ASEC REPORT

VOL.24 | 2012.01

안철수연구소 월간 보안 보고서

이 달의 보안 동향
2011년 보안 동향 분석
2011년 세계 보안 동향
2012년 보안 위협 예측

AhnLab

AhnLab Security Emergency response Center

ASEC (AhnLab Security Emergency response Center)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 ㈜안철수연구소의 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.

CONTENTS

1. 이달의 보안 동향

01. 악성코드 동향

a. 악성코드 통계 05

– 악성코드 감염보고 최다 20
– 악성코드 대표진단명 감염보고 최다 20
– 악성코드 유형별 감염보고 비율
– 악성코드 유형별 감염보고 전월 비교
– 악성코드 월별 감염보고 건수
– 신종 악성코드 감염보고 최다 20
– 신종 악성코드 유형별 분포

b. 악성코드 이슈 10

– 김정일 위원장 사망을 이용한 애드웨어 유포
– 김정일 위원장 사망을 악용한 악성 전자 문서 파일 유포
– 국내 연예인 사생활 동영상으로 위장한 악성코드 유포
– 2012년 버전으로 위장한 허위 클라우드 백신
– 악성코드를 위한 안티바이러스 체크 웹 사이트
– 아크로뱃 제로데이 취약점을 악용한 타깃 공격
– 여러 가지 취약점을 이용한 제우스봇 전파 메일 발견
– 구글 안드로이드 마켓에 업로드된 악성 애플리케이션

02. 시큐리티 동향

a. 시큐리티 통계 19

– 12월 마이크로소프트 보안 업데이트 현황

03. 웹 보안 동향

a. 웹 보안 통계 21

– 웹사이트 보안 요약
– 월별 악성코드 배포 URL 차단 건수
– 월별 악성코드 유형
– 월별 악성코드가 발견된 도메인
– 월별 악성코드가 발견된 URL
– 악성코드 유형별 배포 수
– 악성코드 배포 순위

b. 웹 보안 이슈 24

– 2011년 12월 침해 사이트 현황

2. 2011년 보안 동향 분석

01. 악성코드 동향

a. 악성코드 통계 25

– 악성코드 감염보고 연간 최다 20
– 악성코드 대표진단명 감염보고 연간 최다 20
– 악성코드 유형별 연간 감염보고 비율
– 악성코드 월별 연간 감염보고 건수
– 연간 신종 악성코드 감염 보고 최다 20
– 연간 신종 악성코드 유형별 분포

b. 악성코드 이슈 29

02. 시큐리티 동향

a. 시큐리티 통계 32

– 2011년 마이크로소프트 보안 업데이트 현황

03. 웹 보안 동향

a. 웹 보안 통계 33

– 웹사이트 보안 요약
– 월별 악성코드 발견 건수
– 월별 악성코드 유형
– 월별 악성코드가 발견된 도메인
– 월별 악성코드가 발견된 URL
– 악성코드 유형별 배포 수
– 악성코드 배포 순위 최다 10

b. 웹 보안 이슈 36

– 침해 사이트 현황

3. 2011년 세계 보안 동향

세계 보안 동향 39

4. 2012년 보안 위협 예측

보안 위협 예측 40

1. 이달의 보안 동향

01. 악성코드 동향

a. 악성코드 통계

악성코드 감염보고 최다 20

2011년 12월 악성코드 감염 보고는 지난 달과 마찬가지로 JS/Agent가 가장 많았다. Exploit/Cve-2011-2140과 Swf/Dropper가 그 다음으로 많이 보고됐으며 새로 발견된 악성코드는 최다 20건 중 총 7건이었다([표 1-1]).

순위	등락	악성코드명	건수	비율
1	—	JS/Agent	1,414,471	23.6 %
2	▲1	Exploit/Cve-2011-2140	673,093	11.2 %
3	▲6	Swf/Dropper	602,840	10.0 %
4	NEW	Java/Cve-2010-0886	501,160	8.4 %
5	NEW	Swf/Exploit	472,412	7.9 %
6	▼2	Textimage/Autorun	464,306	7.7 %
7	▲3	Html/Agent	312,722	5.2 %
8	▼3	Win-Trojan/Agent.465408.T	196,643	3.3 %
9	▼7	JS/Downloader	163,062	2.7 %
10	NEW	Html/Iframe	160,986	2.7 %
11	▼3	JS/Redirector	150,603	2.5 %
12	▲1	Swf/Agent	115,136	1.9 %
13	▼2	JS/Exploit	108,185	1.8 %
14	NEW	JS/Cve-2010-0806-cc	106,364	1.8 %
15	▼9	Swf/Cve-2011-2140	105,452	1.8 %
16	▼4	Als/Bursted	97,523	1.6 %
17	▼2	Win32/Induc	95,597	1.6 %
18	NEW	JS/Shellcode	89,320	1.5 %
19	NEW	Win-Trojan/Adload.428032.B	85,293	1.4 %
20	NEW	JS/Cve-2010-0806	83,779	1.4 %
			5,998,947	100.0 %

[표 1-1] 악성코드 감염보고 최다 20

악성코드 대표진단명 감염보고 최다 20

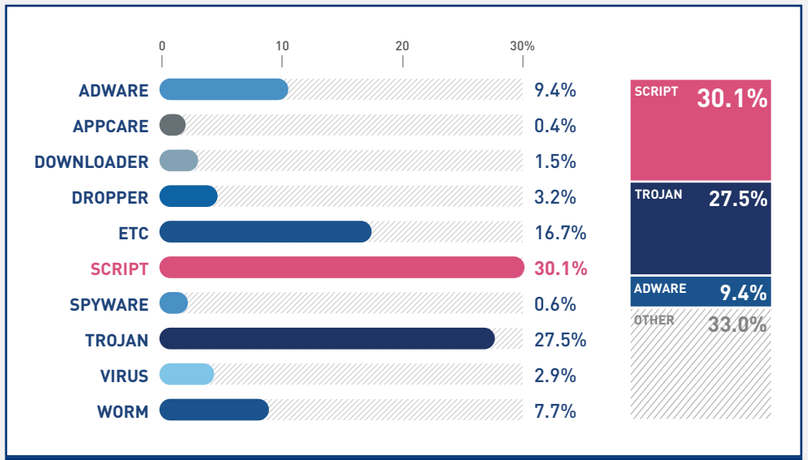
[표 1-2]는 악성코드의 주요 동향을 파악하기 위하여, 악성코드별 변종을 종합한 악성코드 대표 진단명 감염 보고 최다 20건이다. 2011년 12월의 감염 보고 건수는 JS/Agent가 총 142만 6157건으로 전체 20건 중 16.5%의 비율로 가장 빈번히 보고된 것으로 조사됐다. Win-Trojan/Agent가 104만 9476건, Win-Adware/Korad이 77만 7141건으로 그 뒤를 이었다.

순위	등락	악성코드명	건수	비율
1	—	JS/Agent	1,426,157	16.5 %
2	—	Win-Trojan/Agent	1,049,476	12.1 %
3	▲2	Win-Adware/Korad	777,141	9.0 %
4	—	Exploit/Cve-2011-2140	673,093	7.8 %
5	▲11	Swf/Dropper	602,840	7.0 %
6	NEW	Java/Cve-2010-0886	501,160	5.8 %
7	NEW	Swf/Exploit	472,412	5.5 %
8	▼2	Textimage/Autorun	464,418	5.4 %
9	—	Win-Trojan/Onlinegamehack	457,790	5.3 %
10	▲8	Html/Agent	312,722	3.6 %
11	▼4	Win-Trojan/Downloader	282,250	3.3 %
12	NEW	Win-Trojan/Korad	213,595	2.5 %
13	▼3	Win32/Conficker	211,492	2.4 %
14	▼1	Win32/Virut	197,554	2.3 %
15	▼3	Win32/Autorun.worm	186,953	2.2 %
16	▲4	Win-Downloader/Korad	179,518	2.1 %
17	▼14	JS/Downloader	163,062	1.9 %
18	▼4	Win32/Kido	162,139	1.8 %
19	NEW	Html/Iframe	160,986	1.8 %
20	▼5	JS/Redirector	150,603	1.7 %
			8,645,361	100.0 %

[표 1-2] 악성코드 대표진단명 감염보고 최다 20

악성코드 유형별 감염보고 비율

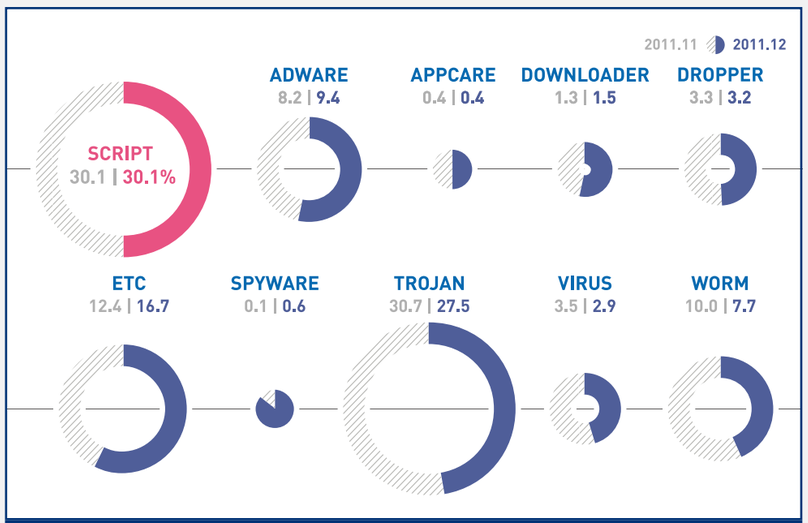
[그림 1-1]은 2011년 12월 한 달 동안 안철수연구소가 고객으로부터 감염이 보고된 악성코드의 유형별 감염 비율을 집계한 결과다. 2011년 12월의 악성코드를 유형별로 살펴보면, 감염 보고 건수 비율은 스크립트(Script)가 30.1%, 트로이목마(Trojan)가 27.5%, 애드웨어(Adware)가 9.4%로 나타났다.



[그림 1-1] 악성코드 유형별 감염보고 비율

악성코드 유형별 감염보고 전월 비교

[그림 1-2]는 악성코드 유형별 감염 보고 비율을 전월과 비교한 것이다. 애드웨어, 다운로더(Downloader), 스파이웨어(Spyware)가 전월에 비해 증가세를 보이고 있는 반면, 트로이목마, 웜(Worm), 드로퍼(Dropper), 바이러스(Virus)는 전월에 비해 감소한 것을 볼 수 있다. 스크립트와 애프케어(Appcare) 계열들은 전월 수준을 유지했다.



[그림 1-2] 악성코드 유형별 감염보고 전월 비교

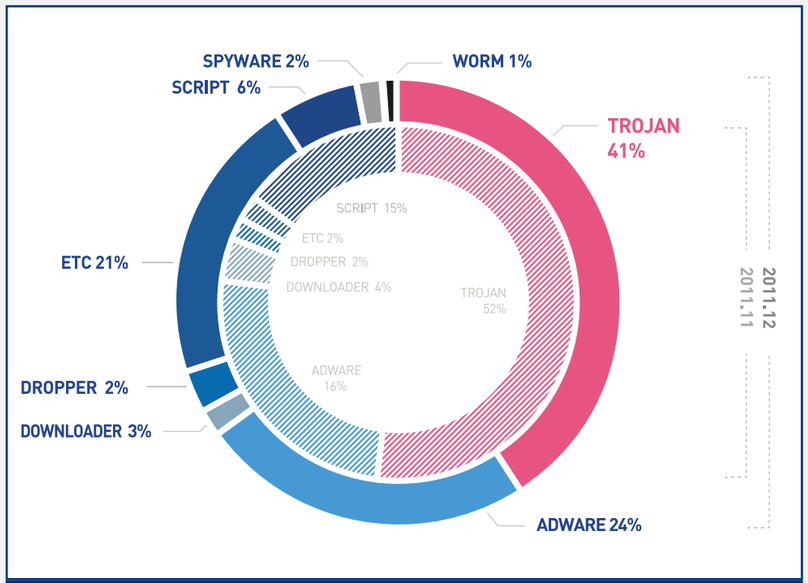
악성코드 월별 감염보고 건수

12월의 악성코드 월별 감염 보고 건수는 1465만 7593건으로 11월의 1255만 9154건에 비해 209만 8439건이 증가했다.

[그림 1-3] 악성코드 월별 감염보고 건수

신종 악성코드 유형별 분포

12월의 신종 악성코드 유형을 보면 트로이목마가 41%로 가장 많았고, 애드웨어가 24%, 스크립트가 6%였다.



[그림 1-4] 신종 악성코드 유형별 분포

신종 악성코드 감염보고 최다 20

[표 1-3]은 12월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 최다 20건이다. 12월에 감염 보고된 신종 악성코드는 JAVA/Cve-2010-0886이 50만 건이 넘어 전체의 29.5%로 가장 많았으며, JS/Cve-2010-0806-cc도 10만 건이 넘게 보고됐다.

순위	악성코드명	건수	비율
1	JAVA/Cve-2010-0886	501,160	29.5 %
2	JS/Cve-2010-0806-cc	106,364	6.3 %
3	Win-Trojan/Adload.428032.B	85,293	5.1 %
4	Win-Trojan/Agent.907888	82,717	4.9 %
5	Win-Spyware/Agent.65536.F	76,663	4.5 %
6	Win-Adware/KorAd.760832	73,991	4.4 %
7	Win-Adware/KorAd.1131008	70,406	4.1 %
8	Win-Trojan/Onlinegamehack.45094	67,053	4.0 %
9	Win-Trojan/Agent.238608	66,520	3.9 %
10	Dropper/Tesa.2764800	61,612	3.6 %
11	Win-Adware/KorAd.901632	61,227	3.6 %
12	Win-Trojan/Sadenav.325728	59,632	3.5 %
13	Win-Trojan/Agent.849488	54,626	3.2 %
14	Win-Trojan/Korad.450560.B	52,721	3.1 %
15	Win-Trojan/Agent.446464.CW	49,986	2.9 %
16	JS/Expliot	49,670	2.9 %
17	Win-Trojan/Korad.458752	49,147	2.9 %
18	Win-Adware/KorAd.733184	43,425	2.6 %
19	Win-Adware/StartPage.114593	42,316	2.5 %
20	Win-Trojan/Agent.554496.S	42,263	2.5 %
		1,696,792	100.0 %

[표 1-3] 신종 악성코드 감염보고 최다 20

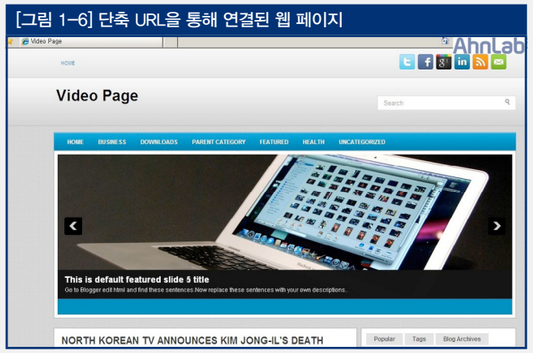
01. 악성코드 동향
b. 악성코드 이슈

김정일 위원장 사망을 이용한 애드웨어 유포

2011년 12월 19일, 북한 방송을 통해 김정일 위원장의 사망 소식이 전 세계에 알려진 다음날 이를 악용한 애드웨어 유포 사례가 발견됐다. 해당 애드웨어는 [그림 1-5]와 같이 김정일 위원장의 사망 관련 동영상 시청을 위해 유튜브 페이지의 단축 URL을 클릭하도록 유도하고 있다.

