ASEC REPORT

안철수연구소에서 발행하는 월간 보안 보고서

2009. Volume.11

안철수연구소

Table Of Contents

이달의 보안 동향

이달의 컬럼 : 새로운 악성코드 명명법

Ⅰ. 이달의 보안 동향

1. 악성코드 동향

악성코드 통계

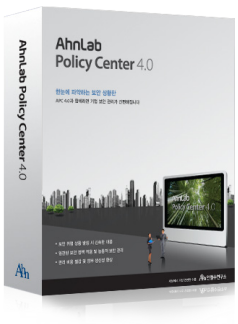
2009년 11월 악성코드 통계현황은 다음과 같다.

순위	등락	악성코드명	건수	비율
1	–	Win32/Induc	732,444	27.8 %
2	–	TextImage/Autorun	417,933	15.9 %
3	–	Win32/Virut.B	146,919	5.6 %
4	–	JS/Shellcode	130,558	5 %
5	–	Win32/Virut	114,499	4.3 %
6	↑ 2	Win32/Conficker.worm.Gen	107,772	4.1 %
7	–	Win32/Parite	101,680	3.9 %
8	↑ 1	TextImage/Sasan	96,372	3.7 %
9	New	TextImage/Viking	92,541	3.5 %
10	–	Win32/Olala.worm.57344	87,185	3.3 %
11	New	ALS/Bursted	83,082	3.2 %
12	New	Win-Adware/Rogue.DDOSClean.182752	78,567	3 %
13	New	VBS/Agent	73,949	2.8 %
14	New	Win32/Traxg.worm.61440	58,583	2.2 %
15	New	VBS/Autorun	57,787	2.2 %
16	New	Win-Trojan/Sadenav.491008	53,545	2 %
17	New	Win-Trojan/Bho.229888	52,962	2 %
18	New	Dropper/MulDrop.64512	52,828	2 %
19	New	Win32/IRCBot.worm.variant	52,468	2 %
20	New	Win-AppCare/HideWin.31232	43,708	1.7 %
합계			2,635,382	100%

[표 1-1] 악성코드 감염보고 Top 20

2009년 11월의 악성코드 감염 보고는 Win32/Induc이 1위를 차지하고 있으며, TextImage/Autorun과 Win32/Virut.B 가 각각 2위와 3위를 차지하였다. 신규로 Top 20에 진입한 악성코드는 총 11건이다.

아래 표는 악성코드의 주요 동향을 파악하기 위하여, 악성코드별 변종을 종합한, 악성코드 대표 진단명별 감염보고 Top 20이다.



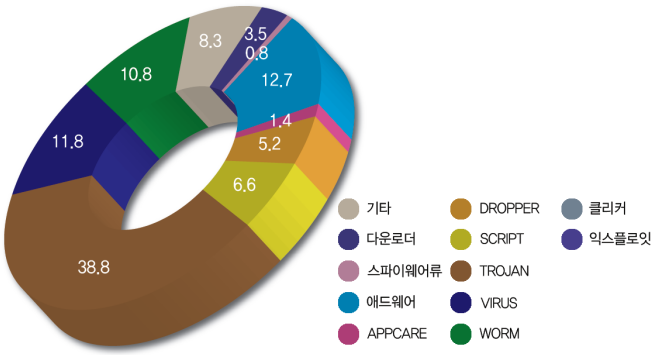
AhnLab Policy Center 4.0

순위	등락	악성코드명	건수	비율
1	–	Win32/Induc	732,511	13.2 %
2	–	Win-Trojan/Agent	648,048	11.7 %
3	–	Win-Trojan/OnlineGameHack	603,441	10.9 %
4	–	TextImage/Autorun	418,444	7.5 %
5	↑ 2	Win-Trojan/Downloader	343,562	6.2 %
6	↓ 1	Win32/Virut	306,339	5.5 %
7	↓ 1	Win32/Conficker	298,290	5.4 %
8	↑ 4	Win-Trojan/Bho	295,336	5.3 %
9	–	Win32/Autorun.worm	276,132	5 %
10	↑ 5	Win-Adware/KorAdware	211,060	3.8 %
11	↓ 3	Dropper/OnlineGameHack	162,899	2.9 %
12	New	Win-Adware/Rogue	160,837	2.9 %
13	↓ 3	Win32/Kido	160,725	2.9 %
14	New	Win-Trojan/Malware	160,009	2.9 %
15	↑ 3	Win-Adware/BHO	155,418	2.8 %
16	↑ 3	Dropper/Malware	131,824	2.4 %
17	↓ 3	JS/Shellcode	130,558	2.4 %
18	New	Win-Adware/Unovt	125,659	2.3 %
19	New	Win-Trojan/Genome	124,844	2.2 %
20	↓ 9	Win-Trojan/Magania	106,489	1.9 %
합계			5,552,425	100 %

[표 1-2] 악성코드 대표진단명 감염보고 Top 20

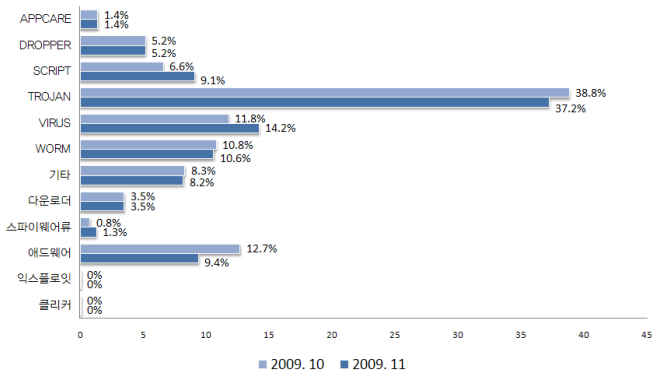
2009년 11월의 악성코드 감염보고 건수는 Win32/Induc이 총 732,551건으로 Top 20 중 13.2%의 비율로 1위를 차지하고 있으며, Win-Trojan/Agent가 648,048건으로 2위, Win-Trojan/OnlineGameHack이 603,441건으로 3위를 차지 하였다.

아래 차트는 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.



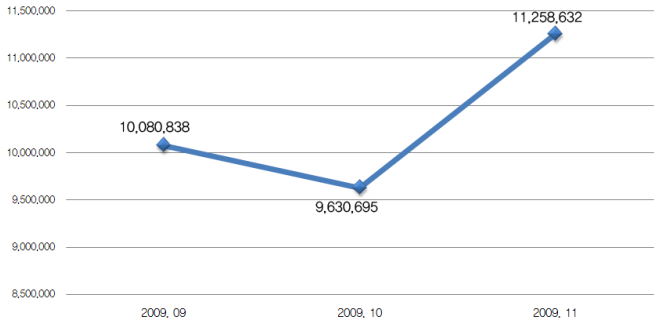
[그림 1-1] 악성코드 유형별 감염보고 비율

악성코드 유형별로 감염보고건수 비율은 Trojan류가 38.8%로 가장 많은 비율을 차지하고, 애드웨어가 12.7%, Virus가 11.8%의 비율을 각각 차지하고 있다.



