ASEC REPORT

안철수연구소에서 발행하는 월간 보안 보고서

2010. Volume. 02

안철수연구소

목 차

이달의 보안 동향

Ⅰ. 이달의 보안 동향

1. 악성코드 동향

악성코드 통계

2010년 2월 악성코드 통계현황은 다음과 같다.

순위	등락	악성코드명	건수	비율
1	–	Win32/Induc	409,725	17.9 %
2	–	TextImage/Autorun	340,320	14.8 %
3	–	Win32/Parite	147,635	6.4 %
4	New	JS/Exploit	132,896	5.8 %
5	New	Win32/Palevo.worm.Gen	126,267	5.5 %
6	↑ 10	Win-Adware/PointKing.722944	119,274	5.2 %
7	–	Win32/Virut.B	102,414	4.5 %
8	↑ 3	Win32/Conficker.worm.Gen	79,639	3.5 %
9	–	Win32/Virut	79,350	3.5 %
10	↑ 3	Win32/Olala.worm.57344	78,224	3.4 %
11	New	Win-Adware/BHO.WiseBar.282624	76,231	3.3 %
12	–	TextImage/Sasan	73,833	3.2 %
13	↑ 2	ALS/Bursted	72,370	3.2 %
14	New	Win-Trojan/Malware.234728	72,047	3.1 %
15	New	Win-Adware/Migame.423928	70,860	3.1 %
16	New	Win-Dropper/Rogue.PCSafe.2373789	69,649	3 %
17	↓ 3	TextImage/Viking	64,048	2.8 %
18	New	HTML/Agent	62,696	2.7 %
19	New	Win-Trojan/OnlineGameHack.324096.C	59,499	2.6 %
20	New	Win-Trojan/Genome.308832.B	58,244	2.5 %
합계			2,295,221	100 %

[표 1-1] 악성코드 감염보고 Top 20

2010년 2월의 악성코드 감염 보고는 Win32/Induc이 1 위를 차지하고 있으며, TextImage/Autorun과 Win32/Parite 가 각각 2위와 3위를 차지 하였다. 신규로 Top 20에 진입한 악성코드는 총 9 건이다.

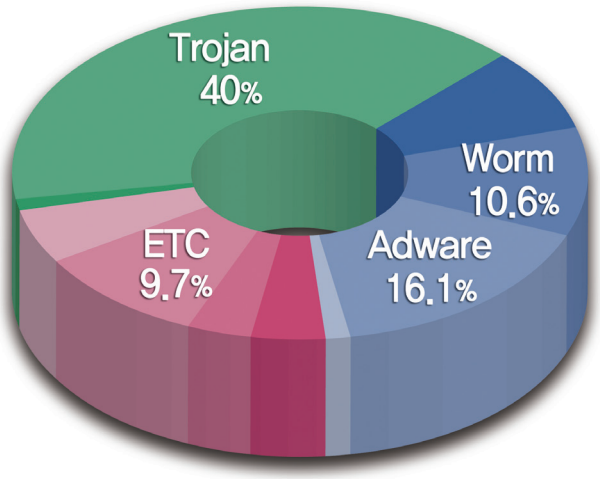
아래 표는 악성코드의 주요 동향을 파악하기 위하여, 악성코드 별 변종을 종합한 악성코드 대표 진단명 감염보고 Top 20이다.

순위	등락	악성코드명	건수	비율
1	–	Win-Trojan/Agent	669,159	12.6 %
2	–	Win-Trojan/OnlineGameHack	517,074	9.8 %
3	↑ 1	Win-Trojan/Downloader	478,916	9 %
4	↓ 1	Win32/Induc	409,835	7.7 %
5	–	TextImage/Autorun	340,646	6.4 %
6	↑ 13	Win-Adware/BHO	333,807	6.3 %
7	↑ 2	Win32/Autorun.worm	259,686	4.9 %
8	↑ 3	Win-Trojan/Malware	247,706	4.7 %
9	↓ 3	Win32/Virut	235,229	4.4 %
10	↓ 3	Win32/Conficker	232,408	4.4 %
11	New	Win-Trojan/Onlinegamehack	221,356	4.2 %
12	New	Win32/Palevo	219,441	4.1 %
13	↓ 1	Win-Trojan/Genome	196,941	3.7 %
14	New	Win-Dropper/Rogue	158,323	3 %
15	↓ 2	Win32/Parite	149,754	2.8 %
16	New	JS/Exploit	132,896	2.5 %
17	↓ 2	Win32/Kido	131,759	2.5 %
18	↓ 1	Win-Adware/KorAdware	125,784	2.4 %
19	New	Win-Adware/PointKing	124,857	2.4 %
20	New	Dropper/Malware	113,744	2.1 %
합계			5,299,321	100 %

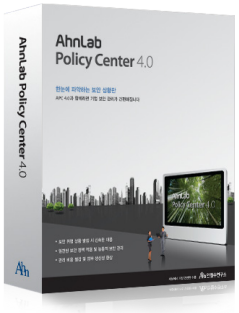
[표 1-2] 악성코드 대표진단명 감염보고 Top 20

2010년 2월의 감염보고 건수는 Win-Trojan/Agent가 총 669,159건으로 Top 20 중 12.6%의 비율로 1위를 차지하고 있으며, Win-Trojan/OnlineGameHack 이 517,074건으로 2위, Win-Trojan/Downloader 이 478,916건으로 3위를 차지 하였다.

아래 차트는 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.