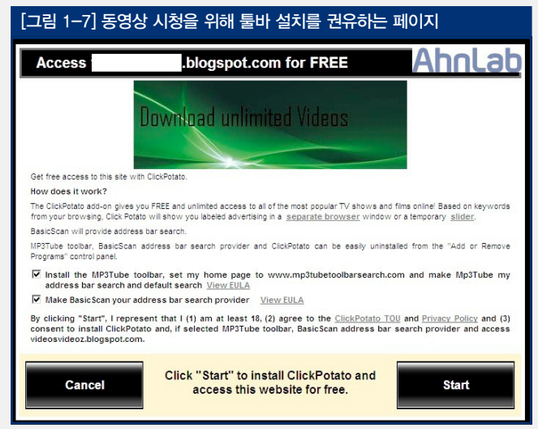
[그림 1-5] 애드웨어 유포를 위한 단축 URL이 포함된 유튜브 페이지

[그림 1-6] 단축 URL을 통해 연결된 웹 페이지



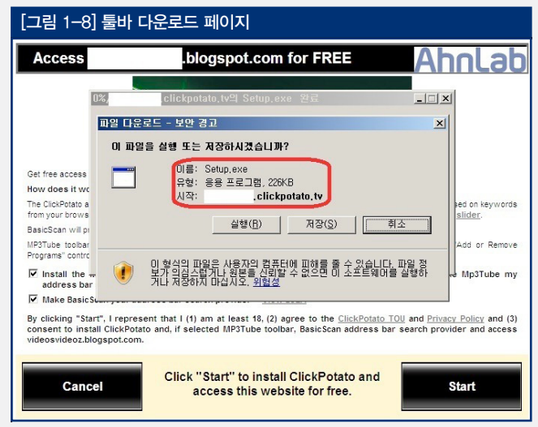
해당 단축 URL을 클릭하면 [그림 1-6]의 웹 페이지로 연결된다. [그림 1-6]의 웹 사이트에서는 정상적인 동영상 시청을 위해 [그림 1-7]과 같이 특정 툴바를 설치하도록 권유한다.

[그림 1-7] 동영상 시청을 위해 툴바 설치를 권유하는 페이지



사용자가 설치에 동의하지 않아 체크 박스를 해제해도 Start 버튼을 클릭하면 [그림 1-8]과 같이 Setup.exe 파일을 다운로드하게 된다.

[그림 1-8] 툴바 다운로드 페이지

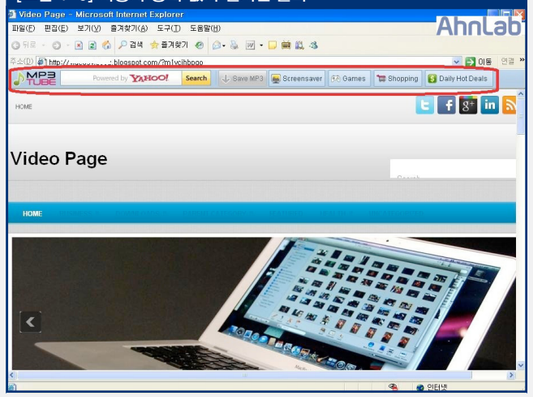


다운로드된 Setup.exe를 실행하면 사용자의 동의 없이 특정 시스템으로부터 다른 파일들을 다운로드 및 실행한다.

설치가 완료되면 [그림 1-9]와 같이 사용자가 동의하지 않은 인터넷

익스플로러 툴바가 나타난다. 또한 인터넷 익스플로러의 시작 페이지를 특정 웹 사이트로 변경하고 사용자가 입력하는 검색 키워드들을 가로채 특정 시스템으로 전송한다.

[그림 1-9] 사용자 동의 없이 설치된 툴바



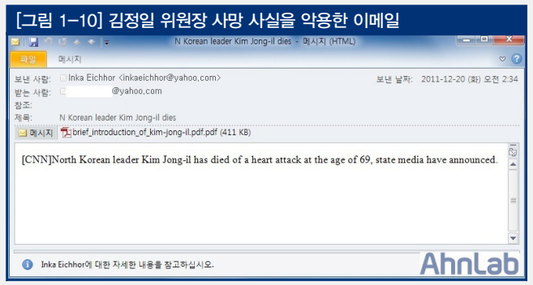
〈V3 제품군의 진단명〉

- Trojan/Win32.ADH
- Adware/Win32.Hotbar
- Trojan/Win32.ADH

김정일 위원장 사망을 악용한 악성 전자 문서 파일 유포

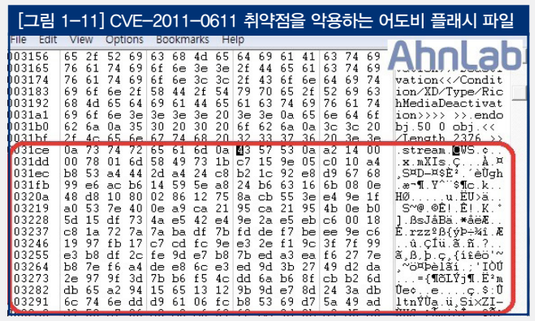
ASEC에서 2011년 12월 20일 북한의 김정일 위원장 사망을 악용한 애드웨어가 유포된 사실을 공개한지 얼마 지나지 않아 트렌드마이크로(Trend Micro)도 블로그 〈Kim Jong Ⅱ Malicious Spam Found〉를 통해 [그림 1-10]과 같이, 취약점이 존재하는 전자 문서 파일을 첨부한 이메일이 유포된 사실을 공개했다.

[그림 1-10] 김정일 위원장 사망 사실을 악용한 이메일



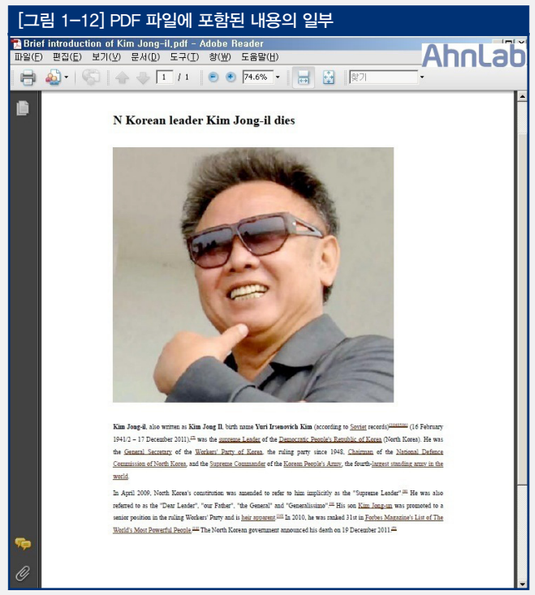
해당 이메일에 첨부된 어도비 아크로뱃 리더(Adobe Acrobat Reader, 이하 PDF) 파일은 CVE-2010-2883 취약점과 함께, 2011년 4월에 발견된 CVE-2011-0611 취약점을 악용하는 어도비 플래시(Adobe Flash) 파일을 포함하고 있다. 해당 PDF 파일을 실행하면 [그림 1-12]와 같이 김정일 위원장의 사진과 함께 그의 일생에 관련된 내용을 보여준다. 해당 파일은 취약점이 없는 정상 파일이지만,

[그림 1-11] CVE-2011-0611 취약점을 악용하는 어도비 플래시 파일



시스템 사용자 모르게 다음의 파일들을 시스템에 생성하고 실행한다.

[그림 1-12] PDF 파일에 포함된 내용의 일부



- C:₩Documents and Settings₩Tester₩Local Settings₩Brief introduction of Kim Jong-il.pdf(45,572바이트)
- C:₩Documents and Settings₩Tester₩Local Settings₩abc.scr(156,672바이트)

생성된 파일 중 Brief introduction of Kim Jong-il.pdf는 [그림 1-11]과 같은 정상 파일이며, 함께 생성된 abc.scr 파일이 악의적인 기능을 수행한다. 생성된 abc.scr은 다음 파일을 다시 생성한다.

-C:₩Documents and Settings₩Tester₩Local Settings₩Application Data₩GoogleUpdate.exe(91,136바이트)

그리고 아래의 레지스트리 키 값을 생성하여 시스템을 재부팅한 후에도 자동 실행되도록 설정한다.

-HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run GoogleUpd = "'C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Application Data₩GoogleUpdate.exe'"

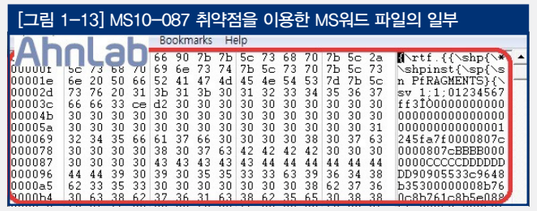
abc.scr에 의해 생성된 GoogleUpdate.exe 파일은 감염된 시스템의 인터넷 접속 여부를 확인하기 위해 구글 웹 사이트로 접속한 후, 특정 시스템들 중 하나로 역접속(Reverse Connection)하여 공격자가 지정한 명령을 수행한다.

GoogleUpdate.exe는 공격자의 명령에 따라 다음의 악의적인 기능들을 수행한다.

- 실행중인 프로세스 확인 및 강제 종료
- CMD 셸 명령 수행
- 파일 업로드 및 다운로드, 삭제

이 외에 트렌드마이크로에서는 마이크로소프트 워드의 "Microsoft Security Bulletin MS10-087 – Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점(2423930)" 취약점을 악용해 유포된 악성코드도 있다고 밝혔다.

[그림 1-13] MS10-087 취약점을 이용한 MS워드 파일의 일부



〈V3 제품군의 진단명〉

- PDF/Cve-2010-2883
- Dropper/Cve-2010-3333
- SWF/Cve-2011-0611
- Win-Trojan/Infostealer.156672
- Win-Trojan/Infostealer.91136.B
- Win-Trojan/PcClinet.80384
- Win-Trojan/PcClinet.118784

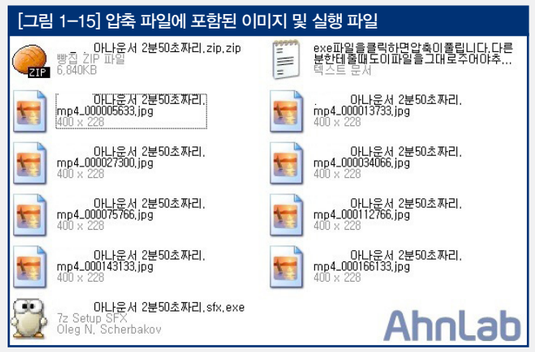
국내 연예인 사생활 동영상으로 위장한 악성코드 유포

최근 국내 유명 연예인 A양을 촬영한 것으로 알려진 사생활 동영상이 유포돼 사회적으로 큰 이슈를 일으켰다. 이를 틈타 2011년 12월 8일 저녁, 소셜 네트워크 서비스인 트위터 등을 통해 해당 연예인의 사생활 동영상으로 위장한 악성코드가 유포됐다.
해당 트위터 계정은 비교적 최근에 생성한 것으로 보이며 계정 사용자에 대한 자세한 정보가 없다. 또한 [그림 1-14]와 같이 별다른 내용 없이 유명 연예인의 동영상 파일로 위장한 ZIP 압축 파일을 다운

[그림 1-14] 유명 연예인 A양 동영상을 다운로드하도록 유도하는 트위터 계정

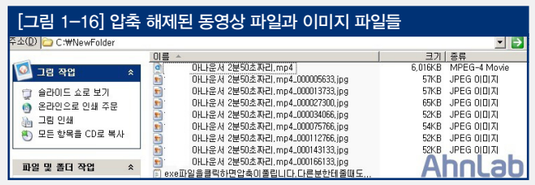
로드하도록 유도하고 있다. 해당 URL을 복사하여 웹 브라우저에서 다운로드를 시도하면 'XXX 아나운서 2분50초짜리.zip' 파일이 다운로드된다.

[그림 1-15] 압축 파일에 포함된 이미지 및 실행 파일



다운로드된 압축 파일에는 [그림 1-15]와 같은 다수의 JPG 파일과 SFX로 압축된 EXE 파일이 들어있다.

[그림 1-16] 압축 해제된 동영상 파일과 이미지 파일들



텍스트 파일은 SFX로 압축된 EXE 파일을 실행해야만 동영상을 볼 수 있는 것처럼 꾸며 'XXX아나운서 2분 50초짜리.sfx.exe' 파일의 실행을 유도한다. 해당 EXE 파일을 실행하면 압축을 풀 경로를

선택하도록 되어 있으며, [그림 1-16]과 같이 실제 성인 동영상 파일과 다수의 이미지 파일을 해당 폴더에 생성한다.

그러나 사용자 모르게 netsecurity.exe 파일도 압축이 풀리면서 실행되고, 윈도우 시스템 폴더(C:₩Windows₩System32)에 netdrvsrty.exe 파일을 생성한다. 이후 윈도우 레지스트리에 다음 키 값을 생성하여 시스템 재부팅 후에도 자동 실행되도록 구성한다.

HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run
netsecurityDRV = "C:₩WINDOWS₩system32₩netdrvsrty.exe"

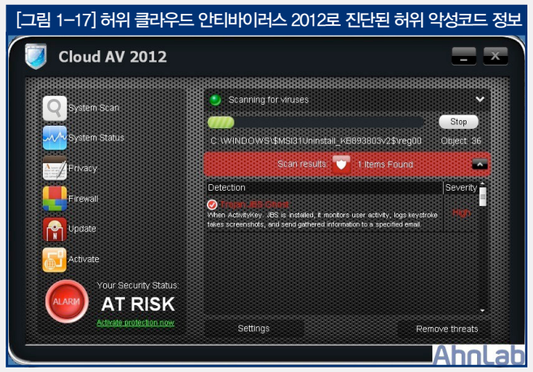
생성된 netdrvsrty.exe는 마이크로소프트 비주얼 C++(Microsoft Visual C++) MFC로 제작됐으며, 코드상으로는 감염된 시스템의 IP 주소를 수집하고, 인터넷 익스플로러의 즐겨찾기 폴더에 웹 페이지 바로가기 파일들을 생성하게 되어 있다. 그러나 테스트 당시에는 코드상으로 존재하는 악의적인 기능들이 정상 동작하지 않았다. 이런 일련의 사항들을 살펴볼 때 이번 유명 연예인의 사생활 동영상으로 위장하여 유포된 악성코드는 제작자의 명령에 따라 즐겨찾기 파일을 조작하는 애드웨어 종류로 판단된다.

