ASEC REPORT

VOL.47 | 2013.11

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 11월 보안 동향

악성코드 동향

01. 악성코드 통계

신종 악성코드 기승

ASEC이 집계한 바에 따르면, 2013년 11월에 감염이 보고된 악성코드는 206만 6944건으로 나타났다. 이는 전월 233만 9014건에 비해 27만 2070건이 감소한 수치다([그림 1-1]). 이 중 가장 많이 보고된 악성코드는 Win-Trojan/Patched.kg이었으며, 지난달과 마찬가지로 Textimage/Autorun과 Als/Bursted가 다음으로 많았다. 또한 총 8건의 악성코드가 최다 20건 목록에 새로 이름을 올렸다([표 1-1]).

그림 1-1 | 월별 악성코드 감염 보고 건수 변화 추이

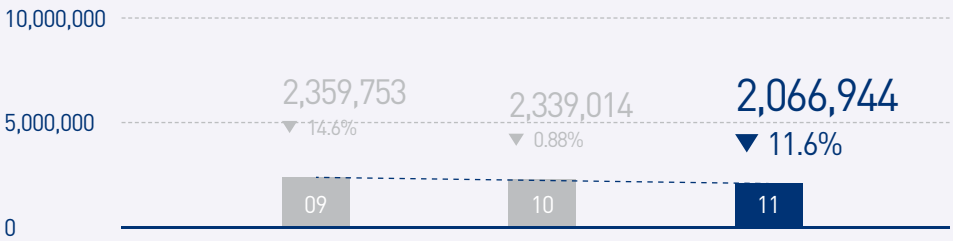


표 1-1 | 2013년 11월 악성코드 최다 20건(감염 보고, 악성코드명 기준)

순위	등락	악성코드명	건수	비율
1	—	Win-Trojan/Patched.kg	308,683	35.5 %
2	—	Textimage/Autorun	85,500	9.8 %
3	—	Als/Bursted	76,855	8.8 %
4	▲1	RIPPER	38,561	4.4 %
5	NEW	Trojan/Win32.fraudl	35,643	4.1 %
6	NEW	JS/Agent	32,586	3.8 %
7	NEW	Trojan/Win32.adh	28,259	3.3 %
8	▼1	Win-Trojan/Wgames.Gen	26,399	3.0 %
9	▲1	Win32/Autorun.worm.307200.F	24,718	2.8 %
10	▲4	Trojan/Win32.onescan	23,864	2.7 %
11	▼3	Trojan/Win32.agent	23,549	2.7 %
12	▼3	Win-Trojan/Agent.21734801	22,165	2.6 %
13	NEW	Trojan/Win32.keygen	20,281	2.3 %
14	NEW	Gif/Iframe	20,038	2.3 %
15	NEW	BinImage/Host	19,553	2.3 %
16	NEW	JS/Decode	19,104	2.2 %
17	▼6	ASD.PREVENTION	16,927	2.0 %
18	▼5	Trojan/Win32.Gen	15,993	1.8 %
19	NEW	Trojan/Win32.wecod	15,855	1.8 %
20	▼4	Win-Trojan/Malpacked5.Gen	15,742	1.8 %
		TOTAL	870,275	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 32만 5335건으로 가장 빈번히 보고된 것으로 조사됐다. Trojan/Win32는 25만 8325건, Win-Trojan/Agent는 11만 3563건을 각각 기록해 그 뒤를 이었다.

표 1-2 | 악성코드 대표진단명 최다 20건

순위	등락	악성코드명	건수	비율
1	—	Win-Trojan/Patched	325,335	24.4 %
2	—	Trojan/Win32	258,325	19.4 %
3	—	Win-Trojan/Agent	113,563	8.5 %
4	—	Textimage/Autorun	85,515	6.4 %
5	—	Als/Bursted	76,855	5.8 %
6	—	Win-Trojan/Onlinegamehack	47,760	3.6 %
7	▲1	Win32/Conficker	44,956	3.4 %
8	▲2	Win32/Autorun.worm	43,334	3.2 %
9	▲3	RIPPER	38,561	2.9 %
10	▲1	Win-Trojan/Downloader	37,781	2.8 %
11	▼2	Adware/Win32	35,782	2.7 %
12	▲2	Win32/Kido	33,663	2.5 %
13	NEW	JS/Agent	32,665	2.4 %
14	▼1	Win32/Virut	32,481	2.4 %
15	—	Win-Trojan/Wgames	26,399	2.0 %
16	—	Backdoor/Win32	22,669	1.7 %
17	NEW	Gif/Iframe	20,038	1.5 %
18	NEW	BinImage/Host	19,553	1.5 %
19	▼2	Win-Trojan/Avkiller	19,396	1.5 %
20	NEW	JS/Decode	19,104	1.4 %
		TOTAL	1,333,735	100.0 %

신종 악성코드, 트로이목마가 96%

[표 1-3]은 11월에 신규로 접수된 악성코드 중 감염 보고가 가장 많았던 20건을 꼽은 것이다. 11월의 신종 악성코드 중 최다는 트로이목마류로, Win-Trojan/Agent.704가 5024건으로 전체의 26.2%, 그 뒤를 이어 Win-Trojan/Agent.704.B가 5168건으로 26.0%를 차지했다.

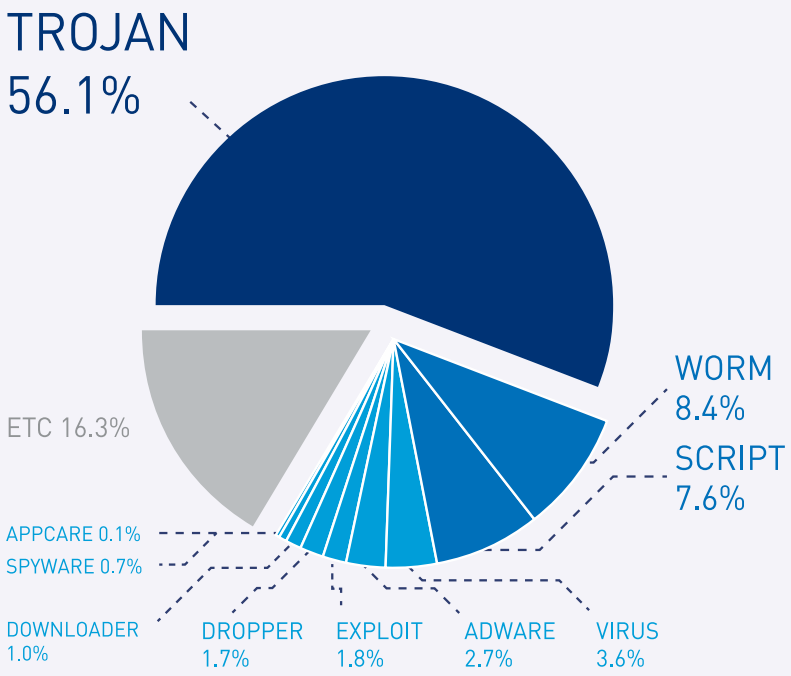
표 1-3 | 11월 신종 악성코드 최다 20건

순위	악성코드명	건수	비율
1	Win-Trojan/Agent.704	5,204	26.2 %
2	Win-Trojan/Agent.704.B	5,168	26.0 %
3	Win-Trojan/Clicker.338896	2,807	14.1 %
4	Win-Trojan/Urelas.426595	1,087	5.5 %
5	Win-Trojan/Agent.71745536	814	4.1 %
6	Win-Trojan/Agent.82610	788	4.0 %
7	Win-Trojan/Stealer.320676	683	3.4 %
8	Win-Trojan/Agent.24576.JPN	483	2.4 %
9	Win-Trojan/Avkiller.65503232	469	2.4 %
10	Win-Trojan/Avkiller.70270976	374	1.9 %
11	Dropper/Onlinegamehack.183700	309	1.6 %
11	Win-Adware/Speedbster.813720	309	1.6 %
13	Win-Trojan/Agent.37888.SP	253	1.3 %
14	Win-Trojan/Vb.253048	223	1.1 %
15	Win-Trojan/Agent.75710464	190	1.0 %
16	Win-Trojan/Clicker.702616	168	0.8 %
17	Dropper/Agent.140759	143	0.7 %
18	Win-Trojan/Morix.86082560	134	0.7 %
19	Win-Trojan/Agent.393728.BM	130	0.6 %
20	Win-Trojan/Agent.704183	128	0.6 %
	TOTAL	19,864	100.0 %

여전히 '트로이목마' 가 강세

[그림 1-2]는 2013년 11월 한 달간 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마가 56.1%로 가장 높은 비율을 나타냈고 웜은 8.4%, 스크립트는 7.6%의 비율을 각각 차지했다.

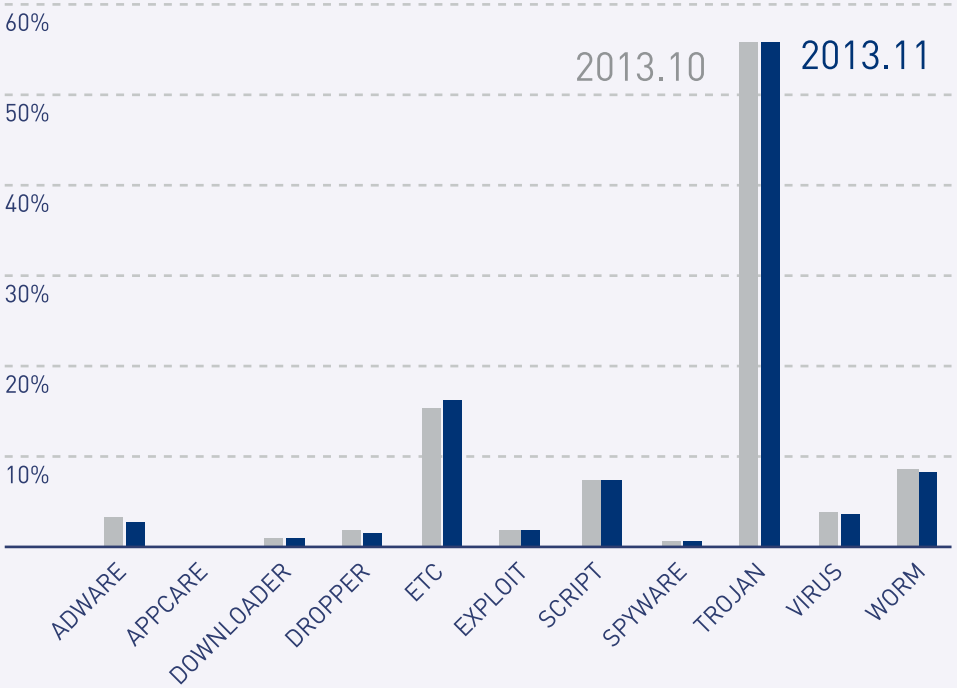
그림 1-2 | 악성코드 유형별 비율



악성코드 유형별 감염보고 전월 비교

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

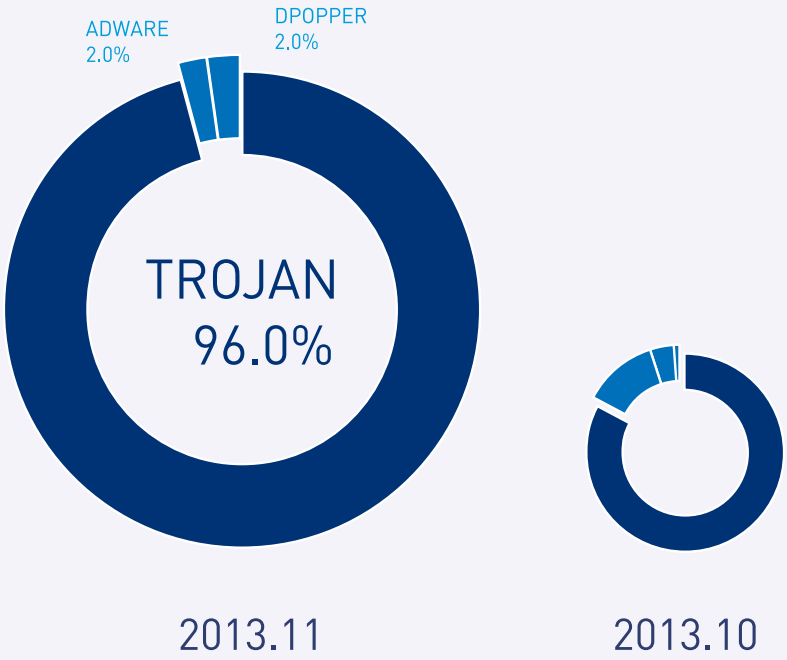
그림 1-3 | 2013년 10월 vs. 2013년 11월 악성코드 유형별 비율



신종 악성코드 유형별 분포

11월의 신종 악성코드를 유형별로 살펴보면 트로이목마가 96%로 가장 많았고 애드웨어가 2%, 드롭퍼가 2%로 각각 집계됐다.