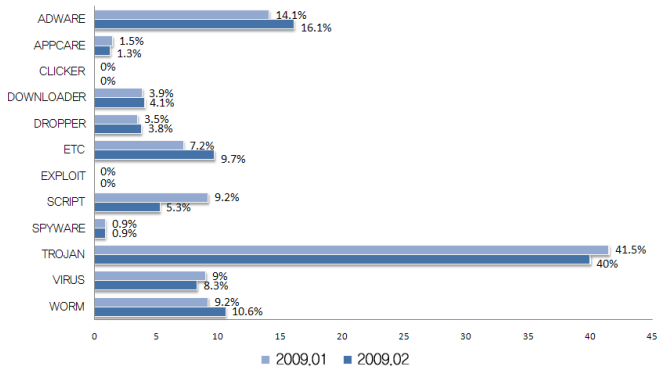


[그림 1-1] 악성코드 유형별 감염보고 비율



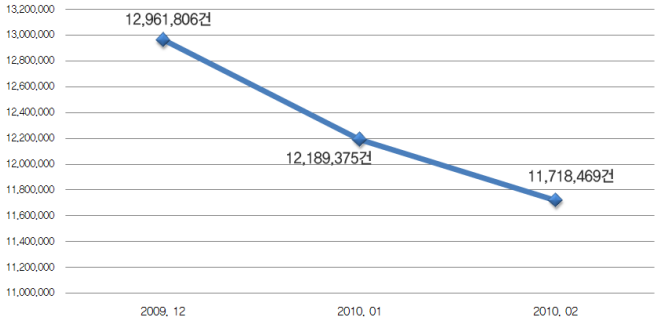
AhnLab Policy Center 4.0

2010년 2월의 감염보고 건수는 악성코드 유형별로 감염보고건수 비율은 트로잔(TROJAN)류가 40%로 가장 많은 비율을 차지하고, 애드웨어(ADWARE)가 16.1%, 웜(WORM)이10.6%의 비율을 각각 차지하고 있다.



[그림 1-2] 악성코드 유형별 감염보고 전월 비교

악성코드 유형별 감염보고 비율을 전월과 비교하면 애드웨어, 웜, 드롭퍼(DROPPER), 다운로더(DOWNLOADER)가 전월에 비해 증가세를 보이고 있는 반면 스크립트(SCRIPT), 트로잔, 바이러스 (VIRUS), 유해가능프로그램(APPCARE)은 전월에 비해 감소한 것을 볼 수 있다. 스파이웨어(SPYWARE) 계열들은 전월 수준을 유지하였다.



[그림 1-3] 악성코드 월별 감염보고 건수

2월의 악성코드 월별 감염보고 건수는 11,718,469건으로 1월의 악성코드 월별 감염 보고건수 12,189,375건 비해 470,906건이 감소하였다.

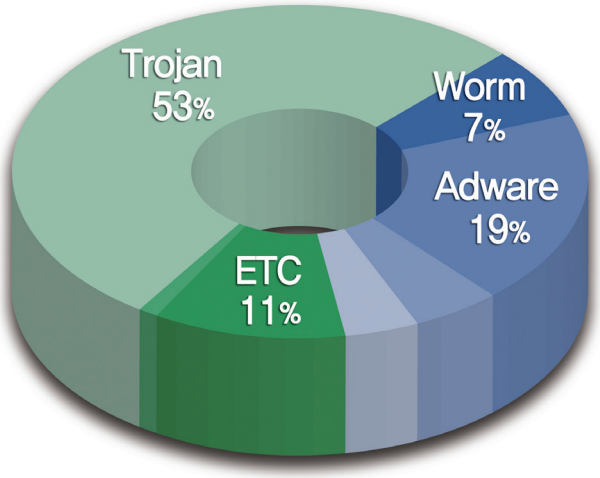
AhnLab V3 MSS

아래 표는 2월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top 200이다.

순위	악성코드명	건수	비율
1	Win-Adware/BHO.WiseBar.282624	76,231	11.8 %
2	Win-Adware/Migame.423928	70,860	11 %
3	Win-Dropper/Rogue.PCSafe.2373789	69,649	10.8 %
4	Win-Dropper/Rogue.ComClean.2194022	50,768	7.9 %
5	Win-Dropper/BHO.Ibrows.660258	39,100	6.1 %
6	Dropper/Malware.294912.N	33,986	5.3 %
7	Win-Adware/Mediacents.155648	32,677	5.1 %
8	ASP/Ace.283136	31,510	4.9 %
9	ASP/Ace.780800	25,893	4 %
10	Win-Trojan/Onlinegamehack.159744.I	24,169	3.7 %
11	Win-Trojan/Downloader.70144.AG	22,353	3.5 %
12	Win-Trojan/OnlineGameHack.159744.AG	21,771	3.4 %
13	Win-Trojan/Unovt.717312	21,222	3.3 %
14	Win-Trojan/Agent.9786	19,907	3.1 %
15	Win32/Palevo.worm.119808.D	18,337	2.8 %
16	Win-Trojan/Downloader.324096.C	18,316	2.8 %
17	Win-Adware/Colorsoft.620929	18,075	2.8 %
18	Win-Adware/BHO.Ibrows.94208.B	16,884	2.6 %
19	Win-Trojan/Malware.218624.L	16,874	2.6 %
20	Win-Adware/Funtvi.70144	16,255	2.5 %
	합계	644,837	100 %

[표 1-3] 신종 악성코드 감염보고 Top 20

2월의 신종 악성코드 감염 보고의 Top 20은 Win-Adware/BHO.WiseBar.28262가 76,231 건으로 전체 11.8 %를 차지하여 1위를 차지하였으며, Win-Adware/Migame. 423928가 70,860건 2위를 차지하였다.



[그림 1-4] 신종 악성코드 유형별 분포

2월의 신종 악성코드 유형별 분포는 트로잔이 53%로 1위를 차지하였다. 그 뒤를 이어 애드웨어가 19%를 각각 차지하였다.

