ASEC REPORT

VOL.28 | 2012.05

안랩 월간 보안 보고서

악성코드 분석 특집

불필요한 옵션 사용으로 발생할 수 있는

스마트폰 보안 위협과 대응

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 ㈜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.

CONTENTS

1. 2012년 4월의 보안 동향

01. 악성코드 동향

a. 악성코드 통계

4월 악성코드 최다 20건

ASEC이 집계한 바에 따르면, 2012년 4월에 감염이 보고된 악성코드는 전체 1140만 9362건인 것으로 나타났다. 이는 지난 달의 1382만 206건에 비해 241만 844건이 감소한 수치다([그림 1-1]). 이 중에서 가장 많이 보고된 악성코드는 Trojan/Win32.adh이었다. Mov/Cve-2012-0754와 Trojan/Win32.Gen이 그 다음으로 많이 보고됐으며, 최다 20건에 새로 포함된 악성코드는 총 8건이었다([표 1-1]).

[그림 1-1] 월별 악성코드 감염 보고 건수 변화 추이

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32.adh	870,167	20.1%
2	NEW	Mov/Cve-2012-0754	415,052	9.6%
3	—	Trojan/Win32.Gen	401,819	9.3%
4	▲1	Malware/Win32.generic	399,827	9.2%
5	▼1	Textimage/Autorun	347,538	8.0%
6	NEW	Trojan/Win32.bho	267,854	6.2%
7	▲2	Trojan/Win32.agent	203,137	4.7%
8	▼2	Adware/Win32.korad	156,582	3.6%
9	▼7	JS/Agent	143,487	3.3%
10	NEW	Downloader/Win32.opentab	129,989	3.0%
11	NEW	Als/Bursted	118,022	2.7%
12	▲5	Downloader/Win32.agent	116,779	2.7%
13	▼6	Trojan/Win32.hdc	111,681	2.6%
14	▲1	Java/Agent	108,113	2.5%
15	▼2	Trojan/Win32.genome	98,377	2.3%
16	▼6	Trojan/Win32.fakeav	96,753	2.2%
17	NEW	Backdoor/Win32.trojan	91,578	2.1%
18	NEW	Win-Trojan/Rootkit.28928.D	87,708	2.0%
19	NEW	Adware/Win32.bho	84,628	2.0%
20	NEW	ASD.PREVENTION	82,889	1.9%
			4,331,980	100.0%

[표 1-1] 2012년 4월 악성코드 최다 20건(감염 보고, 악성코드명 기준)

악성코드 대표진단명 감염보고 최다 20

[표 1-2]는 악성코드의 주요 동향을 파악하기 위하여 악성코드별 변종을 종합한 악성코드 대표진단명 최다 20건이다. 2012년 4월에는 Trojan/Win32가 총 261만 1473건으로 최다 20건 중 33.6%의 비율로 가장 빈번히 보고된 것으로 조사됐다. Adware/Win32가 53만 1968건, Malware/Win32가 50만 1202건으로 그 뒤를 이었다.

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32	2,611,473	33.6%
2	—	Adware/Win32	531,968	6.8%
3	▲4	Malware/Win32	501,202	6.4%
4	▲2	Win-Trojan/Agent	452,292	5.8%
5	▲4	Downloader/Win32	419,032	5.4%
6	NEW	Mov/Cve-2012-0754	415,052	5.3%
7	▼4	Win-Trojan/Downloader	388,041	5.0%
8	▲2	Win-Trojan/Onlinegamehack	357,080	4.6%
9	▼1	Textimage/Autorun	347,611	4.5%
10	▲1	Backdoor/Win32	225,293	2.9%
11	▼6	Win-Adware/Korad	218,398	2.8%
12	▲2	Win-Trojan/Rootkit	209,591	2.7%
13	▼1	Win32/Conficker	166,002	2.1%
14	▼1	Win32/Virut	164,033	2.1%
15	▼11	JS/Agent	143,973	1.9%
16	▼1	Win32/Autorun.worm	134,621	1.8%
17	▲3	Win-Trojan/Korad	131,524	1.7%
18	▼2	Win32/Kido	129,835	1.7%
19	NEW	Als/Bursted	118,022	1.5%
20	▼1	Java/Agent	108,113	1.4%
			7,773,156	100.0%

[표 1-2] 악성코드 대표진단명 최다 20건

4월 신종 악성코드

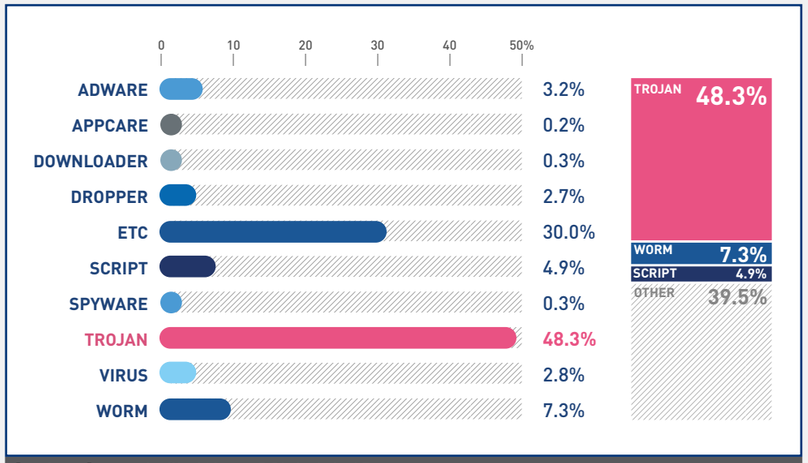
[표 1-3]은 4월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 최다 20건이다. 4월의 신종 악성코드는 Win-Trojan/Korad.229376이 4만 3537건으로 전체의 11.3%였으며, Win-Trojan/Downloader.1273856.C가 4만 2271건으로 그 다음으로 많이 보고됐다.

