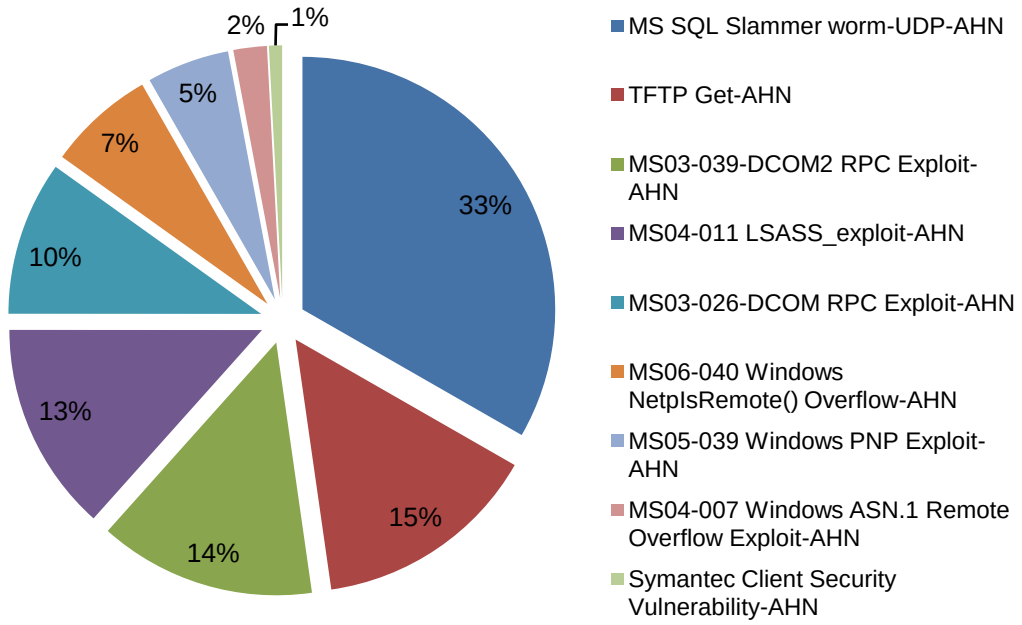
행사장에 있었던 한 사람에 의하면, 이것은 많은 양의 SYN Flooding 형태 또는 SYN 쿠키의 형태와 크게 달라 보이지 않으며 데모에서는 최신 패치가 적용된 윈도우 XP 시스템이 초당 30-40개의 조작된 연결을 통해 3분 안에 다운되었다고 한다. 즉, 7000개 정도의 패킷으로 많은 양의 DoS 공격이 아니었으며 이것은 100Mbit/s 에서 0.1%도 안되는 적은 양이다. 세부적 정보가 알려져 있지 않은 상태에서 또 다른 분석가는 이것은 알려져 있는 공격형태와 크게 다르지 않으며, 공격선상에서의 좀더 확장된 형태의 다른 공격방법일 뿐이라고도 하였다. 최근 DDoS 공격 피해 사례가 급증하고 시점에서 또 다른 TCP/IP DoS 공격의 발표는 참으로 반갑지 않은 소식이다. 실제 공격에 활용될 경우, 그 피해가 상상하기 어려울 정도이기 때문에 본사를 비롯한 많은 전문가들이 이에 집중하고 있다.

[그림 1-10] T2 컨퍼런스의 발표 현장 사진

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

(4) 네트워크 모니터링 현황 – TCP 445 포트 공격 시도

이번 달 네트워크 모니터링 시스템 상에서 탐지된 트래픽을 포트 기준으로 분류하여 살펴보면, 지난 9월과 마찬가지로 TCP/445 포트가 최상위 포트를 차지하였다. [그림 1-11]에 나와 있는 바와 같이 상위 위협 탐지 이벤트들에 포함된 대부분의 이벤트들이 해당 포트를 사용하는 MS 관련 취약점들이라는 점과도 일치한다.

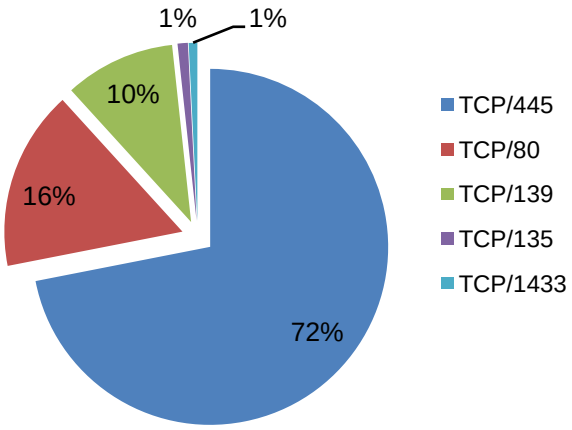


[그림 1-11] 상위 위협탐지 이벤트

최근에는 MS 관련 취약점을 통해 대규모의 자동화된 웜을 이용하는 확산 공격에서 벗어나, 웹을 기반으로 하는 웹 집중형의 공격이 인기를 얻고 있다. 따라서, 위협 탐지 이벤트들에서도 새로운 MS 관련 취약점을 활용한 공격이 발견되는 사례보다는 기존에 웜 확산을 위해 애용되었던 취약점들이 꾸준히 상위를 차지하고 있다.

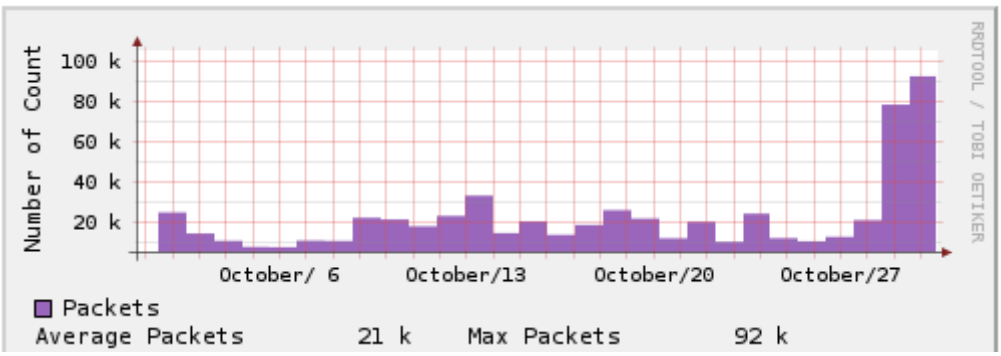
이러한 웹 집중 공격에 맞추어 안철수 연구소의 네트워크 모니터링 시스템에서도 웹 트래픽 유도 기능을 도입하여 이에 대한 모니터링을 시작하였고, 그 결과 이 달 [그림 1-12] 상위 TOP 5 포트 상에 TCP/80 포트가 비교적 큰 비중을 차지하게 되었다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림 1-12] 상위 TOP 5 포트

다음 [그림 1-13]은 최근 1개월 간의 TCP/445 포트 상의 트래픽 추이만을 살펴본 그래프이다. 10월 27일 이후로 TCP/445 포트 상의 트래픽이 급격하게 증가된 것이 발견되었다. 이 시점을 살펴보면 바로 MS08-067 서버 서비스 취약점이 발표된 직후라는 점을 주목하여야 한다. TCP/445, TCP/139 포트는 기존의 많은 MS 관련 취약점들이 주로 사용하는 포트이기 때문에 네트워크 상에서 항상 가장 높은 위치를 차지하기는 하지만, 이와 같이 급격한 증가를 보인 것은 해당 취약점으로 인한 트래픽 발생이 존재하였을 가능성이 높다는 것을 알 수 있다. 아직은 이를 본격적으로 활용한 대량의 공격 조짐은 나타나고 있지 않지만, 이미 확산을 위해 활용된 사례가 발견되었으므로 해당 포트에 대한 지속적인 모니터링이 필요할 것으로 보인다.

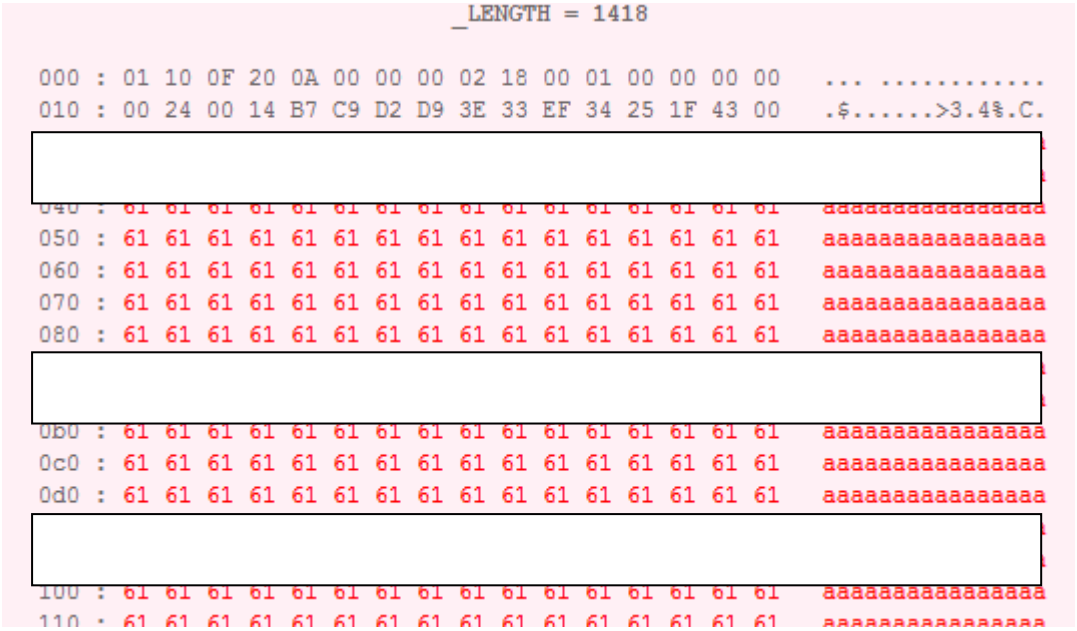


[그림 1-13] TCP/445 포트 상의 트래픽 추이

이 달에는 위협 탐지 이벤트 중에 지난 2007년 11월에 보고된 시만텍 안티바이러스 제품에서 발견된 버퍼오버플로우 취약점(이벤트명: Symantec Client Security Vulnerability-AHN) 이벤트가 탐지되었다. 해당 취약점은 다른 MS 관련 취약점들과 함께 각종 봇(Bot)류에서 지속적으로 애용되고 있는 취약점으로 다음과 같은 트래픽 패턴을 갖는다. 해당 취약점은 봇의 전파 목적으로 사용되기 때문에 간간히 트래픽 상에서 발견되고는 있지만, 취약점 자체가 특

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

정 제품에만 해당되고 안티바이러스 제품의 업데이트는 필수 항목이기 때문에 현재 피해는 거의 없을 것으로 추정된다.



[그림 1-14] 시만텍 취약점 패킷

마지막으로 국가별 공격 발생지 분포 그래프를 살펴보면, 다음 [표 1-1]에서 보듯이 지역적 영향으로 주로 아시아권 국가들이 많은 비중을 차지하였지만 대략 38개의 다양한 발생지로부터 공격 이벤트가 발생되었다. 기존의 공격 발생지로 많이 알려진 국가별 순위와 큰 차이 없이 이 달에도 한국을 비롯하여 미국(US), 일본(JP), 중국(CN), 홍콩(HK) 등의 국가들이 차례로 높은 비중을 차지하였다.