그림 1-4 | 신종 악성코드 유형별 분포



악성코드 동향

02. 악성코드 이슈

PC 내 파일을 암호화하는 랜섬웨어 CryptoLocker

최근 시스템에 저장된 문서, 이미지 파일 등을 암호화하여 금전적 대가를 요구하는 CryptoLocker 랜섬웨어가 발견돼 사용자들의 주의가 요구된다. 이번에 발견된 CryptoLocker 랜섬웨어는 이메일의 첨부 파일을 통해 유포되었으며, 일정 시간이 지나면 암호화 키가 삭제되어 복구할 수 없다는 메시지를 사용자에게 보여준다.

[그림 1-5]는 악성코드 감염 후 사용자에게 나타나는 화면이다. 암호화된 파일 리스트를 확인하는 메뉴와 파일 복구를 위해 300달러를 요구하는 내용을 확인할 수 있다.

그림 1-5 | CryptoLocker 감염 화면

CryptoLocker 랜섬웨어는 시스템에 저장된 워드(Word), 엑셀(Excel), 파워포인트(PowerPoint), 이미지 파일 등 다양한 파일을 암호화한다.

3fr, accdb, ai, arw, bay, cdr, cer, cr2, crt, crw, dbf, dcr, der, dng, doc, docm, docx, dwg, dxf, dxg, eps, erf, indd, jpe, jpg, kdc, mdb, mdf, mef, mrw, nef, nrw, odb, odm, odp, ods, odt, orf, p12, p7b, p7c, pdd, pef, pem, pfx, ppt, pptm, pptx, psd, pst, ptx, r3d, raf, raw, rtf, rw2, rwl, srf, srw, wb2, wpd, wps, xlk, xls, xlsb, xlsm, xlsx

파일 복구 비용으로 300달러를 결제하는 방법 이외에 비트코인으로 결제하는 메뉴도 제공한다([그림 1-6]).

그림 1-6 | CryptoLocker 감염 화면

랜섬웨어에 감염되면 다음과 같은 경로에 악성 파일이 생성된다. 해당 파일은 윈도우 시작 레지스트리 키에 등록되어 부팅 시 자동으로 실행된다.

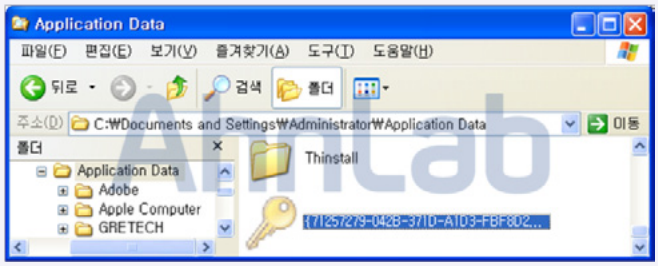


그림 1-7 | 파일 생성 정보

[그림 1-8]은 시스템에서 암호화된 파일을 나타내는 화면이다. 파일은 공개 키 방식으로 암호화되어 있어 제작자 서버에 저장된 개인 키가 없으면 파일을 복구하는 것이 불가능하다. 악의적인 목적으로 제작된 랜섬웨어는 사용자가 복구 비용을 지불하더라도 파일이 정상적으로 복구되지 않을 수 있다.

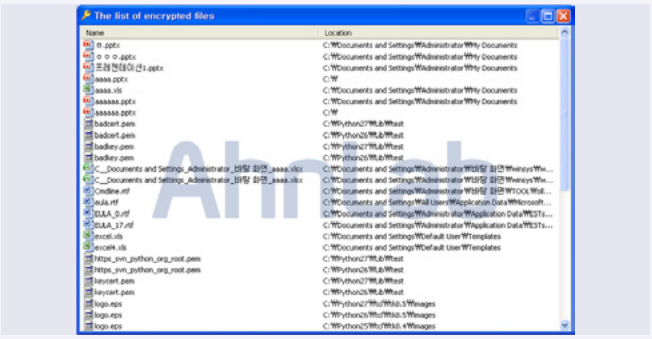


그림 1-8 | 암호화된 파일들

실제로, 암호화된 문서 파일(PPT)을 실행하면 파일이 열리지 않는 것을 확인할 수 있다([그림 1-9]).

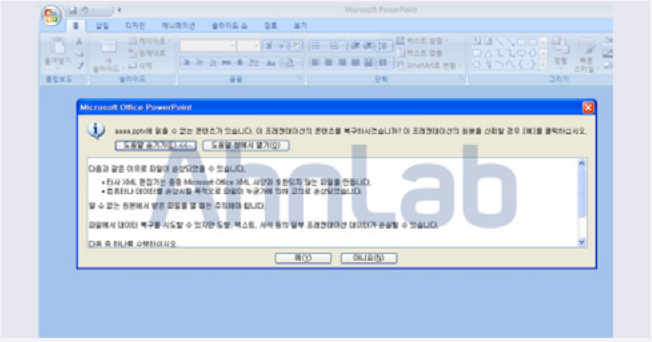


그림 1-9 | 암호화된 파일 실행

CryptoLocker 랜섬웨어에 감염되면 특정 서버(212.**.***.4)로 접속을 시도한다.

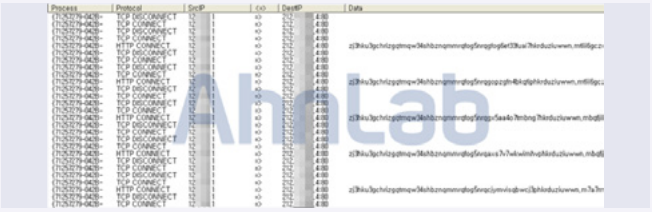


그림 1-10 | 네트워크 연결 정보

최근 랜섬웨어 제작자가 운영하는 것으로 추정되는 CryptoLocker Decryption Service 웹사이트가 확인되었다. 파일 복구를 위해 10BTC(비트코인)을 요구하며, 파일이 정상 복구되는지 테스트 할 수 없었다.

그림 1-11 | CryptoLocker Decryption Service

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

Trojan/Win32.Blocker (AhnLab, 2013.09.23.04)

악성 매크로를 포함한 엑셀 파일

악성코드를 감염시키는 가장 손쉬운 방법은 사회공학적인 기법을 사용하는 것이다. 악성코드를 불법 소프트웨어, MP3, 영화 자료로 속여서 배포하거나 공신력 있는 기관 · 업체로 위장해 악의적인 코드가 담긴 문서를 배포하기도 한다. 이번에 발견된 것은 엑셀 파일로 된 악성코드인데, 악성 매크로가 포함되어 있어 문서를 열어볼 경우 악성코드에 감염된다. 파일 이름은 'payment Pending List.xls' 이며 파일 내부에서 추가로 악성코드를 다운로드 및 저장하는 경로가 확인됐다.

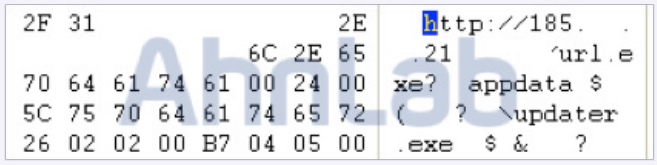


그림 1-12 | 하드코딩된 악성코드 유포 URL

악성 엑셀 파일을 열면 보안 알림 창이 뜨며 매크로를 사용할 것인지 선택하게 한다. 매크로를 포함하여 엑셀 파일을 열면 url.exe 파일을 다운로드 하기 위해 악성코드 유포지로 연결을 시도하지만 현재 해당 파일은 존재하지 않는다.

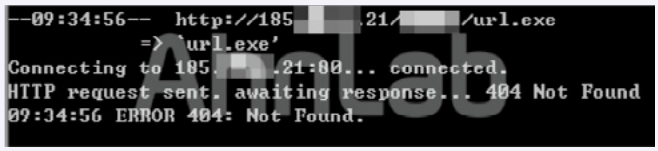


그림 1-13 | 악성코드 유포 사이트 연결 시도

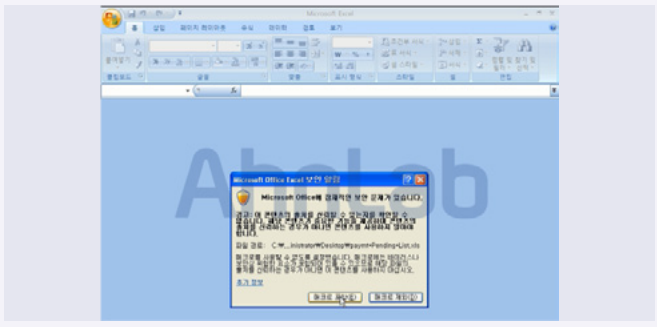


그림 1-14 | 악성 엑셀 파일 실행 화면

악성코드 유포 사이트는 라트비아에 위치한 것으로 확인된다. 현재 악성코드 유포 사이트 경로가 존재하지 않지만 해당 도메인을 통해 지속적인 악성코드 유포가 시도되고 있는 것으로 보인다. 따라서 해당 도메인을 차단해야 하며 급여나 택배, 우편 또는 이력서와 같은 사회공학적 기법에 자주 활용되는 유형의 문서들에 대해서 좀 더 각별한 주의가 필요하다.