순위	악성코드명	건수	비율
1	Win-Trojan/Korad.229376	43,537	11.3%
2	Win-Trojan/Downloader.1273856.C	42,271	10.9%
3	Win-Trojan/Fakealert.183320	39,752	10.3%
4	Win-Trojan/Korad.331776	33,787	8.7%
5	Win-Trojan/Downloader.1448448	28,271	7.3%
6	Win-Trojan/Tearspear.820224	24,221	6.3%
7	Win-Trojan/Agent.1720320.G	22,785	5.9%
8	Win-Adware/KorAd.331776.D	15,958	4.1%
9	Win-Trojan/Avkill.37760	14,577	3.8%
10	Win-Trojan/Onlinegamehack.115712.AB	14,441	3.7%
11	Win-Trojan/Agent.1990420	13,854	3.6%
12	Win-Adware/KorAd.331776.C	13,457	3.5%
13	Win-Trojan/Zapchast.217272	11,102	2.9%
14	Win-Trojan/Rootkit.1385472	10,969	2.8%
15	Win-Trojan/Onlinegamehack.30639	10,667	2.8%
16	Win-Trojan/Onlinegamehack.90112.GE	10,334	2.7%
17	Win-Trojan/Dllbot.133120.B	10,065	2.6%
18	Win-Trojan/Avkiller.38144	9,251	2.4%
19	Win-Trojan/Onlinegamehack.81920.EO	8,712	2.3%
20	Win-Trojan/Agent.1381376	8,558	2.1%
		386,569	100.0%

[표 1-3] 4월 신종 악성코드 최다 20건

4월 악성코드 유형별 감염 보고

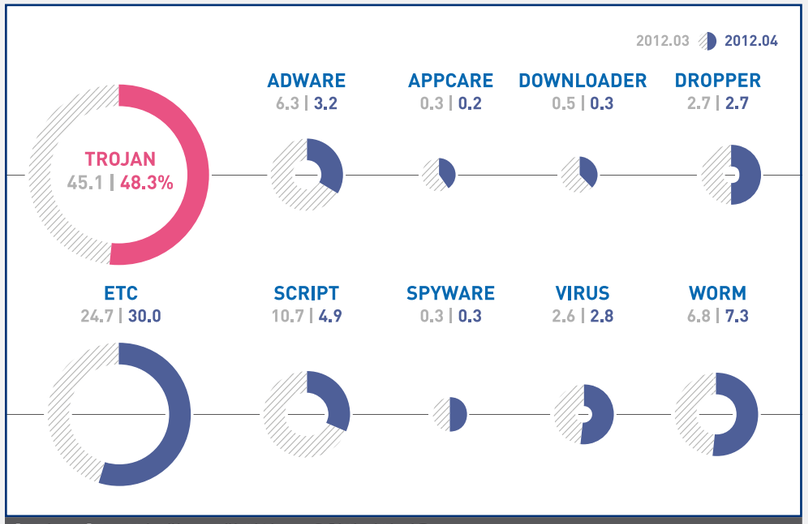
[그림 1-2]는 2012년 4월 한 달 동안 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 2012년 4월의 악성코드를 유형별로 살펴보면., 트로이목마(Trojan)가 48.3%, 웜(Worm)이 7.3%, 스크립트(Script)가 4.9%인 것으로 나타났다.



[그림 1-2] 2012년 4월 악성코드 유형별 감염 비율

악성코드 유형별 감염보고 전월 비교

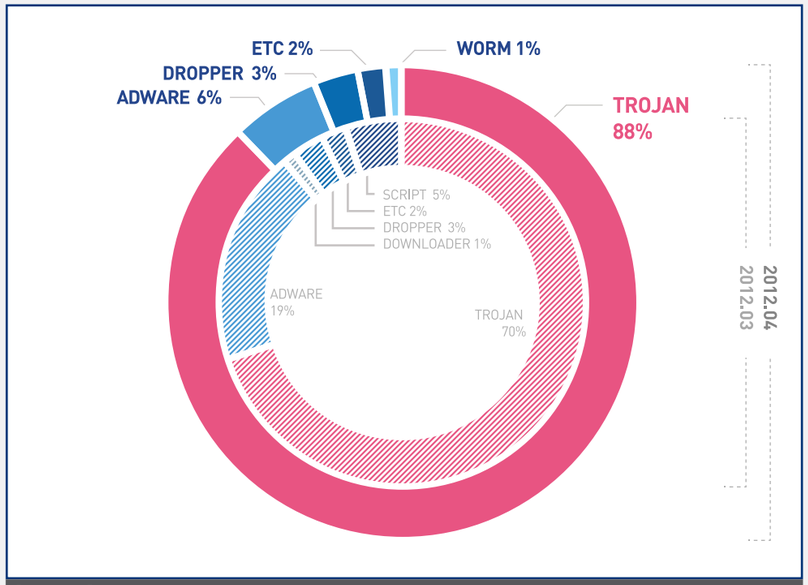
[그림 1-3]은 악성코드 유형별 감염 비율을 전월과 비교한 것이다. 트로이목마, 웜, 바이러스(Virus)가 전월에 비해 증가세를 보이고 있는 반면, 스크립트, 애드웨어(Adware), 다운로더(Downloader), 애프케어(Appcare) 계열들은 감소한 것을 볼 수 있다. 드롭퍼(Dropper), 스파이웨어(Spyware) 계열들은 전월 수준을 유지하였다.



[그림 1-3] 2012년 4월 vs. 3월 악성코드 유형별 감염 비율

신종 악성코드 유형별 분포

4월의 신종 악성코드를 유형별로 보면 트로이목마가 88%로 가장 많았고, 애드웨어가 6%, 드롭퍼가 3%였다.



[그림 1-4] 신종 악성코드 유형별 분포

01. 악성코드 동향
b. 악성코드 이슈

Social Engineering and Malicious Document

정치, 사회, 경제 등 사회 전반에 걸쳐 사람들의 관심을 끈 이슈들은 항상 악성코드를 유포하는 데 악용됐다. 최근에 발견된 사례를 보면 다음과 같다.