상위 10개 국가	백분율(%)	상위 10개 국가	백분율(%)
KR	34	IN	5
US	22	TW	3
JP	16	PH	2
CN	8	ZA	2
HK	6	MY	2

[표 1-1] 국가별 공격 발생지 분포

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

(5) 중국 보안 이슈 – 10월 중국 보안 이슈

일본 국영 석유 공사 홈페이지의 악성코드 유포

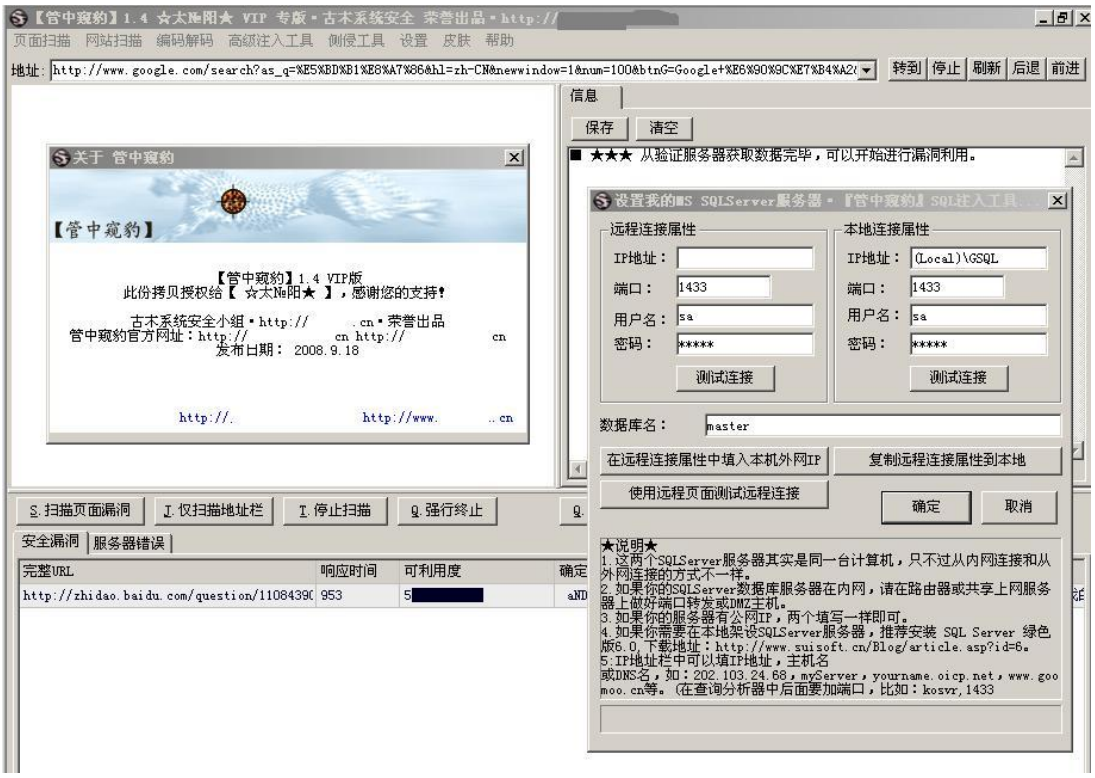
10월 21일경 일본 정부에서 운영하는 석유 가스 공사인 JOGMEC(Japan Oil, Gas and Metals National Corporation) 홈페이지에서 악성코드를 유포하는 사고가 발생한 것으로 요미우리 신문과 중국 언더그라운드 웹 사이트를 통해 알려졌다. 이번 사고로 약 2400명 정도가 해당 악성코드에 감염되어 개인 정보가 중국으로 전송된 것으로 알려졌다. 이번 사고에 사용된 악성코드에 대해서는 알려지지 않았으나 최근 많은 홈페이지 해킹에 사용된 SQL 인젝션 기법이 사용된 것으로 알려져 있다.

이번 보안 사고는 지난 6월 일본 정보와 중국 정부간에 맺어진 중국 동부 해안 지역의 석유 자원 개발 합의문이 일본 정부와 기업들에게 많은 이익을 가져다 주는 불평등한 합의문이라는 것에 대한 항의적인 성격으로 발생한 것으로 알려졌다. 이러한 보안 사고는 최근 몇 년간 지속적으로 발생하는 금전을 목적으로 하는 악성코드 유포와 더불어서 정치적인 목적의 해킹이 결합된 형태의 보안 사고로 볼 수 있을 것이다.

대규모 SQL 인젝션 공격에 사용되는 자동화된 공격 툴

2008년의 주요 동향으로 웹 서버를 통해 악성코드 유포를 위한 기법으로 SQL 인젝션이 많이 사용되고 있고, 이러한 공격 기법을 자동으로 수행하는 툴들을 지난 ASEC Report에서 몇 차례 다루었다. 이러한 자동화 된 공격 툴 중에서 지난 9월 중순 고급형으로 제작된 SQL 인젝션 공격 툴이 상용으로 판매되고 있는 것을 중국 언더그라운드 웹 사이트를 통해서 확인되었다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림 1-15] 상용으로 판매되는 중국에서 제작된 SQL인젝션 공격툴

이번에 발견된 SQL 인젝션 공격 툴들은 과거에 발견된 공격 툴에 비해서 한 층 발전된 형태의 공격 툴로서 다음과 같은 다양한 기능들을 포함하고 있었다.

1. 검색 엔진과 연동한 취약한 웹 사이트 검색 기능: SQL 인젝션에 취약한 웹 사이트들을 찾아 내기 위해서 Get과 Post 등의 특정 단어들을 검색어로 이용하여 중국의 바이두(Baidu)와 구글 웹 사이트와 자동으로 연동되도록 설정할 수 있다.
2. MS-SQL 데이터베이스에 대한 자동화된 공격 기능: MS-SQL 데이터베이스의 관리자 계정과 해당 데이터베이스에 존재하는 취약점 들을 연동하여 자동으로 공격을 수행 할 수 있다.

이러한 형태의 자동화된 공격 툴이 고급화가 이루어지고 상용으로 판매 됨에 따라서 해킹에 대한 고급지식이 없는 사람들 역시 해당 툴의 구매를 통해서 다량의 해킹과 악성코드 유포가 가능하다. 그리고 이러한 자동화된 공격으로부터 예방하기 위해서는 웹 서버뿐만 아니라 웹 어플리케이션과 데이터베이스 시스템 등 웹 사이트와 연동된 다양한 시스템들을 점검하고 공격에 이용될 가능성이 있는 취약점이 존재하는지 점검 하도록 해야 될 것 이다.

중국 언더그라운드에서 제작된 MS08-067 취약점을 이용하는 악성코드

10월 24일 마이크로소프트에서는 “MS08-067 서버 서비스의 취약점으로 인한 원격 코드 실행 문제점 (958644)” 취약점에 대한 패치를 긴급으로 배포하게 되었다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

[그림 1-16] 중국에서 제작된 MS08-067 취약점에 대한 공격 코드

그러나 해당 보안 패치 보다 하루 정도 빠르게 해당 취약점을 이용하는 악성코드가 유포되었다.

해당 악성코드는 V3 Internet Security 에서 Dropper/Gimmiv.397312, Win-Trojan/Gimmiv.336384, Win-Trojan/Gimmiv.49152와 Win-Trojan/Gimmiv.57344로 진단이 가능하며, 해당 악성코드가 감염을 위해 네트워크로 전송하는 공격 패킷은 "MS08-067 Server Service Exploit" 룰로 차단이 가능하다.

이번에 유포된 해당 악성코드의 제작 국가에 대해서 많은 정보 보호 전문가들은 중국 언더그라운드에서 제작한 것으로 추정되고 있으며, 실제 중국 언더그라운드 해킹 웹 사이트들에서는 [그림 1-16]과 같이 기존에 알려진 해당 취약점에 대한 PoC(Proof of Concept) 코드와는 조금 다른 형태의 공격 코드들이 알려져 있었다. 이렇게 악성코드에 사용될 소지가 높은 취약점들의 악의적인 이용 주기가 점점 짧아 지고 있으며 이러한 악성코드와 해킹과 같은 공격에 대비하기 위해서는 주기적으로 보안 업체의 최신 및 긴급 보안 정보를 통해 신속한 대응 전략을 수립하는 정책이 필요하다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

II. ASEC 컬럼

(1) MS08-046의 EMF 취약점

지난 8월 달에 공개된 MS08-046 취약점은 윈도우 이미지 색깔 관리 시스템에서 발생하는 버퍼 오버플로우 취약점이다. 과거 이미지 관련 취약점들이 지속적으로 발표되었고 최근에도 EMF/WMF 관련 취약점이 발견되고 있다. 현재 이 취약점의 원격코드 실행 가능한 공격코드는 미공개 상태이며, 탐색기(Explorer.exe) 자체 DoS 상태 코드만이 확인되었다. 이번달 ASEC report 컬럼에서는 해당 취약점에 대해서 세부적으로 살펴보고자 한다.

MSCMS(Microsoft Color Management System)은 마이크로소프트사에서 제공하는 색 관리를 위하여 사용되는 시스템으로, 이를 통해 EMF(Enhanced Metafile) 형식을 포함한 다양한 이미지 형식이 처리된다. 특히, EMF 파일은 그래픽 드로잉 명령, 오브젝트, 속성 등의 정보는 갖는 가변길이의 레코드들로 구성되어 있다.

EMF 파일의 EMR_SETICMPROFILEW와 같이 일부 특정 레코드 형식이 mscms.dll OpenColorProfileW() 함수를 통해 처리되는 과정에서 해당 취약점으로 인한 버퍼 오버플로우가 발생하게 된다. 이는 EMR_SETICMPROFILEW 레코드 내부의 Data 필드를 통해 전달되는 파라미터에 대한 올바른 검증절차가 수행되지 않기 때문에, 고정된 크기로 할당된 버퍼 이상의 데이터를 복사하는 과정에서 Heap 기반의 버퍼 오버플로우가 발생하게 되는 것이다. 앞서 할당된 Heap 버퍼의 경계를 넘어 Overwrite 된 메모리가 추후 다른 코드 상에서 참조되면서 Access Violation을 발생하며 Explorer.exe의 서비스 거부(Denial of Service)상태를 야기하게 된다.

우선 EMF(Enhanced MetaFile)의 구조를 들여다 보면 다음과 같이 다수의 EMF 레코드들로 구성되어 있다.

```
EMF file = EMF Header Record + EMF Records + EMF EOF(End-of-File) Record
```

EMF 레코드들은 다수의 그룹으로 분류되는데, 기본적으로 EMF 파일의 시작과 끝을 정의하는 “Control Record” 타입에 속하는 다음과 같은 레코드들이 있다.

- EMR_HEADER(0x00000001)
- EMR_EOF(0x0000000E)

특히, 해당 취약점은 그래픽 속성 값을 정의하고 관리하는 “State Record” 형식에 속하는 다음의 레코드들을 처리하는 과정에서 발생한다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

- EMR_SETICMPROFILEA(0x00000070)
- EMR_SETICMPROFILEW(0x00000001)

struct Header header	
enum RecordType iType	EMR_HEADER (1)
DWORD nSize	88
struct RECTL rclBounds	
struct RECTL rclFrame	
DWORD dSignature	1179469088
DWORD nVersion	65536
DWORD nBytes	900
DWORD nRecords	4
WORD nHandles	7
WORD sReserved	0
DWORD nDescription	0
DWORD offDescription	0
DWORD nPalEntries	0
struct SIZEL szlDevice	
struct SIZEL szlMillimeters	

[그림 2-1] EMF 헤더 구조

문제를 발생하는 코드의 내부 콜 구조는 다음과 같다.