〈V3 제품군 진단명〉
– Downloader/Win32.Korad
– Trojan/Win32.Sysckbc
– Dropper/Agent.6596635

2012년 버전으로 위장한 허위 클라우드 백신

연말연시에는 사회적인 분위기를 악용하는 사회공학 기법을 활용한 악성코드나 보안 위협들이 발견될 가능성이 높다. 크리스마스 카드로 위장한 악성코드, 신년 축하 카드로 위장한 악성코드 등이 발견됐다. 금전적인 목적으로 꾸준히 유포됐던 허위 백신들 중 [그림 1-17]과 같이 2012년도 최신 버전으로 위장한 사례가 2011년 11월 30일 발견됐다. 이 허위 백신은 2012년도 최신 버전이라고 표기

[그림 1-17] 허위 클라우드 안티바이러스 2012로 진단된 허위 악성코드 정보



한 것 외에도, 최근 다양한 보안 위협들에 대응하기 위해 개발 및 사용되는 클라우드 안티바이러스(Cloud Anti-Virus)로 위장했다.

이번에 발견된 허위 클라우드 안티바이러스 2012는, 외형적인 인터페이스 부분을 제외하곤 과거에 발견됐던 것과 기능이나 동작 면에서 동일하다.

업데이트를 위해 최신 엔진을 다운로드하는 것처럼 꾸미지만 실제로 다운로드되는 파일은 없다.

또한 다른 허위 백신들과 마찬가지로 금전 결제를 유도하는데, 약 5만 7000원을 신용카드로 결제하면 허위로 표기된 악성코드 모두를 치료 가능한 것처럼 보여준다.

[그림 1-18] 금전 결제를 유도하는 허위 백신

금전 결제를 유도하는 허위 백신들 모두가 악성코드에 감염됐다는 허위 정보를 보여주므로 신뢰할 수 있는 보안 제품을 사용하는 것이 중요하다.

〈V3 제품군의 진단명〉
– Trojan/Win32.Jorik
– Win-Trojan/Fakescanti.1976320

악성코드를 위한 안티바이러스 체크 웹 사이트

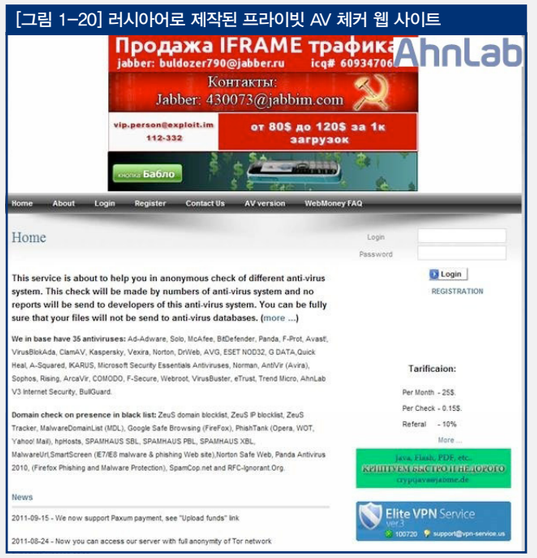
최근 발생하고 있는 APT(Advanced Persistent Threat) 보안 사고의 상당수는 기업 내부 네트워크에서 사용하는 메일이나 메신저, SNS 등을 이용해 백도어(Backdoor) 기능을 수행하는 악성코드를 전파해 감염을 시도한다.

이렇게 전달되는 악성코드 대부분은, 공격자에 의해 사전에 안티바이러스 소프트웨어로 진단되는지 테스트를 거침으로써 공격 성공률을 높이고 있다. 이러한 테스트는 [그림 1-19]와 같이 최근 러시아에서 발견된 프라이빗 AV 체커(Private AV Checker) 웹 사이트를 통해 유료로 진행된다. 이번에 발견된 웹 사이트는 35개의 안티바이러스 제품들에 대한 검사가 가능하며 1회 검사에 1센트, 20달러(약 2만 2000원)를 지불하면 500회까지 검사할 수 있다고 광고하고 있다. 해당 웹 사이트는 러시아 웹 사이트에서 제공하는 API(Application

Program Interface)를 이용해 제작된 것으로 확인됐다. 러시아어로 제작된 [그림 1-20]의 웹 사이트 역시 35개의 안티바이러스 소프트웨어에 대한 검사가 가능하며 그 중에는 안랩의 V3 Internet Security 8.0도 포함돼 있었다. 1회 사용은 15센트, 한 달 사용은 25달러(약 2만 7500원)라고 광고하고 있다.

[그림 1-19] 프라이빗 AV 체커 웹 사이트

[그림 1-20] 러시아어로 제작된 프라이빗 AV 체커 웹 사이트



이 외에도 악성코드를 유포하기 위한 웹 사이트가 보안 업체들의 블랙 리스트(BlackList)에 포함돼 있는지 확인하는 기능과 별도의 VPN(Virtual Private Network) 서비스도 제공하고 있으며, 검사되는 파일은 보안 업체로 전달되지 않는다는 점을 강조하고 있다. 이런 웹 사이트들은 악성코드의 공격 성공률을 높일 수 있는 환경을 만들어주기 때문에 그 위험성이 크다.

아크로뱃 제로데이 취약점을 악용한 타깃 공격

한국 시각으로 2011년 12월 7일 새벽, 어도비는 보안 권고문 〈APSA11-04 Security Advisory for Adobe Reader and Acrobat〉을 통해 어도비 아크로뱃에서 알려지지 않은 제로데이(Zero-Day) 취약점 CVE-2011-2462가 발견됐음을 알렸다. 이번에 발견된 제로데이 취약점에 영향을 받는 어도비 아크로뱃 버전들은 다음과 같다.

– Adobe Reader X (10.1.1) and earlier 10.x versions for Windows and Macintosh
– Adobe Reader 9.4.6 and earlier 9.x versions for Windows, Macintosh and UNIX
– Adobe Acrobat X (10.1.1) and earlier 10.x versions for Windows and Macintosh
– Adobe Acrobat 9.4.6 and earlier 9.x versions for Windows and Macintosh

그리고 보안 권고문을 통해 해당 제로데이 취약점을 악용한 타깃 공격이 발생했으며, 해당 취약점을 보고한 업체는 미국 군수 방위 업체인 록히드 마틴(Lockheed Martin)이라고 밝혔다.

이번 타깃 공격과 관련해 시만텍(Symantec)은 〈A New Zero-Day PDF Exploit used in a Targeted Attack〉 블로그를 통해 이메일의 첨부 파일로 제로데이 취약점인 CVE-2011-2462가 존재하는 PDF 파일이 유포됐으며 공격 대상이 된 기업들은 통신, 제조, 유통, 컴퓨터 하드웨어 업체들이라고 전했다.

ASEC에서는 이번 타깃 공격이 11월 말에서 12월 초를 전후해 발생한 것으로 추정하고 있으며, 취약한 PDF 파일은 최소 2개 이상인 것으로 파악하고 있다.

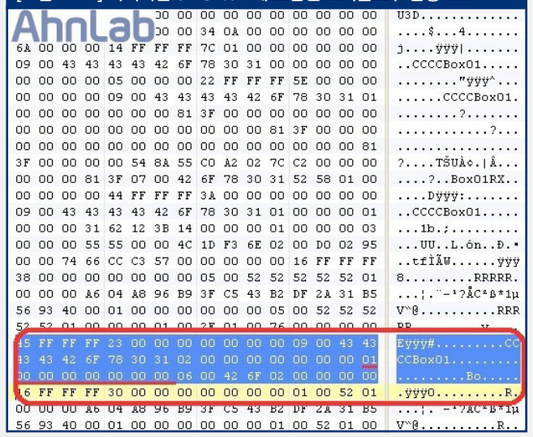
일반적으로 PDF 파일은 Universal 3D 파일 포맷(이하 U3D) 같은 3차원 이미지를 포함할 수 있다. U3D 이미지 파일은 일반적인 블록 헤더뿐만 아니라 블록 타입의 특별한 블록 데이터를 가질 수 있다. 이 블록들 중 힙(Heap)에 객체를 생성할 때 사용되는 ShadingModifierBlock은 '0xFFFFFF45' 값을 가진다.

[그림 1-21] 취약한 PDF 내부에 포함된 악의적인 3D Stream

이런 오브젝트들의 포인트도 힙에 저장되며, 포인터를 위해 메모리에 할당되는 양은 포인터 사이즈에 U3D 파일의 Shader List Count 필드를 곱한 것이다. 그러나 포인터가 '0xe0' 형태의 힙 메모리에 초기화되지 않은 상태로 설정될 경우, 이를 악용한 힙 변형이 발생할 수 있다. 이번에 발견된 취약한 PDF들은 [그림 1-21]과 같은 악의적인 3D Stream을 포함하고 있다.

해당 악의적인 3D Stream의 압축을 해제하면 [그림 1-22]와 같은 U3D 파일이 생성되며, 붉은 색 박스로 표시된 부분에 의해 실질적인 오버플로우(Overflow)가 발생한다.

[그림 1-22] 악의적인 3D Stream에 포함된 오버플로우 발생 코드



OpenAction을 통해 취약한 PDF 파일이 실행될 때 [그림 1-23]과 같은 14번 오브젝트에서 AcroJS를 포함한 15번 오브젝트 부분의 스크립트를 실행하도록 되어 있다.

[그림 1-23] 14번 오브젝트에 포함된 AcroJS 코드

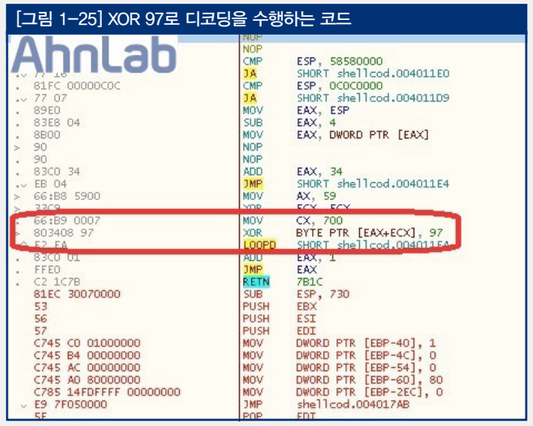
```
4 0 obj
<</Type /Catalog /Outlines 5 0 R /Pages 6 0 R /OpenAction 14 0 R /AcroForm 3 0 R >>
endobj

14 0 obj
<</S /JavaScript /JS 15 0 R >>
endobj
```

[그림 1-24] 15번 오브젝트에 포함된 셸 코드와 AcroJS

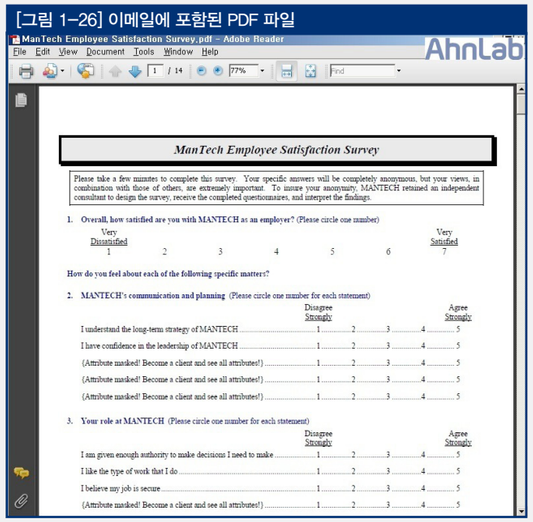
15번 오브젝트에는 [그림 1-24]와 같이 힙 스프레이를 통해 셸 코드를 메모리에 적재하는 AcroJS가 포함돼 있다.

[그림 1-25] XOR 97로 디코딩을 수행하는 코드



메일로 전달된 CVE-2011-2462 제로데이 취약점을 가지고 있는 PDF 파일을 실행하면 [그림 1-26]과 같은 정상 PDF 파일을 보여준다. 그러나 실제로는 사용자 모르게 다음 파일들이 시스템에 생성 및 실행된다.

[그림 1-26] 이메일에 포함된 PDF 파일



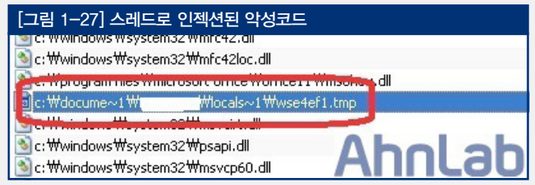
- C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩ctfmon.exe
- C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩ManTech Employee Satisfaction Survey.pdf
- C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩pretty.exe
- C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩WSE4EF1.TMP

생성된 파일들 중 ManTech Employee Satisfaction Survey.pdf는 [그림 1-24]와 같이 취약한 PDF 파일이 실행될 때 감염된 시스템의 사용자가 악성코드로 의심하지 않도록 보여주는 정상 파일이다. 생성된 ctfmon.exe 파일은 자신의 복사본을 동일한 위치에 pretty.exe 파일로 재생성하며 DLL 파일인 WSE4EF1.TMP를 드롭(Drop)한다. 해당 파일들 모두 마이크로소프트 비주얼 C++로 제작됐으며 실행 압축돼 있진 않다. 그리고 ctfmon.exe는 다음의 레지스트리 키 값을 생성해 시스템 재부팅 후에도 자동 실행되도록 구성한다.

HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run
office = "C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩pretty.exe"

드롭된 WSE4EF1.TMP는 다음의 프로그램들이 실행돼 프로세스를 생성할 때 [그림 1-27]과 같이 스레드(Thread)로 해당 프로세스에 인젝션(Injection)된다.

[그림 1-27] 스레드로 인젝션된 악성코드



- Microsoft Outlook
- Microsoft Internet Explorer
- Firefox

인젝션에 성공하면 다음 시스템으로 HTTPS 접속을 시도하게 되나 테스트 당시에는 정상적인 접속이 이루어지지 않았다.

'hxxps://www.pr[삭제]her.com/asp/kys[삭제]_get.asp?name=getkys.kys'

정상적으로 접속되면 다음의 악의적인 기능들을 수행하는데, 악성코드들은 기존 다른 침해 사고에서 발견됐던 원격 제어 형태의 백도어다.

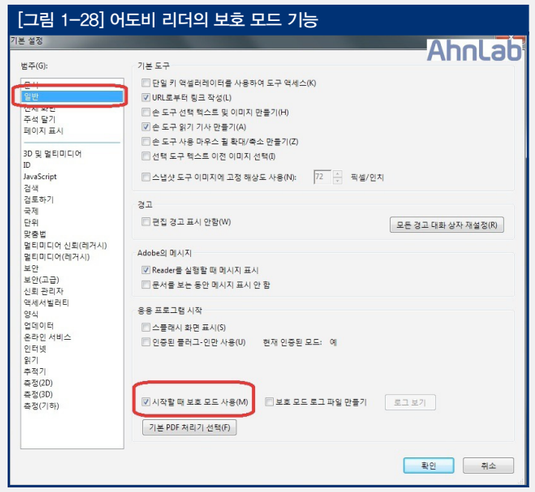
- 파일 업로드 및 다운로드
- CMD 셸 명령 수행
- 시스템 강제 종료 및 재부팅
- 프록시(Proxy) 서버

이번에 발견된 어도비 아크로뱃에 존재하는 제로데이 취약점 CVE-2011-2462를 악용한 타깃 공격은 취약한 PDF 파일과 감염되는 악성코드 등 전반적인 사항들을 고려했을 때, 기업 내부에 존재하는 중요 데이터를 탈취하기 위한 목적으로 제작 및 유포된 것으로 추정된다. 타깃 공격에 악용된 CVE-2011-2462 취약점에 대한 보안 패치는 어도비에 의해 현지 시각으로 12월 12일 배포됐다.