[그림 1-2] 악성코드 유형별 감염보고 전월 비교

악성코드 유형별 감염보고 비율을 전월과 비교하면, Trojan과 애드웨어가 전월에 비해 증가세를 보이고 있는 반면, Virus와 Script는 전월에 비해 감소한 것을 볼 수 있다. Dropper, Worm, 다운로더 계열들은 전월 수준을 유지하였다.



[그림 1-3] 악성코드 월별 감염보고 건수

11월의 악성코드 월별 감염보고 건 수는 11,258,632건으로 10월의 악성코드 월별 감염 보고건수 9,630,695건에 비해 1,627,937건이 증가하였다.

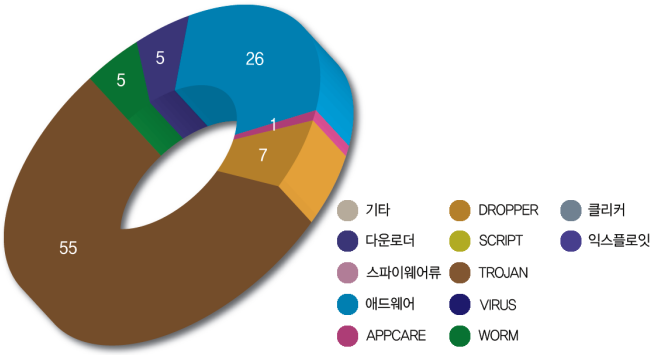
AhnLab V3 MSS

아래 표는 11월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top 200이다.

순위	악성코드명	건수	비율
1	Win-Adware/Rogue.DDOSClean.182752	78,567	11.1 %
2	Win-Trojan/Sadenav.491008	53,545	7.6 %
3	Win-Trojan/Bho.229888	52,962	7.5 %
4	Dropper/MulDrop.64512	52,828	7.5 %
5	Win-Trojan/Genome.97280.D	42,490	6 %
6	Win-Trojan/Bho.223232.C	39,320	5.6 %
7	Win-Trojan/Bho.239616.B	38,135	5.4 %
8	Win-Trojan/Banker.743936.J	35,765	5.1 %
9	Win-Trojan/Genome.211456	33,265	4.7 %
10	Win-Downloader/GomWorld.90112	32,563	4.6 %
11	Win-Trojan/Bho.312320.B	31,636	4.5 %
12	Win-Trojan/Bho.724992	31,495	4.5 %
13	Win-Trojan/Bho.603136	29,185	4.1 %
14	Win-Trojan/Agent.14848.PB	28,140	4 %
15	Win-Trojan/Agent.28672.AHC	21,808	3.1 %
16	Win-Downloader/LastLog.591360	21,722	3.1 %
17	Win-Adware/BHO.Unovt.617472	21,490	3 %
18	Win-Adware/LastLog.618496	21,031	3 %
19	Win-Trojan/Agent.717824.G	21,007	3 %
20	Win-Trojan/Agent.294912.BH	20,631	2.9 %
합계		707,585	100 %

[표 1-3] 신종 악성코드 감염보고 Top 20

11월의 신종 악성코드 감염보고의 Top 20은 Win-Adware/Rogue.DDOSClean.182752가 78,567건으로 전체 11.1%를 차지하여 1위를 차지하였으며, Win-Trojan/Sadenav.491008이 53,545건으로 2위를 차지하였다.



[그림 1-4] 신종 악성코드 유형별 분포

11월의 신종 악성코드 유형별 분포는 Trojan이 55%로 1위를 차지하였다. 그 뒤를 애드웨어가 26%, Dropper가 7%를 각각 차지하였다.

악성코드 이슈

지난 달 '검은 화면에 마우스포인트'만 나타나는 부팅장애로 잘 알려진 Win-Trojan/Daonol의 변형이 11월 한달 내내 지속적으로 발견되었다. 그리고 MBR Rootkit처럼 물리적 디스크에 자신을 쓰고 실행하는 악성코드가 발견 되기도 하였다. 해당 악성코드는 일반적인 방법으로는 진단 할 수 없기 때문에 안티 바이러스 연구가들에게 큰 화제거리가 되었다. 그리고 중국산 백도어인 Win-Trojan/Hupigon의 변형이 치료에 어려

움을 주어 일부 고객들이 진단과 치료에 있어서 큰 어려움을 겪었다. 그리고 국외에서는 iPhone에서 동작하는 악성코드가 최초로 발견, 보고되었다. 해당 악성코드는 iPhone를 해킹하여 사용하는 기기에만 감염되는 특정을 가지고 있으며, 국내에는 아직 발견, 보고 되지 않았다. 끝으로 P2P 웜으로 잘 알려진 Win32/Waledac.worm이 다시 발견 되었는데 해당 악성코드가 다시 활동할 것으로 보여 사용자들로 하여금 주의가 요구된다.

Win-Trojan/Daonol 의 지속적인 변형 등장

지난 달 국내에도 다수의 피해를 입혔던 Win-Trojan/Daonol 변형이 11월 한달 지속적으로 발견, 보고 되었다. 이렇게 지속적으로 발견 되는 것은 지난 달에도 언급했듯이 PDF와 SWF 파일의 취약점으로 Daonol 트로이목마에 감염 되기 때문이다. 자세한 취약점 항목은 다음과 같다.

1. APSB09-15 Adobe Acrobat and Acrobat Reader Remote Code Execution
2. APSB08-11 Adobe Flash Player Invalid Pointer Vulnerability

[그림 1-5] Daonol 트로이목마 감염과 연관이 있는 취약점 정보

지난 달 국내에도 다수의 피해를 입혔던 Win-Trojan/Daonol 변형이 11월 한달 지속적으로 발견, 보고 되었다. 이렇게 지속적으로 발견 되는 것은 지난 달에도 언급했듯이 PDF와 SWF 파일의 취약점으로 Daonol 트로이목마에 감염 되기 때문이다. 자세한 취약점 항목은 다음과 같다.

NTDLL.DLL : ZwOpenKey
KERNEL32.DLL : CreateProcessW, ExitProcess
WS2_32.DLL : WSASEnd, WSARecv, connect, send, recv

[그림1-6] 후킹 되는 윈도우 함수

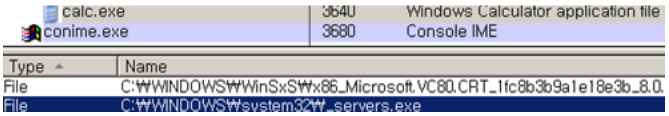
이번 달에 발견된 변형들 역시 같은 문제점을 가지고 있었다. 안철수연구소는 이러한 다수의 피해문의를 접수 받았지만, 악성코드에 의해서 발생한 예기치 못한 문제점은 안티 바이러스 프로그램으로 해결 할 수 없는 것이 존재한다. 이러한 경우 지난 호에 언급했듯이 Daonol 전용백신을 이용하면 악성코드 제거는 물론 이러한 문제점을 메모리 패치를 통하여 실행되지 못했던 응용 프로그램들을 실행시킬 수 있다.