Gdi32!fpOpenColorProfileW()

➔ mscms!OpenColorProfileW()

➔ mscms!InternalOpenColorProfile() *** 버퍼 오버런이 발생하는 지점**

실제 코드 상에서는 다음과 같은 파라미터 값을 가지고 함수를 호출한다.

```
77e3b63c 752b              jnz     GDI32!IcmRealizeColorProfile+0x4e (77e3b66
77e3b63e 837e2400          cmp      dword ptr [esi+0x24],0x0
77e3b642 7425              jz      GDI32!IcmRealizeColorProfile+0x4e (77e3b66
77e3b644 57                push     edi
77e3b645 6a03              push     0x3
77e3b647 6a03              push     0x3
77e3b649 6a01              push     0x1
77e3b64b 8d4620            lea      eax,[esi+0x20]
77e3b64e 50                push     eax
77e3b64f ff15003ce677 call dword ptr [GDI32!fpOpenColorProfileW (77e63c00)]
```

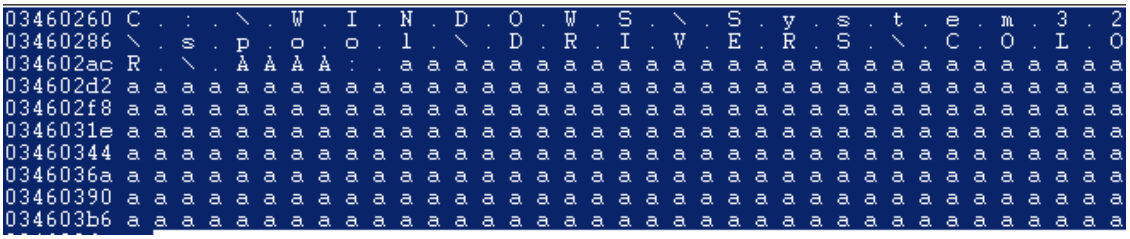
해당 데이터를 가지고 mscms!OpenColorProfileW() 함수는 내부적으로 다시 mscms!InternalOpenColorProfile() 함수를 호출한다. 이 함수 안에서 버퍼 오버플로우가 발생한다.

해당 함수는 프로파일 정보를 담고 있는 ProfileData 문자열이 디렉토리를 포함하는 파일명으로 판단되는 경우, 바로 프로파일 파일을 생성하지만, 파일명만 존재한다고 판단되는 경우, 윈도우 COLOR 디렉토리 정보(GetColorDirectory() 함수 호출)를 얻어와 ProfileData와 조합하게 된다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

```
BOOL WINAPI GetColorDirectory(
    PCTSTR pMachineName,  /* NULL인 경우, 로컬 시스템 */
    PTSTR pBuffer,
    PDWORD pdwSize          /* 104h */
);
```

이 때, 프로파일 파일 경로 저장을 위해서는 고정된 104h 크기의 버퍼가 할당되는데, 해당 버퍼에 획득된 윈도우 COLOR 디렉토리 정보를 포함하여 지금과 같이 과도하게 긴 문자열 profileData(0x3876dd8) 데이터가 추가되는 경우, 고정 길이 104h 크기 이상의 경계를 넘어서 메모리를 덮어씌우기(Overwrite) 하게 된다.



현재 이 취약점의 코드실행 공격코드는 공개되어 있지 않지만, 언더그라운드 사이에서는 이미 공유되었을 수 있고 원격에서 코드가 실행 가능하다는 점에서 위험도가 높다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

(2) VB2008 컨퍼런스 참관기

10월 초에 캐나다 오타와에서 18번째 국제 바이러스 컨퍼런스인 바이러스 블레틴 2008 컨퍼런스가 개최되었으며, 안철수연구소에서는 3명의 연구원이 참석하여 국제적인 악성코드의 주요 흐름과 이슈에 대한 파악하였다.

올해도 작년처럼 대체로 기술적 발표는 드물었다. 악성코드는 새로운 기법 등장 없이 2004년을 시작으로 2006년부터 급격한 악성코드 수 증가와 악성코드 제작에 금전적 목적이 들어가는 것 외에는 공격하는 쪽과 막는 쪽의 소모전 양상이 강하기 때문으로 보인다.

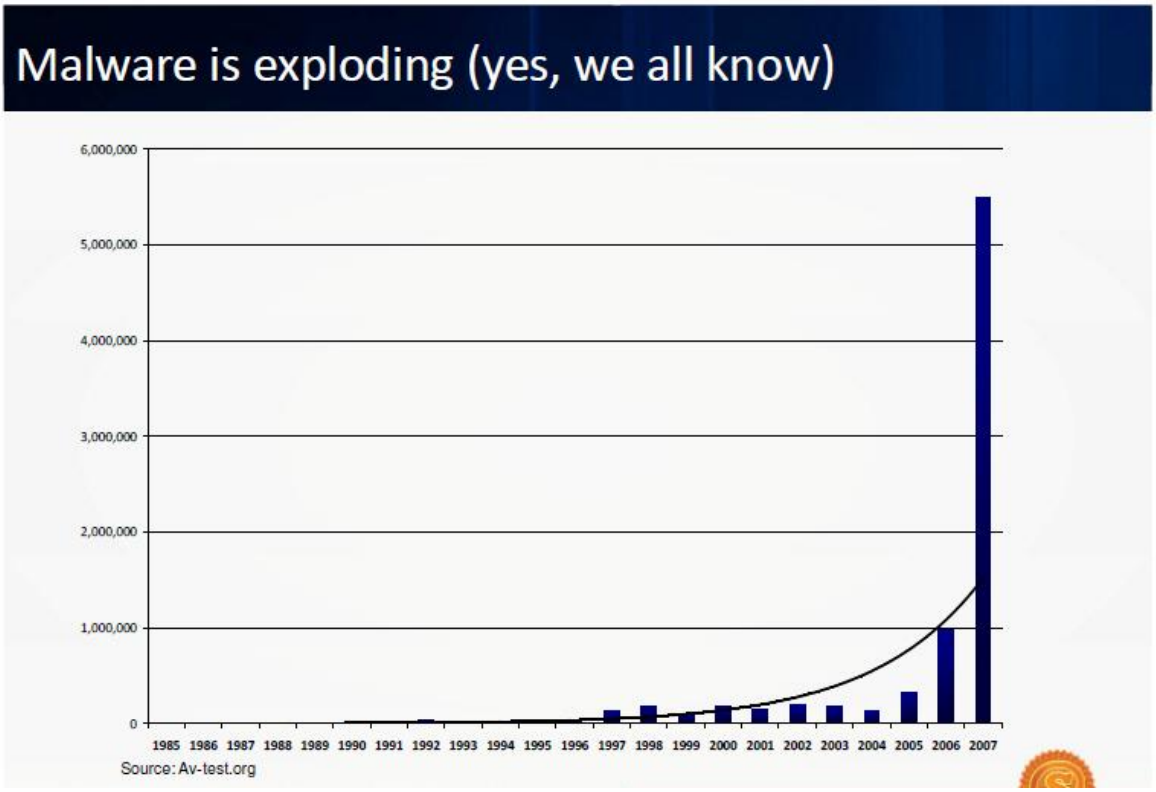
기조 연설

바이러스 블루틴 편집자인 헬렌(Helen Martin)의 오프닝 연설은 증가하는 온라인 뱅킹과 이를 노리는 피싱에 대한 내용이었다. 이후 기조 연설을 맡은 선벨트 사(Sunbelt)의 알렉스(Alex Eckelberry)는 성경 구절을 인용한 '백신 업계여 어디로 가시나이까? (The AV industry: quo vadis?)'에서 현재 백신 업계의 신화와 현실 그리고 해결책에 대한 얘기를 했다.

몇 년 동안 악성코드 수가 급격히 증가하면서 기존 시그니처를 통한 대처에 한계가 서서히 보이고 이에 "AV는 죽었다.(AV is dead.)", "윈도우 비스타와 함께라면 백신 프로그램은 필요 없다. (With Vista, you don't need antivirus.)" 등의 말이 쏟아져 나왔다. 하지만, 여러 논란은 있었지만 여전히 백신은 악성코드를 막는 가장 유용한 수단이다.

현황에 대해서는 업계 사람들이 모두 알고 있는 악성코드의 엄청난 증가(이 자료는 독일 AV-test에서 발표한 자료로 악성코드 수는 집계 방법에 따라 달라질 수 있지만 2004년을 시작으로 2006년부터 해마다 급격히 증가하고 있음은 모두 인정하고 있다.)와 업계가 마케팅에 중점을 두고 연구개발비에 큰 비용을 들이지 않는 점에 대한 얘기가 나왔다.

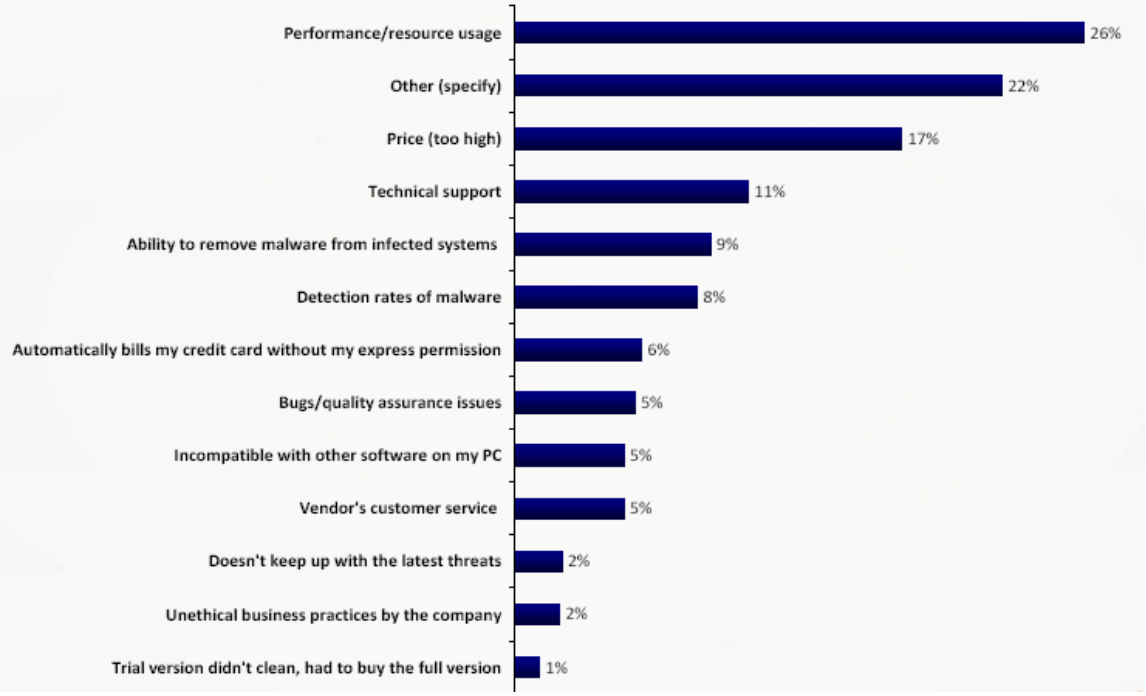
Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림 2-2] 악성코드의 폭발적 증가

2008년 9월 개인과 기업 사용자를 대상으로 설문조사 결과도 흥미로 왔는데 개인사용자와 기업 사용자를 중심으로 설문조사를 했을 때 제품 만족도의 차이가 비교적 컸다. 개인 사용자의 가장 큰 불만 사항으로 퍼포먼스와 리소스 사용을 1위로 꼽고 있어 백신 프로그램이 지나치게 비대화해 졌고 사용자들이 큰 불만을 가지고 있음을 알 수 있다. 그 다음으로 가격, 기술지원, 악성코드 진단과 제거로 나타났다. 기업 사용자들은 퍼포먼스, 악성코드 제거, 가격, 악성코드 진단, 기술 지원 순으로 문제점으로 제기했다.