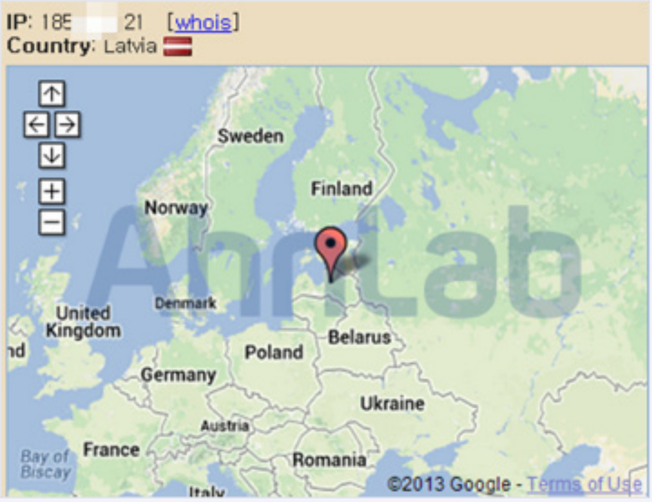


그림 1-15 | 악성코드 유포지

이러한 파일들은 보통 이메일의 첨부 파일로 많이 유포되므로 의심스러운 첨부 파일은 실행하지 말고 안티바이러스 검사를 하고 취약점이 발견된 소프트웨어는 반드시 최신 패치를 설치하여야 한다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
XLS/Downloader (V3, 2013.10.31.00)

USB에 생성되는 '바로가기' 파일

USB에 바로가기 아이콘이 생성된다는 고객들의 문의가 종종 접수되고 있다. USB 바로가기 아이콘을 생성하는 것은 Autorun, VBS 등의 악성코드류인데, 꾸준하게 감염 피해가 보고되고 있다. 가장 흔하게(?) 발견되는 악성코드 중 하나라 할 수 있다.
감염 증상은 주로 'USB에 바로가기 재생성', '바로가기 바이러스' 등이다. 악성코드에 감염되면 [그림 1-16]과 같이 '바로가기' 파일이 생성된다.

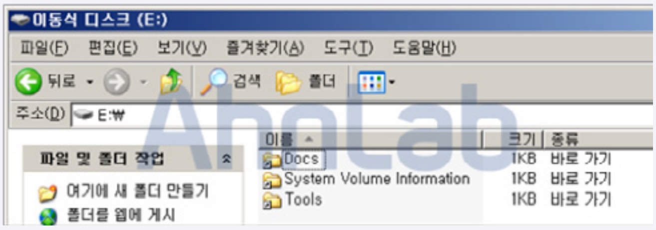


그림 1-16 | 바로가기 파일 생성 증상

이처럼, 윈도우 기본 폴더 속성으로는 바로가기 파일만 보인다. 그렇지만, [그림 1-17]과 같이 폴더 속성을 변경할 경우, 원래의(정상의) 폴더들과 USB 저장매체를 통한 감염체(여기서는 tehwgbroif.vbs) 모두 숨김 속성으로 설정되는 것을 볼 수 있다.

그림 1-17 | 폴더 속성 변경 후 폴더 내용

생성된 바로가기 파일 속성을 확인해보면, [그림 1-18]과 같이 숨김 파일 속성으로 생성된 VBS 파일이 실행되도록 연결된다.

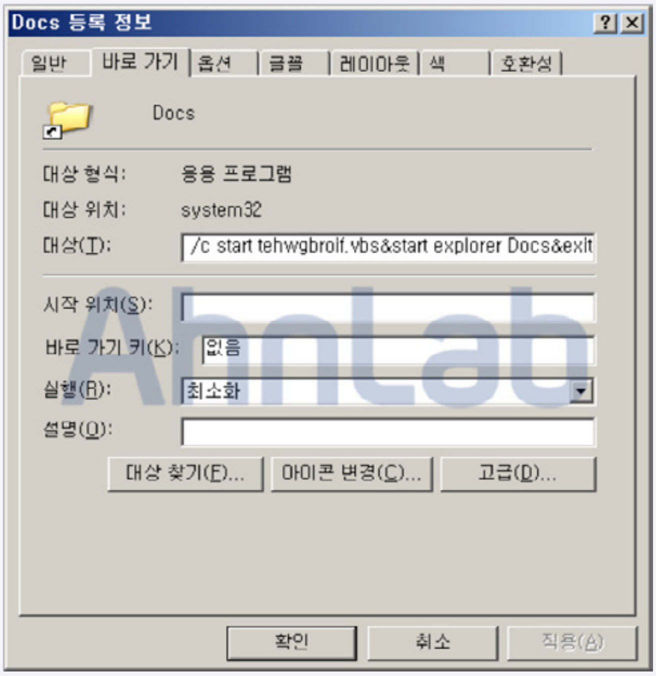


그림 1-18 | 바로가기 파일 속성

VBS 스크립트에 감염되면, 시작프로그램에 악성 VBS 파일을 생성하고 연결된 외장 저장매체에 바로가기 파일을 지속적으로 생성한다.

그림 1-19 | 파일 변화

그리고 레지스트리 "HKCU₩Software₩₩Microsoft₩₩Windows₩₩CurrentVersion₩₩Run" Key에 등록하여 시스템 재시작 시 자동으로 실행되며 폴더 속성을 변경한다.

그림 1-20 | 레지스트리 변화

또한, 이라크(iq)에 존재하는 특정 서버로 연결을 계속 시도하나, 확인 당시에는 연결되지 않았다.

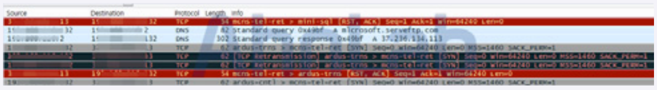


그림 1-21 | 네트워크 연결

디코딩된 스크립트 코드를 보면, [그림 1-22]와 같이 특정 서버로 연결하기 위한 네트워크 설정 정보가 확인된다.

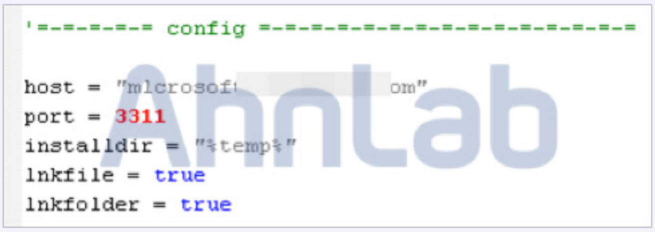


그림 1-22 | 네트워크 설정 정보

그리고 내부에는 [그림 1-23]과 같이 관련 스크립트가 동작할 것으로 보이는 다양한 실행 명령들이 보인다.

그림 1-23 | 실행 명령으로 보이는 일부 코드 정보

참고로, 이러한 부류의 악성코드는 진단 · 치료를 수행하더라도, 생성된 바로가기 파일 삭제 및 숨겨진 파일에 대한 설정은 변경되지 않는다.

따라서, 치료를 수행한 이후에는 파일의 종류가 '바로가기'인 파일을 수동으로 삭제하고, 숨김 속성으로 설정된 폴더 및 파일은 ASEC 블로그 내용(http://asec.ahnlab.com/171 4. 치료 후 폴더 복원 방법)을 참고하여 조치해야 한다.

V3 제품에서는 아래와 같이 진단이 가능하다.

<V3 제품군의 진단명>
VBS/Agent (2013.11.13.00)

MS 오피스 제로데이 취약점(CVE-2013-3906) 주의

지난 11월 5일 MS는 윈도우 오피스, 링크 제품에 영향을 미치는 제로데이 취약점(CVE-2013-3906)에 대한 보안 권고문을 발표하였다. 악성 TIFF 이미지 파일이 삽입된 오피스 파일, 이메일, 웹 페이지 등을 사용자가 실행할 경우 악성코드에 감염될 수 있다. 현재 MS에서 CVE-2013-3906 취약점에 대한 보안 패치를 제공하고 있다.

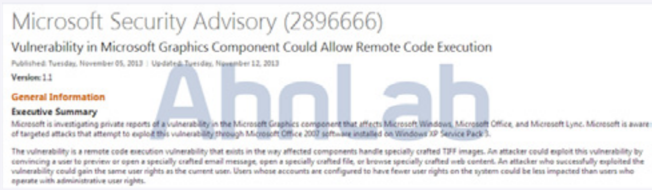


그림 1-24 | Microsoft 보안 권고

실제로 CVE-2013-3906 취약점을 이용한 공격 사례가 보고되었으며 변종 악성코드가 유포되고 있다. [그림 1-25]는 악성코드 유포에 사용된 메일을 나타내는 화면이다. 이 메일의 첨부 파일에는 2가지 취약점(CVE-2013-3906, CVE-2012-0158)을 이용하는 악성코드가 각각 첨부되어 있다.

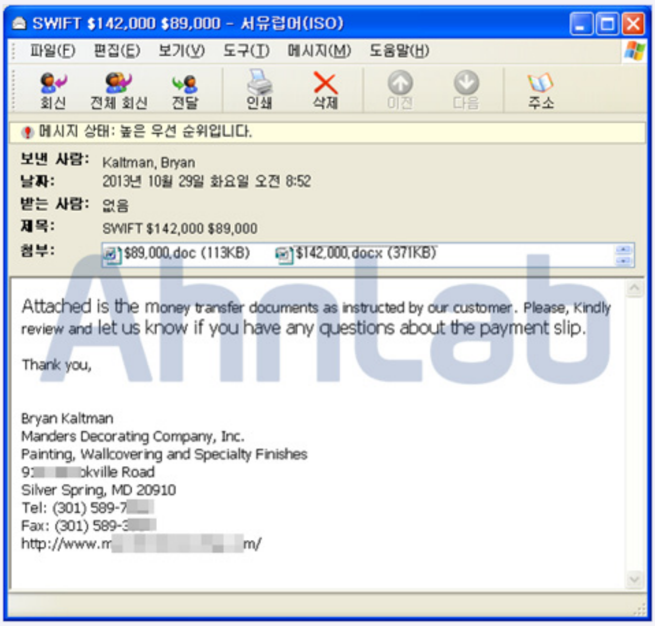


그림 1-25 | 악성 이메일

CVE-2013-3906 취약점을 이용하는 워드 문서를 분석해보면 다수의 ActiveX와 공격코드에 존재하는 악성코드 다운로드 URL 정보를 확인할 수 있다.

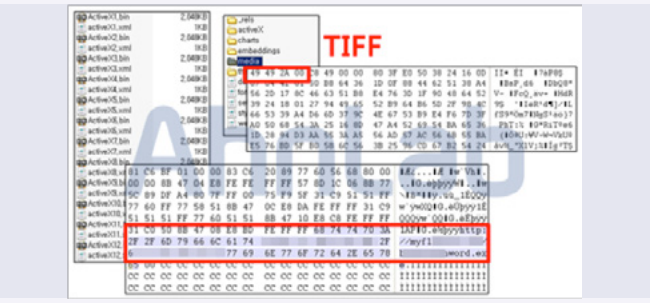


그림 1-26 | 워드 파일 내부의 공격코드

취약점을 통해 실행되는 악성코드(winword.exe)는 WINRAR SFX 파일로 ISI.doc 워드 문서와 Updates.exe 악성코드를 내부에 포함하고 있다.