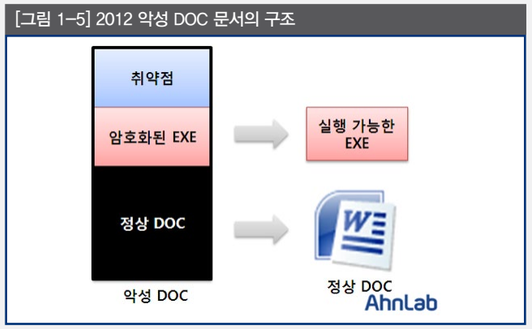
1. 티베트 봉기 기념일
2. 2012 런던 올림픽
3. 북한 로켓(광명성 3호) 발사
4. 특정 지역 또는 기관, 기업 등의 이슈를 이용한 타깃 공격
5. 그 외 다수

위 이슈들을 이용한 악성코드의 공통점은 바로 사용자들이 많이 사용하는 응용 프로그램(대표적으로 MS 오피스, 플래시 플레이어, 어도비 리더 등)의 취약점을 이용하는 문서 파일로 위장했다는 점이다.

악성코드가 실행 파일 확장자(exe나 dll 같은)를 가졌다면 사용자도 한 번쯤은 의심했을 테지만, 사회적인 이슈를 주제로 한 문서 파일 형태라면 얘기가 달라진다. 어느 누가 문서 파일에 악성코드가 존재하리라고 생각할까? 하지만 악성코드 제작자들은 바로 이러한 허점을 노린다.

이번에 국외에서 발견된 악성 DOC 파일 역시 사용자들이 관심이 있을 만한 '2012 런던 올림픽 소식'을 포함하였다. 첨부된 문서 파일을 열어보면 MS 워드의 취약점(CVE-2010-3333)을 통해 생성된 악성코드에 감염된다.

[그림 1-5] 2012 악성 DOC 문서의 구조

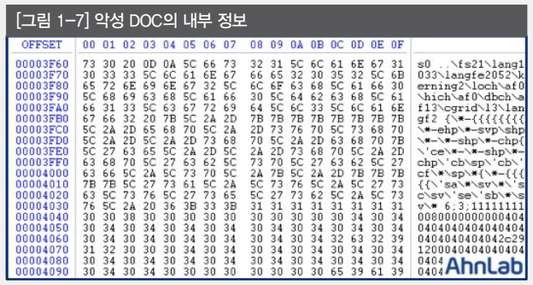


악성 DOC의 구조는 [그림 1-5]와 같으며, 해당 문서를 실행하면 [그림 1-6]과 같이 2012 런던 올림픽에 관한 내용의 정상 DOC 문서가 열린다.

[그림 1-6] 정상 DOC 문서

악성 DOC는 [그림 1-6]과 같이 정상 DOC 문서를 사용자에게 보여주지만 [그림 1-7]의 MS 워드의 취약점(CVE-2010-3333)을 이용하여 악성코드를 생성 및 실행한다.

[그림 1-7] 악성 DOC의 내부 정보



[그림 1-7]과 같은 악성 DOC의 내부에 존재하는 취약점 코드가 암호화된 EXE를 복호화한 후 악성코드 파일을 생성 및 실행한다. 그리고 악성 EXE가 실행되면서 %SYSTEM%₩cydll.dll을 생성하는데 해당 DLL은 감염된 PC의 하드웨어 정보를 C&C(114.***.89.***, CN) 서버로 전송한다. 하지만 C&C 서버가 동작하지 않아 추가적인 동작은 확인하지 못했다.

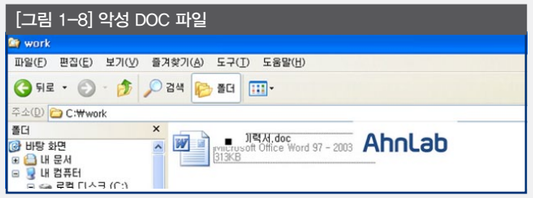
〈V3 제품군의 진단명〉
– DOC/Cve-2010-3333(2012.04.25.03)
– Backdoor/Win32.Etso(2011.09.05.00)
– Win-Trojan/Etso.54272(2012.04.25.03)
– Win-Trojan/Etso.73483(2012.04.25.03)

악성 DOC 문서를 첨부한 스피어 피싱 메일

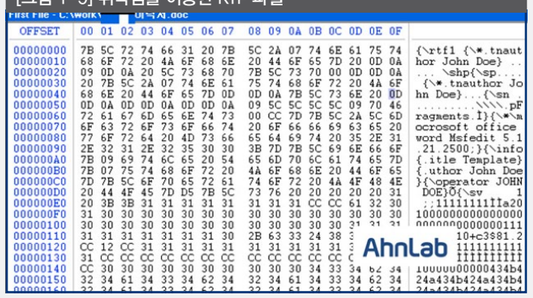
악성 DOC 문서가 첨부된 발신인이 불분명한 스피어 피싱 메일이 발견되었다. 스피어 피싱은 특정 조직이나 인물을 겨냥해 신뢰할 만한 대상으로 속여 악성 메일을 보내는 공격이다. ID와 비밀번호를 입력하게 하거나, 악성코드를 다운로드하도록 가짜 사이트로 유도하거나, 취약점이 담긴 문서 파일을 보내 정보를 빼낸다. 이런 일련의 공격은 PC 단위에서 보안을 철저히 하지 않으면 대규모 공격의 진원지로 악용될 수 있다.

이번에 발견된 메일에는 '박XX이력서.doc' (DOC/Dropper) 문서 파일이 첨부되었다. 이 DOC 파일은 RTF(Rich Text Format) 파일이며 RTF 취약점을 이용하여 시스템을 감염시킨다.