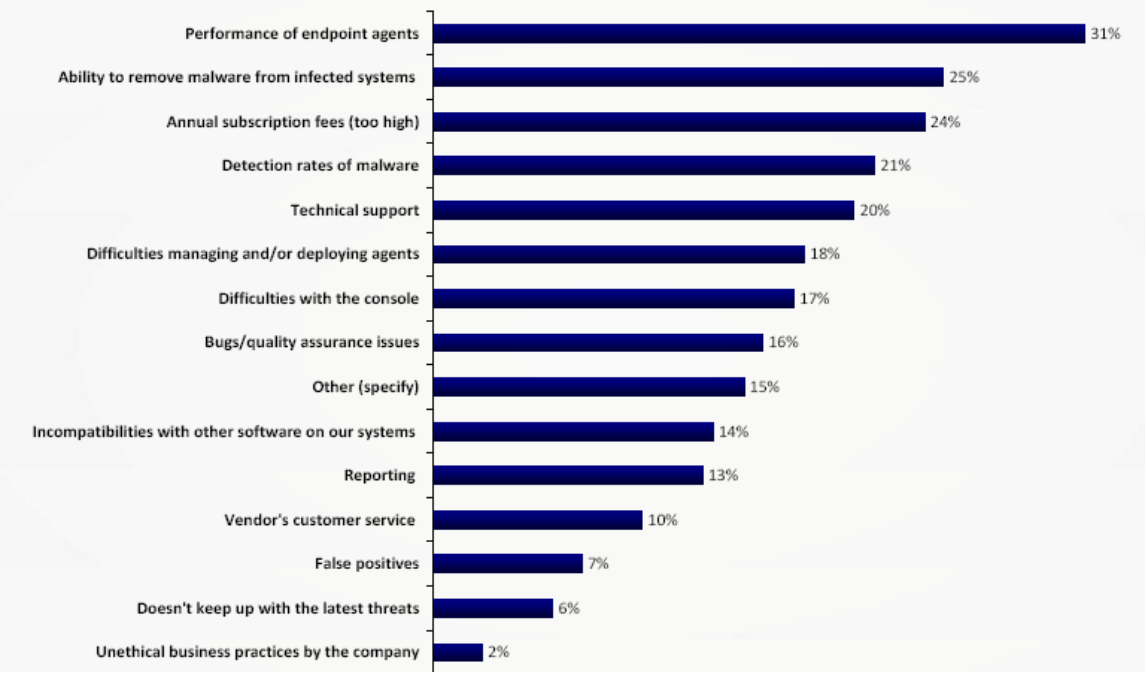
Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림 2-3] 개인의 백신에 대한 불만 설문 조사 결과

개인과 기업의 사용하는 제품 종류가 달랐는데 기업은 아무래도 관리 이슈 등이 있어 고객 지원이 상대적으로 좋은 큰 회사 제품을 선택하는 것으로 보인다. 기술지원의 경우 많은 업체에서 기술 지원에 어려움이 있으며 전화의 경우 무료로 가능한 업체는 15개 업체 중 5개였으며 나머지는 유료 혹은 설치와 알려진 문제에 대해서만 무료로 진행되는 경우가 많았다고 지적했다. 다소 놀라운 결과였는데 서비스는 무료로 인식되는 우리나라와는 조금 다른 문화적 차이가 아닐까 싶다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림 2-4] 기업 담당자의 백신에 대한 불만 설문 조사 결과

전화 통화가 힘들다, 메일 답변이 느리다 등의 문제는 대부분의 업계에서 발생하는 문제이며 결국 문제를 해결하는 업체가 고객들의 선택을 받을 수 있음을 알 수 있었다. 또한 최근 어떻게 하면 동일한 기능에 시스템 자원 소비가 적고 시스템 속도 저하를 못 느끼게 만드는가에 초점이 맞춰진 것도 이런 고객 불만이 반영된 결과가 아닐까 싶다.

MBR 루트킷 의 등장

1988년 흔히 최초의 컴퓨터 바이러스로 분류되는 브레인 바이러스(Brain virus)가 등장한 이후 부트 레코드에 감염되는 부트 바이러스는 구시대 유물로 취급되었다. 하지만, 무덤에 잠자던 부트 바이러스를 다시 깨운 건 2005년 블랙햇(BlackHat)에서 마스터 부트 레코드(Master Boot Record)를 변조한 루트킷의 POC가 공개되면서부터라고 할 수 있다. 2년 후 2007년 새로운 유형의 루트킷이 등장했으며 이후 계속 기술적인 발전을 하고 있다. 20년 전 최초의 컴퓨터 바이러스는 부트 바이러스 형태가 많았는데 20년 후 유행이 다시 돌아온 것은 아닐까? 하지만, 이 기법이 주류가 되기는 제작 방법도 어렵고 현실적으로 한계가 많지만 기술적인 이슈를 좋아하는 사람에게는 좋은 내용이었다.

안철수연구소 바이러스 신고센터와 VCC

독일 아비라(Avira)사는 VCC(Virus Control Center)에 대해서 발표 했다. 하지만, 안철수연구소의 바이러스신고 센터는 VCC보다 더 향상된 기능을 제공하고 10월 8일부터 서비스가

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

시작되었다.[1] 안철수연구소의 개편된 신고센터는 샘플 접수부터 처리 현황, 결과까지 이력을 확인할 수 있는 시스템에서 진일보해 단순 샘플 신고뿐 아니라 사용자 시스템에서 의심스러운 파일까지 수집할 수 있으며 내부적으로 정보를 공유할 수 있게 되어 있다.

테스트! 테스트! 테스트!

둘째 날 섹션의 대부분이 스팸에 대한 내용이었다면 마지막 날 섹션 중 상당수는 테스트에 대한 내용이었다.

블루틴의 존 하웨즈(John Hawes)는 RAP에 대한 발표를 했다. 오늘의 업데이트가 내일은 무용지물인 현실을 반영해 특정 기간 업데이트 없이 새로 발견되는 악성코드를 얼마나 진단할 수 있는지 테스트하는 것으로 행동 검사(Behavior detection), 휴리스틱 진단(Heuristic detection), 제네릭 진단(Generic detection)으로 테스트 한다. 현재 RAP 단계는 테스트 시스템을 검증하고 문제점을 계속적으로 수정하는 단계이다.

맥아피의 이고르 무틱(Igor Muttik)은 '미래를 위한 테스트 재정립(Rebuilding testing for the future)'에서 악성코드들이 진화하고 변화하는 것에 따른 새로운 테스트 기법과 방안이 필요하다는 논의를 꺼냈다.. 관련 내용은 현재 업계에서 테스트 표준을 준비하고 있다.

가상화

가상화 인프라가 계속 구축되면서 그에 따른 보안이슈들에 대한 얘기가 나왔다. 여러 가지 가상화 기술에 대한 소개가 있었고 가상화 서버에 대한 위협들과 미래에 있을 위협들에 대한 소개를 했으며 그에 따른 보안업체들의 대응 관점에서의 얘기가 있었다.

가상화는 새로운 패러다임의 컴퓨팅을 구축하고 있고, 예전과는 다른 전혀 새로운 취약점 및 위협들과 만나게 될 것이란 얘기가 있었다. 소개된 위협 중, 가상화되어 있는 서버가 마이그레이션(Migration) 과정에서 해커에 의해 탐지 당하거나 루트킷 공격에 의해 서버군 전체가 장악되는 이야기가 흥미로웠다.

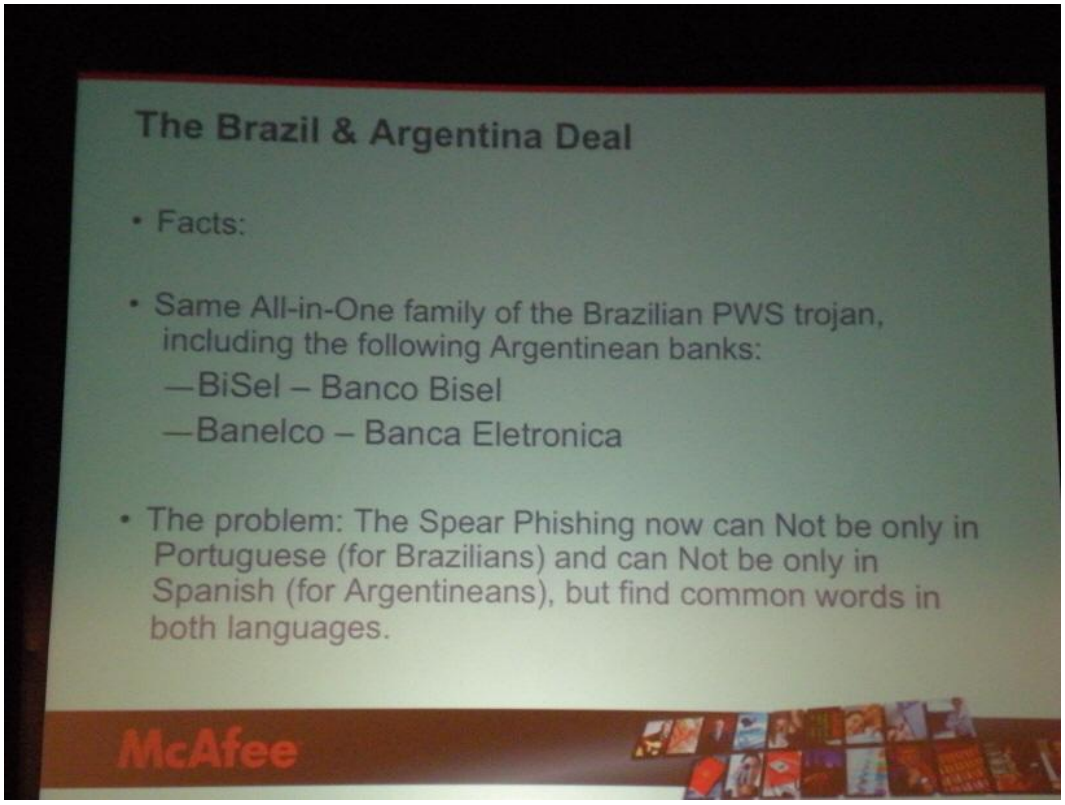
악성코드 연합 전선

중남미의 은행 계좌 탈취를 위한 악성코드에 대하여 잘 알려져 있지는 않지만, 그쪽 지역에서는 심각한 문제를 유발하고 있는 것으로 알려져 있다. 그러나, 브라질에는 지역 백신 회사가 없으며 악성코드 분석 및 대응과 관련하여 알려진 사람도 드문 편이다.