어도비는 해당 제로데이 취약점에 대한 임시 방안으로 어도비 리더의 버전을 10.0으로 업그레이드하고 해당 버전에 포함돼 있는 보호 모드(Protected Mode)와 보호 뷰(Protected View) 기능을 활성화할 것을 권고했다.

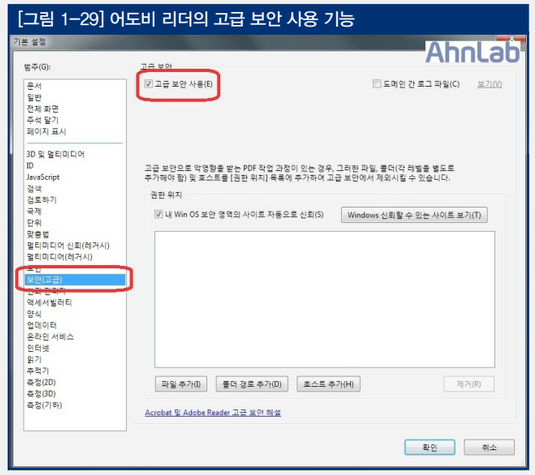
메뉴 → 편집 → 기본 설정 → 일반 → 시작할 때 보호 모드 사용(활성)

[그림 1-28] 어도비 리더의 보호 모드 기능



메뉴 → 편집 → 기본 설정 → 보안(고급) → 고급 보안 사용(활성)

[그림 1-29] 어도비 리더의 고급 보안 사용 기능



〈V3 제품군의 진단명〉

- PDF/CVE-2011-2462
- Win-Trojan/Agent.39936.BAT
- Backdoor/Win32.CSon

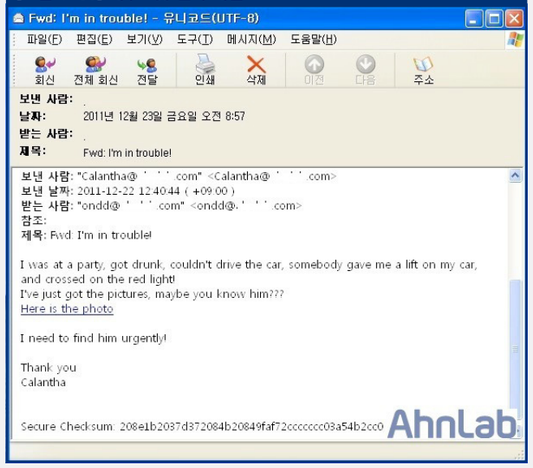
여러 가지 취약점을 이용한 제우스봇 전파 메일 발견

2011년 12월 23일 국내에서 제우스 봇(Zeus Bot) 유포를 위해 여러 가지 애플리케이션들의 취약점을 악용해 웹 페이지 접속을 유도하는 이메일이 발견됐다. 이번에 유포된 이메일의 제목은 〈Fwd : I'm in trouble〉이며 본문 내용은 다음과 같다.

> I was at a party, got drunk, couldn't drive the car, somebody gave me a lift on my car, and crossed on the red light!
> I've just got the pictures, maybe you know him???
> Here is the photo.
> I need to find him urgently!
>
> Thank you.
> 〈보낸 사람〉

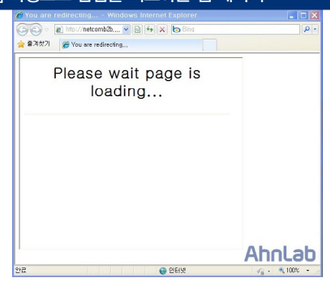
유포된 이메일의 형태는 [그림 1-30]과 같다.

[그림 1-30] 제우스봇 전파 메일



해외 보안 업체 컴터치(Commtouch)는 블로그 〈The "I' m in trouble" massive malware outbreak〉를 통해 이러한 이메일의 변형들도 상당수 존재할 것이라고 경고했다. 메일 수신자가 이메일 본문의 'Here is the photo'를 클릭하면 악성코드 감염을 시도하는 특정 웹 페이지로 연결된다.

[그림 1-31] 악성코드 감염을 시도하는 웹 페이지



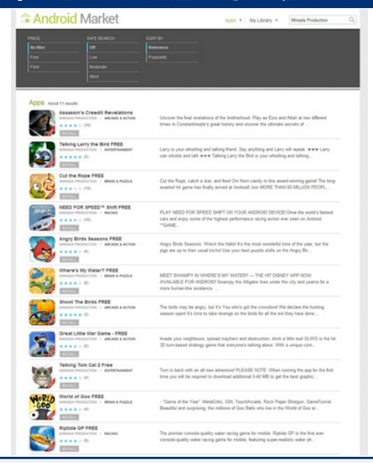
해당 웹 페이지는 다른 웹 페이지를 로딩하는 것으로 위장한 'Please wait page is loading...' 문구를 보여주며 다양한 애플리케이션들의 취약점을 악용해 악성코드 감염을 시도한다. 해당 웹 페이지에 존재하는 난독화된 스크립트를 풀어보면 "Microsoft 보안 권고(2219475) Windows 도움말 및 지원 센터의 취약점으로 인한 원격 코드 실행 문제점"과 함께 자바, 어도비 플래시 등에 존재하는 다양한 취약점들을 악용해 악성코드 감염을 시도하는 것으로 분석됐다.
해당 취약점들을 통해 다운로드되는 파일은 인터넷 뱅킹 정보 유출을 위해 제작된 제우스 봇 악성코드다.

〈V3 제품군의 진단명〉
– Win-Trojan/Obfuscated.Gen

구글 안드로이드 마켓에 업로드된 악성 애플리케이션

2011년 초, 구글 공식 안드로이드 마켓에 악성 애플리케이션이 업로드됐던 것과 같이, 이번에 또 다시 악성 애플리케이션이 업로드됐다. 유럽 지역 국가에서는 이 악성코드가 유명 모바일 게임으로 위장해 프리미엄 번호로 SMS를 전송함으로써 과금을 유발했다. 국내 피해 사례에 대한 보고는 없었다. 해당 악성코드들은 [그림 1-32]과 같이 Angry birds, Assasin Creed 등 인기 게임의 아이콘, 애플리케이션명으로 위장하고 있어 정상 게임과 구분이 어렵다.

[그림 1-32] 안드로이드 마켓에 유포된 악성코드 〈출처 : 시만텍 블로그〉



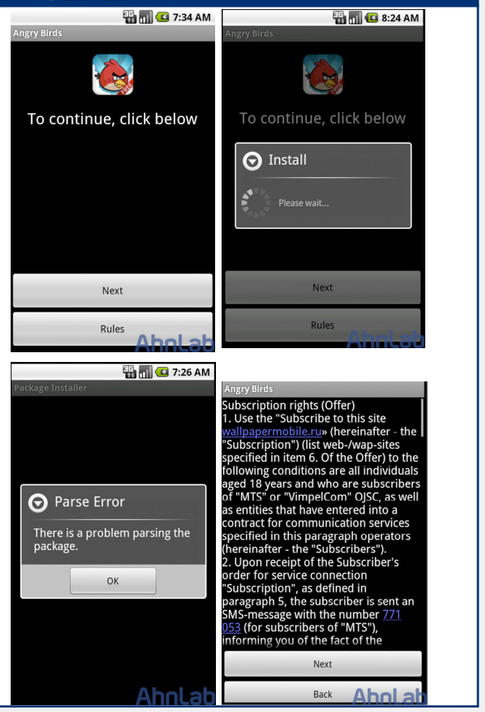
[그림 1-33] 악성 애플리케이션

[그림 1-34] 정상 애플리케이션

해당 악성코드는 구글 공식 안드로이드 마켓(http://market.android.com)을 통해 유포됐고, 현재는 마켓에서 제외됐다.

해당 애플리케이션을 설치하면 [그림 1-35]와 같이 정상 게임에선 볼 수 없는 화면이 나오며, 게임을 하기 위해 http://91.xxx.xxx.148/app URL을 통한 추가적인 애플리케이션 다운로드를 유도한다(현재 정상 접속은 불가능한 것으로 확인된다).

[그림 1-35] 실행 화면/Rules



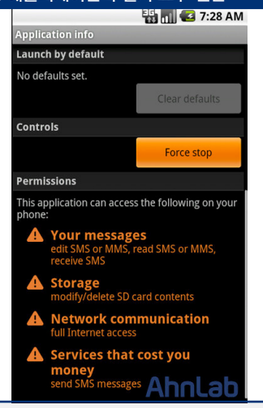
첫 화면의 Rules를 클릭하면 해당 프로그램이 SMS를 전송한다는 약관을 보여준다. 이는 이전 ASEC 리포트에서 언급했던 FakeInst 변종과 유사하다. 악성코드는 sim card에서 단말기의 국가 코드를 파싱해 국가에 맞는 과금 번호(premium number)로 문자를 전송한다. 과금 관련 코드는 [표 1-5]와 같이 총 18개의 유럽 지역 국가에 대해서 발송하도록 설정돼 있다.

해당 악성코드는 [그림 1-36]과 같이 'SMS 과금 관련 권한'을 보면 구분이 가능하므로, 애플리케이션 설치 시 항상 권한을 주의깊게 살핀 후 설치하는 습관을 갖도록 하자.

[표 1-5] 문자 과금 대상 국가

국가 코드	송신 번호	국가 이름
am	1121	Armenia
az	9014	Azerbaijan
by	7781	Belarus
cz	90901599	Czech Republic
de	80888	Germany
ee	17013	Estonia
fr	81185	France
gb	79067	United Kingdom
ge	8014	Georgia
il	4545	Israel
kg	4157	Kyrgyzstan
kz	7790	Kazakhstan
lt	1645	Lithuania
lv	1874	Latvia
pl	92525	Poland
ru	7781	Russian Federation
tj	1171	Tajikistan
ua	7540	Ukraine

[그림 1-36] 악성 애플리케이션의 설치 요구 권한

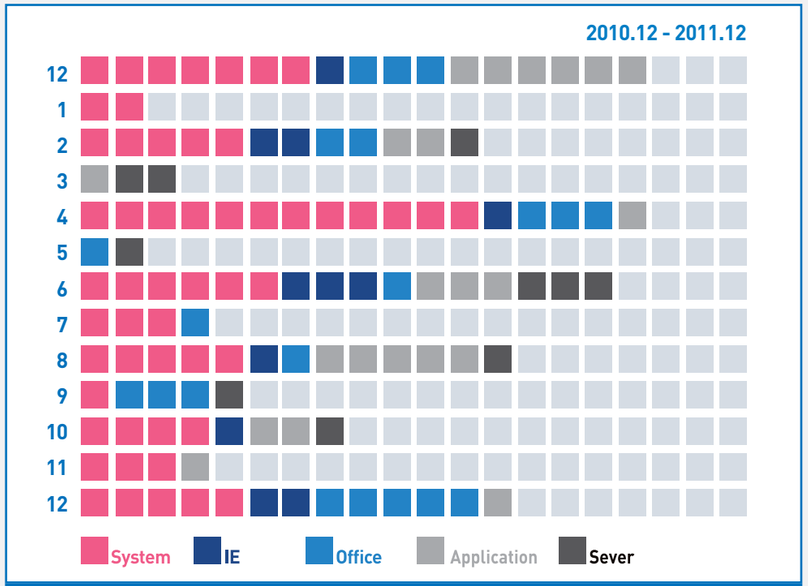


〈V3 mobile 제품군의 진단명〉
– Android-Trojan/Pavelsms

02. 시큐리티 동향
a. 시큐리티 통계

12월 마이크로소프트 보안 업데이트 현황

마이크로소프트로부터 발표한 보안 업데이트는 13건이며 총 13건의 패치가 제공됐다. 이 중 악성코드로 이용될 수 있는 보안 취약점은 9가지로, 많은 악성코드들이 이용할 가능성이 큰 만큼 각별한 주의와 업데이트가 필요하다.



[그림 2-1] 공격 대상 기준별 MS 보안 업데이트

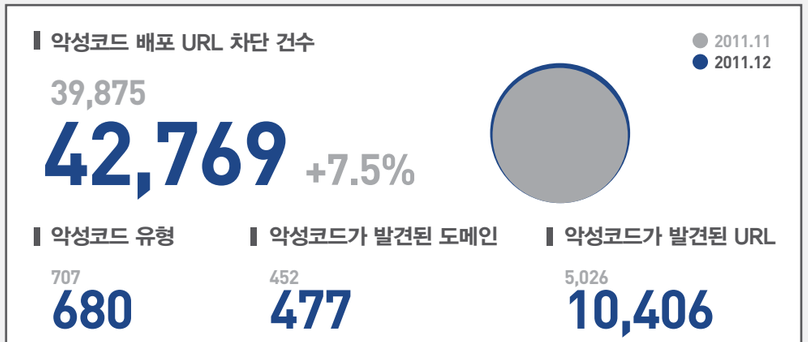
위험도	취약점
긴급	Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드 실행 문제점(2639417)
긴급	ActiveX 킬(Kill) 비트 누적 보안 업데이트(2618451)
긴급	Windows Media의 취약점으로 인한 원격 코드 실행 문제점(2648048)
중요	Microsoft Office IME(중국어)의 취약점으로 인한 권한 상승 문제점(2652016)
중요	Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점(2590602)
중요	Microsoft Publisher의 취약점으로 인한 원격 코드 실행 문제점(2607702)
중요	OLE의 취약점으로 인한 원격 코드 실행 문제점(2624667)
중요	Microsoft PowerPoint의 취약점으로 인한 원격 코드 실행 문제점(2639142)
중요	Windows Active Directory의 취약점으로 인한 원격 코드 실행 문제점(2640045)
중요	Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점(2640241)
중요	Windows CSRSS(Client/Server Runtime Subsystem)의 취약점으로 인한 권한 상승 문제점(2620712)
중요	Windows 커널의 취약점으로 인한 권한 상승 문제점(2633171)
중요	Internet Explorer 누적 보안 업데이트(2618444)

[표 2-1] 2011년 12월 주요 MS 보안 업데이트

03. 웹 보안 동향
a. 웹 보안 통계

웹사이트 보안 요약

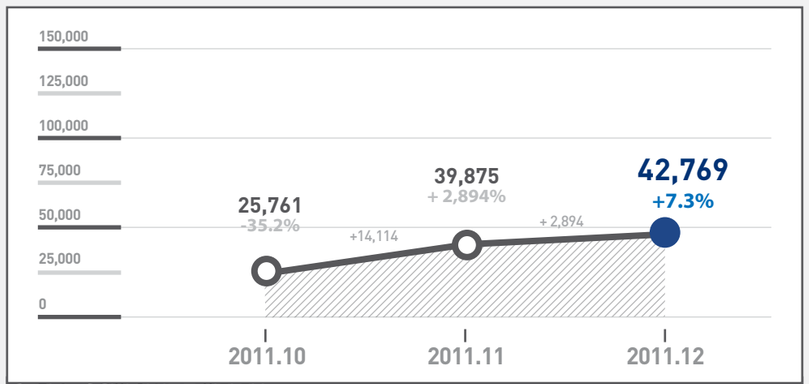
안철수연구소의 웹 브라우저 보안 서비스 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 따르면, 2011년 12월 악성코드를 배포하는 웹 사이트의 차단 건수는 총 4만 2769건이다. 또한 악성코드 유형은 680건이며, 악성코드가 발견된 도메인은 477건, 악성코드가 발견된 URL은 1만 406건이다. 이를 2011년 11월과 비교해보면 악성코드 유형은 감소했으나 나머지 항목은 증가했다.