[그림 1-8] 악성 DOC 파일



[그림 1-9] 취약점을 이용한 RTF 파일

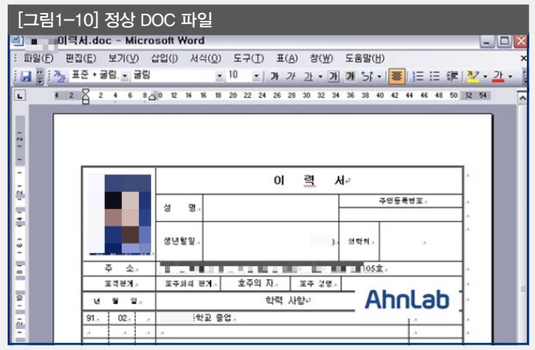


DOC 파일을 실행하면 정상적인 DOC 파일의 복사본을 생성한 다음 복사된 정상 DOC 파일을 사용자에게 보여주어 악성코드 감염을 인지하지 못하도록 위장하고 악성코드 파일들을 생성한다. 또한, 윈도우 시작 시 자동으로 동작하도록 레지스트리에 값을 등록한다.

[생성되는 파일]
– 'C:₩ Documents and Settings₩[사용자 계정]₩ Local Settings₩Temp₩msvcrt71.exe'
(Win-Trojan/Agent.16224.P)
– 'C:₩WINDOWS₩Tasks₩snmp.exe'
(Win-Trojan/Agent.16224.P)
– 'C:₩ Documents and Settings₩[사용자 계정]₩ Local Settings₩Temp₩박OO이력서.doc'
(정상 문서)

[등록된 레지스트리]
– HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩snmp
"C:₩WINDOWS₩Tasks₩snmp.exe"

[그림1-10] 정상 DOC 파일



ASEC에서 분석 시 실제 C&C 서버로 연결되지는 않았으나, 감염된 악성코드를 통해 C&C 서버로 연결되어 정보 수집과 공격 명령을 받아 악의적인 동작을 수행했을 것으로 추정된다.

스피어 피싱 메일의 감염을 예방하기 위해서는 불분명한 발신자가 보낸 메일과 의심스러운 첨부 파일을 주의해야 한다. 또한, 최신 엔진으로 업데이트한 보안 제품으로 파일을 검사하여 이상이 있을 경우 보안 업체에 신고해야 한다. 마지막으로 윈도우 보안 패치를 항상 최신으로 유지하여 각종 취약점을 예방하는 것이 중요하다.

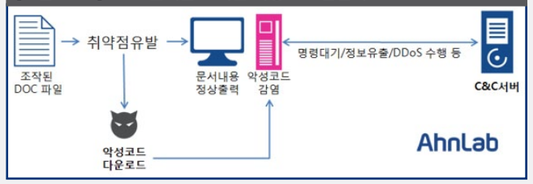
〈V3 제품군의 진단명〉
– DOC/Dropper
– Win-Trojan/Agent.16224.P

북한 광명성 3호 발사 및 핵 실험을 주제로 한 악성코드

광명성 3호 및 핵 실험 관련 악성코드가 유포되었다. 이번에 발견된 악성코드는 'North Korea', 'North Korea satellite launch', 'North Korea nuclear test' 등의 키워드를 사용하였으며 최근 국제 사회의 가장 주된 관심사였던 북한의 로켓 관련 이슈를 다뤘기 때문에 전형적인 사회공학 기법으로 볼 수 있다.

이번에 발견된 악성코드 파일의 동작 구조는 그림 [1-11]과 같다.

[그림 1-11] DOC 문서를 조작한 악성코드 감염 구조도

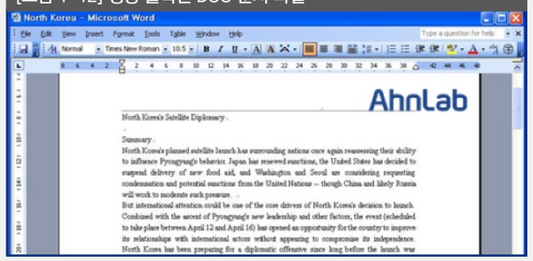


각각의 악성코드 파일들은 다음의 구조와 기능을 수행한다.

1. North Korea.doc

A. 문서 내부에 있는 SWF 플래시 스크립트가 로딩되면서 인터넷 익스플로러를 통해 특정 웹 페이지(hxxp://gis.usda.****.com/)로 이동한다. [그림 1-11]에서 설명한 것과 같이 해당 DOC 문서의 내용을 [그림 1-12]와 같이 정상적으로 사용자에게 보여준다.

[그림 1-12] 정상 출력된 DOC 문서 파일

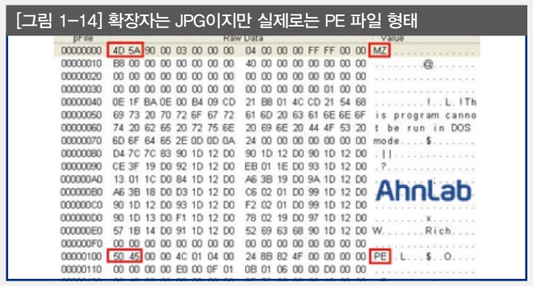


B. 특정 웹 페이지로 이동하면 [그림 1-13]의 코드가 실행된다.

[그림 1-13] 특정 웹 페이지 이동 시 실행되는 HTML 코드

C. CVE-2012-0507 취약점을 유발하는 코드를 호출하고 특정 경로에 있는 JPG 파일을 불러온다. 확장자는 JPG이지만 실제 파일 내부를 살펴보면 [그림 1-14]와 같이 PE 파일임을 확인할 수 있다.

[그림 1-14] 확장자는 JPG이지만 실제로는 PE 파일 형태



D. 이 파일의 정보를 살펴보면 [그림 1-15]에 언급된 javacpl.exe 파일로 위장하고 있다는 것을 알 수 있다.

[그림 1-15] Javacpl.exe 파일로 위장한 ZA102498414.jpg 파일

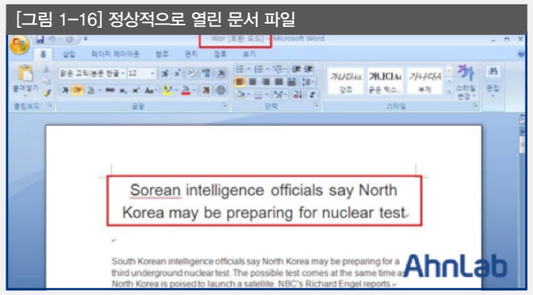
E. 해당 파일에 감염되면 키보드, 마우스 입력 값을 후킹하며, 특정 C&C 서버로 연결되어 명령을 수신한다.