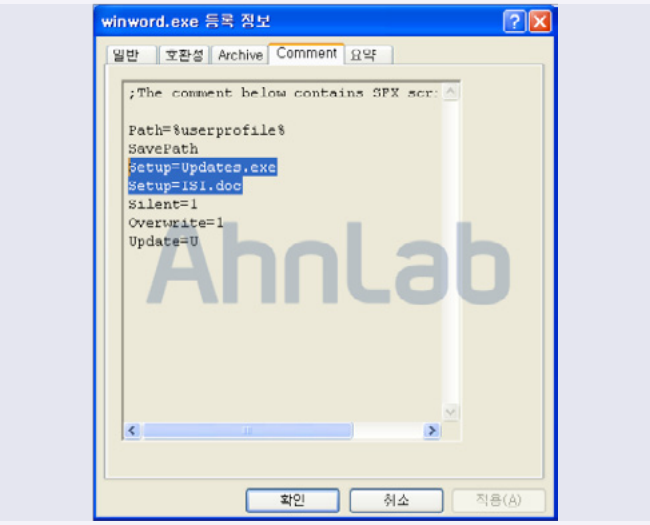


그림 1-27 | winword.exe 악성코드

해당 악성코드(winword.exe)가 실행되면 사용자가 악성코드에 감염된 것을 인지할 수 없도록 정상 워드 문서(ISI.doc)가 실행된다.

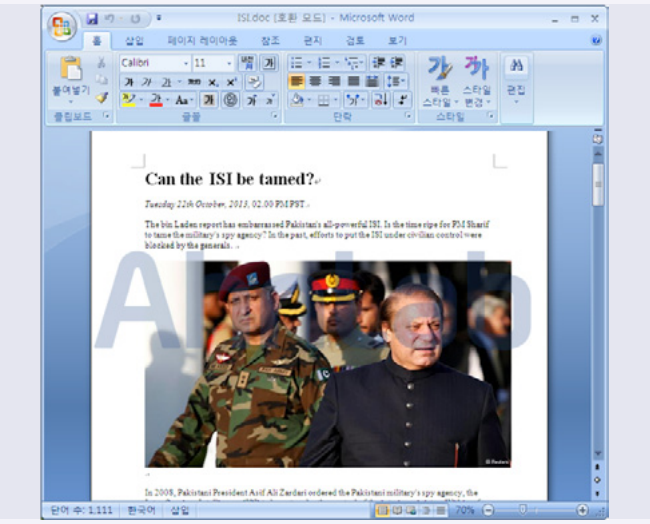


그림 1-28 | 워드 문서 실행 화면

워드 문서 파일(ISI.doc)이 로딩되는 동안 백도어 악성코드(Updates.exe)가 함께 실행되며 윈도우 시작 시 자동 실행되도록 시작프로그램에 등록된다.

그림 1-29 | 파일 생성 정보

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Exploit/Cve-2013-3906 (2013.11.07.02)
RTF/Cve-2012-0158 (2013.11.09.00)
DOC/Agent (V3, 2013.11.13.00)
Trojan/Win32.Agentb (2013.11.12.00)

새터민 자기소개서로 위장한 악성 한글 파일 출현

새터민의 자기소개서로 위장한 악성 한글 파일이 발견되었다. 이러한 파일들은 스피어 피싱으로 사용하려고 제작되었을 것으로 판단된다. 해당 악성 한글 파일이 실행되면 아래 경로에 dll 파일이 생성된다. 또한, 정상 한글 파일을 만들어 보여주어 사용자가 감염 사실을 깨닫지 못하도록 한다.

[생성되는 파일]
C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩V3I.kor

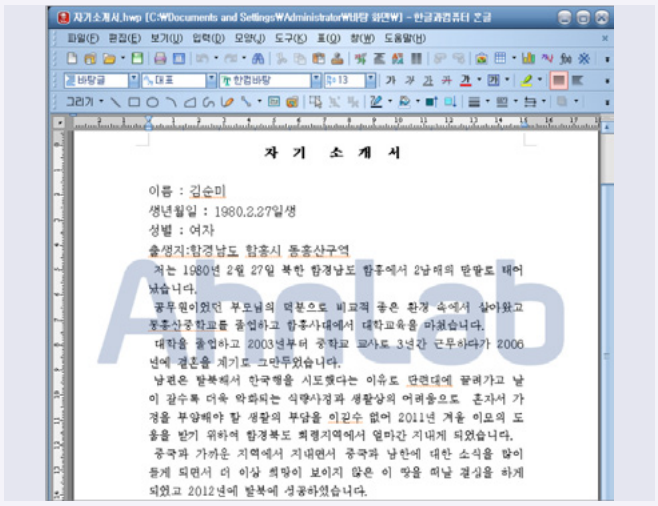


그림 1-30 | 새터민 자기소개서로 위장한 악성 한글 파일

C:₩HNC₩Hwp70 경로에 랜덤한 8자리 숫자와 영문 조합의 gif 파일이 생성된다. 해당 파일은 이미지 파일이 아니며 탈취할 정보를 저장하기 위해 생성한 파일이다. 탈취한 정보는 아래와 같다.

- 프로세스 목록
- 사용자 네트워크 구성 정보
- 환경 변수

또한 '*.hwp, *.doc, *.docx, *.xls, *.xlsx' 와 같은 문서 파일들을 수집해 외부로 유출하는 기능도 있다. 수집된 gif 파일은 일본에 위치한 시스템으로 전송한다. 수집된 시스템 정보를 통해 추가 공격이 이루어질 것으로 예상된다.

이러한 공격과 감염을 예방하기 위해서는 출처가 불분명한 메일의 첨부 파일은 안티바이러스 제품으로 검사하거나 사전에 분석을 의뢰해야 한다. 또한, 실제 발신자에게 확인 요청을 한 후 열람해야 한다. 운영체제뿐만 아니라 애플리케이션 취약점도 공격에 자주 이용되므로 애플리케이션 보안 패치도 최신으로 유지하는 것이 좋다.

그림 1-31 | 정보 유출 시도

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
HWP/Exploit (2013.11.14.00)
Trojan/Win32.XwDoor (2013.10.07.04)

신용카드 명세서로 위장한 악성코드 변종 유포

신용카드 명세서로 위장한 악성코드 변형이 이메일을 통해 유포되었다. 지난 4월에 보고된 후 10월 30일에 악성코드 변형이 ASD 클라우드 서버에 수집되었다. 이후 파일 이름만 변경되어 11월 15일에도 이메일로 유포된 것으로 보고되었다.

*******20131115_04922.zip 압축 파일이 메일에 첨부되었으며, 압축 파일을 풀면 [그림 1-32]와 같이 html 파일로 위장한 exe 파일을 볼 수 있다.

그림 1-32 | 압축 해제된 파일

파일 이름과 확장자 사이에 공백과 점(period) 문자를 다수 포함해 실제 카드 명세서 파일인 html 파일로 오인해서 실행하도록 유도한다.

[파일명]
*******card_20131115_53430.html .....
.....HTML.exe

또한, 해당 파일 실행 시 [그림 1-33]과 같이 실제 카드 명세서 페이지가 나타나게 하여 사용자가 악성코드 감염을 알지 못하도록 한다.

그림 1-33 | 가짜 신용카드 명세서

파일을 실행하면 아래와 같은 파일을 생성하고, 시스템을 시작할 때 자동 실행되도록 레지스트리에 등록한다.

[파일 생성]
C:₩Windows₩System32₩mshelp.htm (정상)
C:₩Windows₩System32₩msimbc.dll
C:₩Windows₩System32₩ruby.exe
C:₩Windows₩System32₩csdujwsxo.dll (랜덤 파일명)
C:₩Windows₩System32₩mshytvjiil.ocx
C:₩Windows₩System32₩mstedgakl.dll
C:₩Windows₩System32₩yqixm.dll (랜덤 파일명)
C:₩Windows₩System32₩anotggnk.dll

[레지스트리 등록]
[HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩GomPlaySvr₩Parameters]
ServiceDll="%SystemRoot%₩System32₩csdujwsxo.dll"
[HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩VbSecurity₩Parameters]
ServiceDll="%SystemRoot%₩System32₩yqixm.dll"

위와 같이 서비스로 등록된 레지스트리는 은폐되어 레지스트리 편집기에서는 보이지 않으며, [그림 1-34], [그림 1-35]와 같이 루트킷 탐지 툴인 Gmer에서 확인이 가능하다.

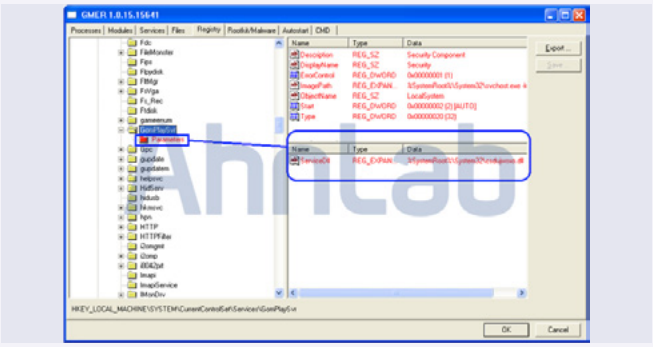


그림 1-34 | 은폐된 레지스트리 내용(GomPlaySvr)

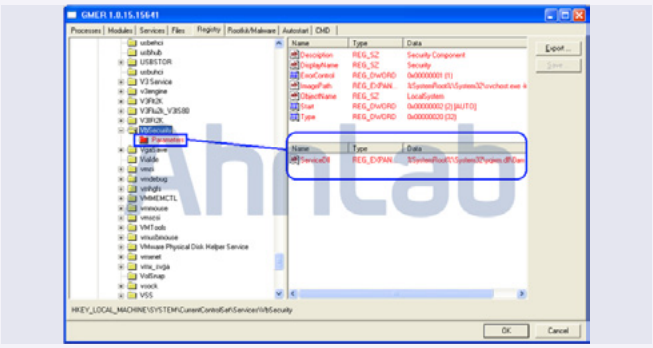


그림 1-35 | 은폐된 레지스트리 내용

생성된 파일 중 mshelp.htm 파일은 신용카드 명세서이고, msimbc.dll 파일은 mshytvjiil.ocx 파일과 동일하며, mstedgakl.dll, anotggnk.dll 또한 같은 파일이다.

각각의 mshytvjiil.ocx, anotggnk.dll 파일은 *******card_20131115_53430..{생략}.exe 파일 실행 시 아래 URL에서 다운로드 되는 arp-ping.exe 파일과 setup_482.exe 파일이다.

hxxp://www.eli******son.com/p******s/downloads/arp-ping-0.3/arp-ping.exe
hxxp://neir***.fuzh****ng.com/setup_482.exe

arp-ping 파일은 [그림 1-36]과 같은 옵션으로 구성되어 있다.

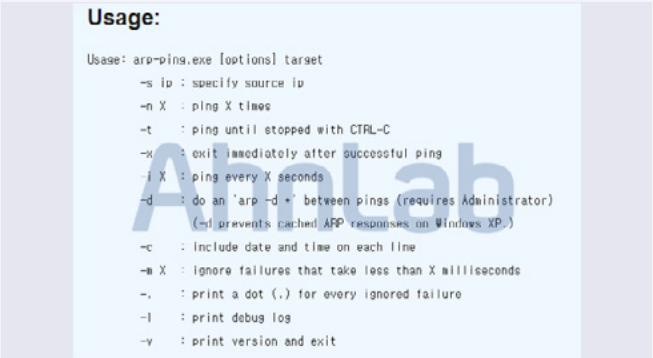


그림 1-36 | arp-ping.exe 옵션

arp-ping.exe 파일은 공격자가 내부 네트워크에 위치한 시스템 상태 확인 등에 악용할 수 있다. [그림 1-37] 같이 setup_482.exe 파일은 중국에서 제작된 인터넷 검색, 스크린 샷, 알림 및 PC 종료 타이머 기능 등을 제공하는 PUP와 같은 프로그램 설치 파일이다. 다만 이 설치 파일은 악성코드 감염 시 설치되지는 않는다.