[표 3-1] 웹 사이트 보안 요약

월별 악성코드 배포 URL 차단 건수

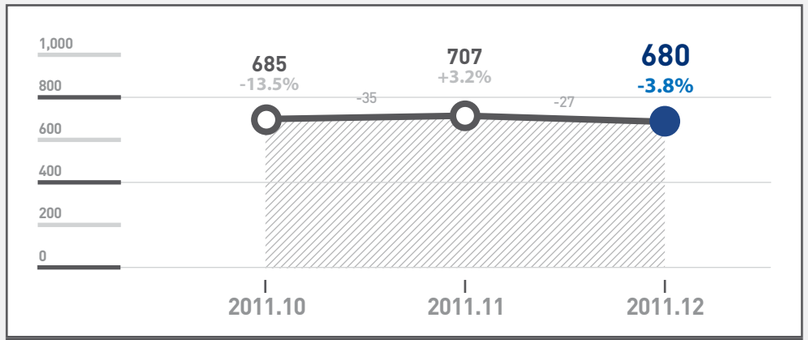
2011년 12월 악성코드 배포 웹 사이트 URL 접근에 따른 차단 건수는 지난달 3만 9875건에 비해 7% 증가한 4만 2769건이었다.



[그림 3-1] 월별 악성코드 발견 건수

월별 악성코드 유형

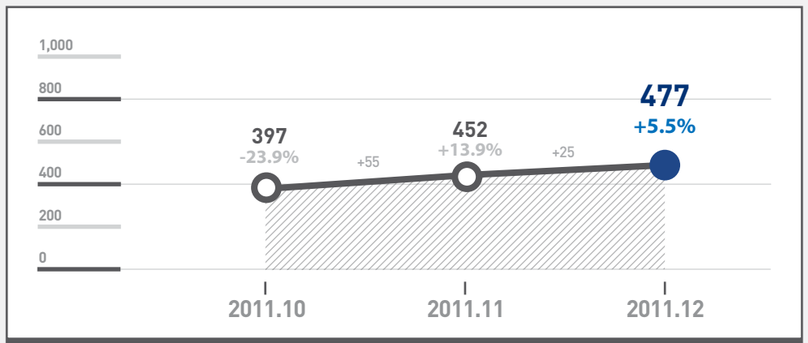
2011년 12월 악성코드 유형은 전달의 707건에 비해 4% 줄어든 680건이었다.



[그림 3-2] 월별 악성코드 유형

월별 악성코드가 발견된 도메인

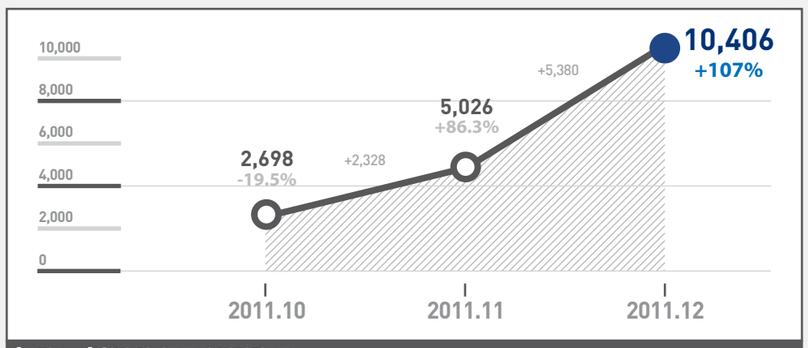
2011년 12월 악성코드가 발견된 도메인은 11월의 452건에 비해 5% 증가한 477건이었다.



[그림 3-3] 월별 악성코드가 발견된 도메인

월별 악성코드가 발견된 URL

2011년 12월 악성코드가 발견된 URL은 전달의 5026건에 비해 107% 늘어난 1만 406건이다.



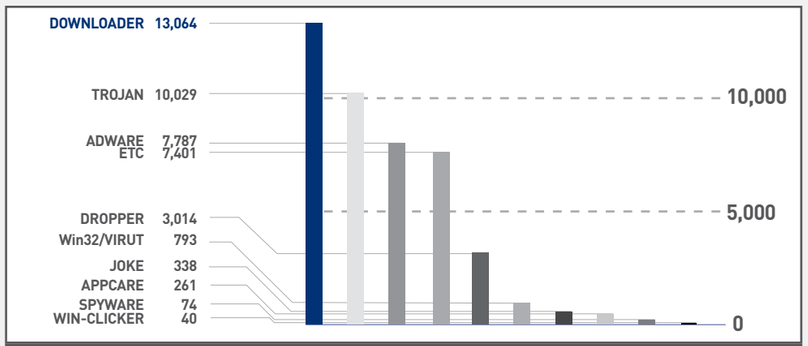
[그림 3-4] 월별 악성코드가 발견된 URL

악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면 다운로더가 1만 3064건/30.5%로 가장 많았고, 트로이목마가 1만 29건/23.4%인 것으로 조사됐다.

유형	건수	비율
DOWNLOADER	**13,064**	**30.5 %**
TROJAN	10,029	23.4 %
ADWARE	7,787	18.2 %
DROPPER	3,014	7.0 %
Win32/VIRUT	793	1.9 %
JOKE	338	0.8 %
APPCARE	229	0.5 %
SPYWARE	74	0.2 %
WIN-CLICKER	40	0.1 %
ETC	7,401	17.4 %
	42,769	**100.0 %**

[표 3-2] 악성코드 유형별 배포 수



[그림 3-5] 악성코드 유형별 배포 수

악성코드 배포 순위

악성코드 배포 건수는 Downloader/Win32.Genome이 4499건으로 가장 많았다. 또 Win-Adware/Woowa.28672.B 등 6건이 새로 등장했다.

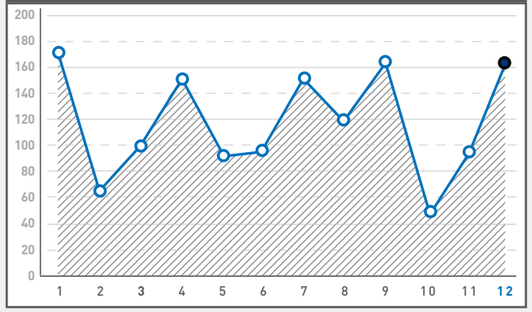
순위	등락	악성코드명	건수	비율
1	**▲1**	**Downloader/Win32.Genome**	**4,499**	**20.5 %**
2	▲3	Downloader/Win32.Korad	3,469	15.8 %
3	▲5	Downloader/Win32.Totoran	3,152	14.3 %
4	▲2	Unwanted/Win32.WinKeygen	2,337	10.6 %
5	NEW	Win-Adware/Woowa.28672.B	1,653	7.5 %
5	NEW	Win-Downloader/Woowa.270336	1,653	7.5 %
7	NEW	Win-Adware/Woowa.61440.B	1,652	7.5 %
8	NEW	Win-Trojan/Downloader.765408	1,417	6.5 %
9	NEW	Adware/Win32.KorAd	1,225	5.6 %
10	NEW	Unwanted/Win32.WinKeyfinder	909	4.2 %
			21,966	**100.0 %**

[표 3-3] 악성코드 배포 최다 10

03. 웹 보안 동향
b. 웹 보안 이슈

2011년 12월 침해 사이트 현황

[그림 3-6] 2011년 12월 악성코드 유포 목적의 침해 사이트 현황



[그림 3-6]은 악성코드 유포를 목적으로 하는 침해 사고가 발생했던 사이트의 현황이다. 2011년 12월은 11월보다 2배 정도 증가했는데, 11월까지 악성코드 유포에서 소강상태를 보였던 언론사, P2P 웹하드 등 다수의 사이트들이 12월 들어 다시 악성코드 유포에 활용됐기 때문인 것으로 추정된다.

[표 3-4] 침해 사이트를 통해서 유포된 악성코드 최다 10

순위	악성코드명	건수
1	**Win-Trojan/Onlinegamehack.86528.BW**	**59**
2	Dropper/Win32.OnlineGameHack	54
3	Win-Trojan/Onlinegamehack.74752.AO	31
4	Trojan/Win32.OnlineGameHack	28
5	Win-Trojan/Onlinegamehack.76288.BL	28
6	Win-Trojan/Onlinegamehack.111616.AJ	26
7	Win-Trojan/Onlinegamehack.121487	21
8	Win-Trojan/Onlinegamehack.136704.O	21
9	Win-Trojan/Onlinegamehack.129113	20
10	Win-Trojan/Onlinegamehack.77312.AY	20

[표 3-4]는 한 달간 침해 사이트를 통해서 가장 많이 유포된 악성코드 10건이다. Win-Trojan/Onlinegamehack.86528.BW는 언론사, P2P 웹하드 사이트를 포함한 59개의 해킹된 사이트를 통해 유포됐지만 빠른 대응 덕분에 큰 피해는 발생하지 않았다. 또 매주 새로운 진단명으로 갱신되는 것을 볼 수 있는데, 이는 금요일 저녁에 악성코드의 유포가 시작되고 새로운 한 주가 시작되는 월요일 아침에 악성코드 유포가 소강상태에 접어드는 사이클이 반복되는 과정에서 새로운 변종들이 발견되기 때문이다.

2. 2011년 보안 동향 분석

01. 악성코드 동향
a. 악성코드 통계

2011 악성코드 감염보고 최다 20

2011년 악성코드 통계 현황은 [표 1-1]과 같다. 2011년의 악성코드 감염 보고는 Textimage/Autorun이 가장 많았으며, JS/Agent와 Win32/Induc이 뒤를 이었다. 새로 상위 20건에 포함된 악성코드는 총 8건이다.

순위	등락	악성코드명	건수	비율
1	—	Textimage/Autorun	9,458,847	24.2 %
2	▲1	JS/Agent	6,217,163	15.9 %
3	▼1	Win32/Induc	2,149,558	5.5 %
4	▲12	Html/Agent	1,859,891	4.8 %
5	▲9	JS/Downloader	1,789,695	4.6 %
6	NEW	JS/Redirect	1,580,959	4.1 %
7	▼2	JS/Exploit	1,545,389	4.0 %
8	—	JS/Iframe	1,446,928	3.7 %
9	NEW	Swf/Agent	1,432,679	3.7 %
10	NEW	Win32/Palevo1.worm.Gen	1,389,561	3.6 %
11	NEW	Exploit/Cve-2011-2140	1,351,151	3.5 %
12	▼6	Win32/Olala.worm	1,090,949	2.8 %
13	▼6	Win32/Conficker.worm.Gen	1,045,633	2.7 %
14	▼10	Win32/Parite	1,036,725	2.7 %
15	NEW	Swf/Dropper	997,347	2.6 %
16	NEW	JS/Redirector	974,413	2.5 %
17	NEW	Swf/Exploit	938,527	2.4 %
18	NEW	Win32/Virut.f	929,265	2.3 %
19	—	JS/Cve-2010-0806	926,738	2.3 %
20	▼8	Als/Bursted	870,959	2.1 %
			39,032,377	100 %

[표 1-1] 2011년 악성코드 감염 보고 최다 20건

악성코드 대표진단명 감염보고 최다 20

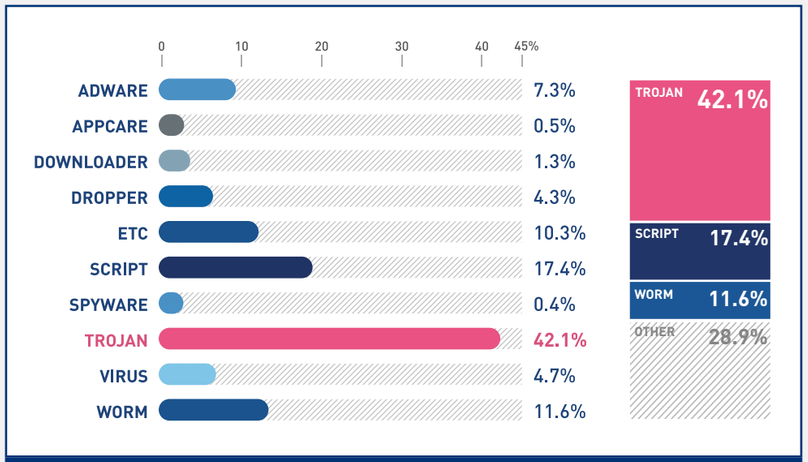
[표 1-2]는 악성코드별 변종 종합 감염 보고 순위를 악성코드 대표 진단명에 따라 정리한 것이다. 이를 통해 2011년 한 해 동안의 악성코드 동향을 파악할 수 있다. 2011년 사용자 피해를 주도한 악성코드 중 최다 감염 보고는 Win-Trojan/Onlinegamehack으로 총 1077만 803건/12.3%로 조사됐다. 또한 Win-Trojan/Agent이 963만 7067건/11%, Textimage/Autorun이 946만 413건/10.8%로 나타났다.

순위	등락	악성코드명	건수	비율
1	—	Win-Trojan/Onlinegamehack	10,770,803	12.3 %
2	—	Win-Trojan/Agent	9,637,067	11.0 %
3	▲1	Textimage/Autorun	9,460,413	10.8 %
4	▼1	Win-Trojan/Downloader	8,788,092	10.0 %
5	▲4	JS/Agent	6,339,235	7.2 %
6	NEW	Win-Trojan/Winsoft	5,319,281	6.1 %
7	NEW	Win-Adware/Korad	4,630,273	5.3 %
8	▼1	Win32/Conficker	3,886,522	4.4 %
9	▼4	Win32/Autorun.worm	3,845,424	4.4 %
10	▼2	Win32/Virut	3,491,801	4.0 %
11	▲6	Win-Trojan/Adload	3,220,138	3.7 %
12	▲2	Dropper/Malware	2,634,813	3.0 %
13	▼2	Win32/Kido	2,587,269	3.0 %
14	▼8	Win32/Induc	2,150,951	2.5 %
15	NEW	Win-Trojan/Patched	1,905,777	2.2 %
16	NEW	Html/Agent	1,859,894	2.1 %
17	▼4	Dropper/Onlinegamehack	1,847,805	2.1 %
18	NEW	JS/Downloader	1,789,696	2.0 %
19	▼4	Win32/Palevo	1,739,145	2.0 %
20	NEW	VBS/Solow	1,604,220	1.9 %
			87,508,619	100 %

[표 1-2] 2011년 악성코드 대표 진단명 감염 보고 상위 최다 20건

악성코드 유형별 감염보고 비율

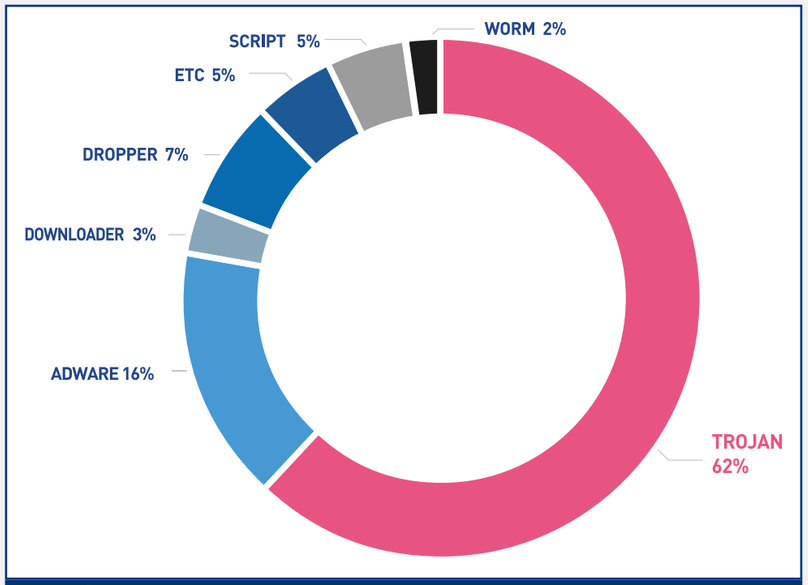
[그림 1-1]은 2011년 한 해 동안 안철수연구소가 고객으로부터 감염이 보고된 악성코드의 유형별 감염 비율을 집계한 결과이다. 2011년 감염 보고 건수 비율은 트로이목마가 42.1%로 가장 많았으며, 스크립트가 17.4%, 웜이 11.6%로 나타났다.