국내 무료백신을 삭제할 목적으로 제작된 악성코드

스팸 메일에 파일 다운로드용 링크를 첨부한 형태로 전파되는 Win-Trojan/Download에 의해 국내 대표 무료백신이 강제로 삭제되는 증상이 발견되었다. 백신관련 프로세스를 강제종료하고 프로그램이 존재하는 폴더를 삭제하도록 제작된 이 악성코드는 한글로 된 메일제목과 파일 다운로드를 위한 링크 형태로 전파되어 해당 메일 수신자들로부터 감염이 다수 신고되었다. 이 악성코드의 다운로드 기능을 수행하는 파일은 백신의 실시간 감시에서 진단/치료가 가능 하지만 백신의 실시간 감시를 끈 상태로 PC를 이용하는 경우에는 백신제품을 다시 설치해야 하는 문제가 있다.

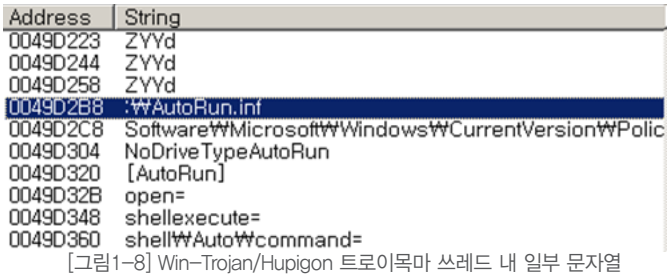
치료방법이 까다로운 Win-Trojan/Hupigon

Win-Trojan/Hupigon은 잘 알려진 중국산 백도어 프로그램이다. 해당 트로이목마는 자신의 진단을 회피하기 위하여 정상 프로그램을 실행 한 후 자신을 실행 프로세스의 원격 파일 핸들로 오픈하는 것으로 유명하다. 이런 경우 일부 안티 바이러스는 이미 다른 프로세스가 오픈 한 경우로 진단을 못하는 경우가 있을 수 있다.



[그림1-7] Win-Trojan/Hupigon 트로이목마가 실행 된 모습

근래에 발견, 보고된 Hupigon 트로이목마는 위 그림처럼 Calc.exe (윈도우 기본 계산기 프로그램)에 원격 파일 핸들을 오픈 해둔다. 변형에 따라서 Share flag값이 Read, Write가 없는 경우도 있다. 1차적으로 이렇게 하여 일부 안티 바이러스 진단과 사용자가 수동으로 자신을 삭제하도록 막고 있다. 대부분 이런 경우 해당 파일 핸들을 찾아 직접 닫거나 하여 제거 할 수가 있다. 그러나 이번에 발견된 변형은 계산기 프로세스에 시작 주소가 불분명한 쓰레드를 생성하고 있다.



[그림1-8] Win-Trojan/Hupigon 트로이목마 쓰레드 내 일부 문자열

이렇듯 정상 프로세스를 실행 한 후 이곳에 악의적인 쓰레드를 생성하여 사용자나 안티 바이러스가 파일을 삭제하여도 다시 파일이 생성 되는 것이다. 따라서 사용자가 정상 프로세스로 간과하여 그냥 두었다면 이후 Hupigon에 재감염되는 현상이 발생하게 된다.

안티 바이러스 프로그램도 이러한 악성코드를 치료 할 수 있도록 되어 있지 못하면 당연히 치료를 할 수 없게 된다. 그 이유는 정상 프로세스에 악의적인 쓰레드가 존재하는 경우에 진단하고 치료 할 수 있도록 되어 있지 않기 때문이다. 이런 경우 일부 안티 바이러스 업체들은 전용백신을 이용하여 치료하도록 유도하고 있는 실정이다. 일부 악성코드들은 안티 바이러스의 취약한 부분을 이용하여 컴퓨터 내부 깊숙이 숨어든다. 안티 바이러스 제품이 출시 될 때는 존재하지 않았던 유형의 악성코드가 등장하여 진단/치료에 어려움을 겪는 경우가 많다. 이러한 경우에는 안티 바이러스 업체들도 전용백신이나 제품의 기능 업데이트와 같은 발 빠른 행보를 하고 있다.

물리적 디스크에 존재하는 악성코드

2008년 1월 MBR Rootkit이 알려졌을 때 많은 안티 바이러스 연구원들은

과거의 부트 바이러스를 떠올렸다. 또한 일부 매스컴에서는 파일로 존재하는 형태가 아니며 그 어디에도 파일의 시작점을 알 수가 없기 때문에 레지스트리에서도 악성코드의 시작점을 찾을 수가 없었다.

이러한 악성코드가 또 다시 등장하였다. 해당 악성코드는 물리적 디스크의 unpartitioned 영역에 자신의 코드를 기록해둔다. 이곳에는 드라이버, DLL 등의 실행 파일 이미지이다. 파일로는 존재하지 않고 물리적 디스크 상에 위치함으로 일반적인 방법으로는 검색되지 않는다. 해당 영역의 코드를 실행하기 위해서 윈도우의 특정 시스템 파일을 패치하여 해당코드를 로드 하도록 해둔다. 정상파일을 패치 한 형태이므로 역시 일반적인 방법으로는 패치된 유무를 확인 하기 매우 어렵다.

또한 안티 바이러스 제품들 역시 unpartitioned 영역을 검사 할 수 있도록 되어 있지 않다. 은폐기능도 있기 때문에 이를 무력화하고 치료를 시도해야 한다. 안철수연구소에는 전용백신(Win-Trojan/Patched.X)을 통해서 해당 악성코드를 대응하고 있다.

사회적 이슈를 악용한 가짜 백신

2009년 7월 7일을 시작으로 며칠간 국내 주요 사이트들이 PC에 감염된 악성코드에 의해 DDOS(Distributed Denial Of Service) 공격을 받아 정상적인 인터넷 서비스를 제공하지 못했었다. 이로 인해 많은 사용자들이 보안 사고의 위험성과 보안의 중요성을 느낄 수 있는 계기가 되었다. 하지만 최근 이런 이슈를 악용한 가짜 백신이 등장했다. 로그 디도스클린(Win-Adware/Rogue.DDOSClean)이 그 대표적 예인데 이 제품의 경우 2009년 7월 7일 발생했던 DDOS공격에 사용된 악성코드를 진단하지 못했으며, 또한 DDOS공격을 예방하거나 치료하는 기술 또한 없다. 더군다나 해당 제작사 홈페이지에서 제공하는 "신종 바이러스 정보" 목록에 등록된 항목 조차 진단하지 못하고 있었다. 즉, 제품의 이름을 사회적 이슈와 연관 지어 상업적인 목적을 극대화 시키는 목적이 다분하다.