F. CVE-2012-0507 취약점은 2012년 4월 현재 보안 업데이트 없이 보안 취약점만 발표된 자바의 제로데이 취약점이다. 해당 보안 업데이트가 제공되기까지 시간이 걸릴 것으로 예상되므로 출처가 확인되지 않은 불확실한 문서는 함부로 열어보지 않는 것이 중요하다.

2. Sorean intelligence officials say North Korea may be preparing for nuclear test.doc

A. 해당 파일은 MS 오피스 취약점인 CVE-2010-3333 취약점을 이용하여 악성코드를 감염시키며 wor.doc 파일을 생성하여 [그림 1-16]과 같이 사용자에게 정상적인 문서 내용을 보여준다.

[그림 1-16] 정상적으로 열린 문서 파일



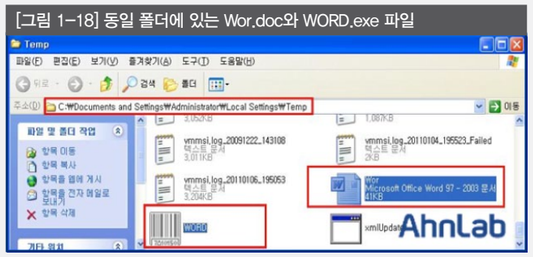
B. 관련 취약점에 대한 보안 업데이트가 공개된 상태이므로 CVE-2010-3333 보안 업데이트를 설치하는 것이 중요하다. 만약 보안 업데이트가 설치되지 않은 PC에서 해당 문서 파일을 실행하면 WORD.exe 악성 파일과 Wor.doc라는 정상적인 DOC 파일이 생성 및 실행된다.

C. WORD.exe 파일이 실행되면 [그림 1-17]과 같이 시작프로그램에 등록되어 부팅 때마다 실행되며, 특정 IP로 지속적인 TCP 연결 상태 확인을 시도한다.

[그림 1-17] 시작프로그램에 등록된 악성코드 프로그램

D. 이 파일은 [그림 1-18]과 같이 'C:₩Documents and Settings₩Administrator₩Local Settings₩Temp₩' 폴더에 위치하며, Wor.doc 파일 역시 같은 곳에 존재한다.

[그림 1-18] 동일 폴더에 있는 Wor.doc와 WORD.exe 파일



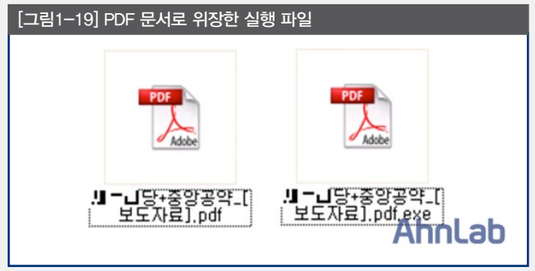
이와 같은 악성코드 대부분은 무작위로 배포되는 스팸 메일의 첨부 파일 형태로 유포된다. 인터넷으로 퍼지는 가십거리 기사들은 비밀 정보를 중시하는 외교, 안보 분야 종사자는 주의하기 때문에 특정 기관에 대한 APT로 이어질 가능성은 크지 않다. 하지만 일반 사용자들은 가십거리나 흥미 위주의 첨부 파일을 무심코 열어볼 가능성이 매우 크므로 항상 주의해야 한다.

〈V3 제품군의 진단명〉
- Dropper/Agent
- Exploit/Cve-2010-3333
- Exploit/Cve-2012-0507
- HTML/Downloader
- RTF/Cve-2010-3333
- Trojan/Win32.Agent
- Trojan/Win32.Zapchast
- Win-Trojan/Downloader.262144.MK

4 · 11 총선 이슈에 발견된 악성코드

4 · 11 총선 당시 특정 정당의 중앙당 공약이라는 보도자료로 위장한 악성코드가 발견되었다. 윈도우 탐색기에서 '알려진 파일 형식의 파일 확장명 숨기기' 옵션이 설정된 경우, 메일에 첨부된 파일은 [그림 1-19]의 왼쪽과 같이 아이콘이 PDF 문서 파일로 보이기 때문에 메일 수신자가 별다른 의심 없이 실행할 가능성이 크다. 숨기기 옵션을 해제하면 [그림 1-19]의 오른쪽과 같이 EXE 파일인 것을 확인할 수 있다.

[그림1-19] PDF 문서로 위장한 실행 파일



'***당+중앙공약_[보도자료].pdf.exe' 파일을 실행하면 아래와 같이 파일이 생성된다.

– C:₩Program Files₩Windows NT₩htrn.dll
– C:₩Program Files₩Common Files₩**당 중앙공약_[보도자료].pdf

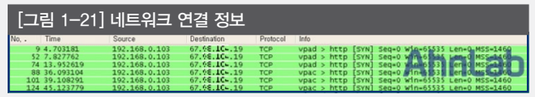
htrn.dll 파일은 다음과 같은 레지스트리 값을 생성하여 시스템 시작 시 자동 실행되도록 '6to4'라는 이름으로 서비스에 등록된다.

– HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩6to4₩Parameters
ServiceDll = C:₩Program Files₩Windows NT₩htrn.dll

[그림 1-20] htrn.dll 서비스 등록

또한 'www.kn**.ac.**.**fw.us (67.**.***.19)' 서버에 주기적으로 연결을 시도하지만, 분석 당시에는 연결되지 않아 추가적인 동작은 확인할 수 없었다.