악성코드 이슈

2월에는 다양한 유형의 악성코드들이 보고 되었다. 정상 시스템 드라이버로 파일을 위장하는 스팸 메일러와 이메일을 통해 변종을 전파하는 웜, 네트워크 트래픽을 증가시키며 BSOD를 발생시키는 악성코드와 같이 꾸

준한 피해를 일으키는 악성코드부터, 동계 올림픽 시즌을 맞아 특정 선수의 경기 동영상을 가장하여 가짜 백신을 설치하는 악성코드와 같이 시대적 흐름에 편승하는 악성코드가 있었으며, 가짜 백신과 번들 형태로 설치되는 애드웨어를 이용하여 금전적인 이득을 노리는 악성코드까지 어느 때보다 다양한 악성코드들의 왕성한 활동을 볼 수 있다.

시스템 파일로 위장한 스팸 메일러

정상 시스템 드라이버 파일로 자신을 위장하고 동작하는 Win-Trojan/Spamer. 791552 악성코드도 발견 되었는데 이는 커널 스팸 메일러로 알려졌다. 그 동안 소강 상태로 보였던 커널 모드, 스팸 메일러가 재등장하였으며, 자신의 진단이나 치료를 어렵게 하는 자기보호 기능이 있기 때문에 이를 진단하고 치료하는데 어려움이 있다. 세부적으로 기능을 살펴보면, 보고된 커널 모드 스팸 메일러(Win-Trojan/Spamer. 7915)는 시스템 드라이버 파일명으로 자신을 위장한 후 메모리에 로드 된다.

[그림 1-5] 변형 취약점 코드가 사용하는 메모리 주소

이후 Service.exe 에 스레드를 생성하여 특정 호스트에 접속도 하고 스팸메일도 발송한다. 드라이버 형태인 해당 악성코드는 자신을 다른 프로세스가 읽지 못하게 하고 시스템 재부팅 관련 커널 콜백 루틴에 자신을 등록하여 삭제 하도록 함으로써 자신을 찾아내기 어렵게 한다 이처럼 자기보호가 된 악성코드와 커널 스팸 메일러는 이번이 처음은 아니다. 자신을 진단 및 치료하게 어렵게 하여 존속성을 보장 받으려는 악성코드의 자기보호 기법은 고도화 되고 있기 때문에 오히려 자신만을 단지 숨기려는 은폐기법 보다 더욱 진단/치료 하는 방법이 까다로워 지고 있다.

허위 유투브 동영상을 가장한 동계 올림픽 관련 악성코드

특정 선수의 경기 동영상을 가장하여 가짜 백신을 설치하는 웹 사이트가 발견 되었다. 이것은 많은 사용자들이 특정 조건으로 검색 시 상위에 노출하여 해당 사이트로 유도한다. 대부분 악성코드로 감염을 유도하거나 허위 사이트로 유도 한다. 앞으로 이러한 형태로 악성코드 설치나 사용자 정보를 훔쳐나가는 형태의 악성코드가 늘어날 전망이다.

[그림 1-6] 특정 선수 유투브 동영상을 위장한 웹 사이트

이메일을 통해 변종을 전파하는 Prolaco 웜

이메일을 통한 악성코드의 전파는 이미 일반적인 악성코드의 한 전파방법이 되었다. 이메일을 통해 전파되는 악성코드들은 친구로부터 축하카드를 받았으니 첨부파일을 확인해 보라는 내용이나 수신자에게 택배가 도착했으니 첨부된 송장의 정보를 확인하라는 등 일반적으로 있을 수 있는 사실을 가장해 사용자를 속이는 사회공학기법을 사용하고 있다. 그러나 2월초 국내에서는 구글 메일로 위장한 Prolaco 웜 변종이 발송하는 메일을 수신하였다는 문의들이 접수되고 있다. 이 변종은 전자메일 제목으로 "Thank you from Google!"을 사용하며 메일 본문에는 구글로 입사지원을 해서 고맙다는 내용과 함께 구글 이미지가 사용되어져 기존에 발견되는 이메일관련 웜과는 다르게 구글처럼 신뢰하는 특정벤더에서 보낸 전자메일로 위장한 특이한 사례였다. 메일에 첨부된 압축파일의 압축을 풀면 pdf문서를 가장한 실행파일이 생성되는데, 아래와 같이 사용자들이 pdf문서를 클릭하여 실행되기 위한 전형적인 악성코드의 수법이다. "document.pdf.exe" (Windows 특성상 사용자에게 파일이 보여질 때, 중간에 공란이 보여지지 않고, "document.pdf" 만이 보여진다.)

전자메일을 통한 악성코드의 감염을 예방하기 위해서는 아래 사항의 안전수칙을 지키는 것이 중요하다.

1) 알지 못하는 발신자로부터 수신되는 메일의 경우, 가급적 열지 않고, 삭제한다.

2) 전자메일에 파일이 첨부되어 있는 경우, 바로 실행하지 않도록 주의하고, 특정폴더에 저장 후 최신엔진으로 업데이트 된 백신제품을 이용하여 먼저 검사를 진행한 후 실행한다.

3) 전자메일에 존재하는 의심스런 URL링크는 클릭하지 않는다.

4) 악성코드의 감염을 예방하기 위해서는 시스템에 설치된 백신제품은 항상 최신엔진을 유지하고 실시간 감시기를 켜놓는다.

5) 악성코드의 감염을 예방하기 위해서는 백신의 최신엔진 유지와 운영체제의 최신보안패치 설치뿐만 아니라, 사용하는 어플리케이션 벤더에서 제공하는 취약점 제거를 위한 보안패치를 모두 설치하도록 한다.