[그림 1-9] DDOS 이슈를 이용학 가짜 백신

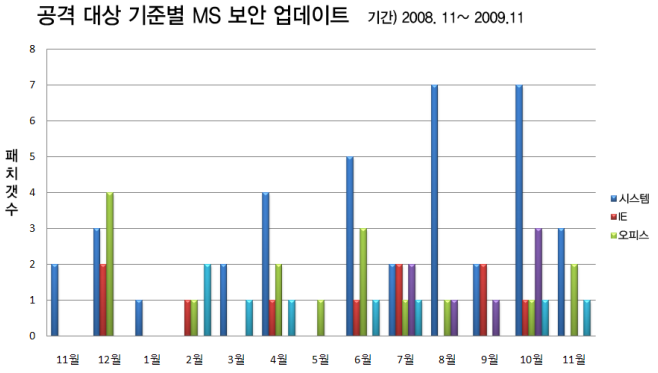
더군다나 해당 가짜 백신은 다운로더 코애드웨어(Win-Downloader/Ko-rAdware.246784)에 의해 사용자 동의 없이 설치되고 동작해 그 피해가 더욱더 컸다. 이러한 가짜 백신은 대부분 다른 서비스 또는 프로그램의 번들로 설치되고 허위 진단 또는 임시파일, 쿠키파일(cookie)등이 위험한 요소라고 진단하고 사용자에게 빨리 치료할 것을 팝업 윈도우를 사용하여 지속적으로 알린다. 실제 치료를 하려고 하면 유료 결제를 요구한다. 따라서 본인이 직접 설치하지 않은 보안 제품이 유료 결제를 통한 치료를 요구하면 가짜 백신을 의심해 보아야 한다. 또한 이러한 가짜 백신은 진단 및 치료 능력이 현저하게 떨어져 구매해도 컴퓨터 보안에는 거의 효과가 없으므로 사용자의 각별한 주의가 필요하다.

2. 시큐리티 동향

시큐리티 통계

11월 마이크로소프트 보안 업데이트 현황

마이크로소프트사로부터 발표된 이달 보안 업데이트는 총 8건으로 긴급(Critical) 3건, 중요(Important) 5건이다.



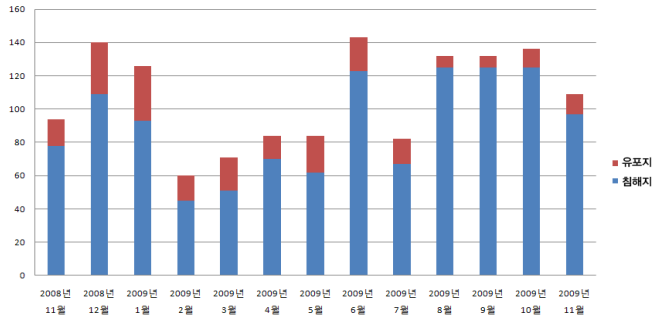
[그림 2-1] 2009년 11월 주요 MS 보안 업데이트 건수

위험도	취약점	PoC
긴급	Web Services on Devices API의 취약점으로 인한 원격 코드 실행 문제점	무
긴급	라이센스 로깅 서버의 취약점으로 인한 원격 코드 실행 문제점	무
긴급	Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드 실행 문제점	무
중요	Active Directory의 취약점으로 인한 서비스 거부 문제점	무
중요	Microsoft Office Excel의 취약점으로 인한 원격 코드 실행 문제점	무
중요	Microsoft Office Word의 취약점으로 인한 원격 코드 실행 문제점	무
중요	윈도우 7 ,윈도우 서버 2008 R2 SMB 원격 공격 취약점 (제로데이)	유
중요	인터넷 익스플로러 6/7 CSS Handling 서비스거부 공격 취약점 (제로데이)	유

[표 2-1] 2009년 11월 주요 MS 보안 업데이트 목록

이번 달은 8건의 보안패치가 발표되었으나, 이 문서를 작성하는 시점까지 알려진 공격코드는 없다. 다만, 인터넷 익스플로러 6과 7버전에 CSS를 처리하는 과정에서 브라우저가 크래쉬 되는 공격코드가 공개되었고, 출시가 얼마 되지 않은 윈도우 7에서 제로데이 취약점이 보고되었다. 이번에 공개된 취약점의 자세한 내용은 시큐리티 이슈에서 언급하기로 하겠다.

악성코드 침해 웹사이트 현황



[그림 2-2] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

2009년 11월 악성 코드를 위해 침해된 웹사이트의 수와 악성 코드 유포지의 수는 96/11로 2009년 10월의 127/9와 비교하여 침해지는 31건 줄었으며, 유포지는 2건 더 늘어났다. 악성코드를 배포하기 위해 사용되는 취약점은 새로운 공격 기법 보다, 기존 오래된 취약점이 현재도 꾸준하게 증가하고 있다. MDAC(Microsoft Data Access Components) 기능의 취약점으로 인한 원격 코드 실행 문제점인 MS06-014가 아직도 꾸준하게 사용되고 있다.

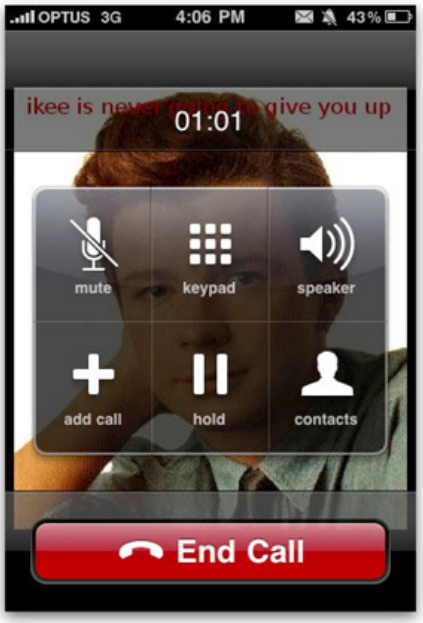
위 취약점의 경우, 윈도우 업데이트를 주기적으로 하는 사용자의 경우 사이트에 접속하여도 취약점에 의해 감염되지는 않다. 하지만 윈도우 업데이트를 하지 않은 사용자의 경우, 악성코드에 감염되며, 이로 인해 시스템 전체 권한을 빼앗길 수 있다. 또한 백신 설치를 통해 악성 프로그램이 다운로드 되는걸 차단하길 권장한다.

시큐리티 이슈

모바일 보안에 대한 위협 증가 – 아이폰(iPhone) 웜 첫 등장

전 세계적으로 스마트폰의 바람이 몰아치고 있다. 그 대표적인 제품이 애플사의 아이폰(iPhone)이다. 국내에도 최근 출시되어 마니아들의 기대가 높아지고 있다. 그런데, 최근 아이폰(iPhone)에서 첫 웜(Worm)이 발견되었다. 호주에서 발견된 이 웜은 이키(Ikee)라고 불리고, 바탕화면을 80년대 가수 릭 애슬리의 사진으로 바꾸고 다른 아이폰(iPhone)에 전파되기 위한 시도를 한다.