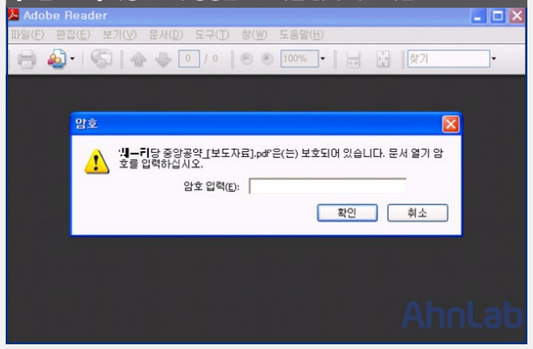
[그림 1-21] 네트워크 연결 정보



'C:₩Program Files₩Common Files' 폴더에 생성된 '***당 중앙공약_[보도자료].pdf' 파일은 정상 PDF 파일이지만 메일 본문에 암호가 걸려 있어 내용은 확인할 수 없었다.

〈V3 제품군의 진단명〉
– Win-Trojan/Agent.1991496(V3, 2012.04.03.02)
– Win-Trojan/Pcclient.10240.L(V3, 2012.04.03.02)

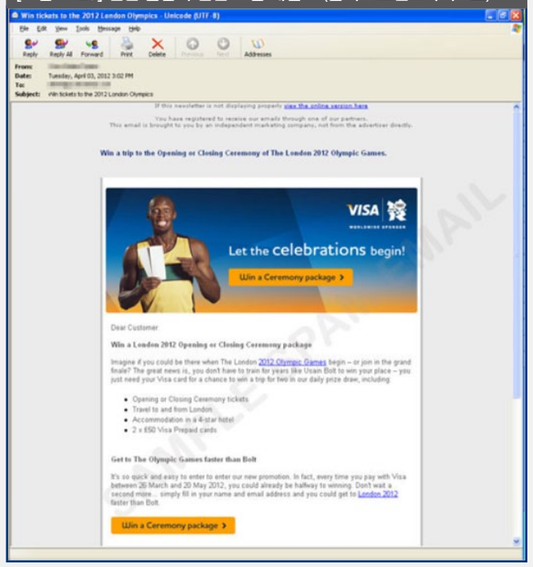
[그림 1-22] 악성코드가 생성한 PDF파일 읽기 시도 화면



런던 올림픽 개최를 이용한 악성코드

런던 올림픽 개최와 관련된 내용으로 CVE-2010-3333 취약점을 이용하는 악성코드가 발견되었다.

[그림 1-23] 런던 올림픽 관련 스팸 메일 – (출처 : 트렌드마이크로)



이러한 형태의 사회공학 기법을 이용한 악성코드 유포는 이번 올림픽뿐만 아니라, 다양한 사회적 이슈와 결합하여 과거부터 꾸준히 발생하였다. 2011년 오사마 빈 라덴 사망, 일본 대지진 등의 이슈들을 통해서 이와 같은 형태로 유포된 바 있다.

〈V3 제품군의 진단명〉
– Dropper/Cve-2010-3333
– Trojan/MSOffice.CVE-2010-3333

핵 안보 정상회담 PDF 문서로 위장한 악성코드

유엔(UN) 공식 홈페이지에는 [그림1-24]와 같이 2012년 3월에 개최된 '2012 서울 핵 안보 정상회담' 과 관련한 PDF 문서가 게재되어 있으며, 정상회담에서 논의될 의제 등에 관한 내용을 담고 있다.

[그림 1-24] UN 공식 홈페이지에 게시되어 있는 핵 안보 정상회담에 관한 PDF 문서

사람들의 관심이 많을 수밖에 없는 사회적인 이슈를 이용하여 위에 언급했던 핵 안보 관련 PDF 문서로 위장한 악성 파일이 발견되었다.

[그림 1-25] PDF 문서로 위장한 악성 파일

[그림 1-24]와 [그림 1-25]는 모두 PDF 문서를 나타내는 아이콘 모양을 갖고 있으며 어도비 리더로 실행했을 때에도 같은 문서 파일을 보여준다. PDF로 위장한 악성 파일을 실행하였을 때 동작하는 주요 정보는 다음과 같다.

[생성되는 주요 파일]
– 'C:₩Documents and Settings₩Administrator₩Local Settings₩Temp₩Winword.js'
악성 Script 부분, 악성 파일 생성 후 삭제
– 'C:₩Documents and Settings₩Administrator₩Local Settings₩Temp₩Adobe.pdf'
정상 PDF 파일
– 'C:₩Documents and Settings₩Administrator₩Local Settings₩Application Data₩Microsoft₩wininit.dll
생성되는 악성 파일
– 'C:₩Documents and Settings₩Administrator₩Local Settings₩Application Data₩Microsoft₩wininit32.exe'
생성되는 악성 파일
– 'C:₩Documents and Settings₩All Users₩Application Data₩ntuser32.bin //wininit32.exe'
백업 파일

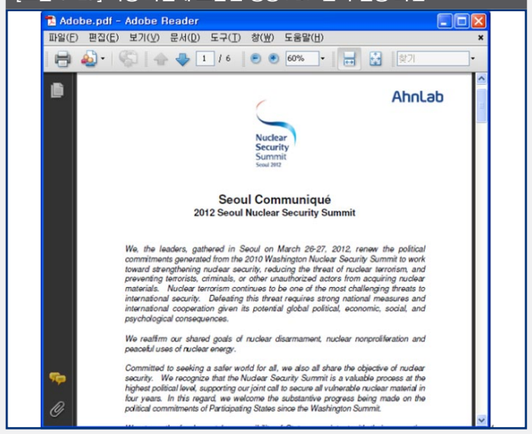
[네트워크 연결 시도 정보]
– 프로세스: explorer.exe 프로토콜: TCP CONNECT IP주소: 58.**.2**.24:80

해당 PDF 파일(악성 파일)은 악성 JavaScript 부분(Winword.js)과 정상적인 PDF 문서 파일(Adobe.pdf)을 포함하고 있다. '%temp%₩Winword.js' 파일은 생성 후 삭제되어 정확한 내용은 확인할 수 없었지만, 같은 폴더 내에 생성된 Adobe.pdf(그림 1-26) 파일이 정상 PDF 문서임을 확인할 수 있었다.

[그림1-26] 악성 파일 실행 후 %Temp% 폴더 내 생성된 실제 정상 PDF 파일

실제 사용자에게 보이는 문서는 %temp% 폴더에 생성된 'Adobe.pdf' 문서 파일이다.