네트워크 트래픽을 증가시키는 Win32/Bredola

2월에 화제가 되었던 또 다른 이슈는 Win32/Bredolab류의 악성코드로 인한 네트워크 트래픽 증가 및 BSOD발생인데, 2월초부터 현재까지 여러 기업고객과 개인고객들로부터 문의가 접수되고 있다. 이 악성코드의 특징은 특정 sys파일이 상당수의 악성코드를 지속적으로 다운로드 하여 감염시스템에 설치되며, 네트워크 트래픽을 증가시켜 네트워크 장애 및 시스템의 자원을 고갈시킨다. 뿐만 아니라 설치되는 특정 sys파일에 의해 BSOD가 발생하기도 하여 시큐리티 대응센터에서는 현재 전용백신 배포와 함께 대응가이드를 제작해서 함께 배포하고 있다. ASEC대응팀 블로

그(http://core.ahnlab. com/120)에서 보다 상세한 정보와 대응가이드를 확인할 수 있습니다.

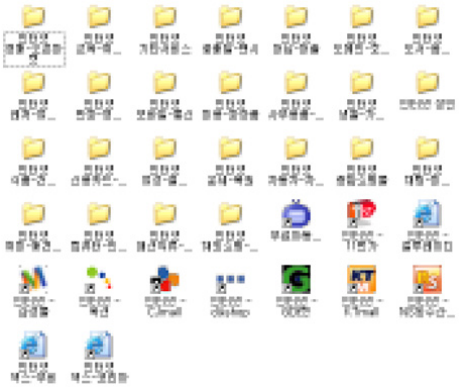
가짜 백신 피해 증가

가짜 백신들로 인한 사용자들의 피해가 끊이질 않고 있다. 이들은 적절한 사용자 동의를 받지 않고 설치되어 동작하며, 윈도우나 웹 브라우저 사용시 자동으로 생성되는 임시 파일들을 악성코드 의심항목으로 진단하고 유료 결제를 통한 치료를 지속적으로 유도한다. 이들은 일정 시간을 간격으로 시스템 검사 작업을 수행하므로 웹 서핑만으로도 생성되는 임시 파일을 악성코드로 진단하고 치료하는 작업을 계속 반복한다. 이는 금전적인 피해는 물론이고 불필요한 검사와 치료 작업을 반복해 시스템 성능을 저하시키는 주범이 되고 있다. 이들은 악성코드 분석을 통한 엔진 업데이트가 아닌, 다른 컴퓨터 보안 회사에서 제공하는 바이러스/스파이웨어 정보를 무단으로 도용해 제품을 제작한다. 그리고 엔진이 항상 최신 버전인 것처럼 사용자를 속이기 위해 현재 시스템의 날짜를 얻어와서 엔진 버전을 표기하고 있다. 또한 이들 업체는 더 높은 수익을 위해 보통 3개 이상의 다른 이름을 가진 가짜 백신을 동시에 운영하고 있다. 보안 업체는 사용자의 컴퓨터를 보안 위협으로부터 안전하게 지켜주는 것을 주 목적으로 서비스를 제공해야 하지만 이들 업체는 오로지 돈벌이를 위해 가짜 제품들을 만들어 내는 사기꾼과도 같다.

[그림 1-7] 시스템 날짜로 엔진 버전을 속임

즐겨찾기, 바로가기 생성 애드웨어의 증가

다수의 인터넷 즐겨찾기와 인터넷 바로가기를 생성하는 애드웨어가 다시 증가하고 있다. 과거엔 ActiveX를 이용해 설치되는 경우가 많았지만 최근에는 주로 애드웨어의 번들로 설치되고 있다. 이러한 애드웨어는 방문객을 유치했을 경우 발생하는 수익에 대해 일정 금액을 방문객 유치자에게 돌려주는 일종의 리베이트로 수익을 가져갈 수 있다. 따라서 사용자의 편리함을 위해 사용되어야 할 인터넷 즐겨찾기와 바로가기를 돈벌이를 위해 악용하는 사례는 앞으로도 증가할 것으로 예상된다



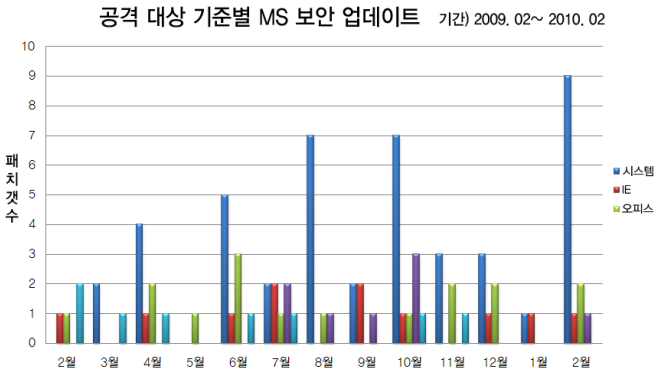
[그림 1-8] 애드웨어에 의해 생성된 즐겨찾기들

2. 시큐리티 동향

시큐리티 통계

2월 마이크로소프트 보안 업데이트 현황

마이크로소프트사로부터 발표된 이번 달 보안 업데이트는 총 13건으로 보통 1건, 중요 7건, 긴급 5건이다.