이번 웜은 모든 아이폰(iPhone)에 영향을 미치는 것이 아니라 Jailbroken이 설치된 아이폰(iPhone)에 한정된다. 이것은 해킹된 버전의 아이폰(iPhone) OS로 사용자가 임의의 프로그램을 설치할 수 있도록 해준다. 이 Jailbroken이 설치되면서 다양한 서비스가 동작되는데, 그 중에 하나인 SSH 서비스가 원격에서 루트 권한으로 접속될 수 있도록 허용되어 있었다. 기본 패스워드가 설정되어 있어 웜은 이 취약점을 이용하여 전파를 시도하였다. SSH 서비스는 원격터미널 접속 프로그램으로 telnet과 달리 안전한 통신을 보장한다. 그러나, 기본 패스워드가 이번 문제를 야기하게 되었다.



[그림 2-3] Ikee 웜에 감염된 아이폰(iPhone)의 배경화면

이번 웜의 동작은 간단한 형태여서, 초기 컴퓨터에서 발생된 웜과 같은 수준이다. 코드에 등록된 특정 IP주소를 대상으로 스캐닝을 시도하는데, 해당 IP는 오스트리아에 있는 호주의 3G 사용고객이다. SSH 서비스를 통해, 로그인을 성공적으로 하게 되면 이 웜은 파일을 복사하고, 다른 공격자에 의한 접속을 막기 위해 SSH 서비스를 중지하게 된다. 다음 그림은 웜의 소스코드에 하드코딩 된 IP 주소 대역의 일부이다.

```
    // and output them like this
    // THATS WHY.
    char *lanRanges = "192.168.0.0-192.168.255.255"; //
#172.16.0.0-172.31.255.255 Ehh who uses it
    char *vodRanges1 = "202.81.64.0-202.81.79.255";
    char *vodRanges2 = "23.98.128.0-123.98.143.255";
    char *vodRanges3 = "120.16.0.0-120.23.255.255";
    char *optRanges1 = "114.72.0.0-114.75.255.255";
    char *optRanges2 = "203.2.75.0-203.2.75.255";
    char *optRanges3 = "210.49.0.0-210.49.255.255";
    char *optRanges4 = "203.17.140.0-203.17.140.255";
    char *optRanges5 = "203.17.138.0-203.17.138.255";
    char *optRanges6 = "211.28.0.0-211.31.255.255";
    char *telRanges = "58.160.0.0-58.175.255.25";
    //char *attRanges = "32.0.0.0-32.255.255.255"; // TOO BIG

    syslog(LOG_DEBUG, "awoadqdoqjdqjwiodjqoi aaah!");
```

[그림 2-4] 아이폰(iPhone) 웜 코드의 일부

다행히 이번 웜은 파일삭제 등과 같은 큰 피해를 주는 기능은 포함하고 있지 않았다. 하지만, 이번 첫 웜이 발표된 후 같은 취약점을 이용한 두 번째 웜이 또 등장하였다. 이로써 모바일 보안에 대한 우려가 현실화되고 있다. 국내도 이제 아이폰(iPhone)을 출시로, 스마트폰의 비중이 점차 늘어날 것으로 예상되는 만큼 스마트폰에 발생할 수 있는 보안 위협에 대한 준비도 차차 마련해 나가야 할 것이다.

윈도우 7과 윈도우 2008의 원격 SMB 공격 취약점

한 블로그를 통해 윈도우7과 2008서버에 영향을 주는 공격코드가 공개되었다. 이번 공격코드는 원격에서 시스템을 크래쉬 할 수 있는 형태로 서비스 거부공격에 해당한다. 크래쉬 되는 형태는 마우스, 키보드, 네트워크 등이 모두 멈춰버리는 형태이다. 취약점은 Netbios 의 헤더 중 SMB 패킷이 4바이트 적거나 큰 경우에 발생할 수 있다. 공격코드 이외도, 간단한 명령어를 통해서도 발생될 수 있는 것으로 알려지고 있으므로 영향을 받는 시스템은 주의가 필요하다.

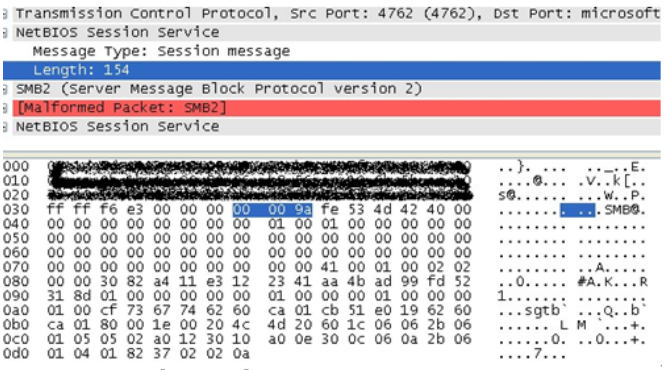
영향을 받는 시스템은 아래와 같다.

– Windows 7 32비트 버전

– Windows 7 64비트 버전

– Windows 서버 2008 R2 64 비트 버전

다음은 공격 패킷의 일부로, 패킷 길이의 헤더를 9e로 셋팅 된 값 보다 4 바이트 작게 설정하여 전달한 패킷의 형태이다.



[그림 2-5] SMB 헤더를 조작한 패킷 형태

이번 취약점을 해결하기 위한 보안패치는 아직 발표되지 않은 상태이다. 임시적으로 방화벽에서 TCP 포트 139번과 445의 접속을 차단할 수 있다. 그러나 해당 포트는 윈도우 환경에서 일반적으로 사용되는 포트이므로, 외부에서의 접근 차단 시 문제는 없는지 검토 후 차단할 것을 권고한다. 이 취약점과 관련한 지속적 정보는 다음 경로에서 확인할 수 있다. 참고로 이 취약점은 10월 달에 발표된 MS09-050의 "SMBv2 원격 코드 실행 취약점" 과는 관련이 없다.

– 제로데이 공격취약점 정보

http://www.microsoft.com/technet/security/advisory/977544.mspx

AhnLab Trusguard

3. 웹 보안 동향

웹 보안 통계

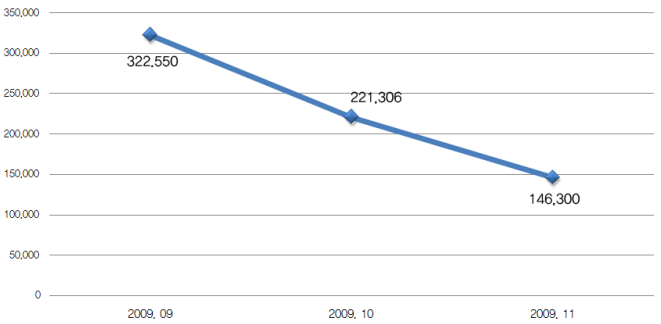
웹 사이트 보안 요약

구분	건수
악성코드 발견 건수	146,300
악성코드 유형	944
악성코드가 발견된 도메인	676
악성코드 발견된 URL	4,341

[표 3-1] 웹 사이트 보안 요약

악성코드 발견 건수는 146,300건, 악성코드 유형은 944건, 악성코드가 발견된 도메인은 676건, 악성코드 발견된 URL은 4,341건이다. 11월에는 웹 보안 통계치의 기반이되는 사이트가드(SiteGuard)의 시스템 증설로 인해 통계 수집기간이 4주에서 3주로 줄어들었다. 이 일로 인해 악성코드 발견건수와 도메인, URL 통계치가 지난달에 비해 감소한 수치를 보였다.