그림 1-37 | www.fuchengyule.com에서 배포하는 프로그램

yqixm.dll 파일은 윈도우 방화벽에 UDP:135, TCP:3306 포트에 대해서 예외 설정을 한다.

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

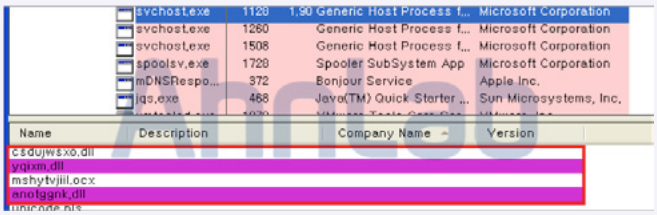


그림 1-38 | svchost.exe 프로세스에 로드된 모듈

211.2**.2**.1**:25 (KR)
221.**4.8.***:443 (KR)
218.1**.1**.1**:137 (KR)
175.**3.3*.2**:137 (KR)
61.**.84.**:23 (KR)
61.**.84.**:8998 (KR)
61.**.84.**:303 (KR)

이외 다수의 GIF, JPEG 포맷의 이미지 파일을 다운로드 하지만, 대부분 정상 파일이고 일부 손상된 파일이 포함되어 있었다. 이후 해당 사이트에서 악성 파일로 변경될 수 있을 것으로 추정된다.

신용카드 명세서는 국내 실정에 맞춰 정상 파일과 구분하기 어렵도록 정교하게 제작되기 때문에 메일에 첨부된 파일을 실행할 때는 각별히 주의해야 한다.

V3 제품에서는 아래와 같은 진단이 가능하다.

〈V3 제품군의 진단명〉

Trojan/Win32.Downloader (2013.11.20.03)

Unwanted/Win32.Arptool (2013.11.20.03)

Trojan/Win32.Iroffer (2013.02.27.05)

Trojan/Win32.Downloader (2013.11.20.05)

Win-Trojan/Agent.464168 (2013.11.20.04)

Trojan/Win32.Agent (2013.11.20.05)

가짜 음성 메시지가 첨부된 악성 스팸 메일 등장

많은 회사가 비용 절감을 위해 인터넷 전화를 도입하고, 협업 강화를 위해 음성 통화, 영상 통화, 인스턴스 메시지, 메일, 음성 사서함 등 다양한 커뮤니케이션 도구가 제공되는 UC 솔루션을 활용하고 있다. UC 솔루션의 음성 사서함 기능을 악용한 것으로 보이는 가짜 음성 메시지, 즉 악성코드가 이메일에 첨부돼 유포되고 있는 것이 최근 확인되었다.

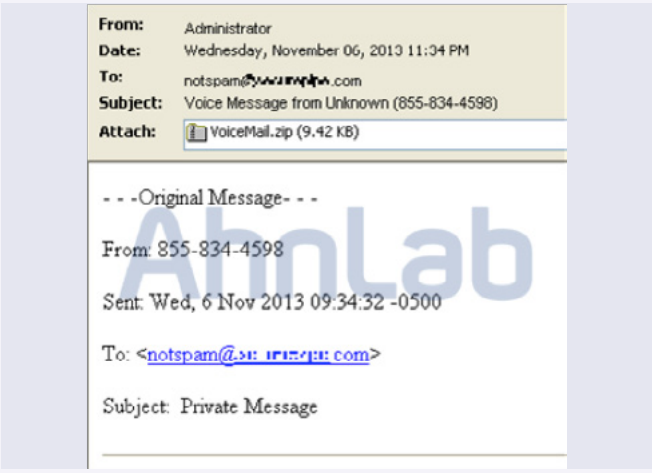


그림 1-39 | 가짜 음성 메시지가 첨부된 메일 원문

메일 제목은 "Voice Messae from Unknown (전화 번호)" 형태로 발송되는데, 발신인과 수신인의 메일 도메인이 동일하기 때문에 내부 메일로 오인할 수 있다.

메일 서버 IP를 사설 IP로 메일 헤더를 조작하여 내부에서 발송된 메일로 보이도록 했다.

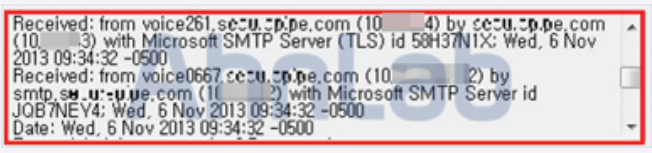


그림 1-40 | 조작된 메일 헤더 정보

해외 보안 블로그(http://blog.dynamoo.com)에 따르면 이러한 가짜 음성 메시지가 첨부된 메일이 지난 10월 23일부터 유포되고 있다. 이후에도 이 같은 형태로 유포되는 다양한 메일이 발견되고 있다.

그림 1-41 | 압축 해제한 첨부 파일

파일을 실행하면 아래와 같은 파일을 생성하고, 시스템 시작 시 자동 실행되도록 레지스트리에 등록한다.

[파일 생성]
C:₩Documents and Settings₩Administrator₩Local Settings₩Temp₩budha.exe
C:₩Documents and Settings₩Administrator₩Local Settings₩Temp₩kilf.exe
C:₩Documents and Settings₩Administrator₩Application Data₩lsoq₩zuryyw.exe

[레지스트리 등록]
[HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Run]
"Zuryyw"="C:₩Documents and Settings₩Administrator₩₩Application Data₩lsoq₩zuryyw.exe"

각 파일에 대한 생성 과정은 다음과 같다.

- VoiceMail.exe 파일이 budha.exe 파일 생성
- Budha.exe 파일이 아래 파일 다운로드
  hxxps://twitter****links.com/wp-con***t/uploads/2011/01/****USA-dt.exe
- 다운로드 된 ml06USA-dt.exe 파일이 자기 자신을 kilf.exe 파일로 생성
- kilf.exe 파일이 zuryyw.exe (랜덤 파일명) 파일 생성

zuryyw.exe 파일은 백도어로 동작하기 위해 윈도우 방화벽에 UDP:6505, TCP:3172 포트에 대해서 예외 설정을 하고, 정상 윈도우 시스템 파일인 explorer.exe 프로세스에 인젝션 되어 아래 C&C 서버로 추정되는 IP로 계속 접속을 시도한다.

217.**.80.**:3521
94.2**.1**.74:9386
31.**.84.1**:9966
46.*.1**.89:14631
195.1**.76.1**:4092
69.1**.162.**:8573
195.2**.149.**0:3642
81.**.213.**:3250
88.1**.4.**:5911
82.2**.169.**8:9129
203.**3.**.34:80

분석 당시 해당 C&C 서버에 정상적으로 접속되지는 않았지만, 해당

악성코드에 감염된 고객 피해 시스템에서 추가 악성코드가 감염된 정황을 확인하였다.

추가로 발견된 악성코드는 FTP 클라이언트 및 메일 클라이언트 등에 저장된 계정 정보를 탈취하는 악성코드와 특정 사이트 접속을 위한 다수의 DNS 쿼리와 메일 서버 접속에 따른 SMTP 트래픽을 유발하는 증상이 나타났다.

음성 메시지로 위장한 악성코드가 첨부된 메일은 내부에서 발송된 메일인 것처럼 메일 헤더를 조작하기 때문에 더욱 주의가 필요하다.

〈V3 제품군의 진단명〉
Downloader/Win32.Agent (2013.11.08.00)
Win-Trojan/Agent.409600.FE (2013.11.08.00)

동영상 파일로 위장한 악성코드

최근 국내 한 기관에서 특정 동영상 파일로 위장한 악성코드가 접수되었다.

사용자가 다운로드 한 특정 파일이 유명 동영상 재생 프로그램에서 실행 가능한 ASF 형태의 파일 아이콘으로 위장하고 있었다. 이에 사용자는 별다른 의심 없이 동영상 파일로 판단하고 실행한 것이다.

하지만, 숨겨진 확장자 설정을 변경하여 확인해보면 ASF 확장자가 아닌 윈도우 실행 파일 형태인 EXE 파일임을 알 수 있다.

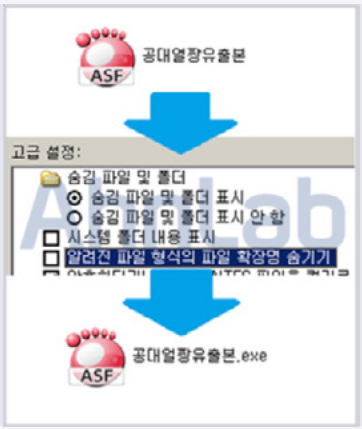


그림 1-42 | 숨겨진 파일 확장자 확인

파일 실행 시 아래와 같이 파일들이 생성되고 실행된다.

```
C:₩서든어택월핵.exe
C:₩도곡동 연하녀 유출본.avi
C:₩WINDOWS₩XXXXXX18F60802.exe
```

생성되는 파일 중 진짜 동영상 파일(도곡동 연하녀 유출본.avi)도 포함하고 있으며, 파일 실행 시 해당 동영상 파일도 함께 실행되므로 사용자는 악성코드 감염에 대해 의심하지 않을 것이다.

```
HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run
" XXXXXX18F60802"  = "C:₩WINDOWS₩XXXXXX18F60802.exe"
```

또한, 지속해서 특정 도메인으로 접속을 시도하며, 추가 파일을 다운로드 하여 실행한다.

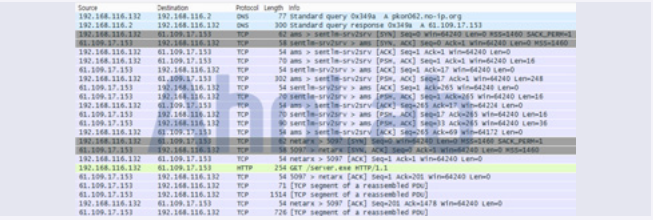


그림 1-43 | 네트워크 연결 로그

이같이 불건전한 동영상 파일로 위장한 악성코드는 지속적으로 유포되고 있으며, 악성코드의 감염 경로로 이용되고 있다.

개인과 회사의 자산을 안전하게 보호하기 위해서 보안의식을 가지고 조금 더 주의할 필요가 있겠다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Downloader/Win32.Generic (2013.11.19.01)
Trojan/Win32.Agent (2013.11.21.04)
Win-Trojan/Cson.179181 (2013.11.25.03)

이력서 문서 파일로 위장한 실행 파일

이력서 파일로 위장한 악성코드가 발견되었다. 이번에 발견된 악성코드는 MS 오피스 워드 문서 아이콘을 사용하지만 확장자가 EXE이다.

그림 1-44 | MS 워드 문서 파일로 위장한 실행 파일

악성코드를 실행하면 정상적인 문서(XXX_XXX_XXX.doc)가 나타나기 때문에 악성코드에 감염된 것을 사용자가 인지하기 어렵다.

그림 1-45 | 이력서 문서 파일 내용

워드 문서가 실행되는 동안 악성코드(Pack_87server.exe)가 함께 생성되며 윈도우 시작 시 자동 실행되도록 시작 레지스트리에 등록된다.