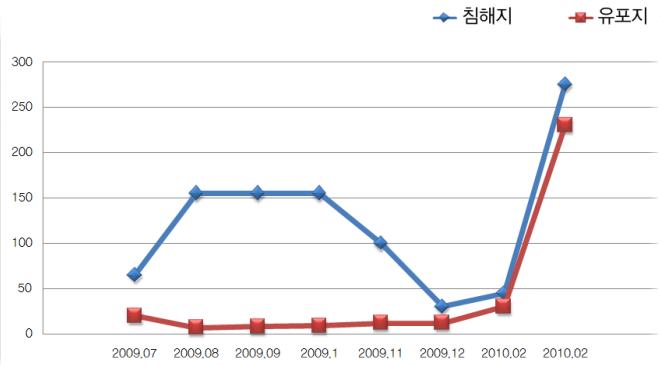
[그림 2-1] 공격 대상 기준별 MS 보안 업데이트

위험도	취약점	PoC
긴급	MS10-006 SMB 클라이언트의 취약점으로 인한 원격코드 실행 문제점	무
긴급	MS10-009 Windows TCP/IP 의 취약점으로 인한 원격코드 실행 문제점	무
긴급	MS10-013 Microsoft DirectShow 의 취약점으로 인한 원격코드 실행 문제점	무

[표 2-1] 2010년 2월 주요 MS 보안 업데이트

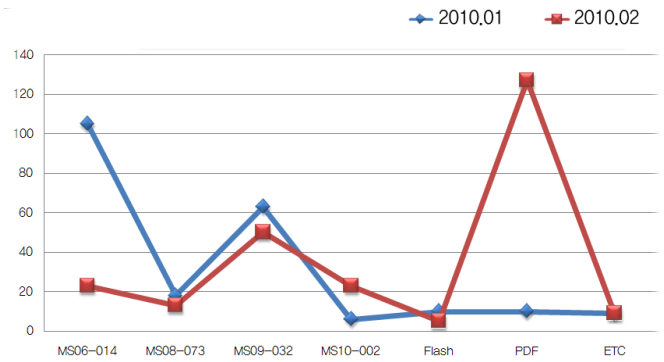
이번 달에는 지난 달에 발표된 2건보다 훨씬 많은 13건의 패치가 발표되었다. 특히, MS10-006 SMB 클라이언트 취약점, MS10-009 Windows TCP/IP 취약점, MS10-013 DirectShow 취약점은 공격자로 하여금 원격에서 원하는 코드를 실행할 수 있는 취약점이기 때문에 주의가 필요하다. 이러한 취약점들은 주로 웹을 이용하여 배포가 많이 이루어 짐으로, 신뢰되지 않은 웹사이트 접속에 유의해야 하며, 백신 설치와 더불어 보안 패치를 반드시 업데이트 해야 안전한 인터넷 환경을 사용할 수 있다.

악성코드 침해 웹사이트 현황



[그림 2-2] 악성코드 배포를 위해 침해된 사이트 / 배포지 수

[그림 2-2]는 2010년 02월 악성코드 침해 사이트 현황을 나타낸 그래프인데 2010년 1월보다 월등히 증가했음을 알 수가 있고 악성코드가 유포될 때 사용했던 취약점의 동향은 전월과 비교했을 때 많은 변화가 있었다. 그에 대한 자세한 원인은 아래에서 알아보겠다.



[그림 2-3] 악성코드 배포를 위해 사용된 취약점

[그림 2-3]은 2010년 2월 한달 동안 침해사고가 발생한 웹사이트들에서 악성코드를 유포하기 위해 서 사용했던 취약점들에 대한 통계인데 이를 통해서 몇 가지 사실을 알 수가 있다.

2010년 2월의 경우 MS06-014취약점의 공격건수는 전월에 비해서 상당히 큰 폭으로 감소했고 최 근에 발견된 MS09-023, MS10-002그리고 PDF관련 취약점에 대한 공격건수가 큰 폭으로 상승했음을 알 수가 있는데 그 원인은 2010년 2월의 침해사고 사이트 / 배포지의 대부분이 Win-Trojan/Daonol 악성코드를 배포하기 위해서 해당 취약점들을 빈번하게 사용했기 때문인 것으로 보 인다.

[그림 2-2/2-3]을 통해서 말하고 싶은 것은 단순히 월별로 어떤 사이트가 침해됐고, 어떤 취약점이 악성코드 유포에 많이 사용되었는가가 중요한 것이 아니라 악성코드가 유포하기 위해서 어떤 대상들을 타깃으로 하는 지를 유심히 살펴보고 자신이 사용하는 프로그램들 중 악성코드가 사용할 수 있는 취약점들이 존재하지 않는지 점검해 볼 필요가 있다.

시큐리티 이슈

Internet Explorer Information Disclosure 취약점

Black Hat DC 2010에서 Microsoft Internet Explorer에서 Security Zone을 우회할 수 있는 취약점에 대한 발표가 있었다. 해당 취약점은 오래 전부터 존재하고 있었던 것으로써 발표 당시, Internet Explorer 7,8의 Protected Mode가 설정되어 있는 경우를 제외한 모든 버전에 해당되는 문제였다. 공격자는 해당 취약점을 이용하여 웹 페이지 접근을 통해 사용자의 로컬 컴퓨터 상에 존재하는 파일들의 정보를 획득하거나 스크립트(SCRIPT) 실행을 통해 임의의 명령을 수행할 수 있다.

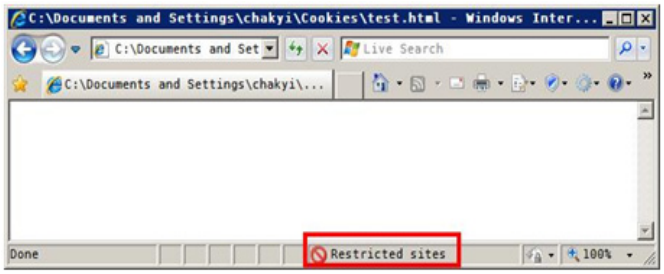
MS Internet Explorer는 시스템의 안전을 위해 다음과 같은 Security Zone 모델을 채택하고 있다.