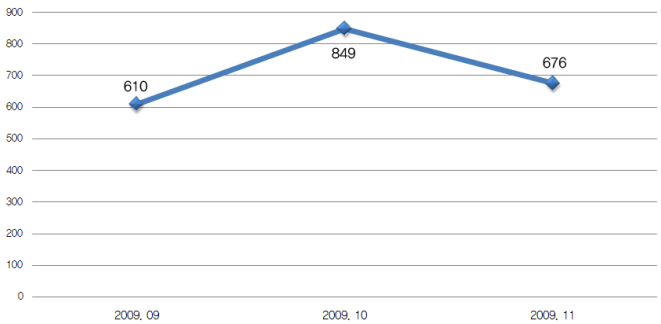
월별 악성코드 발견 건수



[그림 3-1] 월별 악성코드 발견 건수

2009년 11월 악성코드 발견 건수는 전달의 221,306건에 비해 66% 수준인 146,300건이다.

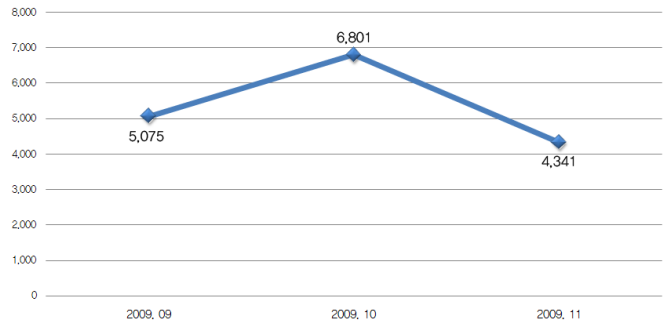
월별 악성코드가 발견된 도메인



[그림 3-3] 월별 악성코드가 발견된 도메인

2009년 11월 악성코드가 발견된 도메인은 전달의 849건에 비해 80% 수준인 676건이다.

월별 악성코드가 발견된 URL



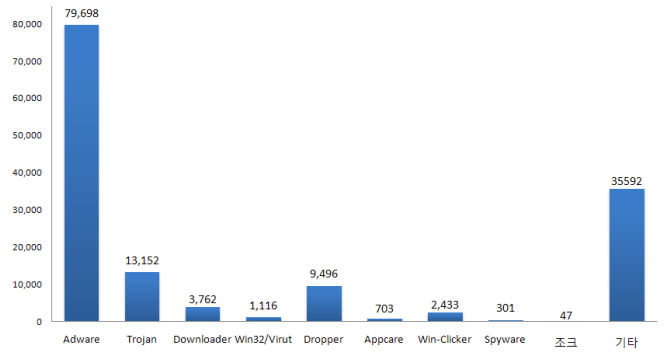
[그림 3-4] 월별 악성코드가 발견된 URL

2009년 11월 악성코드가 발견된 URL은 전달의 6,801건에 비해 64% 수준인 4,341건이다.

악성코드 유형별 배포 수

유형	건수	비율
Adware	79,698	54.5 %
Trojan	13,152	9 %
Downloader	3,762	2.6 %
Win32/Virut	1,116	0.8 %
Dropper	9,496	6.5 %
AppCare	703	0.5 %
Win-Clicker	2,433	1.7 %
Spyware	301	0.2 %
조크	47	0 %
기타	35,592	24.3 %
합계	146,300	100 %

[표 3-2] 월별 유형별 배포 수



[그림 3-5] 월별 유형별 배포 수

악성코드 유형별 배포 수에서 Trojan류가 79,698건 전체의 54.5%로 1위를 차지하였으며, Trojan류가 13,152건 전체의 9%로 2위를 차지하였다.

악성코드 배포 Top 10

순위	등락	악성코드명	건수	비율
1	–	Win-Adware/Shortcut.InlivePlayerActiveX.234	46,442	45.2 %
2	–	Win32/Induc	26,979	26.2 %
3	↑ 4	Win-Dropper/KorZlob.5132206	5,949	5.8 %
4	↑ 1	Win-Adware/BHO.HiMyCar.237568	5,938	5.8 %
5	↓ 2	Win-Adware/Shortcut.IconJoy.642048	4,732	4.6 %
6	↑ 2	Win-Adware/Shortcut.K2Com.Sobang.266240	3,334	3.2 %
7	New	Win-Adware/BHO.HiMyCar.49152	3,058	3 %
8	↑ 2	Win-Adware/Shortcut.INBEE.iomeet.267270	2,542	2.5 %
9	New	Win-Adware/Shortcut.Bestcode.0002	1,976	1.9 %
10	New	TextImage/Viking	1,857	1.8 %
합계			102,807	100 %

[표 3-3] 악성코드 배포 Top 10

악성코드 배포 Top 10에서 Win-Adware/Shortcut.InlivePlayerActiveX.234가 지난달과 같이 46,442건으로 1위를 차지하였으며, Top 10에 Win-Adware/BHO.HiMyCar.49152 등 3건이 새로 등장하였다.

웹 보안 이슈

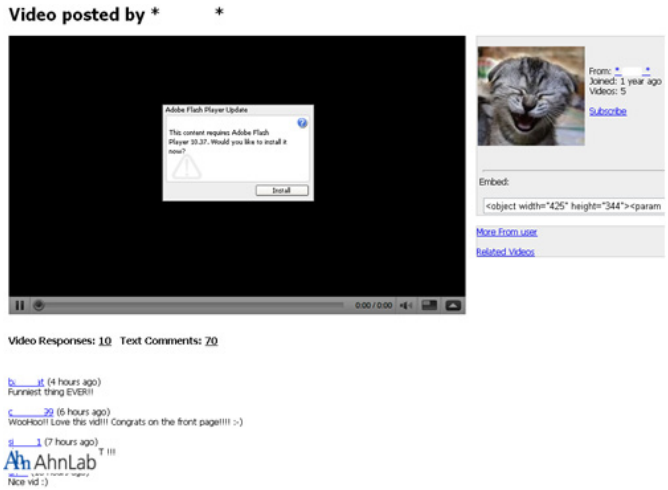
유튜브(YouTube) 동영상 관련 코덱으로 위장한 Koobface 웜 유포