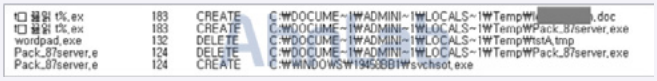


그림 1-46 | 파일 생성 정보

[그림 1-47]은 윈도우 시작 레지스트리에 등록된 악성코드(svchsot.exe)를 나타내는 화면이다.

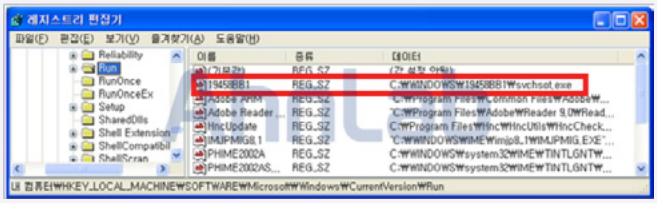


그림 1-47 | 시작 레지스트리에 등록된 악성코드

또한, 매시간 동작하도록 윈도우 예약 작업에도 등록된다.

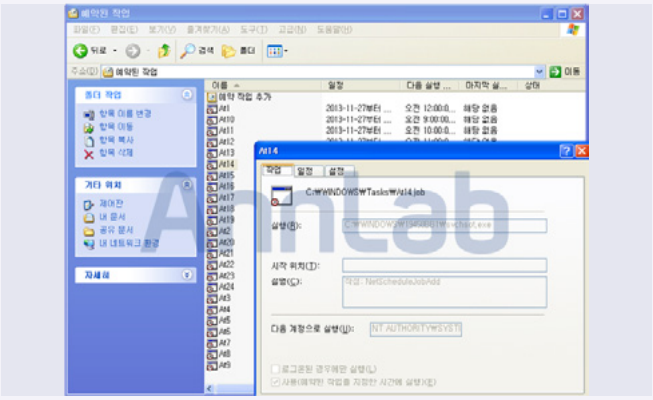


그림 1-48 | 예약 작업에 등록된 악성코드

해당 악성코드는 사용자의 키보드 입력 정보를 수집하여 system32 폴더 하위의 특정 파일에 저장한다.

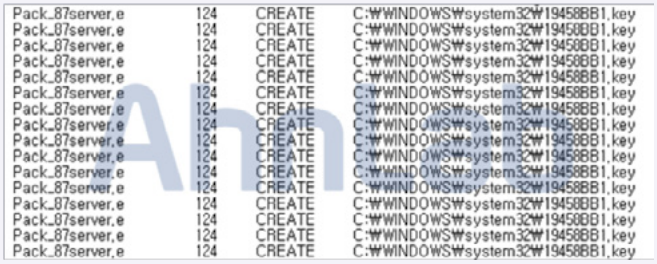


그림 1-49 | 파일 생성 정보

해당 악성코드는 주기적으로 특정 C&C 서버에 연결을 시도하며 이를 통해 정진옥보 유출 및 추가 위협이 발생할 수 있다.

그림 1-50 | 네트워크 연결 정보

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

Trojan/Win32.QQPass (AhnLab, 2013.11.21.00)

악성코드 동향

03. 모바일 악성코드 이슈

정상 앱을 가장한 광고 앱 주의

요즈음 ' 스미싱' 형태의 악성 앱이 다수 발견되고 있다. 특히 서드 파티 마켓에 업로드 된 악성 앱을 조심해야 한다.

최근 인기 있는 앱으로 둔갑한 악의적 앱이 적지 않다. 이러한 앱들 중에 한 가지를 살펴보면 다음과 같다.

그림 1-51 | 정상 앱을 가장한 광고성 앱

[그림 1-51]은 게임 앱으로 가장하였지만, 정상 앱과 다르게 광고가 포함되어 있다. '1' 은 앱의 아이콘이며 '2' 는 앱을 설치한 다음 수시로 팝업되어 나타나는 아이콘이다.

해당 앱 설치 시에 광고에 대한 안내는 찾아볼 수 없었다. 하지만 앱을 사용하고 있지 않고 다른 작업을 하는 중에도 광고가 나타난다.

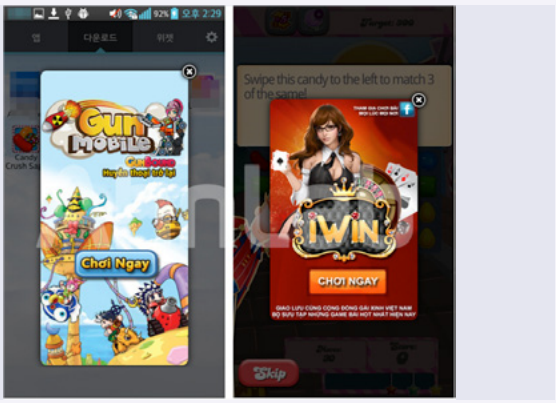


그림 1-52 | 광고 팝업 화면

무심코 광고를 클릭하면 apk(앱) 파일이 다운로드 되어 원하지 않는 데이터 비용이 발생할 수도 있다.

그림 1-53 | 광고 클릭 후 apk 다운로드

사용자가 원하지 않는 바로가기를 생성하기도 한다.

그림 1-54 | 바로가기 생성

이러한 앱은 대부분 정상 앱과 비교하여 다수의 권한을 요구한다.

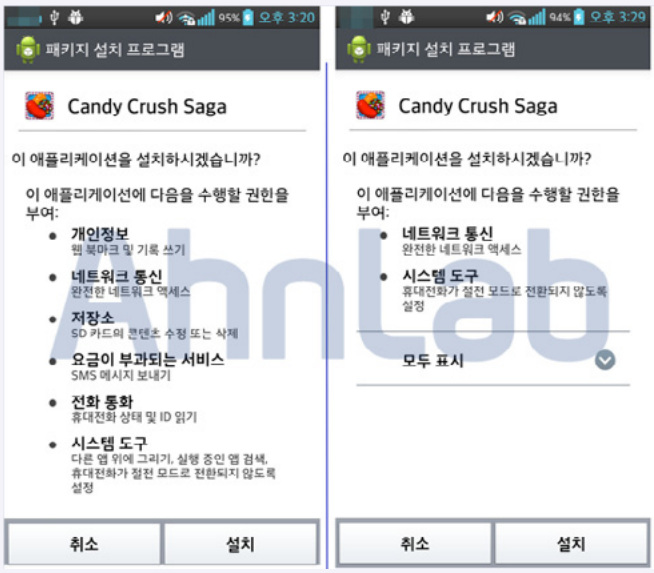


그림 1-55 | 악성 앱(왼쪽) / 정상 앱(오른쪽)

스마트폰 사용자는 안정성이 확인되지 않은 apk(앱)을 다운로드 하지 않아야 한다. 앱 설치는 반드시 공식 마켓을 이용하고, 제작사 및 사용자 평판을 확인하고 설치하는 습관이 중요하다.

신뢰할 수 있는 기업의 웹사이트로 위장한 모바일 사이트

초기 스미싱을 이용해 전파하는 악성 앱은 문자의 내용으로 URL을 클릭하게 해 자동으로 파일이 다운로드 되는 것을 유도했지만, 최근에는 정상으로 보이는 웹페이지를 구축해 사용자들을 안심시킨 후 악성 앱을 배포하는 기법도 함께 사용되고 있다.

지난 11월 AhnLab V3 Plus 모바일 사이트로 꾸민 URL을 포함하는 스미싱 메시지가 전파되었다. "강남 한복판 칼부림 20대 여성 4명 사망 설치 후 열기 http://ahn**ab.kr" 라는 스미싱 메시지에 포함된 URL을 클릭하면 악성 앱 ' App.apk' 가 다운로드 되고, AhnLab V3 모바일 안티바이러스 배포 사이트로 가장한 웹페이지가 나타난다.

안랩에서 제공하고 있는 모바일 트랜잭션 보안 솔루션은 'AhnLab V3 Plus' 인데, 악성 웹페이지는 'AhnLab V3+ Plus Mobile' 이라는 제품명으로 사용자를 교묘하게 속였다.

가짜 AhnLab V3 Plus 모바일 사이트는 2개의 페이지로 이루어져 있으며, 설명서 보기라는 버튼을 누르면 11월 공지사항과 함께 모바일 백신 설치 매뉴얼을 보여주면서 악성 앱 설치를 유도한다.

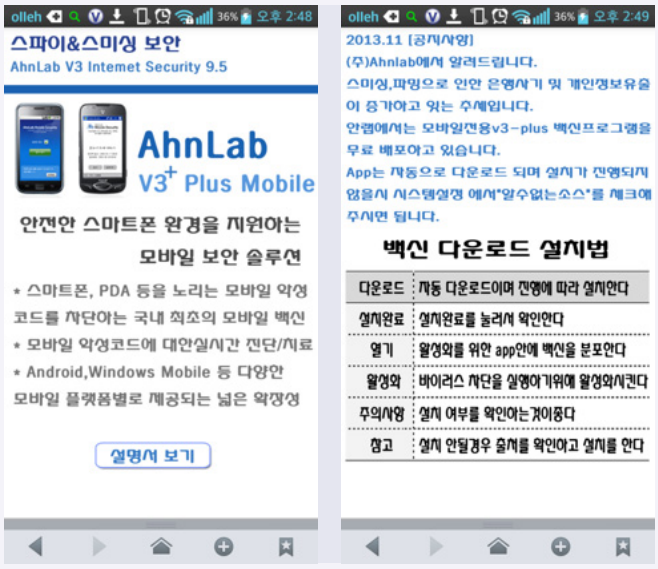


그림 1-56 | AhnLab V3 Plus 모바일 사이트로 위장한 허위 사이트

한편, 과거 PC에서 유행하던 것과 마찬가지로 가짜 안티바이러스 사이트를 통해 앱을 배포하는 형태도 확인되었다. 스마트폰을 이용해 웹서핑 중 광고나 피싱 URL을 클릭해 가짜 안티바이러스 사이트로 접속되면, 허위 감염 메시지를 보여주면서 사용자에게 불안감을 조성해 앱 설치를 유도하는 것이다. 테스트 시 확인된 최종 다운로드 앱은 악의적인 기능을 포함하지 않았다. 하지만, 악성코드 제작자가 동일한 방법을 이용해 악성코드를 배포할 수도 있기 때문에 스마트폰 사용 시 주의가 필요하다.

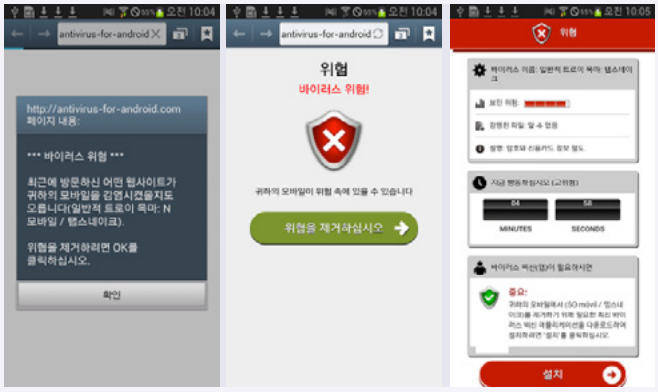


그림 1-57 | 안티바이러스 앱으로 위장한 악성 앱

음란 페이지로 가장해 모바일 악성 앱 배포

스미싱 메시지에 포함된 URL이 통해 음란 사이트를 가장한 웹페이지로 접속을 유도해 모바일 악성 앱을 배포하는 사례가 확인되었다. [그림 1-58]처럼 내용이 확인되지 않은 스미싱 메시지에 포함된 URL을 클릭하면 좌측 화면의 웹사이트가 실행되고, 곧 중앙의 신규 가입 페이지가 출력된다. 사용자이름, 주민등록번호, 휴대폰번호를 입력하고 실명인증을 진행하면 우측 다운로드 페이지로 연결되면서 악성 앱이 다운로드 된다.