[1] http://kr.ahnlab.com/info/noticeView.ahn?num=50079915

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

최근 맥아피 브라질 연구소에서 남미의 은행계좌 탈취 트로이목마 현황 및 최근 악성코드 제작자들의 협력에 대해 발표했다. 과거 식민지의 영향으로 브라질은 포르투갈어를, 나머지 국가는 스페인어를 사용한다. 브라질과 그 외 남미 국가는 사용하는 언어가 다르지만 최근 브라질과 멕시코, 아르헨티나 등의 남미 국가에서 연합해 하나의 악성코드로 여러 은행계정을 탈취할 수 있다고 한다. 악성코드 제작 동기가 금전적 목적이 되면서 범죄도 점차 조직화, 국제화 되는 게 아닐까 하는 우려도 해본다.



[그림 2-5] 악성코드 제작자 연합전선

이외 인터넷 뱅킹 보안에 대해서는 패널 토론도 있었는데 인터넷 뱅킹과 관련해 해외에는 타 은행간 이체는 허용하지 않는 경우가 많으며 돈이 유출되어도 은행에서 보상하는 곳이 많다고 한다. 하지만, 정확하게 얼마나 피해가 발생했는지는 자료가 공개되고 있지 않는다고 한다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

III. ASEC 월간 통계

(1) 10월 악성코드 통계

Top 10 피해 통계

10 월순위		악성코드명	건수	%
1	new	Win-Trojan/Bagle.858628	49	21.6%
2	new	Win-Trojan/Autorun.250651	44	19.4%
3	new	Win-Trojan/Agent.137728.AN	22	9.7%
4	new	Win-Trojan/Agent.73728.JC	22	9.7%
5	new	Win-Trojan/Agent.80384.AL	20	8.8%
6	new	Win-Trojan/OnlineGameHack.22016.BD	16	7.0%
7	new	Win-Trojan/XPack.36864	14	6.2%
8	new	Win-Trojan/Tervemoy.86016.B	14	6.2%
9	new	Win-Trojan/Agent.75264.AX	13	5.7%
10	new	Win-Trojan/OnlineGameHack.170376	13	5.7%
합계			227	100.0%

[표 3-1] 2008년 10월 악성코드 피해 Top 10

[표 3-1]은 2008년 10월 악성코드로 인한 피해 Top 10에 랭크 된 악성코드들로서 이들 악성코드들로 인한 총 피해건수는 227건이다. 이는 10월 한 달 접수된 총 피해건 수(2,995건)의 7.6%에 해당하며, 지난 9월 389건(10.2%)보다 줄어든 것으로 나타났다. 이는 특정 악성코드로 인하여 다수의 고객 피해가 발생하는 것이 아니라, 악성코드가 대량 제작 배포되고 생명 주기가 짧은 현상을 간접적으로 보여준다.

지난달과 비교하여 두드러진 차이점은 8, 9월에 1위를 차지한 허위 백신류의 악성코드의 수가 현저하게 줄어든 것과 2008년도 하반기에는 악성코드 피해가 점차 줄어들고 있다는 것이다. 또한 지난 8월과 동일하게 트로이목마가 Top 10을 모두 차지하였다. Win-Trojan/Bagle.858628는 악성코드내에 하드코딩된 이메일주소로 감염된 시스템에서 수집된 정보를 훔쳐 자체 SMTP엔진을 이용하여 메일을 발송하는 악성코드로 10월에 49건이 접수되면서 1위로 랭크 되었다.

Win-Trojan/Bagle.858628과 Win-Trojan/Autorun.250651이 21%, 19%로 가장 많은 비중을 차지 하였으며, Win-Trojan/Agent류의 악성코드가 10%, 10%, 9%로 그 뒤를 잇고 있다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

나머지 악성코드들은 대부분 7%~6%의 비율로 큰 차이를 나타내지는 않고 있다. 하지만 10월은 9월에 비하여 Win-Trojan/Autorun류의 악성코드가 5.9%(23건)에서 19%(44)로 증가하여 다소 많은 피해를 준 것으로 나타났다.

10 월순위	대표 진단명	건수	%
1	Win-Trojan/Agent	383	30.3%
2	Win-Trojan/OnlineGameHack	281	22.2%
3	Win-Trojan/Downloader	172	13.6%
4	Win-Trojan/Autorun	97	7.7%
5	Dropper/OnlineGameHack	81	6.4%
6	Win32/Autorun.worm	81	6.4%
7	Win-Trojan/Bagle	54	4.3%
8	Win-Trojan/Fakeav	44	3.5%
9	Dropper/Agent	38	3.0%
10	Win-Trojan/Zlob	34	2.7%

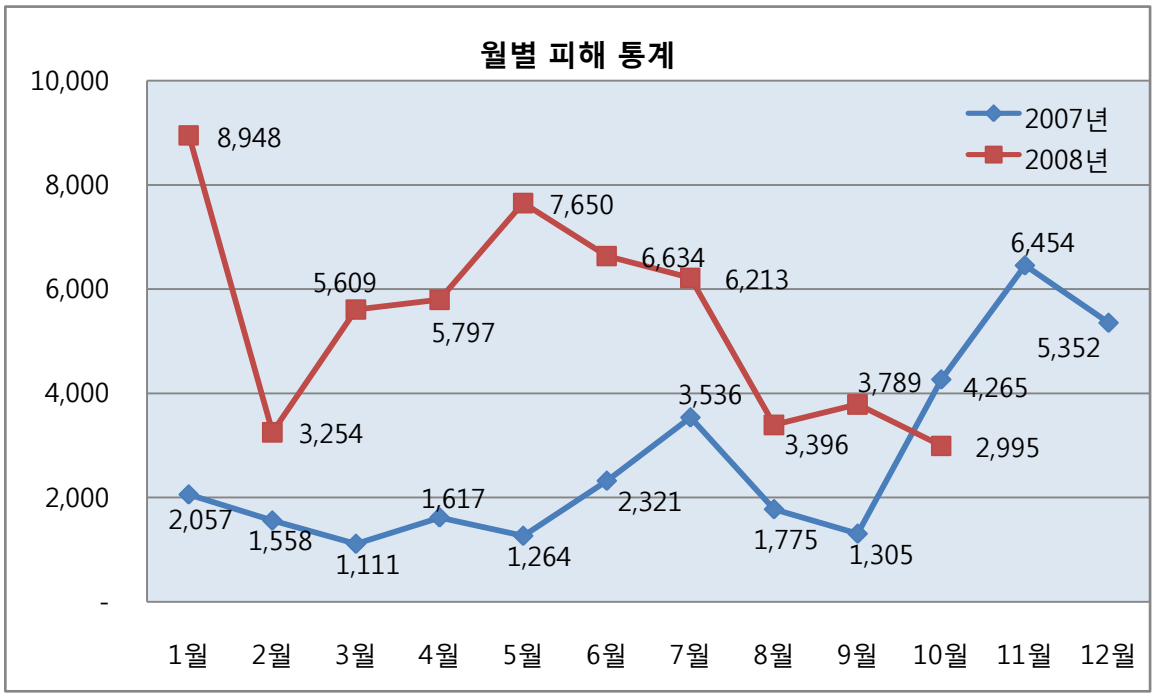
[표 3-2] 2008년 10월 악성코드 유형별 Top 10

[표 3-2]는 2008년 10월 악성코드의 대표진단명을 기준으로 유형별 피해 순위를 나타내고 있다. 유형별 Top 10에 포함된 악성코드 총 피해건수는 1,265건으로 10월 한 달 접수된 총 피해건 수(2,261)의 55.9%로 절반이상을 차지하고 있다. 이러한 Trojan 악성코드 대부분은 OnlineGameHack류의 악성코드이며, 이 악성코드가 줄어들지 않는 이유는 중국에서 제작된 웹사이트 취약점을 이용한 악성코드 삽입 툴이 지속적으로 국내 웹사이트를 공격하고 있기 때문으로 추정된다.

특정 악성코드의 피해를 나타내는 [표 3-1]과는 달리 전체적으로 보았을 때 여전히 온라인 게임핵 악성코드가 상위권에 랭크 되어 있으며, [표 3-1]의 10위권에서 밀려난 허위백신류의 Win-Trojan/Fakeav는 대표진단명에서 8위를 차지하고 있는데, 이는 다양한 변종이 발생하였으나 그 피해는 점차 줄어들고 있는 것으로 해석된다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

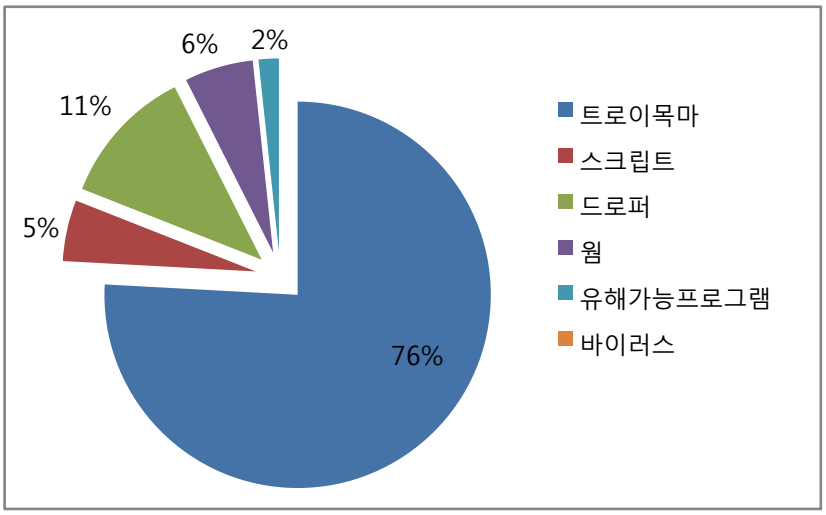
월별 피해신고 건수



[그림 3-1] 2007,2008년 월별 피해신고 건수

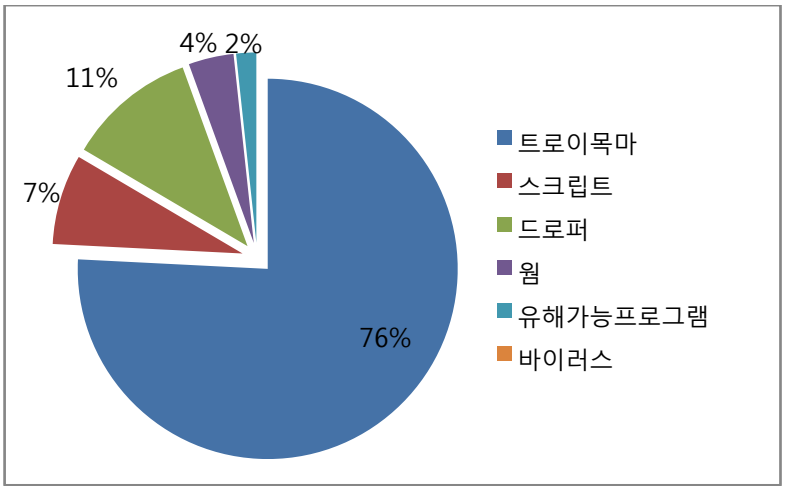
[그림 3-1]은 월별 피해신고 건수를 나타내는 그래프로 10월은 전체 2,995건의 피해신고가 접수되었으며 지난달 3,789건과 비교하여 약 21% 정도 감소한 것으로 나타났다. 지난 5월을 기점으로 꾸준한 감소세를 보였던 피해신고 건수가 9월에 소폭 상승하면서 2007년과 유사하게 증가할 것으로 예상하였으나 다시 감소하였다. 이러한 추이는 악성코드의 연말 특수(미국 대선, 크리스마스 등)로 인한 스팸 메일 증가가 예상되면서 더욱더 잠재적인 위험을 내포하고 있을 것으로 추정된다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림 3-2] 2008년 10월 악성코드 유형별 피해신고 건 수

[그림 3-2]는 2008년 10월 전체 악성코드 유형별 피해신고 건 수를 나타내고 있는 그래프이다. Top 10의 유형과 마찬가지로 전체 피해신고 유형을 봤을때에도 트로이목마가 76%로 높은 비중을 차지하고 있으며 7월, 8월, 9월을 거쳐 점차 감소하고 있던 드로퍼는 게임핵류의 악성코드 증가로 인해 11%로 증가하였다. 웜은 지난달 9%에서 3% 감소한 6%로 소폭 감소하였다.