[그림 1-27] 악성 파일에 포함된 정상 PDF 문서 실행 화면

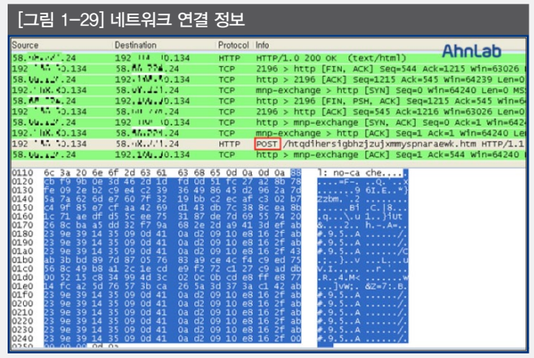


악성 PDF 문서를 통해 생성되는 악성코드는 [그림 1-28]과 같다. 특히, 'wininit.dll' 파일은 explorer.exe 프로세스에 로드되어 특정 IP(58.**.2**.24)에 접속을 시도하는 백도어다.

[그림 1-28] 생성되는 실제 악성코드

[그림 1-29]의 네트워크 연결 정보를 보면 특정 IP(58.**.2**.24)에 연결을 시도하여 특정 정보를 수집해가는 것을 확인할 수 있다.

[그림 1-29] 네트워크 연결 정보

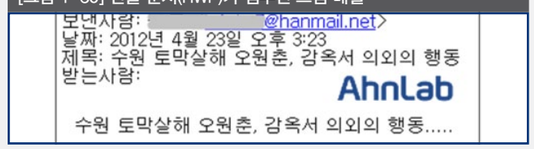


〈V3 제품군의 진단명〉
– PDF/Exploit-downloader(V3, 2012.04.19.00)
– Win-Trojan/Agent.44032.VC(V3, 2012.04.18.03)
– Trojan/Win32.Cosmu(AhnLab, 2012.04.16.05)

사회공학 기법을 이용하여 유포되는 악성 HWP 파일

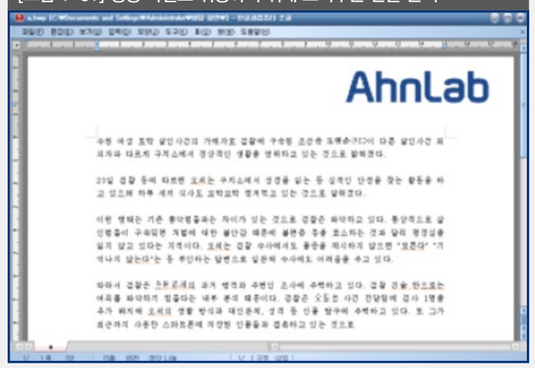
최근 일부 기업에서 [그림 1-30]과 같은 형태의 한글 문서(HWP)가 첨부된 스팸 메일이 접수되었다.

[그림 1-30] 한글 문서(HWP)가 첨부된 스팸 메일



이와 같은 형태의 사회적인 이슈를 이용한 악성코드는 계속 유포되고 있으며 2012년 4월 수원에서 발생한 사건 역시 악성코드 유포에 사용되었다.
해당 파일을 실행하면 정상 파일인 것처럼 위장하기 위해 정상적인 한글 문서를 보여준다. 하지만 사용자의 시스템에 취약점이 존재하면 그 취약점을 통해 악성코드를 감염시킨다.

[그림 1-31] 정상 파일로 위장하기 위해 보여주는 한글 문서



호기심을 자극하는 제목의 메일을 받았을 때는 열어보기 전에 한 번 더 신중하게 생각해야 한다. 또한 꾸준한 보안 업데이트를 통해 시스템에 존재하는 취약점을 없애야 한다.

〈V3 제품군의 진단명〉
– HWP/Agent(2012.04.24.00)
– Backdoor/Win32.Cson(2012.04.24.00)
– Trojan/Win32.Visel(2012.04.24.00)

국내 주요 금융기관 피싱 사이트 다수 발견

몇 달 전부터 국내 주요 금융기관을 대상으로 하는 피싱 사이트들이 크게 증가하여 온라인 뱅킹사용자들의 주의가 요구된다. 국내 은행을 대상으로 제작된 피싱 사이트는 [그림 1–32]와 같은 문자 메시지를 발송하여 접속을 유도하였다.

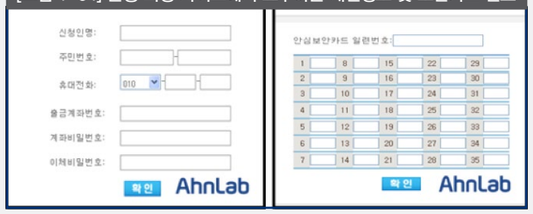
[그림 1–32] 은행을 사칭한 피싱 문자 메시지들

이들은 실제 은행 홈페이지와 유사한 URL 주소와 웹 사이트를 만들어 개인정보를 요구하는 수법을 사용하였다. 스마트폰의 대중화에 따라 모바일 웹 페이지를 대상으로 제작된 사이트도 발견되고 있다. [그림 1–33]은 최근 발견된 농협 모바일 웹 피싱 사이트이다.

[그림 1–33] 농협 모바일 웹 피싱 사이트 (좌: 정상 사이트, 우: 피싱 사이트)

정상적인 모바일 홈페이지와 매우 유사하지만, 피싱 사이트에서는 접속한 사용자들이 '보안강화 서비스 신청하기'를 클릭하도록 유도하고 있다. 또 보안 승급이라는 특정 서비스를 완료하기 전에는 아무런 서비스가 되지 않는다. [그림 1–34]는 피싱 사이트에서 요구하는 개인정보 및 보안카드 번호 입력 페이지다.

[그림 1–34] 은행 피싱 사이트에서 요구하는 개인정보 및 보안카드 번호



얼마 전 이와 같은 형태로 제작된 KB국민은행 피싱 사이트가 발견되었으며, 유출된 정보로 예금된 자산이 인출되거나 정기예금을 담보로 큰 금액이 대출되는 등의 피해 사례가 있었다.