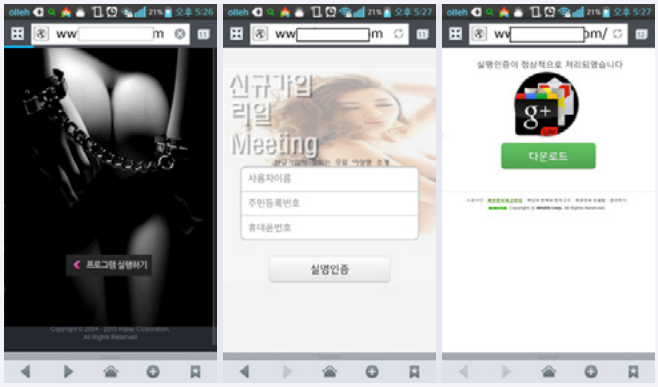


그림 1-58 | 스미싱 메시지를 통해 유포된 음란 사이트에서 배포한 악성 앱

[그림 1-59]는 악성 앱을 배포하는 사이트의 소스코드이다. 입력된 데이터를 체크해 데이터가 존재하면 특정 사이트로 전달하고 파일을 다운로드 한다. 분석 시점에 파일 다운로드는 되지 않도록 변경되어 있었다.

그림 1-59 | 악성 사이트의 소스코드

웹서핑 중 자동으로 다운로드 되는 앱

지난 11월, 알 수 없는 앱이 안드로이드 스마트폰을 이용해 웹서핑 중 자동으로 다운로드 되는 일이 있었다. 안랩에서 서비스하고 있는 '안전한문자'로 수집한 앱 배포 URL을 분석한 결과, 5일간 96개의 URL을 통해 mobogenie_1501.apk이 다운로드 된 것이 확인되었다.

포털 사이트에 ' mobogenie_1501.apk' 라는 파일명으로 검색하면 수많은 사람들이 웹서핑 중 앱이 자동으로 다운로드 되는 것을 경험했음을 알 수 있다.

[그림 1-60]은 안전한 문자에 의해 수집된 mobogenie_1501.apk 배포 URL과 국내 포털 사이트에서 파일명으로 검색한 결과이다.

그림 1-60 | 포털 사이트 검색 결과

그림 1-61 | 안랩 '안전한문자'에 의해 수집된 Mobogenie 배포 사이트 목록

이것은 Mobogenie에서 의뢰한 마케팅 파트너사에 의해 행해진 일이다. 마케팅 파트너사는 제작사의 앱 홍보를 위해 다양한 사이트에서 앱이 자동으로 다운로드 되도록 했다. 이로 인해 수많은 사람들이 웹사이트 서핑 중 Mobogenie 앱을 다운로드 하게 되었다. 이 사건으로 Mobogenie 제작사는 웹사이트에 사과문을 게재하고 공식 마켓을 통해서만 앱을 다운로드 할 것을 공지했다.

We have been made to understand that some of our users have been inconvenienced by the automatic download of Mobogenie on to their PCs. While it has never been our intention to spam any user, we would like to apologise to them for the same. Having learnt that there was a technical issue with one of our promotional arms, we have tried our best to fix it at the earliest possible.

Team Mobogenie keeps a close tab on all its promotions, and recommends the download of the Mobogenie application only from reliable sources such as Google Play, Mobogenie.com and other partner networks. We ensure that there shall be no more inconvenience caused to any Android user in future.

If you face this problem or anything similar again, please do report it with the following:

1. A screenshot of the site you are visiting
2. A website / app / popup that forced you to install Mobogenie automatically
3. Any other method that you suspect made you install Mobogenie

Write in to us at support@mobogenie.com. We also welcome your feedback and questions on your experience using the application.

Thank you.

Team Mobogenie

Social tagging: Mobogenie

그림 1-62 | Mobogenie 제작사의 공식 사과문

다운로드 된 앱이 사용자의 스마트폰에 문제를 일으키지는 않았지만, 웹사이트를 방문하는 것만으로도 앱이 다운로드 될 수 있다는 것이 확인된 것이다. 이 방법을 악성코드 제작자가 이용할 수도 있다.

안드로이드의 특성상 다운로드 된 앱이 자동으로 설치되지는 않지만 사용자의 실수에 의해 설치될 가능성은 있다. 많은 개인정보를 저장하고 있는 스마트폰을 안전하게 이용하기 위해 '알 수 없는 소스'를 해제한다면 악성 앱이 자동으로 다운로드 되더라도 스마트폰에 설치되는 것을 방지할 수 있다.

보안 동향

01. 보안 통계

11월 마이크로소프트 보안 업데이트 현황

2013년 11월 마이크로소프트사에서 발표한 보안 업데이트는 총 8건으로 긴급 3건, 중요 5건이다. 긴급 업데이트에는 인터넷 익스플로러(Internet Explorer) 누적 보안 업데이트와 시스템 관련 업데이트가 2건 포함되어 있으며, 중요 업데이트에는 시스템 관련 업데이트 3건과 Office 관련 업데이트가 2건 포함되어 있다. 시스템 관련 취약점과 인터넷 익스플로러 관련 취약점은 공격자들에게 자주 악용되므로, 보안 패치를 신속하게 적용하는 것이 권장된다.

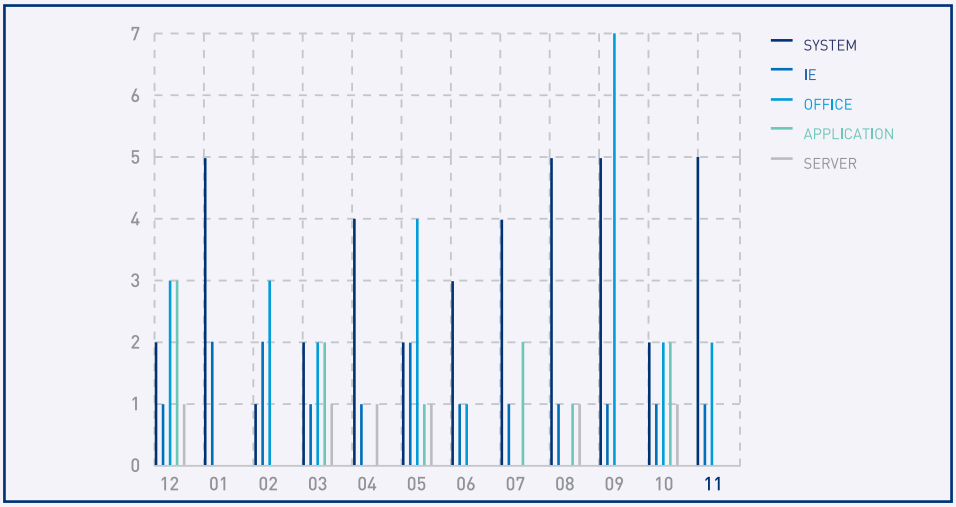


그림 2-1 | 공격 대상 기준별 MS 보안 업데이트

긴급
MS13-088 Internet Explorer 누적 보안 업데이트
MS13-089 Windows 그래픽 장치 인터페이스의 취약점으로 인한 원격 코드 실행 문제점
MS13-090 ActiveX 킬(Kill) 비트 누적 보안 업데이트
중요
MS13-091 Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점
MS13-092 Hyper-V의 취약점으로 인한 권한 상승 문제점
MS13-093 Windows Ancillary Function Driver의 취약점으로 인한 정보 유출 문제점
MS13-094 Microsoft Outlook의 취약점으로 인한 정보 유출 문제점
MS13-095 디지털 서명의 취약점으로 인한 서비스 거부 문제점

표 2-1 | 2013년 11월 주요 MS 보안 업데이트

보안 동향

02. 보안 이슈

비트코인 지갑 저장소를 노린 공격 발생

비트코인(Bitcoin)은 컴퓨터를 통해 복잡한 수학 연산을 수행하는 대가로 지급받는 가상 화폐이다. 비트코인은 거래 시 익명성이 보장되기 때문에 인터넷 암시장에서 사용되기도 하여 많은 논란을 낳고 있다. 최근에는 다른 사용자의 PC를 감염시켜 비트코인 채굴에 사용하는 것을 목적으로 하는 악성코드도 다수 보고되고 있다. 채굴하여 얻은 비트코인은 '지갑'에 보관되는데, 이러한 지갑을 온라인상에 안전하게 보관하는 서비스를 제공하던 Inputs.io가 해커들로부터 공격 당한 것으로 알려졌다.

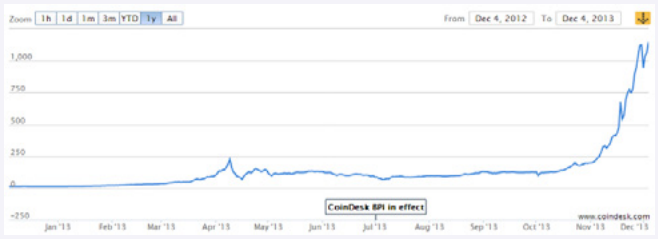


그림 2-2 | 최근 1년간 비트코인 화폐 가치 변화 추이 (출처: www.coindesk.com)

Inputs.io의 개발자로 알려진 Tradefortress는 두 번의 해킹 공격으로 인하여 4100BTC(비트코인의 화폐 단위)가 도난당했다는 사실을 홈페이지에 공지하였다. 이것은 당시 비트코인 화폐 가치로 환산했을 때 약 120만 달러에 해당한다. Inputs.io와 비슷한 서비스를 제공하던 Bitfloor도 지난 9월 해커들로부터 공격을 받아 약 24000BTC를 도난당한 뒤 서비스를 종료한 바 있다. 비트코인이 더욱 대중화되고, 그 화폐적 가치를 인정받을수록 비트코인 서비스를 대상으로 한 해커들의 공격도 한층 증가할 것으로 예상된다.

그림 2-3 | 해킹에 대해 언급하고 있는 Inputs.io의 웹페이지

Apache Struts 2 취약점 업데이트 권고

지난 7월 공개된 바 있는 Apache Struts 2 취약점(CVE-2013-2248, CVE-2013-2251) 방어 방법을 우회하는 공격이 발견되면서 업데이트 적용이 재차 권고되었다.

이 취약점은 Apache Struts 2.0.0 버전부터 2.3.15 버전까지 영향을 받으며, 공격자가 원격 서버로 URL 요청 시에 action, redirect, redirectAction 파라미터로 전달되는 인자 값을 조작하여 원하는 명령을 실행할 수 있다.

```
GET /struts.action?redirect:${%23a%3d(new%20java.lang.ProcessBuilder(new%
20java.lang.String[]{'192.168.30.141'})).start(),%23b%3d%23a.getInputStream(),%23c%
3dnew%20java.io.InputStreamReader(%23b),%23d%3dnew%20java.io.BufferedReader(%23c),%23e%
3dnew%20char[50000],%23d.read(%23e),%23matt%3d%23context.get
('com.opensymphony.xwork2.dispatcher.HttpServletResponse'),%23matt.getWriter().println
(%23e),%23matt.getWriter().flush(),%23matt.getWriter().close()} HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0)
```

그림 2-4 | Apache Struts 2 취약점 공격 예

만약 해당 공격에 노출되면 공격자에 의해 서버가 장악되는 것은 물론, 시스템 파괴나 내부 데이터 유출까지 이어질 수 있으므로 2.3.15 버전 이상으로 반드시 업데이트 해야 한다.