- 인터넷(Internet)
- 로컬 인트라넷(Local Intranet)
- 신뢰할 수 있는 사이트(Trusted Sites)
- 제한된 사이트(Restricted Sites)

이 중, 중요한 파일이나 악용소지가 있는 파일들은 최소한의 권한으로 호출되도록 제한된 사이트(Restricted Sites) 영역으로 구별되어 있다. 일반적인 웹사이트들은 인터넷 영역(Internet Zone)이라 하여 일반적인 권한을 갖게 되고, 사용자 컴퓨터 내에서의 호출은 로컬 영역(Local Machine Zone)에 포함된다.

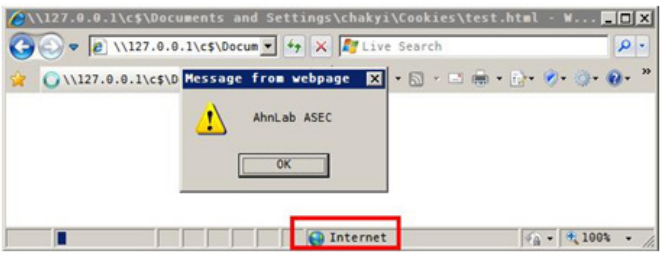
다음과 같은 스크립트 파일은, 시스템에서 사용자의 쿠키(cookie)가 저장되는 위치(Document and Settings₩userid₩Cookies)에서 열면 제한된 사이트(Restricted) 영역으로 인식하여, 정상적으로 실행되지 않는다.

```
<script>alert('AhnLab ASEC');</script>
```
[그림2-4] 스크립트 내용



[그림 2-5] 실행 결과 : 제한된 사이트 영역

그러나, URL 경로 상에 다음과 같이 '₩₩127.0.0.1₩c$' 을 추가하여 접근할 경우, InternetExplorer가 이를 인터넷(Internet Zone) 영역으로 인식하여 스크립트를 정상적으로 호출할 수 있게 된다. – file://127.0.0.1/C$/example.dat



[그림 2-6] 실행 결과 : 인터넷 영역

해당 공격이 성공적으로 이루어지기 위해서는 우선적으로 원하는 파일을 로컬 시스템 상에 올려야 하며, 해당 파일이 HTML 파일로 해석되게 할 수 있는 방법을 찾아야만 한다.

사용자의 로컬 시스템 상에 악의적인 동작을 수행하는 스크립트 파일을 올리는 방법은 웹 서버에서 set-cookie 헤더를 이용하는 방법, url history를 이용하는 방법 등의 이미 공개된 다양한 취약점이나 우회방법을 이

용할 수 있다. 만약, 공격자가 악성코드를 사용자의 시스템에 생성하는 것이 성공하였다면 다음과 같은 형태의 코드를 이용하여 동작시킬 수 있다.

```
<script language="Javascript">
        var obj = document.createElement("object");
        obj.data = "file://127.0.0.1/C$/.../index.dat";
        obj.type = "text/html";
        obj.id = "obj_results";
        obj.width = "500px";
        obj.height = "300px";
        document.body.appendChild(obj);
</script>
```

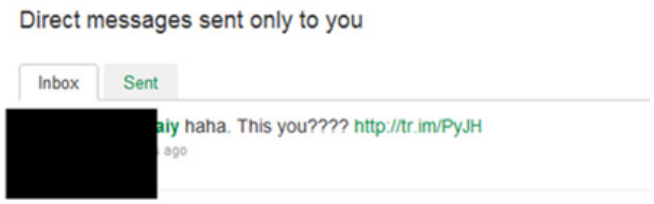
[그림 2-7] 동적 생성 태그를 이용한 방법

이러한 점을 이용하여 공격자는 사용자의 시스템에서 직접 스크립트를 실행시킬 수 있기 때문에 사용자의 시스템의 어떠한 파일에도 접근할 수 있는 권한을 갖게 된다.

일반적인 악성코드가 웹 페이지에 삽입되는 것과는 달리 cookie, url 접근 history 파일 및 다양한 경로를 통해 악성코드가 실행될 수 있기 때문에 해당 취약점을 이용하는 실제 공격이 발생한다면 일반적인 방식으로 탐지하기가 어려울 수 있다.

Twitter Direct Message Phishing Spam

Twitter의 Direct Message 기능을 피싱 공격에 사용하는 스팸이 발생하였다. 해당 스팸은 사용자에게 "haha. This you???? http://tr.im/PyJH" 라는 메시지를 전송하고, 사용자가 메시지에 포함된 URL을 클릭하면 가짜 Twitter 로그인 페이지로 이동하게 한다.



[그림 2-7] DoS 공격시 발생하는 네트워크 패킷

가짜 Twttier 로그인 페이지의 주소의 형태가 twitter.login 으로 시작하고 있고, 로그인 페이지는 실제 Twitter 로그인 페이지와 육안으로 식별할 수 없을 정도로 비슷하기 때문에 사용자는 주의하지 않는다면 별다른 의심 없이 로그인을 시도할 수 있다. 자세한 내용은 웹 보안 이슈에서 다루고자 한다.