[그림 1-1] 2011년 악성코드 유형별 감염 보고 비율

2011년 신종 악성코드 유형별 분포

2011년의 신종 악성코드 유형을 보면 트로이목마가 62%로 가장 많았고, 애드웨어가 16%, 드롭퍼가 7%인 것으로 나타났다.



[그림 1-2] 2011년 신종 악성코드 유형별 분포

2011년 신종 악성코드 감염 보고 최다 20건

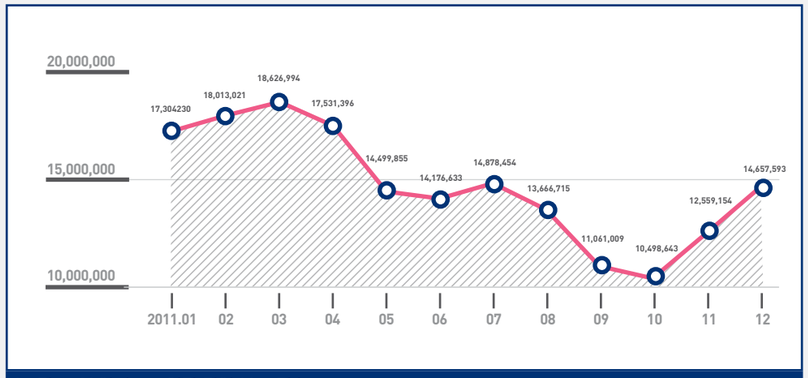
[표 1-3]은 2011년에 신규 접수된 악성코드 중 고객으로부터 감염이 보고된 악성코드 상위 20건이다. Win-Trojan/Patched.CR가 75만 7876건으로 전체의 25.8%, Win-Trojan/Overtls11.Gen가 70만 456건/23.9%인 것으로 나타났다.

순위	악성코드명	건수	비율
1	Win-Trojan/Patched.CR	757,876	25.8 %
2	Win-Trojan/Overtls11.Gen	700,456	23.9 %
3	Win-Trojan/Downloader.59904.AK	278,527	9.5 %
4	Win-Trojan/Winsoft17.Gen	222,208	7.6 %
5	Win-Trojan/Adload.77312.LPU	181,176	6.2 %
6	Win-Trojan/Winsoft18.Gen	104,026	3.5 %
7	Win-Trojan/Winsoft.263168.KX	75,337	2.6 %
8	Win-Trojan/Winsoft.263168.LO	73,994	2.5 %
9	Win-Trojan/Agent.339968.EI	69,762	2.4 %
10	Win-Trojan/Agent.323584.FK	68,946	2.3 %
11	Win-Trojan/Winsoft.281088.GHF	52,943	1.8 %
12	Win-Trojan/Winsoft.281088.GGM	46,160	1.6 %
13	Win-Trojan/Winsoft.263168.LR	40,889	1.4 %
14	Win-Trojan/Fakeav.182312	40,350	1.4 %
15	Win-Trojan/Adload.267776.F	39,963	1.4 %
16	Win-Trojan/Adload.267264.B	39,301	1.3 %
17	Win-Trojan/Downloader.163840.BG	38,461	1.3 %
18	Win-Trojan/Downloader.550912	37,049	1.3 %
19	Win-Adware/BHO.WowLinker.615424	34,842	1.2 %
20	Win-Trojan/Adload.321536.D	33,034	1.0 %
		2,935,300	100 %

[표 1-3] 신종 악성코드 감염 보고 최다 20건

악성코드 연간 감염 보고 건수

2011년의 악성코드 감염 보고 건수는 1억 7747만 3697건으로 2010년의 1억 4609만 7262건에 비해 3137만 6435건이 증가한 것으로 나타났다.



[그림 1-3] 악성코드 연간 감염 보고 건수

01. 악성코드 동향
b. 악성코드 이슈

모바일 악성코드 급증

1. 과금형 악성코드 폭발적 증가

2011년을 대표하는 안드로이드 악성코드로는 과금형 악성코드를 꼽을 수 있다. 과금형 악성코드는 안드로이드 플랫폼 자체가 전화나 문자 기능이 포함된 스마트폰 OS라는 점을 악용한 예이다. 우리가 흔히 알고 있는 문자 과금 방식(premium call)을 주로 이용하며, 감염 시 추가 과금을 유발하는 특정 번호로 문자를 보내 사용자들에게 금전적인 피해를 준다. 가장 최근에 발견된 과금 악성코드는 Android-Trojan/Pavelsms(http://asec.ahnlab.com/751)로, 해외에선 ruFraud라는 이름으로 알려져 있다. 감염 시 스마트폰의 가입 국가를 파악하고 유럽 내 스마트폰일 경우 각 국가에 맞는 프리미엄 문자를 보내는 것이 특징이다.

2. 유명 애플리케이션으로 위장한 Fake 악성코드

Google Search, Google+, Angry bird, Opera, Skype 등 사용자층이 두터운 유명 애플리케이션으로 위장한 악성코드가 배포된 사례가 있었다. 위장형 악성코드는 주로 서드 파티 마켓을 통해 배포됐으며, 실제 정상 애플리케이션과 아이콘 • 애플리케이션 이름이 완전히 동일해 사용자가 쉽게 구분할 수 없었다. 다른 위장형 악성코드로는 정상 애플리케이션과 완전히 동일하게 동작하면서 추가로 악성코드를 삽입, 재배포하는 리패키징(repackaging)형 악성코드가 있다(참조: http://asec.ahnlab.com/258).

3. 사생활 침해형 애플리케이션 증가

스마트폰은 통화 및 문자 송수신, 카메라, GPS 등 PC보다 좀더 생활에 밀착된 기능이 많아 민감한 정보들이 들어있기 마련이다. 만약 이러한 정보들이 임의로 유출될 시에는 심각한 사생활 침해 문제가 발생할 수 있다. Android-Spyware/Nicky와 같은 악성코드는 GPS를 통해 수집된 사용자 위치 정보, SMS 송수신, 전화 송수신 내역뿐만 아니라 보이스 레코딩 기능을 악용해 사용자의 통화 내용까지도 훔쳐가는 기능을 내장하고 있어서 큰 충격을 주었다(참고: http://asec.ahnlab.com/320 , http://core.ahnlab.com/290). 앞으로도 이러한 디지털 스토커(digital stalker)형 악성코드가 지속적으로 증가할 전망이다.

4. 온라인 뱅킹 정보를 노리는 악성코드 발생

온라인 뱅킹 정보를 갈취하는 것으로 악명 높은 제우스 봇이 다양한 모바일 환경에서도 동작하도록 제작, 유포됐다. Zitmo(Zeus In The Mobile)로 불리는 이 악성코드는 symbian, blackberry를 거쳐 최근엔 안드로이드 플랫폼까지 침투했다. 안드로이드의 Zitmo 악성코드는 트러스티어(Trusteer)라는 해외의 뱅킹 보안 업체의 제품을 위장해 유포됐으며, 온라인 뱅킹에 접속할 때 2-factor 인증 방식을 깨기 위해 SMS 수신 내역까지 감청하는 치밀함을 보여준 것이 특징이다.

스톰웜 봇넷

스톰웜은 트로이목마 악성코드로, 지난 2007년 1월 17일 처음 발견돼 19일부터 급속도로 퍼지기 시작, 전 세계 PC의 8%를 감염시켰다. 해당 악성코드는 이메일을 통해 날씨에 관한 긴급 뉴스라고 속여 사람들이 실행 파일을 다운로드하도록 유도했다. 이후 2008년 'FBI vs FaceBook'을 가장한 새로운 스톰웜 공격이 확산됐는데, 이처럼 사회적 이슈가 되는 것이나 이슈가 될만한 키워드를 이메일을 통해 전파하는 웜의 형태를 스톰웜(Storm Worm)이나 웨일덱(Wale Dac)이라 부르는 경우가 있다. 스팸 메일 속에 포함된 위장 링크를 클릭하면 웜에 감염되는데, 이후 감염된 PC들은 스팸 메일 발송지로 악용된다. 현재까지도 관련 악성 샘플이 지속적으로 증가하는 추세이고 주로 메일을 통해 전파되니 의심스러운 메일을 함부로 열람하거나 첨부파일을 열지 않도록 주의해야 한다.

윈도우 그래픽 렌더링 엔진 취약점 공격 사례 등장

Windows Graphics Rendering Engine(Shimgvw.dll)에서 thumbnail image(탐색기 보기 옵션 중 '미리보기')를 처리하면서 발생하는 Stack-based Buffer Overflow 취약점으로 임의의 코드를 실행할 수 있다.

메일은 국내 ISP 업체를 통해 발송됐으며, 송신자 메일 주소는 'Taiwan Yahoo WebMail Address(@yahoo.com.tw)'이다. 이를 통해 국내 좀비 PC를 이용해 무작위로 스팸 메일이 발송됐다고 추정할 수 있다. 메일 본문은 중국어로 이루어졌으며, 첨부 파일은 7z으로 압축된 43개의 정상 이미지 파일과 취약한 doc 파일이다. 이

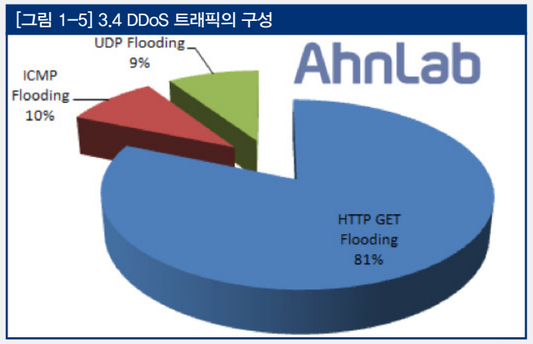
[그림 1-4] 공격에 사용한 이메일 내용

첨부 파일의 압축을 풀고 미리보기 옵션을 사용하면 취약점으로 인해 악성코드에 감염된다. 이 악성코드는 특정 웹 사이트를 통해 악의적인 파일을 다운로드 및 실행한다.

3.4 DDoS : 네트워크 관점으로 되돌아보기

공격은 크게 3가지 Flooding과 1개의 C&C 서버와의 통신에 이용되는 네트워크로 나눌 수 있다. DDoS 공격 유형별로 발생된 패킷 분포를 보면 HTTP가 가장 많으며, 다음과 같은 수준의 패킷 발생을 보여주고 있다.

[그림 1-5] 3.4 DDoS 트래픽의 구성



HTTP GET Flooding(81%) 〉 ICMP Flooding(10%) 〉 UDP Flooding(9~10%)

[표 1-4]는 악성코드 감염으로 인해 발생하는 트래픽을 산출한 것으로, 공격 대상 한 곳에서 바라본 좀비 PC 1대당 트래픽 정보를 기준으로 추산한 것이다. 그리고 이 당시 감염 추정으로 판단되는 좀비 PC의 수는 3만 1030대로 설정했다.

*** 1차 감염으로 추정되는 3만 대 기준**

[표 1-4] 활동 좀비 PC 수별 공격 트래픽 유입 현황(공격 대상 1곳 기준)

감염PC 수	Avg. packets/sec	Avg. packet size	Avg. bytes/sec	Avg. Mbit/sec
1PC	25	174	4.2K	0.033M
31,030PCs	776K	–	130M	1G

[표 1-5] 좀비 1PC당 공격 유형 트래픽 현황
(감염 PC 1대->공격 대상 1곳, Active Attack Traffic)

공격 유형	Avg. packets/sec	Avg. packet size	Avg. bytes/sec	Avg. Mbit/sec
HTTP GET Flooding	20.43	144.522	2,952.56	0.024
ICMP Flooding	2.355	129.414	302.13	0.002
UDP Flooding	2.335	406.229	948.38	0.008
attack total	25.12		4,203.07	0.034

대규모 SQL 인젝션 '리자문' 발생

최근 웹센스(WebSense)를 통해서 대규모 SQL 인젝션 공격이 알려졌다. 이 공격은 리자문(LizaMoon)이라 불리며, 대략 22만 6000개 이상의 사이트가 침해당한 것으로 알려졌다.

[그림 1-6] 구글에서 리자문과 관련한 검색 결과

소니 플레이스테이션 네트워크 7700만 명 정보 유출

전 세계적으로 많은 게임 사용자층을 확보하고 있는 소니 플레이스테이션 네트워크에서 약 7700만 명의 데이터 유출이라는 초유의 사건이 발생했다. 이름, 주소, 이메일 주소, 생년월일, 사용자 아이디, 사용자 패스워드, 로그인 정보 등 많은 정보가 유출된 것으로 보인다. 소니에 의하면 플레이스테이션 네트워크와 큐리오시티 서비스는 4월 17일과 4월 19일 사이에 침해 사고가 발생한 것으로 보이며, 얼마나 많은 정보가 유출됐는지는 자세히 밝히지 않았다. 신용카드 정보도 유출됐는지에 대한 정확한 증거는 없지만 유출 가능성이 있어 앞으로 이 정보를 이용한 악의적인 사건 • 사고가 발생할 소지가 충분하다.

해외 인터넷 뱅킹 노리는 제우스 소스 유출과 스파이아이 동향

해외 인터넷 뱅킹 악성코드로 유명한 제우스(Zeus) 2.0.8.9 버전 소스가 유출됨에 따라 국내 인터넷 뱅킹에도 적신호가 켜졌다. 물론 유출된 소스는 최신 버전이 아니며 해외에 특화돼 있지만 어떤 식으로든 악용될 소지가 있기 때문에 주의를 기울일 필요가 있다.

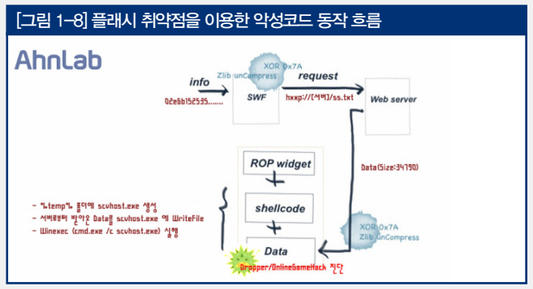
스파이아이(SpyEye)는 12월 이후 접수되는 샘플은 감소하는 추세이나 꾸준히 새로운 C&C 서버가 등장하며 활발히 활동하고 있는 것으로 보인다. 확보된 샘플에서 스파이아이 C&C 서버의 국가 정보를 보면 미국이 34%로 가장 많은 비중을 차지하고 있고 우크라이나가 16%, 러시아가 15%이며 한국도 12%를 차지하고 있다.