2009년 11월 9일 오후, 해외에서 유튜브(YouTube) 동영상 관련 코덱으로 위장한 Koobface 웜이 유포되고 있는 것이 보고 되었다. 이번에 유포된 Koobface 웜은 기존의 다른 웜들이 페이스북(Facebook)의 댓글이나 게시물들을 자동으로 생성하여 다른 페이스북 사용자들의 시스템에 감염을 시도하는 일반적인 형태가 아니였다. 해당 Koobface 웜은 아래 [그림 3-6]과 같이 구글(Google) 리더에 유튜브 동영상으로 위장하여 컴퓨터 사용자에게 해당 동영상이 정상적으로 플레이가 되지 않는 것처럼 보여준다. 해당 유튜브 동영상을 정상적으로 보기 위해 가운데 플레이 버튼을 클릭하게 되면 다시 아래 [그림 3-6]의 이미지와 같은 웹 사이트로 연결이 되며 정상적인 시청을 위해서는 Adobe Flash Player 10.37을 설치해야 된다는 안내 문구를 보여주게 된다. 안내 문구에 존재하는 설치를 클릭하게 되면 38,912바이트의 Setup.exe파일이 다운로드되며 실행되는데 해당 파일은 Koobface 웜의 변형이다. 해당 Koobface 웜에 감염이 되면 윈도우 시스템 폴더(C:₩Windows₩System32)에 자신의 복제본을 ld15.exe 라는 피일명으로 생성하고 인터넷에 존재하는 다른 시스템에서 개인 정보 유출을 목적으로 제작된 다른 악성코드 변형들을 다운로드 하게 된다. 해당 Koobface 웜과 다운로드 되는 악성코드들은 V3 제품군에서 다음과 같이 진단한다.

- Win32/Koobface.worm.38912.E
- Win32/Koobface.worm.131584
- Win-Trojan/Agent.56064
- Win32/Koobface.worm.51200.B

이러한 사회공학적인 기법을 이용하는 악성코드들로부터 시스템을 보호

하기 위해서는 취약점에 대한 패치와 V3 365클리닉과 같은 방화벽과 백신을 함께 제공하는 통합 보안제품을 설치하고, 사이트로부터 악성코드 감염을 예방하는 사이트가드(Siteguard)와 같은 소프트웨어 설치가 중요하다. 하지만 무엇보다 중요한 것은 전자메일에 존재하는 의심스러운 웹 사이트 링크를 클릭하지 않는 사용자의 지혜이다.



[그림 3-6] 유튜브 동영상을 코덱으로 위장한 Koobface 웜 유포용 안내문구

Adware 설치와 찰떡궁합인 BHO에 대한 이해

이번 달에는 BHO를 이용한 Adware들이 Top 10에 2건이 올랐다. 4위를 차지한 Win-AdWare/BHO.HiMyCar.237568와 7위를 차지한 Win-Adware/BHO.HiMyCar.49152들은 모두 BHO를 이용하는 Adware들이다. 그럼, Adware나 Spyware와 함께 언급되는 BHO는 도대체 무엇인가? BHO는(Browser Helper Objet)는 브라우저 도우미 개체라고 불리며, 윈도우 탐색기와 IE기능을 확장할 때 사용하는 기능이다. BHO에 등록된 Adware나 Spyware들은 실행파일형태가 아니라, 확장자가 DLL형태로 윈도우 탐색기나 IE에 의하여 실행되기 때문에 윈도 작업관리자에서 확인이 불가능하게 되며, 윈도우 시작 시에 윈도우 탐색기에 의하여 자동 실행되는 특징을 가지고 있다. 이와 같이 Adware나 Spyware를 설치 및 실행할 수 있는 최적의 요건을 갖추었기 때문에, BHO를 많이 이용한다. 주로 BHO에 감염되면, 실행파일과 DLL파일을 Windows의 시스템 폴더 아래에 생성한다. 그와 함께 다수의 레지스트리를 생성하는 특징이 있다. 이를 통해 사용자가 사용하는 Internet Explorer에 입력되는 키워드를 감시하는 기능을 가지고 있으며, 시작페이지를 사용자가 원하지 않는 페이지로 변경하거나 광고 등을 띄우며 시스템 장애나 Internet Explorer 오류의 원인이 되기도 한다.

그럼 BHO는 어떻게 제거하면 될까? BHO를 수동으로 제거하는 방법은 다음과 같다.

1. 제어판 -> 인터넷 옵션 -> 고급 -> 타사 브라우저 확장명 사용 체크를 해제하고, IE(Internet Explorer)를 종료한 후에 해당 BHO의 DLL 파일을 찾아서 삭제한다.

2. 최근에는 툴바와 같은 불필요한 프로그램들이 BHO를 이용하므로, 불필요한 프로그램들은 [시작]-[제어판]-프로그램 추가/제거]에서 삭제를 한다.

지속적으로 BHO는 악성코드 유포에 사용되기 때문에, 사용자들의 주의가 필요하다. 무턱대고 출처가 분명하지 않은 프로그램을 설치하지 않도록 웹 서핑 시에 사용자들의 주의가 필요하다.

AhnLab SiteGuard Pro

II. 칼럼 : 새로운 악성코드 명명법

1. 악성코드 명명법

1980년대 중반 컴퓨터 바이러스가 등장하면서 세계 각지에서는 퇴치 프로그램을 제작하였다. 이때 각기 다른 방식으로 진단명을 부여하면서, 명명법에 일관성이 없고 혼란스러워지는 문제를 초래하였다.. 이러한 문제를 해결하기 위해 CARO(Computer Antivirus Researchers Organization) 멤버들이 1991년 모여 컴퓨터 바이러스 이름안(computer virus naming scheme)를 만들게 되었다. 여기서 변형은 '.'로 띄어쓰기는 '_' 등이 결정되었으며 안철수 박사의 V3도 이 명명법에 맞춰 진단명을 변경하였다. 하지만, 1990년대 중 후반 매크로 악성코드, 윈도우 악성코드, 스크립트 악성코드 등 새롭게 등장하는 유형의 악성코드를 표현할 수 없는 문제가 발생했다.

업체별로 각기 다른 진단명이 사용되다 닉 피츠제랄드(Nick FitzGerald)는 2002년 AVAR 컨퍼런스에서 새로운 진단명안을 제안하였다.

〈malware_type〉://〈platform〉/〈family_name〉.〈group_name〉.〈infective_length〉.〈variant〉〈devolution〈modifiers〉

현재 마이크로소프트, F-시큐어 등의 업체에서 이 안과 유사한 방식으로 진단명을 짓고 있다. 하지만, 다른 업체들은 이전에 사용되던 고유의 진단명을 수정하기 어렵고 폭발적으로 증가하는 이 명명법을 사용해도 악성코드 변형 구분이 힘들어지는 현실 속에 〈패밀리이름〉.〈그룹이름〉 대신 〈이름〉으로 간단히 쓰고 있다.

2. 기존 명명법의 문제점

안철수연구소는 현재 사용중인 악성코드 명명법이 약 10년 전쯤에 만들어져 스파이웨어 등의 새로운 유형 및 악성코드 길이가 증가하면서 악성코드 길이를 나타내는 숫자가 더 이상 불필요하다는 문제 인식이 대두되었다.