3. 웹 보안 동향

웹 보안 통계

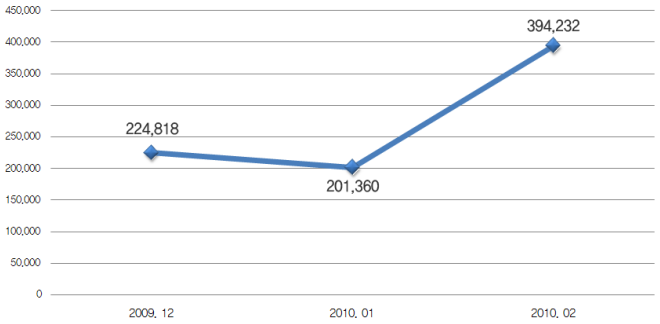
웹 사이트 보안 요약

구분	건수
악성코드 발견 건수	394,232
악성코드 유형	1,042
악성코드가 발견된 도메인	975
악성코드 발견된 URL	5,090

[표 3-1] 웹 사이트 보안 요약

악성코드 발견 건수는 394,232 건이고, 악성코드 유형은 1,042 건이며, 악성코드가 발견된 도메인은 975 건이며, 악성코드 발견된 URL은 5,090 건이다. 2010년 2 월은 2010년 1월 보다 악성코드 유형, 악성코드가 발견된 도메인, 악성코드 발견된 URL 은 다소 감소하였으나, 악성코드 발견 건수는 증가하였다.

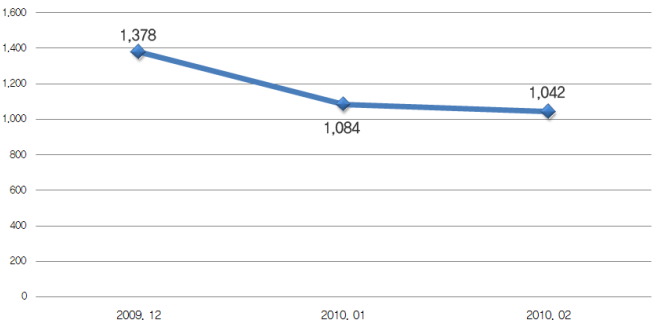
월별 악성코드 발견 건수



[그림 3-1] 월별 악성코드 발견 건수

2010년 2월 악성코드 발견 건수는 전달의 201,360 건에 비해 196 % 수준인 394,232 건이다.

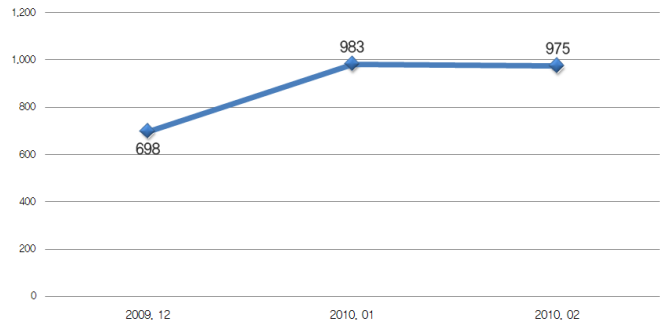
월별 악성코드 유형



[그림 3-2] 월별 악성코드 유형

2010 년 2월 악성코드 유형은 전달의 1,084건에 비해 96% 수준인 1,042건이다.

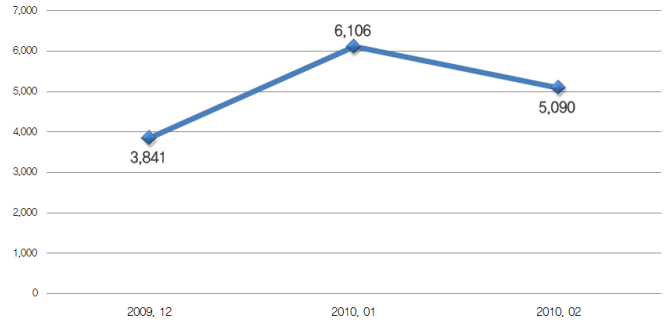
월별 악성코드가 발견된 도메인



[그림 3-3] 월별 악성코드가 발견된 도메인

2010년 2월 악성코드가 발견된 도메인은 전달의 983건에 비해 99%수준인 975건 이다.

월별 악성코드가 발견된 URL



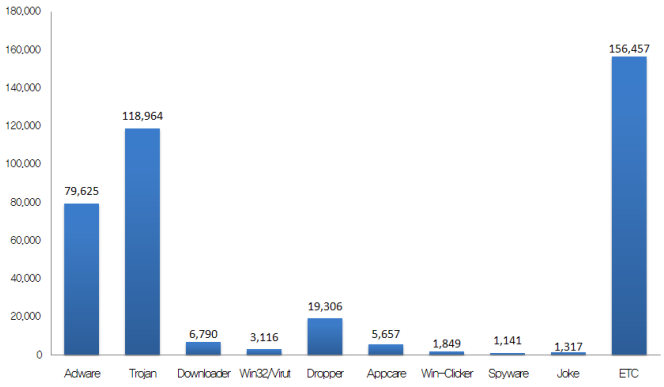
[그림 3-4] 월별 악성코드가 발견된 URL

2010년 2월 악성코드가 발견된 URL은 전달의 6,106 건에 비해 83% 수준인 5,090 건이다.

악성코드 유형별 배포 수

유형	건수	비율
ADWARE	79,625	20.2 %
TROJAN	118,964	30.2 %
DOWNLOADER	6,790	1.7 %
Win32/VIRUT	3,116	0.8 %
DROPPER	19,306	4.9 %
APPCARE	5,657	1.4 %
WIN-CLICKER	1,849	0.5 %
SPYWARE	1,141	0.3 %
JOKE	1,317	0.3 %
ETC	156,467	39.7 %
합계	394,232	100 %

[표 3-2] 악성코드 유형별 배포 수



[그림 3-5] 악성코드 유형별 분포

악성코드 유형별 배포 수에서 트로잔(TROJAN)류가 118,964건으로 전체의 30.2%로 1위를 차지하였으며, 애드웨어(ADWARE)류가 79,625건, 전체의 20.2%로 2위를 기록하였다.