[그림 1-7] 제우스 C&C 서버 맵

어도비 플래시 제로데이

어도비 플래시 취약점을 이용한 악성코드가 특정 사이트를 해킹해 배포됐다. 어도비의 보안 패치가 나오기 전에 유포된 취약점을 이용한 플래시 파일이며, 악성코드가 배포된 사이트를 접속한 사용자는 악성코드에 감염됐을 가능성이 크다.

[그림 1-8] 플래시 취약점을 이용한 악성코드 동작 흐름



PDF 취약점을 악용한 Jailbreak 3.0

iOS 4.3.3 버전을 탑재한 아이폰 • 아이패드를 5초만에 탈옥시킬 수 있는 jailbreakme 3.00이 공개됐다. iOS 사용자들은 아이폰 • 아이패드에 탑재된 사파리(Safari) 브라우저를 통해, [그림 1-9]의 www.jailbreakme.com에 접속해서 Free 버튼을 눌러 Cydia를 설치하는 것만으로 간단하게 탈옥을 완료할 수 있다.

해당 취약점은 공개적으로는 jailbreak 목적으로 사용됐지만, 악의적인 의도로 작성된 PDF 파일 링크를 통해 얼마든지 타인의 스마트폰을 장악할 수 있다는 점에서 매우 심각한 위협이 될 수 있다.

[그림 1-9] Jailbreak 3.0

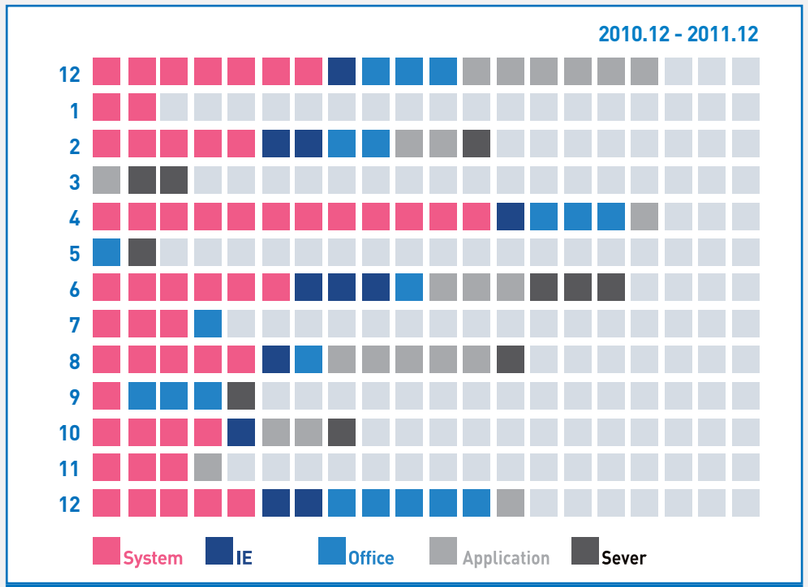
DNS 서버 이상? BIND 제로데이!

DNS BIND 애플리케이션에 크래시가 일어나 DSN 서비스가 중지되는 제로데이 공격이 발생했다. BIND(Berkeley Internet name Daemon)는 네임서버를 운영하기 위해 설치하는 서버 측 소프트웨어로 미국 기준으로 DNS의 90% 이상이 사용하고 있다. 해당 제로데이(CVE-2011-4313)는 캐시에 존재하지 않는 레코드를 돌려주는 과정에서 발생하는 취약점이다. 크래시가 나면 "INSIST(! dns_rdataset_isassociated(sigrdataset))" 로그를 남긴다.

02. 시큐리티 동향
a. 시큐리티 통계

2011년 마이크로소프트 보안 업데이트 현황

2011년 한 해 마이크로소프트에서 발표한 보안 업데이트는 총 99건으로 2010년 103건에 비해 4건이 적었다. 전년도와 비슷한 형태의 시스템 관련 취약점들이 나타났으며, 마이크로소프트의 인터넷 익스플로러, 오피스뿐만 아니라 어도비의 PDF 및 SWF 취약점 등의 애플리케이션 취약점도 꾸준히 발생했다.

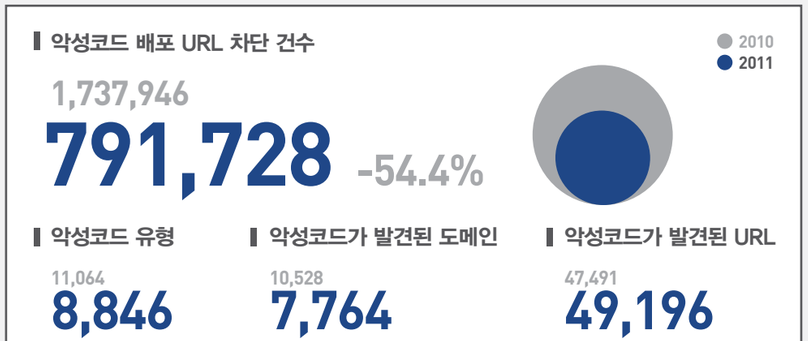


[그림 2-1] 공격 대상 기준별 MS 보안 업데이트

03. 웹 보안 동향
a. 웹 보안 통계

웹사이트 보안 요약

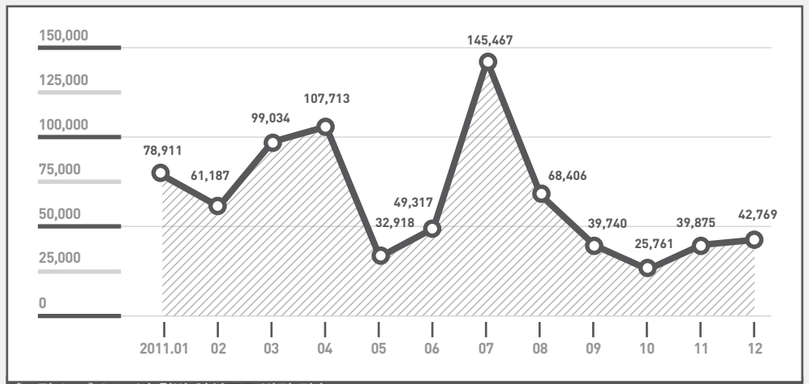
안철수연구소의 웹 브라우저 보안 서비스 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 따르면, 2011년 악성코드를 배포하는 웹 사이트의 차단 건수는 총 79만 1728건이었다. 또한 악성코드 유형은 8846건이며, 악성코드가 발견된 도메인은 7764건, 악성코드가 발견된 URL은 4만 9196건이었다.



[표 3-1] 2011년 웹 사이트 보안 요약

월별 악성코드 배포 URL 차단 건수

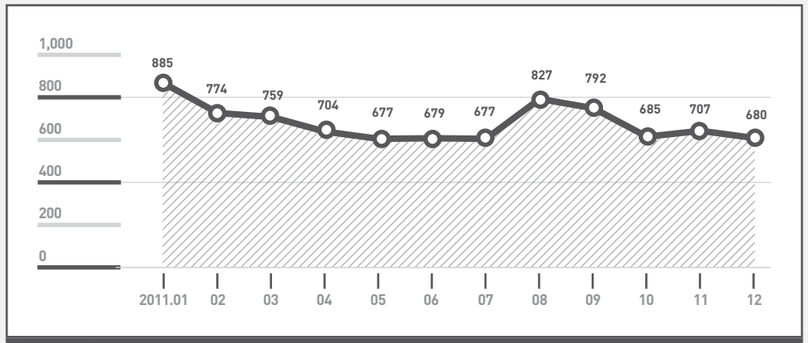
2011년 악성코드 배포 웹 사이트 URL 접근에 따른 차단 건수는 전년도 173만 7946건의 46% 수준인 79만 1728건이었다.



[그림 3-1] 2011년 월별 악성코드 발견 건수

월별 악성코드 유형

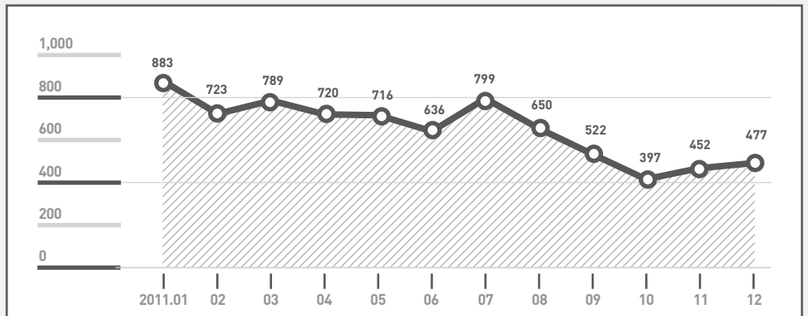
2011년 악성코드 유형은 전년도의 1만 1064건의 80% 수준인 8846건이었다.



[그림 3-2] 2011년 월별 악성코드 유형

월별 악성코드가 발견된 도메인

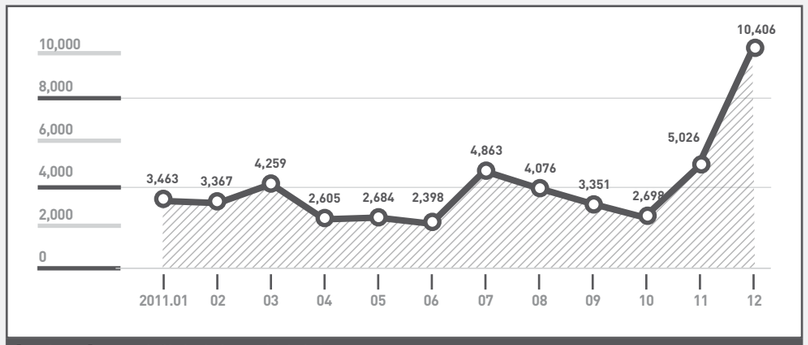
2011년 악성코드가 발견된 도메인은 전년도의 1만 528건의 74% 수준인 7764건이다.



[그림 3-3] 2011년 월별 악성코드가 발견된 도메인

월별 악성코드가 발견된 URL

2011년 악성코드가 발견된 URL은 전년도의 4만 7491건에 비해 4% 증가한 4만 9196건이다.



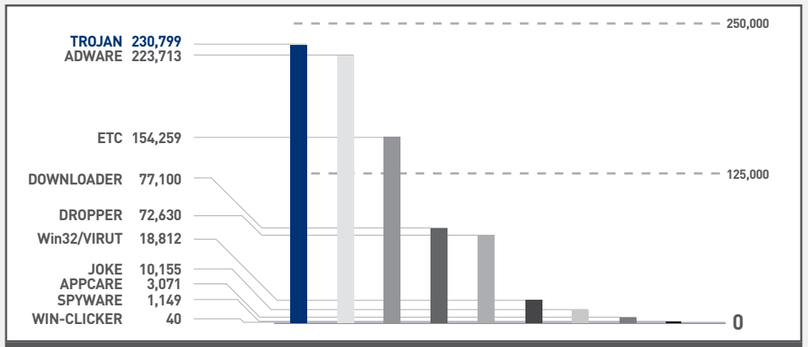
[그림 3-4] 2011년 월별 악성코드가 발견된 URL

악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면, 트로이목마가 23만 799건/29.2%로 가장 많았고, 애드웨어가 22만 3713건/28.3%로 조사됐다.

유형	건수	비율
TROJAN	**230,799**	**29.2 %**
ADWARE	223,713	28.3 %
DOWNLOADER	77,100	9.7 %
DROPPER	72,630	9.2 %
Win32/VIRUT	18,812	2.4 %
JOKE	10,155	1.3 %
APPCARE	3,071	0.4 %
SPYWARE	1,149	0.1 %
WIN-CLICKER	40	0.1 %
ETC	154,259	19.3 %
	791,728	**100.0 %**

[표 3-2] 2011년 악성코드 유형별 배포 수



[그림 3-5] 2011년 악성코드 유형별 배포 수

악성코드 배포 순위 최다 10

악성코드 배포 최다 10건 중에서 Win32/Induc이 6만 9889건으로 가장 많았고 Win-Adware/ADPrime.8372410이 5만 488건으로 뒤를 이었다.

순위	등락	악성코드명	건수	비율
1	**▲1**	**Win32/Induc**	**69,889**	**8.9 %**
2	NEW	Win-Adware/ADPrime.837241	50,488	6.4 %
3	▼2	Win-Adware/Shortcut.InlivePlayerActiveX.234	37,975	4.8 %
4	NEW	Win-Trojan/Agent.286616	34,689	4.4 %
5	NEW	Win-Trojan/Downloader.765408	32,665	4.2 %
6	NEW	Virus/Win32.Induc	24,697	3.1 %
7	NEW	Win-Adware/ToolBar.Cashon.308224	22,782	2.9 %
8	NEW	Win-Downloader/KorAd.83968	22,549	2.9 %
9	NEW	Win-Adware/Shortcut.Unni82.3739648	19,412	2.5 %
10	NEW	Win-Adware/KorZlob.3919486	14,617	1.9 %
			329,763	**42.0 %**

[표 3-3] 2011년 악성코드 배포 최다 10

03. 웹 보안 동향
b. 웹 보안 이슈

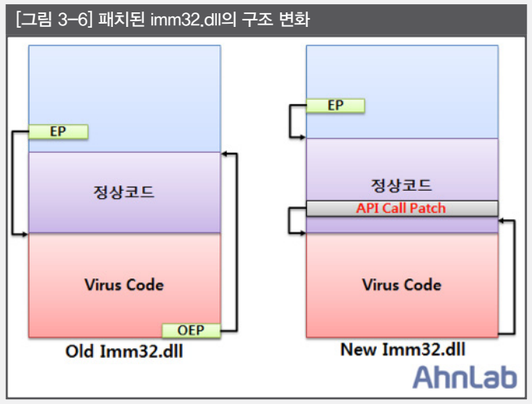
2011년, 해킹된 웹 사이트를 통해서 유포된 악성코드들의 특징을 요약해 보면 다음과 같다.

시스템 파일 변조

악성코드에 의한 시스템 파일 변조는 오래 전부터 있었지만 2011년에는 그 현상이 두드러졌다. imm32.dll부터 ws2help.dll에 이르기까지 다양한 시스템 파일들이 악성코드에 의해서 변조됐는데, 그 중 눈에 띄는 imm32.dll과 ws2help.dll의 경우를 살펴보자.

imm32.dll을 이용하는 악성코드는 자신이 생성한 악성 DLL을 로딩하도록 imm32.dll을 패치했고, 시간이 지남에 따라 패치 방식에도 변화가 있었다.

[그림 3-6] 패치된 imm32.dll의 구조 변화



[그림 3-6]을 보면 패치된 imm32.dll(New Imm32.dll)은 특정 API 호출 부분을 패치해 악성 DLL을 로딩하는 코드가 존재하는 영역으로 분기한다. ws2help.dll의 경우 정상 ws2help.dll을 다양한 파일명으로 백업한 후 악성 DLL을 ws2help.dll로 생성하는데, 일부 변종에서는 버그로 인해서 부팅 시 BSOD가 발생했다. 그 원인을 살펴보면, 시스템 재부팅 시에 악성코드로 변경된 ws2help.dll 파일이 시스템 프로세스에 인젝션할 때 안티 디버깅으로 익셉션을 유발하며, 그 처리 과정에서 EIP 레지스터가 1바이트씩 밀려 전혀 다른 명령을 수행함으로써 잘못된 메모리 주소를 참고했기 때문이다.