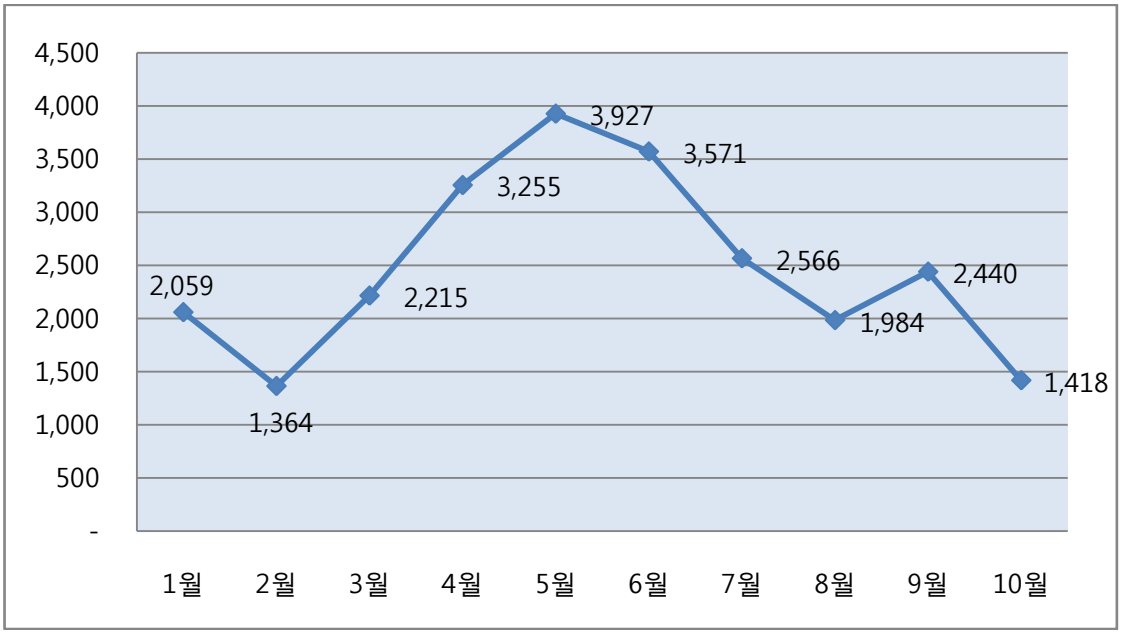
[그림 3-3] 2008년 10월 피해 신고된 악성코드의 유형별 현황

[그림 3-3]은 10월 한달 간 접수된 유형별 신고건수로 [그림 3-2]의 유형별 피해신고 건수와 마찬가지로 트로이목마가 76%로 여전히 높은 비율을 차지하고 있다. 나머지 스크립트 7%, 드로퍼 11%, 웜 4%, 유해가능프로그램이 2%를 골고루 차지하고 있으며 여전히 바이러스는 전체 비율에서 1%도 안 되는 비율을 차지하고 있다.

바이러스의 경우 Win32/Kashu.B가 Autorun류의 악성코드와 동일하게 USB와 같은 저장매

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

체를 통해 유포되었던 경우가 있었으나 진단 및 치료가 가능했던 바이러스였기에 크게 이슈가 되지 않고 조기에 차단될 수 있었다.



[그림 3-4] 2008년 월별 피해신고 악성코드 종류

[그림 3-4]는 2008년 월별로 피해신고가 되는 악성코드의 종류를 나타낸 그래프이다. 월별로 신고되는 [그림 3-1]의 월별 피해신고 건수와 마찬가지로 3개월간 꾸준히 감소하다가 9월에 반등을 하였으나 10월에는 큰 폭으로 감소하였다. 2008년의 11월과 12월은 2007년 연말 악성코드 추이와 유사하게 윈도우 보안취약점을 이용한 젤라틴 웜이 첨부된 스팸 메일이 유포될 가능성을 배제할 수 없기에 더더욱 남아 있는 기간 동안에 악성코드 종류가 어떻게 증가할지 쉽게 예측하기 어려워졌다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

국내 신종(변형) 악성코드 발견 피해 통계

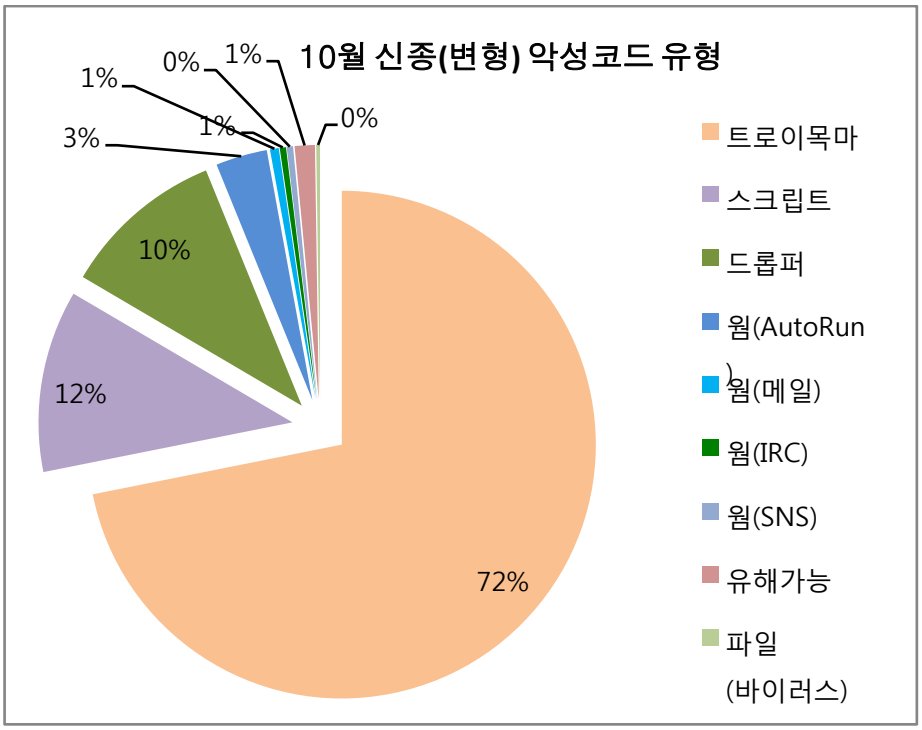
10월 한 달 동안 접수된 신종 (변형) 악성코드의 건수 및 유형은 [표 3-3] 과 같다.

	웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
08 월	55	1094	195	88	1	0	0	0	10	0	1443
09 월	64	867	97	91	2	0	0	0	13	0	1134
10 월	58	899	130	145	3	0	0	0	16	0	1251

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

이번 달 신종 및 변형 악성코드는 10% 가량 상승하였다. 특히 스크립트, 드롭퍼, 트로이목마 유형이 증가하였다. 스크립트와 드롭퍼 유형은 전월 대비 각각 59%, 34% 증가 하였다. 온라인 게임 계정을 탈취하는 악성코드 유형이 전월 대비 12% 가량 증가하면서 관련 드롭퍼와 스크립트 유형의 악성코드들도 상승한 것으로 추정된다.

다음은 이번 달 악성코드 유형을 상세히 분류하였다.



[그림 3-5] 2008년 10월 신종 및 변형 악성코드 유형

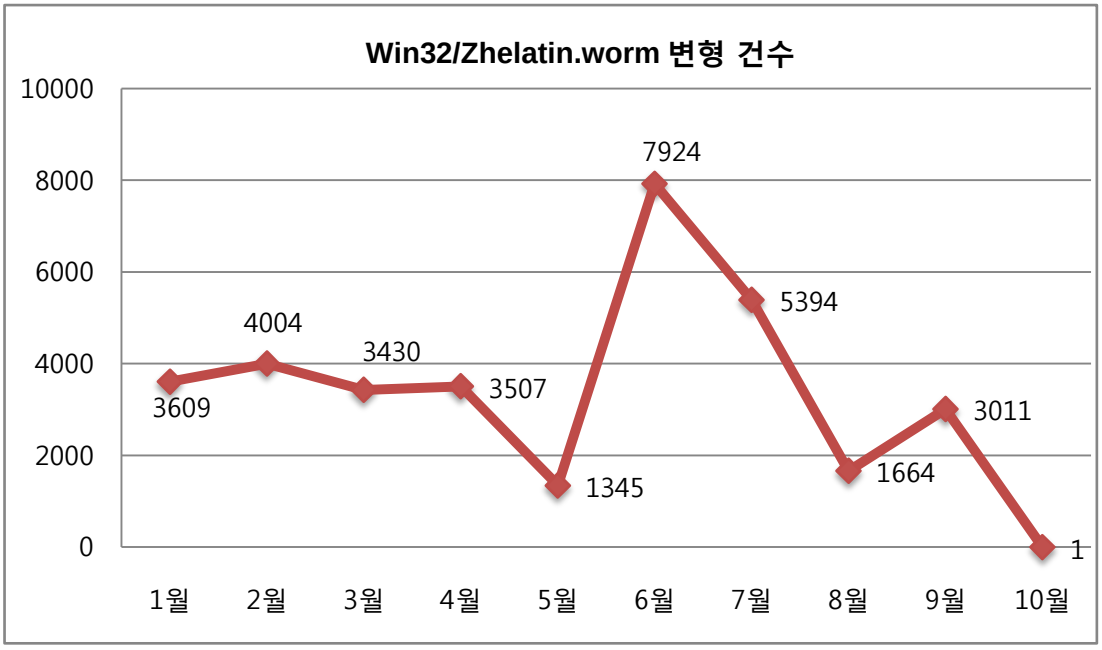
트로이목마 유형은 전월 대비 4% 가량 증가하였다. 스크립트와 드롭퍼 유형은 위에서 언급했듯이 이번 달 증가율이 높았다. 웜 유형에서는 Autorun 계열이 가장 많은 변형을 차지하

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

고 있으며 이번 달 다수의 변형이 발견된 Facebook 관련 웜도 새롭게 웜 유형으로 추가하였다. Facebook 관련 악성코드는 미국내 대표적인 SNS(Social Networking Service)로 이를 노리는 악성코드는 기존에 이미 알려졌고 V3에서도 진단 되고 있다. 이 악성코드는 해당 사이트에 접속 되어 있는 경우 사용자의 버디 리스트의 개인 페이지내에 방명록 또는 덧글 형태로 악의적인 웹 사이트로 유도 하도록 하여 자신을 전파 한다.

국내에서의 SNS 관련 악성코드는 아직 위와 같은 수준은 아니고 일부 포털의 사용자들의 쪽지함에 악성코드가 업로드된 링크를 보내어 클릭을 유도하는 형태가 보고 되었다. 이것은 대부분 사회공학기법으로 호기심어린 사진이나 메시지등으로 사용자를 기만하고 있으므로 출처가 불분명하거나 버디 리스트내 사람에게 온 내용이라고 할지라도 의심스럽다면 반드시 메시지를 보낸 사용자에게 확인이 필요하다.