이 취약점과 관련한 정보는 다음 경로에서 확인 가능하다.

- http://struts.apache.org/release/2.3.x/docs/s2-016.html
- http://struts.apache.org/release/2.3.x/docs/s2-017.html

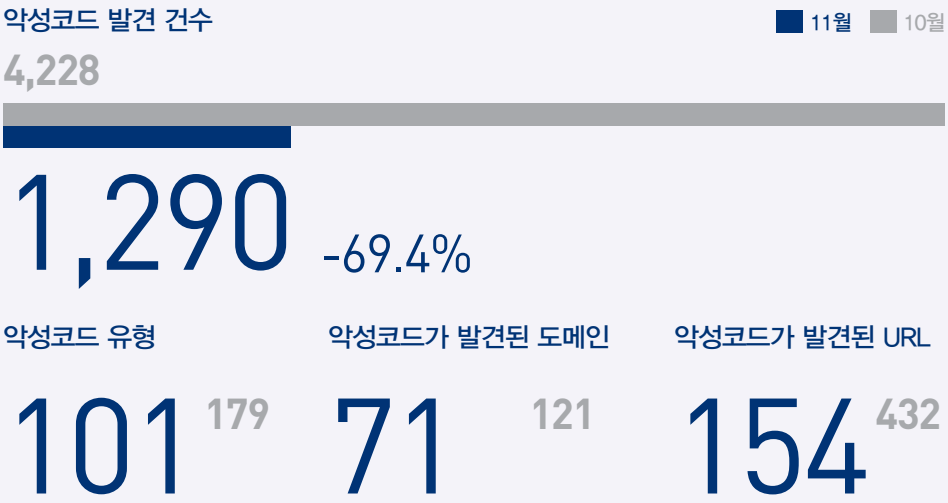
웹 보안 동향

01. 웹 보안 통계

웹사이트 악성코드 동향

안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹사이트 보안 통계 자료에 의하면, 2013년 11월 웹을 통한 악성코드 발견 건수는 모두 1290건이었다. 악성코드 유형은 총 101종, 악성코드가 발견된 도메인은 71개, 악성코드가 발견된 URL은 154개로 각각 집계됐다. 전월과 비교해 웹을 통한 악성코드 발견 건수, 악성코드 유형, 악성코드가 발견된 도메인, 악성코드가 발견된 URL 수는 감소한 것으로 나타났다.

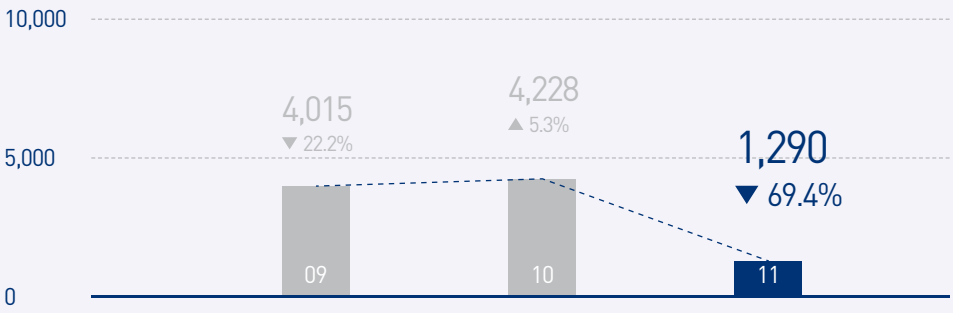
표 3-1 | 2013년 11월 웹사이트 보안 현황



월별 악성코드 배포 URL 차단 건수

2013년 11월 웹을 통한 악성코드 발견 건수는 전월의 4228건의 31% 수준인 1290건이었다.

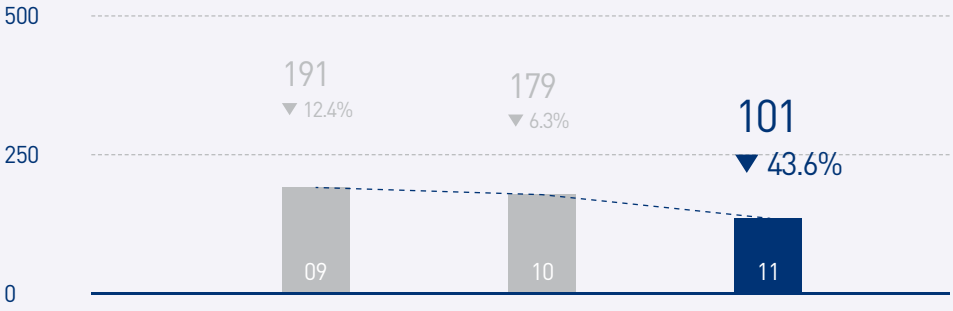
그림 3-1 | 월별 웹을 통한 악성코드 발견 건수 변화 추이



월별 악성코드 유형

2013년 11월 악성코드 유형은 전달 179건의 56% 수준인 101건이다.

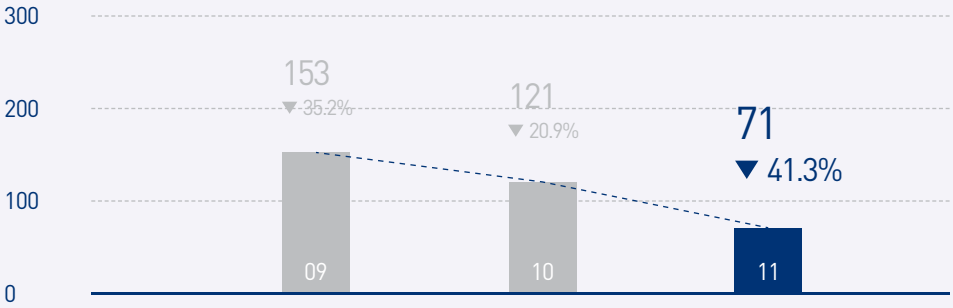
그림 3-2 | 월별 악성코드 유형 수 변화 추이



월별 악성코드가 발견된 도메인

2013년 11월 악성코드가 발견된 도메인은 71건으로, 전월의 121건과 비교해 59% 수준이었다.

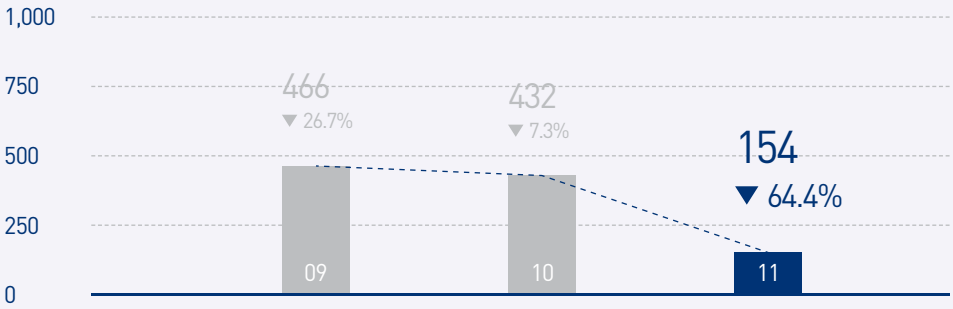
그림 3-3 | 악성코드가 발견된 도메인 수 변화 추이



월별 악성코드가 발견된 URL

2013년 11월 악성코드가 발견된 URL은 전월 432건과 비교해 36% 수준인 154건이다.

그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이



월별 악성코드 유형

악성코드 유형별 배포 수를 보면 트로이목마가 812건(62.9%)으로 2/3 정도를 차지했고, 애드웨어는 230건(17.8%), 스파이웨어는 136건(10.5%)인 것으로 조사됐다.

유형	건수	비율
TROJAN	812	62.9 %
ADWARE	230	17.8 %
SPYWARE	136	10.6 %
DROPPER	16	1.3 %
Win32/VIRUT	7	0.5 %
DOWNLOADER	5	0.4 %
ETC	84	6.5 %
	1,290	100.0 %

표 3-2 | 악성코드 유형별 배포 수

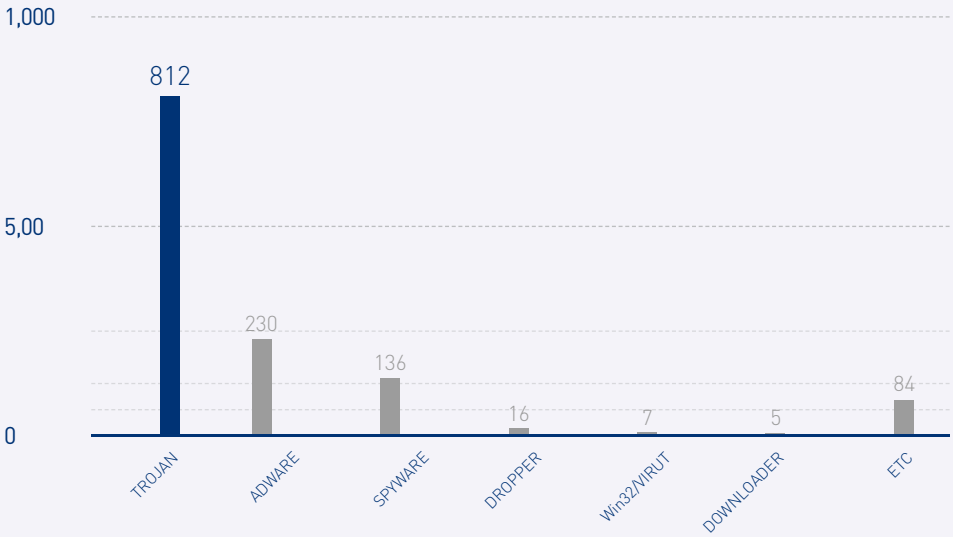


그림 3-5 | 악성코드 유형별 배포 수

악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서는 Trojan/Win32.Agent가 254건(28.6%)으로 가장 많았으며, Trojan/Win32.Agent 를 포함해 4건이 새로 나타났다.

순위	등락	악성코드명	건수	비율
1	NEW	Trojan/Win32.Agent	254	28.6 %
2	▲4	Spyware/Win32.Gajai	136	15.3 %
3	▲1	Adware/Win32.DelBar	131	14.7 %
4	▲3	Win-Trojan/Downloader.12800.LU	88	9.9 %
5	NEW	Trojan/Win32.Starter	66	7.4 %
6	NEW	Adware/Win32.Clicker	48	5.4 %
7	NEW	Trojan/Win32.Jorik	45	5.1 %
8	▲2	Trojan/Win32.ADH	43	4.8 %
9	—	Trojan/Win32.KorAd	42	4.7 %
10	▼2	Win32/Induc	36	4.1 %
		TOTAL	889	100.0 %

표 3-3 | 악성코드 배포 최다 10건

ASEC REPORT CONTRIBUTORS

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

AhnLab