[그림 3-7] ws2help.dll 교체 악성코드의 버그

```
kd> dd 0006F718 + 0xb8
0006f7d0  10018132 0000001b 00010346 0006f9e4
0006f7e0  00000023 0000027f 00000000 00000000

kd> u 10018132
10018132 80b0000000ffff  xor     byte ptr [eax-1000000h],0FFh
10018139 ff              ???
                         ???
                         inc     dword ptr [eax+0B8h]
```

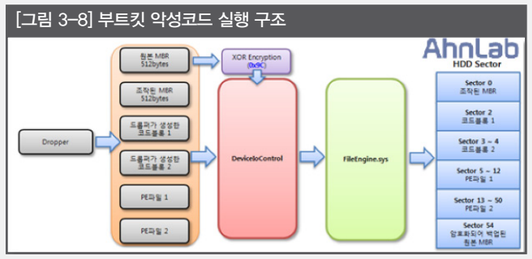
AhnLab

그러나 최근 일부 변종은 자신의 구성 파일 일부가 존재하지 않으면 악성 DLL로 교체된 ws2help.dll을 삭제해 백업된 정상 ws2help.dll과의 연결고리를 끊음으로써 의도적으로 부팅 시 BSOD를 발생시킨다.

부트킷의 등장

부트킷은 감염된 PC의 MBR(PC가 부팅하는 데 필요한 정보들이 저장된 물리적인 하드 디스크 영역, 512바이트)을 조작해, 부팅 시 악성 DLL을 생성해 특정 사이트로부터 계정 정보 탈취 목적을 가진 악성코드를 지속적으로 다운로드 및 실행케 한다.

[그림 3-8] 부트킷 악성코드 실행 구조



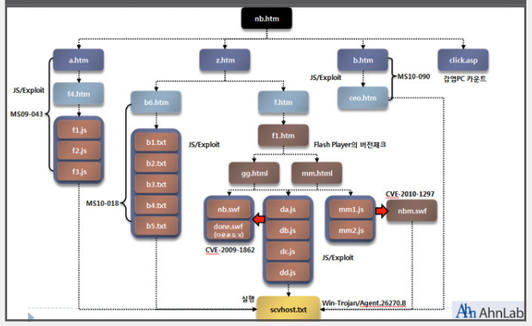
다중 취약점을 이용하는 것은 기본

2011년에도 응용 프로그램(인터넷 익스플로러, 파이어폭스 같은 브라우저, 어도비 플래시 플레이어 등)들에 존재하는 취약점을 이용한 트로이목마가 가장 많이 유포됐는데, 그 주 목적은 탈취한 정보를 현금화하는 것이었다. 현금화를 위한 공격 대상에서 해외와 국내를 비교해 보면, 해외는 제우스나 스파이아이 본넷(SpyEye Bonet)을 이용한 온라인 뱅킹 정보, 국내는 특정 온라인 게임 사용자의 계정 정보라는 차이가 있었다. 국내 온라인 게임 사용자의 계정 정보를 탈취하기 위한 트로이목마를 일반적으로 온라인 게임핵으로 명명하는데, 해킹된 웹 사이트와 웹 응용 프로그램의 취약점이 결합된 형태의 유포 방식을 주로 사용했다. 가장 많이 사용한 취약점 5건을 분석한 결과는 [표 3-4]와 같다.

[표 3-4] 5대 응용 프로그램 취약점

순위	취약점 ID	응용 프로그램
1	MS10-018	Internet Explorer
2	CVE-2011-2110	Adobe Flash Player
3	CVE-2011-2140	Adobe Flash Player
4	CVE-2011-0611	Internet Explorer
5	CVE-2011-0609	Adobe Flash Player

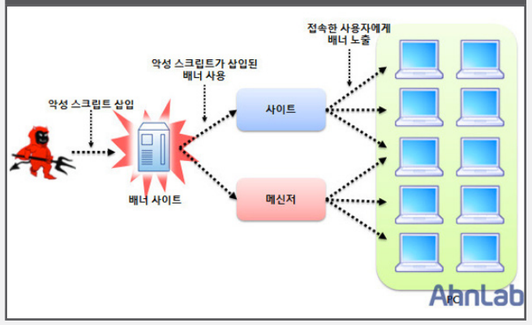
[그림 3-9] 다중 취약점을 이용한 악성코드 유포 사례



배너 광고를 이용한 악성코드 유포 사례

2011년 악성코드를 유포했던 사이트들을 분석해보면 상당수의 사이트에서 배너 광고를 통해 악성코드를 유포했다. 해당 사이트 자체가 취약해서 해킹된 것이 아니라 외부(광고업체)에서 제공받은 배너 광고에 악성코드가 포함돼 있었던 경우가 대부분이다. 배너 광고의 가장 큰 목적은 수익이기 때문에 기업, 개인 구분 없이 운영하는 사이트나 블로그에서 사용되고 있지만, 배너 광고 제공 업체가 해킹당하면 자신의 사이트 또는 블로그가 한순간에 악성코드 유포지로 전락하게 된다는 것에 주의할 필요가 있다.

[그림 3-10] 배너 광고를 통한 악성코드 유포 사례



3. 2011년 세계 보안 동향

세계 악성코드 동향

2011년은 특정 업체 및 산업군에 따른 타깃 공격이 다수 진행됐다. 대부분의 보안 업체는 2012년에도 타깃 공격의 꾸준한 증가를 예측하고 있다.

세계 악성코드 통계

대부분의 악성코드는 특정 지역에서만 발견되는 여러 가지 변형이 소규모로 보고되고 있다. 이러한 악성코드의 지역화에 따라 백신 프로그램에서 유사 변형을 하나의 진단명으로 통합해 진단하거나 통계를 내고 있다. 주요 보안 업체 악성코드 통계에 따르면 컨피커 웜(Conficker worm), 오토런 웜(Autorun worm), 바이럿 바이러스(Virut virus), 샐리티 바이러스(Sality virus), 허위 보안 프로그램 등이 꾸준히 보고되고 있다.

악성코드 배포 방식

홈페이지 해킹 후 취약점을 이용해 코드를 삽입해서 사용자가 웹 사이트 방문 시 감염시키는 방식과 USB 메모리를 통한 직접 전파가 주를 이뤘다. 이외에도 메일을 통한 배포와 페이스북, 트위터 등의 소셜 네트워크를 이용한 전파도 계속됐다.

정보 유출과 APT

공격자에 의한 정보 유출 및 시도가 계속 보고되고 있으며 상당수 공격은 지능형 타깃 위협(Advanced Persistent Threat)으로 분류될 수 있다. 2010년 이란 원전 가동을 중지시킨 걸로 알려진 스턱스넷 웜(Stuxnet worm)의 동일 제작자들이 만든 걸로 추정되는 듀큐(Duqu)가 발견됐다. 스턱스넷과 달리 자체 전파 기능과 산업 제어 시스템(Industrial control systems) 관련 기능은 없고 사용자 키 입력 내용을 저장하는 키로거 등의 정보 수집용으로 제작됐다. 특히 설치된 후 특정 기간(보통 한 달 정도)만 활동한 후 기간이 지나면 스스로 삭제됐다. 맥아피가 8월 표적 공격에 대해 발표한 데 이어 시만텍에서도 포이즌아이비 백도어(Poisonivy backdoor)를 이용한 중국발 공격으로 화학 업체 40곳 이상이 공격받았다고 발표했다. 11월에는 노르웨이 주요 방위 산업체와 에너지 기업에 대한 표적 공격이 발표됐다.

정치 목적의 공격

2011년 10월 26일 대한민국 서울시장 선거일에 중앙선거관리위원회와 박원순 후보 홈페이지에 한나라당 보좌관 주도로 DDoS 공격이 발생해 충격을 주었다. 12월 4일 러시아 하원총선에서도 반정부 성향 언론사와 선거감시기구 사이트가 DDoS 공격을 받았다. 해킹그룹 어노니머스 역시 이스라엘 주요 정부 기관 웹 사이트를 공격하거나 미 전략 싱크탱크 스트래트포 글로벌 인텔리전스 고객 명단을 해킹하는 등 정치적 목적의 공격이 계속되고 있다. 이는 앞으로도 정치적 목적의 사이버공격이 일상화될 수 있다는 우려를 낳고 있다.

4. 2012년 보안 위협 예측

APT 공격 경로 지능화

기업과 기관을 겨냥한 APT 공격이 2012년에도 지속적으로 이어지는 한편, 공격 경로가 지능화할 것으로 예상된다. 이제껏 주된 공격 방식은 타깃 기업/기관의 특정 구성원에게 업무 메일로 위장하는 것이었다. 즉, SNS(소셜 네트워크 서비스) 등에서 이메일을 손쉽게 수집해 신뢰할 수 있는 사람으로 위장해 취약점이 포함된 문서를 첨부하거나 취약점이 존재하는 웹 사이트 주소를 본문에 삽입해 악성코드를 감염시키는 것이다. 널리 사용되는 소프트웨어의 업데이트 관련 파일을 변조한 경우도 있었다. 앞으로는 조직 내부로 반입하기 쉬운 스마트폰이나 보안 관리가 어려운 기술지원 업체의 장비나 소프트웨어 등을 이용한 내부 침입도 발생할 것으로 예측된다.

PC 악성코드 수준의 스마트폰 악성코드 등장

스마트폰, 특히 안드로이드 겨냥 악성코드는 2010년에 악성코드 제작/유포의 가능성을 점쳐보는수준이었다면, 2011년에는 금전적 이득을 취할 수 있는 방법을 찾아 대량 제작된 시기였다. 2012년에는 감염의 효율을 높이기 위해 과거 PC용 악성코드에 사용된 기법이 본격적으로 활용될 것으로 예측된다.
즉, 스마트폰 내부에서 자신을 숨기는 은폐 기법과 모바일 운영체제에 존재하는 취약점을 악용한 루트 권한 탈취 등이 있을 수 있다. 그리고, 사회공학 기법을 악용해 웹 사이트에서 악성코드 다운로드를 유도하거나 모바일 웹 브라우저에 존재하는 취약점으로 인해 악성코드가 자동 감염되게 하는 기법도 등장할 것으로 예측된다. 스마트폰에 설치된 인터넷 뱅킹 및 온라인 쇼핑 관련 앱에서 금융/신용카드 정보를 탈취하는 기법도 나올 것으로 예측된다.

SNS 통한 보안 위협 증가

SNS가 전 세계인과 정보를 빠르게 공유하는 창구인 만큼 악용 사례도 급증하고 있다. 단축 URL이 전체 주소가 전부 보이지 않는다는 점을 악용해 악성코드 유포 사이트나 피싱 사이트를 단축 URL로 유포하는 경우가 있었다. 2012년에는 단축 URL 악용 사례가 더 증가하는 한편, SNS가 APT(Advanced Persistent Threat) 공격의 경유지로 이용될 가능성도 있다.

애플리케이션 취약점 공격 국지화

2011년에는 운영체제 같은 범용 애플리케이션의 취약점을 공격하는 경우는 줄어든 반면, 특정 지역에서만 사용되는 애플리케이션의 취약점을 악용한 사례는 증가했다. 아래아한글을 비롯해 동영상 재생 소프트웨어, P2P 및 웹하드 프로그램의 취약점을 악용한 악성코드 유포가 대표적이다. 취약점을 가진 파일을 이메일로 전송하거나 웹 사이트 접속 시 자동으로 악성코드를 감염시키는 방식으로 유포한다. 이런 추세는 2012년에도 이어지는 한편, 애플리케이션 취약점이 APT 공격 등 다양한 보안 위협에 악용되리라 예측된다.

특정 국가 산업/기관 시스템 공격 시도 증가

금전적 이익이나 정치적, 종교적 이유로 특정 국가의 산업/기관 시스템을 공격하는 시도가 더욱 증가할 것이다. 이런 공격에 국가 기관이 직간접적으로 개입돼 국가 간 사이버 전쟁으로 확대될 수도 있다. 사용자 부주의로 내부 시스템이 인터넷이나 외부 시스템에 연결돼 있을 때 이를 통해 공격이 들어올 가능성이 있다. 또한 국가 산업/기관 시스템용 특정 소프트웨어의 취약점을 이용해 공격이 이루어질 것으로 예측된다.

가상화 및 클라우드 환경 공격 본격화

최근 가상화 기술을 기반으로 클라우드 서비스 등을 사업 모델을 삼는 기업이 증가하고 있다. 그러나 가상화와 클라우드 서비스는 자원 활용의 극대화라는 장점이 있지만, 악용되면 또 하나의 보안 위협이 될 수 있다. 실제로 2011년에 대표적인 가상화 제품의 보안 취약점이 다수 발견됐으며, 실제 금융 정보 탈취를 위한 스파이아이 악성코드가 아마존 클라우드 서비스를 악용해 배포되기도 했다. 2012년에는 가상화 및 클라우드 서비스의 본격화에 맞추어 다양한 공격이 시도될 것으로 예상된다.

스마트 TV 등 네트워크로 연결되는 시스템에 대한 공격 증가

스마트폰, 스마트 TV를 비롯해 네트워크에 연결되는 임베디드 소프트웨어가 탑재된 기기에 대한 보안 위협이 증가할 것으로 예측된다. 특히 교체 주기가 비교적 길고 실생활과 밀접한 가전 제품은 지속적인 공격에 노출될 가능성이 높다. 실제로 인터넷 접속이 가능한 DVD 리코더를 악용한 공격이 일본에서 일어났다. 한 보안 컨퍼런스에서는 닌텐도DS 단말기에 리눅스를 설치해 외부에서 특정 시스템을 제어하는 것을 시연하기도 했다. 단순 반복 작업만을 담당했던 임베디드 시스템이 네트워크에 연결됨에 따라 해킹 또는 DDoS 공격의 타깃이 될 가능성이 점차 높아지고 있다.

이 밖에 정치 · 사회적 목적을 이루고자 시스템을 해킹하거나 DDoS 공격을 시도하는 행위인 핵티비즘(Hacktivism) 활동이 2012년에 특히 많이 발생할 것으로 예측된다. 우리나라의 대선과 총선, 미국과 러시아의 대선 등 전 세계적 이슈가 많기 때문이다.

VOL. 24
ASEC REPORT Contributors

집필진
책임 연구원 차 민 석
선임 연구원 김 소 헌
선임 연구원 안 창 용
선임 연구원 장 영 준
주임 연구원 이 도 현
주임 연구원 조 주 봉
연구원 이 정 신

참여연구원 ASEC 연구원
SiteGuard 연구원

편집장
선임 연구원 안 형 봉

편집인 안철수연구소
마케팅실

디자인 안철수연구소
UX디자인팀

감 수
상 무 조 시 행

발행처 (주)안철수연구소
경기도 성남시 분당구
삼평동 673
(경기도 성남시 분당구
판교역로 220)
T. 031-722-8000
F. 031-722-8901

AhnLab