메일 웜은 주춤 하였는데 특히 올 한해 대표적인 메일 웜이였던 Win32/Zhelatin.worm (이하 젤라틴 웜) 은 이번 달 한 건도 사용자들로부터는 접수되지 않았다. 이뿐만 아니라 다른 경로부터 접수 및 모니터링 되는 곳에서도 젤라틴 웜은 단지 1건만 보고 되었다. 다음은 올해 젤라틴 웜에 대한 안철수연구소 보고 건수[1]이다.



[그림 3-6] 2008년 젤라틴 웜 접수 건 수

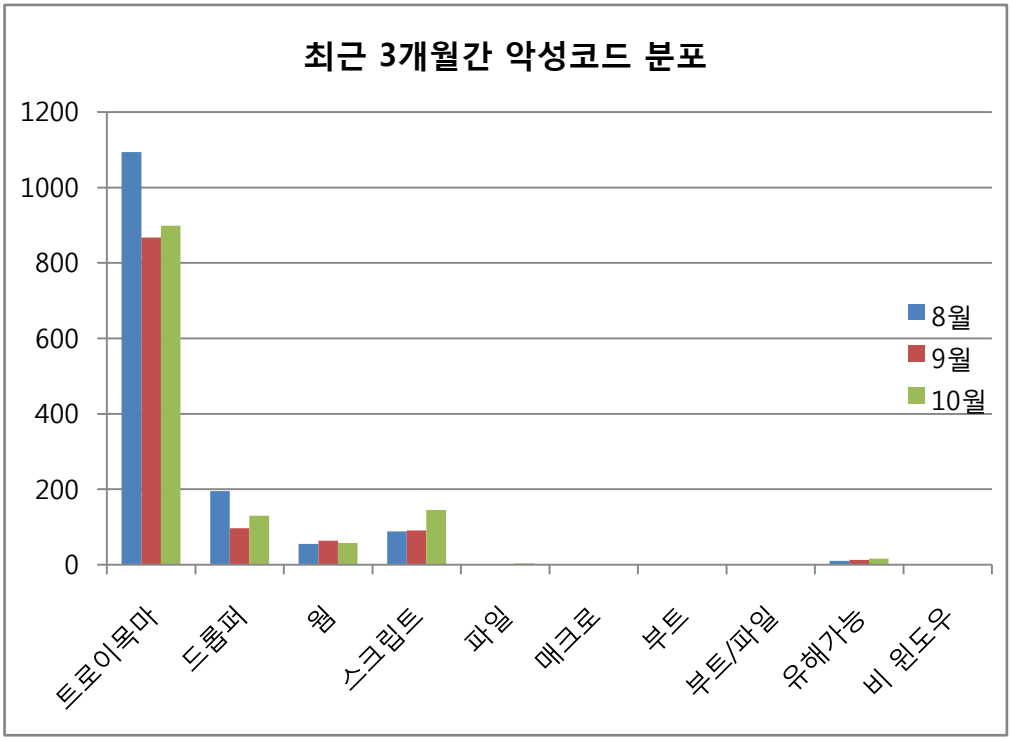
6월 이후 하락 추세에 있으며 9월은 상승 하였으나 이는 실제로 문제가 될 수 있는 사용자 접수는 오히려 하락 한 경우이다. 즉, 기타 경로의 접수처의 샘플은 상승 하였으나 이것은

[1] 이는 사용자 및 기타 경로로 접수된 모든 것을 나타낸다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

실제 사용자로부터 접수된 샘플의 의미는 아니다. 10월은 거의 보고 되지 않았다. 해당 악성코드가 주춤하거나 활동이 둔화된 이유로 여러가지 이유로 추정하고 있는데 그중 유력한 것은 Bot 마스터가 새로운 형태의 변형을 준비하고 있거나 누군가에 의해서 Bot C&C 서버들이 그 기능을 하지 못한 것으로 보고 있다. 이론적으로 P2P 형태의 Bot C&C 서버도 인증을 통과하여 이를 제어 할 수 있다면 더 이상 Bot 들은 기능을 상실 할 수 밖에는 없다. 그러나 젤라틴 웜과 같은 거대한 봇넷을 구성하는 악성코드들은 그 종류가 많으므로 젤라틴 웜이 감소 하였다고 해서 전체적인 악성코드가 감소하지는 않았다.

다음은 최근 3개월간 악성코드 분포이다.

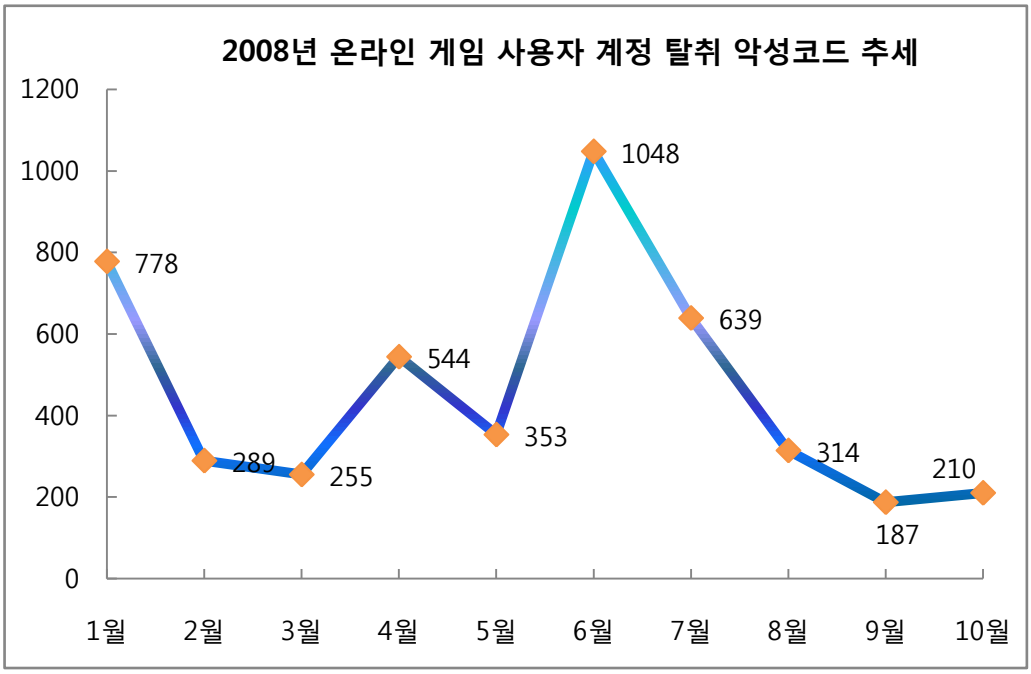


[그림 3-7] 2008년 최근 3개월간 악성코드 분포

트로이목마, 드롭퍼, 스크립트 유형등이 전월 대비 상승 하였다. 8월, 9월을 뜨겁게 달구었던 가짜 백신들은 주춤했다. 안철수연구소는 전용백신을 10월 한 달 동안 꾸준히 업데이트 하였고 제품에서도 진단 및 치료기능을 향상하여 타사 대비 치료에 우위를 가지고 있다. 그러한 결과로 실제로 연구소로 접수 되었던 미진단 가짜 백신은 9월 64개에서 10월은 30개 정도로 감소 하였다. (V3 사용자 접수 샘플 기준)

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

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.



[그림 3-8] 온라인 게임 사용자 계정 탈취 트로이목마 현황

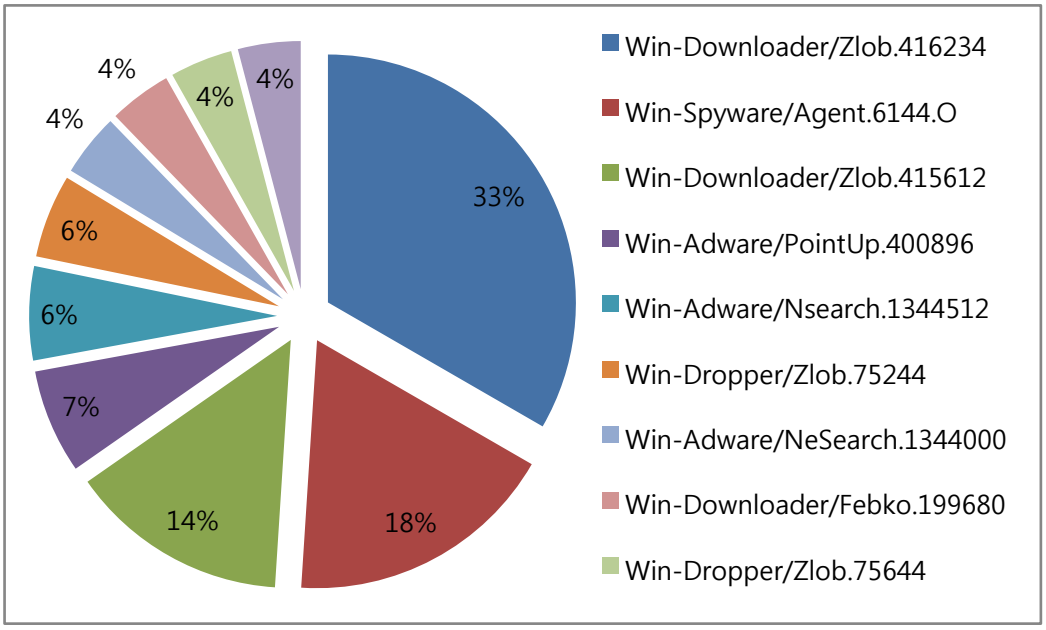
전월 대비 12% 상승한 해당 악성코드는 그래도 이전과 비교하면 여전히 적은 수가 발견, 보고 되고 있다. 특이할 만한 것은 이번 달에는 특정 온라인 게임을 노리는 악성코드가 디버깅 중이라고 판단 되면 해당 시스템의 MBR(Master Boot Record)을 쓰레기 값으로 쓰고 특정 메시지를 삽입하여 부팅시 출력하는 형태가 보고 되었다. 사용자들에게는 별다른 이상이 없지만 안티 바이러스 연구원들처럼 분석을 위하여 해당 악성코드를 디버거로 디버깅 한다면 MBR이 손상될 우려가 있다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

(2) 10월 스파이웨어 통계

순위		스파이웨어 명	건수	비율
1	New	Win-Downloader/Zlob.416234	49	33%
2	New	Win-Spyware/Agent.6144.O	26	18%
3	New	Win-Downloader/Zlob.415612	21	14%
4	New	Win-Adware/PointUp.400896	10	7%
5	New	Win-Adware/Nsearch.1344512	9	6%
6	New	Win-Dropper/Zlob.75244	8	6%
7	New	Win-Adware/NeSearch.1344000	6	4%
8	New	Win-Downloader/Febko.199680	6	4%
9	New	Win-Dropper/Zlob.75644	6	4%
10	New	Win-Downloader/Nsearch.197632	6	4%
합계			147	100%

[표 3-4] 2008년 10월 스파이웨어 피해 Top 10



[그림 3-9] 2008년 10월 스파이웨어 피해 Top 10

스파이웨어 즐롭(Win-Spyware/Zlob)의 피해가 10월에도 계속되고 있는 가운데 국내에서 제작된 애드웨어 NeSearch(Win-Adware/NeSearch)가 단일 스파이웨어로서는 많은 피해를 입혔다. 최근 국내제작 스파이웨어의 피해는 외국산에 비해 상대적으로 감소하였으나 NeSearch를 포함하여 다운로더 Kwsearch(Win-Downloader/Kwsearch), 다운로더 카지노(Win-Downloader/Casino) 등의 피해는 지속적으로 접수되고 있다. 이들 국내제작 스파이웨

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

어는 보안프로그램의 진단을 피하기 위한 목적으로 지속적으로 변형을 배포하며, 정상 프로그램으로 위장하거나 랜덤한 파일이름을 사용하여 설치되는 공통점이 있다.