이에 기존 명명법을 보강하는 새로운 진단명 계획을 세웠으며 새로운 명명법의 목표는 다음과 같다.

1. 새로운 악성코드를 포함한 진단명 정립
2. 진단명을 통한 정보 극대화
3. 지나치게 길지 않은 진단명

3. 안랩의 새로운 명명법

안철수연구소는 내년 초를 목표로 기존 명명법을 보강한 새로운 명명법을 결정했다.

[플랫폼]-[종류]/[이름]{-[상세이름]}.[변형]

1. 진단명의 최대 길이는 크게 제한이 없지만 가급적 45자 이내로 한다.

2. 플랫폼은 악성코드의 제작 언어나 실행 환경 등을 표시한다.

3. 종류는 악성코드의 가장 큰 특징을 담고 있는 분류이다.

4. 이름은 특징적 구분에 따라 다른 이름을 사용한다. 이때 분석가의 필요에 따라 상세이름이 올 수 있다. 이름과 상세이름은 '-'로 구분한다. 이름은 첫 글자만 대문자이고 나머지는 소문자로 한다.

5. 변형은 알파벳 대문자로 표기한다. (A, B, C … AA, AB, AC … ZZ, AAB, AAC…ZZZ...) 이때 욕설, 비속어 등이 나올 수 있어 자동으로 변형이 부여될 때는 모음 (A, E, I, O, U)은 제외한다.

플랫폼은 이전과 동일하게 사용한다. 악성코드의 가장 큰 특징을 나타내는 종류는 Adware, AppCare, Packer, Spyware, Trojan, Virus, Worm을 사용하며 이는 윈도우 실행 파일(Win32, Win64)와 리눅스(Linux)에만 구분된다. 즉, 스크립트, 매크로 등 다른 플랫폼은 종류를 구분하지 않는다.

추천 이름은 유사 특징을 가진 유형을 정리한 것으로 분석가에 따라 다른 이름을 정할 수 있다.

추천 이름	설명
Agent	프로세스에 떠서 악의적 행동을 하는 프로그램
Autorun	Autorun.inf 를 생성하며 전파되는 웜
Backdoor	사용자 정보를 빼가기 위한 목적의 백도어
Constructor	악성코드나 기타 관련 코드나 프로그램을 생성하는 도구
Dnschanger	DNS 주소 변경
Downloader	다운로드 기능이 있는 악성코드
Dropper	다른 악성코드를 떨어뜨리는 악성코드
Exploit	취약점을 이용한 유형
Favadd	웹브라우저에 사용자가 원하지 않는 즐겨찾기 추가
Ircbot	악성 IRC봇
Killav	백신, 방화벽 등 보안 프로그램 삭제 혹은 무력화
Obfuscated	코드를 꼬아둔 일종의 패커류
Patched	다른 파일을 감염 시키는 기능이 없이 패치 된 형태
Proxy	프락시 기능
Qhost	HOST 파일 변경
Xema	특별하게 부를 이름이 없을 경우 사용. (애매에서 나온 이름)

[표 4-1] 대표이름

상세 이름은 악성코드 추천 이름에서 별도 구분이 필요하다고 판단 될 때 사용한다. 예를 들어 보통 다운로더를 Win32-Trojan/Downloader.A로 표시하는데 분석가가 별도의 구분이 필요하다고 생각될 때 Win32-

Torjan/Downloader-Foo.A와 같이 명명할 수 있다.

변형은 대문자로만 표현되며 최초 이름에는 A 가 붙으며 이후 B, C … Z 순으로 나가며 Z 이후에는 AA, AB .. ZZ 로 사용되며 ZZ 이후에는 AAA 가 된다. 단, 자동으로 변형이 부여될 때는 욕설, 비속어, 음란 단어가 만들어지는걸 예방하기 위해 모음(A, E, I, O, U)을 사용하지 않는다. 따라서 자동으로 변형이 부여될 때는 BD 다음 변형은 BE가 아닌 BF이다.

일반적인 변형 외에 정보형 변형은 진단명 다음에 붙는다.

정보형 변형	설명
Generic	포괄적 진단(Generic detection)으로 여러 변형에 대해 한번에 진단함
Suspicious	의심스러운(suspicious) 진단으로 확인을 위해 샘플을 접수 받아야 함
Variant	여러 변형(variant)에 대한 하나의 진단명 (매우 많은 변형이 존재할 때 사용하며 사용이 제한적)

[표 4-2] 정보 변형

단, 여러 Generic 이름이 올 수 있으므로 이때는 이름에 숫자를 붙인다.

예)
Win32-Worm/IRCBot.Generic
Win32-Worm/IRCBot1.Generic

4. 새로운 명명법 예

새로운 명명법을 기존 명명법과 비교하면 다음 표와 같다. 악성코드의 경우 사이즈가 붙는데 예에서는 편의상 12345로 통일했으며 새로운 명명법의 변형도 A로 통일 했다.

기존 명명법	새로운 명명법	비고
Win32/Virut	Win32-Virus/Virut.A	윈도우 바이러스는 종류에 Virus를 붙임
Win32/Bagle.worm.12345	Win32-Worm/Bagle.A	윈도우 웜은 종류에 Worm을 붙임
Dropper/Agent.12345	Win32-Trojan/Dropper.A	플랫폼이 없이 단독으로 사용되던 Dropper는 윈도우 플랫폼일 경우 Win32를 붙이고 Dropper는 타입이 아닌 이름으로 내려감
Win-Trojan/Downloader.12345	Win32-Trojan/Downloader.A	Win은 Win32으로 변경되며 숫자는 제외됨
Win-Trojan/Fakeav.Gen	Win32-Trojan/Fakeav.Generic	Gen은 Generic으로 풀어 씀

[표 4-3] 새로운 명명법 예

5. 참고자료

[1] 박준용, “[ASEC][SZ]진단명정책.doc”, 2005년 7월

[2] 바이러스명명원칙.ppt

[3] “V3 제품군 진단 명칭”, 2001년 1월 12일

[4] “V3 제품군 진단 명칭 (접두어)”, 2005년 7월 11일

[5] Nick FitzGerald, “A Virus by Any Other Name : Towards the Revised CARO Naming Convention”, AVAR Conference, 2002

[6] Peter Szor, “The Art of Computer Virus Research and Defense”, p.38 – 46

ASEC REPORT 집필진

2009년 Vol.11

편 집 장	선임 연구원	허 종 오
집 필 진	선임 연구원	박 태 환
	선임 연구원	정 진 성
	선임 연구원	정 관 진
	선임 연구원	차 민 석
	선임 연구원	허 종 오
	주임 연구원	박 시 준
	주임 연구원	조 주 봉
감 수	상 무	조 시 행
참여연구원		ASEC 연구원
		SiteGuard 연구원

Ahn 안철수연구소