악성코드 배포 Top 10

순위		악성코드명	건수	비율
1	New	Win32/MyDoom.worm.32256	73,308	25.1 %
2	New	Win-Trojan/Downloader.65904	59,876	20.5 %
3	New	Win32/Prolaco.worm.607232	46,911	16.1 %
4	↓ 3	Win-Adware/Shortcut.InlivePlayerActiveX.234	41,278	14.1 %
5	↓ 1	Win-Trojan/OnlineGameHack.324096.C	20,862	7.1 %
6	New	Win-Dropper/ToolBar.Dream.326567	13,468	4.6 %
7	↓ 4	Win32/Induc	12,241	4.2 %
8	↓ 6	Win-Trojan/Agent.57344.AHB	11,964	4.1 %
9	↓ 4	Win-Adware/Shortcut.IconJoy.642048	6,954	2.4 %
10	New	Win-Adware/Shortcut.InlivePlayerActiveX.102400.B	5,089	1.7 %
합계			291,951	100 %

[표 3-3] 악성코드 배포 Top 10

악성코드 배포 Top 10에서 Win32/MyDoom.worm.32256이 73,308 건으로 1 위를 차지하였으며, Top 10에 Win32/MyDoom.worm.32256등 5건이 새로 등장하였다.

웹 보안 이슈

트위터를 이용한 피싱 사이트 등장

해외 시각으로 2010년 2월 24일, 한 블로그를 통해 유명 소셜 네트워크 서비스(Social Network Service) 웹 사이트인 트위터(Twitter) 사용자간 전송 가능한 다이렉트 메시지(Direct Messages)로 악의적인 피싱(Phishing) 웹 사이트로 연결되는 링크가 포함된 것이 발견되었다. 해당 블로그에서는 아래 이미지와 동일하게 트위터에 등록되어 있는 개인 사용자들에게 직접 전달되는 다이렉트 메시지가 전송 되었다.

[그림 3-6] 다이렉트 메시지

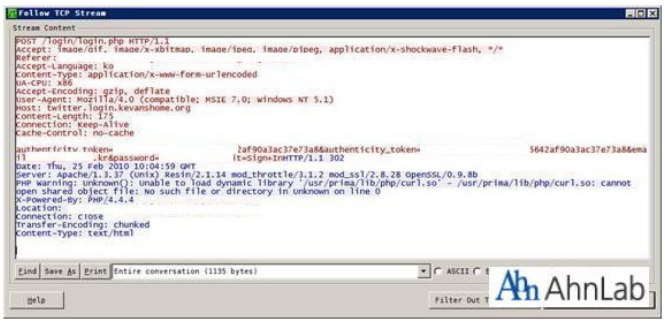
해당 메시지에는 일반적으로 트위터 사용자들이 많이 사용하는 단축 URL(URL Shortening) 기법이 적용된 웹 사이트 링크가 포함되어 있었다. ASEC에서는 다이렉트 메시지로 전달된 해당 단축 URL을 분석 한 결과, 해당 웹 사이트 링크를 클릭하게 되면 아래 이미지와 같이 허위로 작성된 트위터 사용자 로그인 웹 사이트로 연결이 된다.

[그림 3-7] 로그인을 유도하는 피싱 사이트

해당 웹 사이트를 통해 사용자 계정과 암호를 실제로 입력하게 되면 아래 이미지에서와 같이 웹 페이지를 표시 할 수 없다는 오류가 발생하게 된다.

[그림 3-8] 로그인시 발생하는 오류창

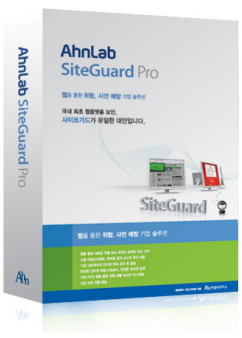
그러나 실제 전송되는 네트워크 패킷(Network Packet)을 분석해보면 아래 이미지에서와 같이 사용자 계정과 암호는 그대로 특정 시스템으로 전송이 되는 것을 확인 할 수 가 있었다.



[그림 3-9] 패킷 분석결과

해당 트위터 피싱 웹사이트와 사용자 계정과 암호가 전송되는 시스템은 중국 허베이(Hebei)에 위치하고 있어 탈취된 개인 정보가 중국으로 전송된 것을 알 수 가 있다. 이번 트위터에서 발생한 단축 URL을 통한 피싱 웹 사이트 연결은 일부 보안 업체에서 우려한 바와 같이 소셜 네트워크 사이트(Social Network Site)들 안에서 단축 URL로 인해 피싱이나 악의적인 웹 사이트로 연결하여 악성코드를 유포하는 등의 보안 위협이 발생 할 수 있다는 것을 증명한 사례로 볼 수 있다. 이렇게 소셜 네트워크 사이트들에 발생할 수 있는 악의적인 웹 사이트 접속으로 인해 피해가 발 생 할 수 있음으로 소셜 네트워크 사이트 내부에서 잘 모르는 사용자가 전송한 단축 URL은 함부로 클릭하지 않는 주의가 필요하다.

따라서, 사이트가드(SiteGuard)와 같은 웹 브라우저 보안 제품과 백신을 시스템에 설치하여 사전에 이러한 보안 위협으로 인한 피해를 사전에 예방하는 것이 중요하다.



AhnLab SiteGuard Pro

2010년 Vol. 02

ASEC REPORT 집필진

편 집 장 선임 연구원 허종오

집 필 진 선임 연구원 정진성
선임 연구원 하동주
선임 연구원 허종오
주임 연구원 박종석
주임 연구원 안창용
연 구 원 하동주

감 수 상 무 조시행

참여연구원 ASEC 연구원
SiteGuard 연구원