순위	대표진단명	건수	비율
1	Win-Downloader/Zlob	283	47%
2	Win-Spyware/Crypter	54	9%
3	Win-Dropper/Zlob	50	8%
4	Win-Spyware/Zlob	44	7%
5	Win-Spyware/Agent	38	6%
6	Win-Clicker/FakeAlert	34	6%
7	Win-Spyware/Xema	30	5%
8	Win-Adware/Kwsearch	28	5%
9	Win-Downloader/Kwsearch	21	4%
10	Win-Spyware/PWS.OnlineGame	18	3%
		597	100%

[표 3-5] 대표진단명에 의한 스파이웨어 피해 Top10

스파이웨어 즐롭에 의한 피해는 [표 3-5]의 대표진단명에 의한 스파이웨어 피해 자료에서 더욱 확실하게 파악할 수 있다. 다운로더 즐롭(Win-Downloader/Zlob)은 스팸메일이나 성인 사이트에서 많이 발견되며 전체 스파이웨어 피해 신고 건수 1,142건의 약 1/4을 차지할 정도로 많은 피해 신고가 접수되었다. 10월에는 안티바이러스XP2008과 같은 허위 안티-스파이웨어 프로그램의 피해가 순위권에 집계되지 않았다. 전용백신 배포와 변형 샘플 모니터링 등의 노력으로 허위 안티-스파이웨어 피해가 감소한 것으로 풀이된다.

2008년 10월 유형별 스파이웨어 피해 현황은 [표 3-6]과 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
8월	365	353	204	310	3	97	3	1	12	1348
9월	418	170	179	275	0	77	0	2	5	1126
10월	274	235	139	452	0	40	0	2	0	1142

[표 3-6] 2008년 10월 유형별 스파이웨어 피해 건수

[표 3-6]은 2008년 10월 유형별 스파이웨어 피해 현황이다. 전체 피해신고 건수는 지난 9월과 비슷한 가운데 다운로더와 애드웨어 피해는 증가하고, 스파이웨어와 드롭퍼, 클리커에 의한 피해는 감소하였다. 다운로더 즐롭의 영향으로 다운로더 계열의 스파이웨어 피해가 크

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

게 증가하였으며, 10월에는 국내제작 애드웨어의 피해가 증가한 것으로 확인되었다.

10월 스파이웨어 발견 현황

10월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 3-7]과 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
8월	223	175	137	182	2	22	1	0	3	745
9월	244	108	112	188	0	30	0	1	1	684
10월	180	138	90	345	0	29	0	2	0	784

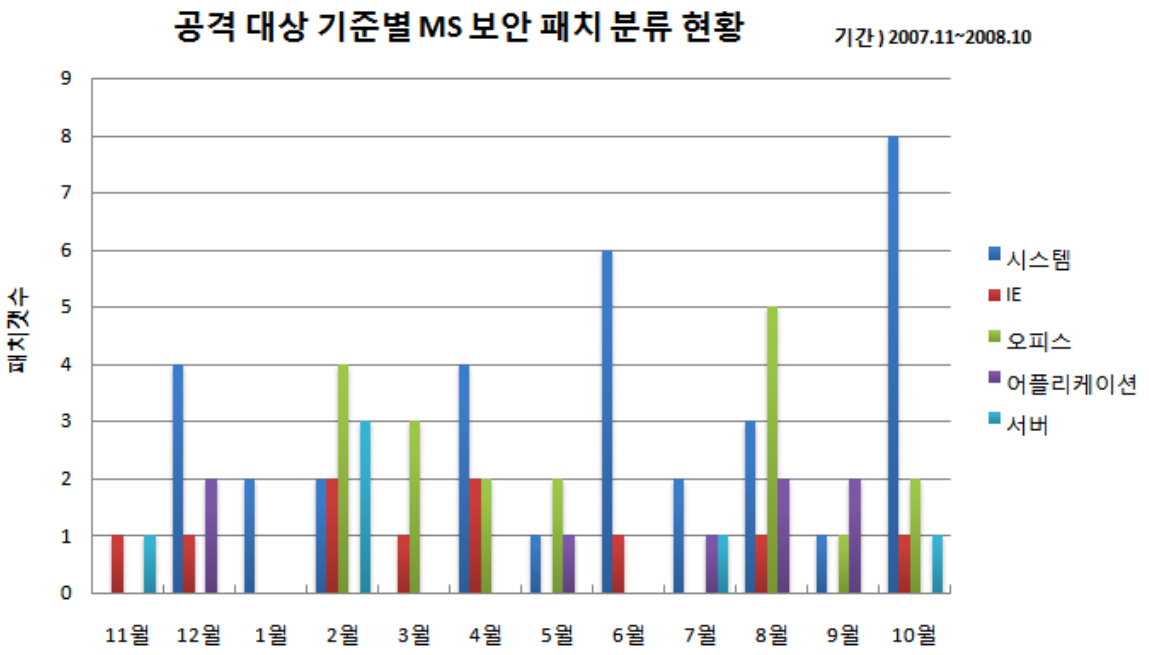
[표 3-7] 2008년 9월 유형별 신종(변형) 스파이웨어 발견 현황

[표 3-7]은 2008년 10월 발견된 신종 및 변형 스파이웨어 통계를 보여준다. 다운로더 즐롭의 변형 샘플 모니터링의 결과로 다운로더 발견 건수가 증가하였다. [표 3-7]의 유형별 스파이웨어 신종(변형) 발견 건수는 [표 3-6]의 유형별 스파이웨어 피해 현황과 비슷한 비율을 나타내고 있다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

(3) 10월 시큐리티 통계

2008년 10월에 마이크로소프트사로부터 발표된 보안 업데이트는 총 12건으로 긴급(Critical) 5건, 중요(Important) 6건, 보통(Moderato) 1건이다. 이 달에는 12건이라는 그 규모뿐만 아니라 대부분 Windows 시스템에서 발생되는 취약점이라는 점과 공격 Exploit이 공개된 사례가 많다는 점에서 기존과 차이를 보인다. 특히, 이 달에는 마이크로소프트사로부터 매주 둘째주 화요일(영문기준)에 발표되는 정기업데이트 외에 MS08-067 서버 서비스 취약점[1]에 대한 긴급 보안업데이트(Out-of-Band)가 발표되기도 하였다. 해당 취약점은 0-day 취약점으로 업데이트 발표와 함께 공격 Exploit 및 취약점을 이용한 악성파일이 본격적으로 발표되었다. 서버 서비스는 윈도우 시스템에서 제공하는 디폴트 서비스로서 그 확산 위험이 크기 때문에 많은 보안 전문가를 비롯한 관계자들이 현재까지도 해당 취약점에 대한 꾸준한 모니터링을 수행하고 있다. 그러나, 무엇보다도 사용자들의 빠른 업데이트 적용이 가장 안전한 방법이 될 것이다.



[그림 3-10] 최근 1년간 공격 대상 기준별 MS 보안 패치 현황

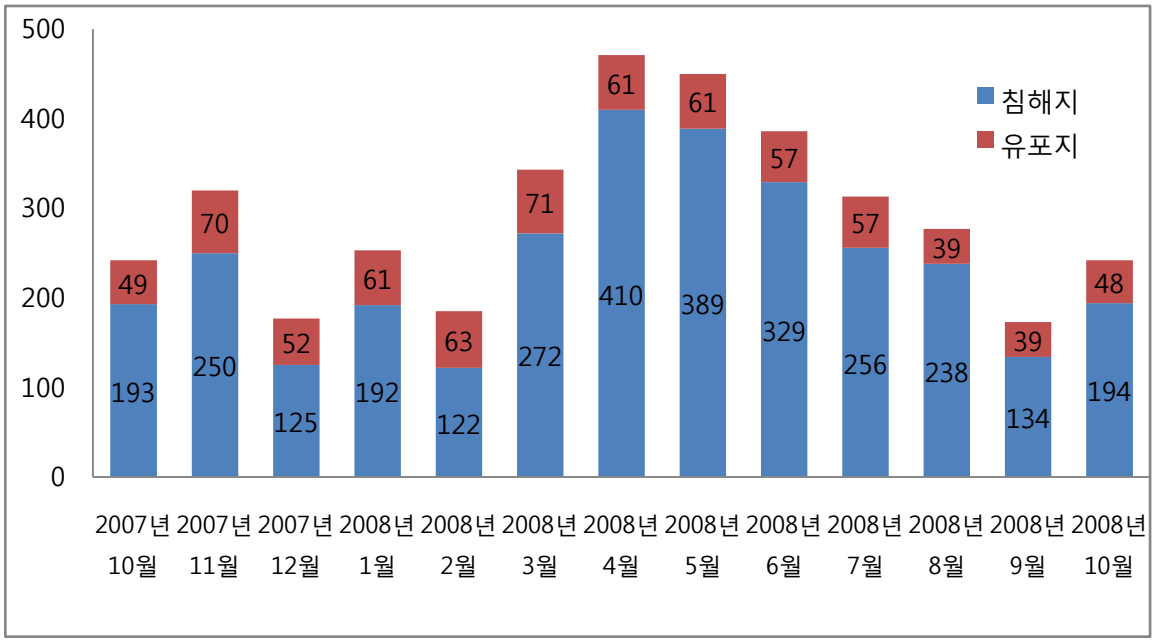
[1] http://www.microsoft.com/korea/technet/security/bulletin/MS08-067.mspx

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

위험도	취약점	PoC
긴급	(MS08-067) **서버 서비스의 취약점으로 인한 원격 코드 실행 문제점**	유
긴급	(MS08-057) **Microsoft Excel 의 취약점으로 인한 원격 코드 실행 문제**	무
중요	(MS08-061) **Windows 커널의 취약점으로 인한 권한 상승 문제점**	유
중요	(MS08-066) **Microsoft Ancillary Function Driver 의 취약점으로 인한 권한 상승 문제점**	유

[표 3-8] 2008년 10월 발표된 주요 MS 보안 패치

2008년 10월 웹 침해사고 현황



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

2008년 10월의 웹 사이트 경유지/유포지 수는 194/48로 지난 달의 134/39으로 침해된 사이트의 수와 유포사이트의 수 모두 증가하였다. 이번 10월의 동향은 지난 달과 큰 차이없이 MS07-017 취약점을 이용한 배포가 현저하게 줄었으며, MS08-041 Microsoft Access Snapshot Viewer 취약점을 이용해 악성코드 배포를 시도한 사례가 종종 발견되고 있다. 하지만 2008년 10월에 많은 제품의 취약점이 배포되었기 때문에 앞으로의 동향을 면밀히 관찰할 필요가 있다. 특히, 갈수록 특정한 공격자에 의해 다수의 침해사고가 발생하고 있다. 따라서 이러한 공격동향을 분석하고 대책을 강구해야 한다. 일반 사용자 역시 AV 제품을 설치하고, 제품의 상태를 항상 최신으로 유지하도록 해야 한다.

Copyright © AhnLab Inc,. 1988-2008. All Rights Reserved.
Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.