[그림 1–35] KB국민은행을 사칭한 피싱 사이트의 개인정보 및 보안카드 정보 입력란

사용자는 이러한 피싱 사이트를 통한 금전적 피해를 입지 않도록 아래의 사항에 대하여 주의해야 한다.
– 보안사항 변경과 같이 중요한 정보는 은행 창구에서만 가능하며, 온라인으로 개인정보 및 보안사항을 절대로 요구하지 않는다.
– 사기 사이트 및 피싱 사이트를 차단하는 사이트가드(SiteGuard)와 같은 웹 브라우저 보안 소프트웨어를 사용하는 것이 중요하다.
– 이메일에 존재하는 의심스러운 웹 사이트 링크는 클릭하지 않는다.

페이스북을 통해 유포되는 보안 제품 무력화 악성코드

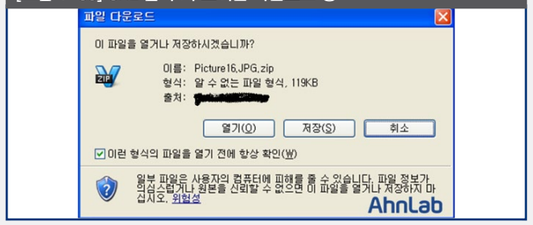
최근 페이스북을 통해 유포된 보안 제품을 무력화하는 악성코드의 감염 피해 사례가 접수되었다. 이 악성코드는 사용자 몰래 페이스북 친구들에게 [표 1–4] 형태의 제목과 URL이 담긴 메시지를 보낸다.

[표 1–4]의 URL을 클릭하면 [그림 1–36]과 같이 압축 파일을 다운로드하며 해당 압축 파일은 [그림 1–37]의 파일을 포함한다.

[표 1–4] 페이스북으로 전파되는 URL

제목	URL
qhahaheq your foto	'http://bit.ly/ImVGVL?9Za8XXX230D'
hahaheq your foto	'http://bit.ly/ImVGVL?9Za8XXXXXD'
qhah ht foto	'http://bit.ly/IMIoA6?Facebook.com-IMG69XXX78063.JPEG'
hahaht foto	'http://bit.ly/IMIoA6?Facebook.com-IMG69XXX806X.JPEG'
...	...

[그림 1–36] URL 클릭 시 보이는 다운로드 창



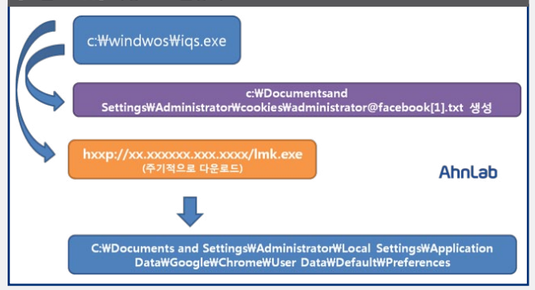
[그림 1–37] 압축 파일에 포함된 파일

[그림 1–37]의 파일명 외에도 [그림 1–38]과 같이 사용자들의 호기심을 유발하는 이름으로 다운로드되기도 한다.

[그림1–38] 호기심을 유발하는 파일명

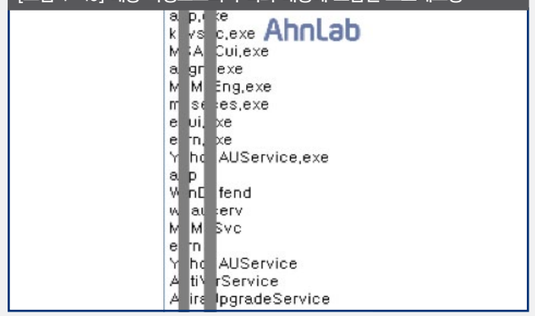
[생성되는 파일]
– C:₩windows₩iqs.exe
– C:₩Documentsand Settings₩Administrator₩cookies₩administrator@facebook[1].txt
– C:₩Documents and Settings₩Administrator₩Local Settings₩Temporary Internet Files₩Content.IE5₩3X2QCS5X₩lmk[1].exe

[그림 1–39] 악성코드 실행 구조



해당 악성코드는 카스퍼스키, Avira 등과 같은 보안 제품들을 무력화하는 기능이 있다.

[그림 1–40] 해당 악성코드의 무력화 대상에 포함된 프로세스명



사용자들은 알 수 없는 웹 사이트 링크나 확인되지 않는 사용자로부터 수신된 메일에 연결된 링크를 함부로 클릭하지 않도록 주의해야 한다.

〈V3 제품군의 진단명〉
– Worm/Win32.Stekct(2012.04.30)
– Trojan/Win32.Phorpiex(2012.04.29)

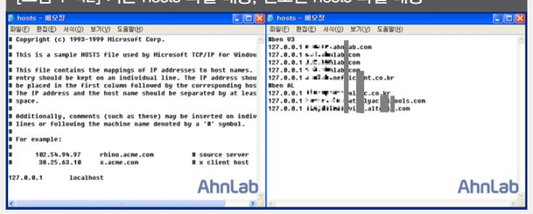
보안 제품의 업데이트를 방해하는 Host 파일 변경 악성코드 주의

hosts 파일을 변조해 보안 프로그램의 업데이트를 방해하는 악성코드가 빈번히 출현해 이를 치료할 수 있는 전용 백신을 최근 한국인터넷진흥원(KISA)에서 보급하였다.

해당 악성코드는 2012년 1월부터 발견됐으나 이후 변종 발견이 미미한 수준이었고 최근에는 피해가 보고되지 않았다. 이 악성코드에 감염되면 Host 파일이 변조되어 보안 프로그램이 업데이트되지 않으므로 주의해야 한다. 주로 Hosts 파일에 특정 제품이 업데이트할 때 사용하는 도메인에 대해 루프백 주소(127.0.0.1)를 설정하는 방법으로 업데이트를 방해한다.

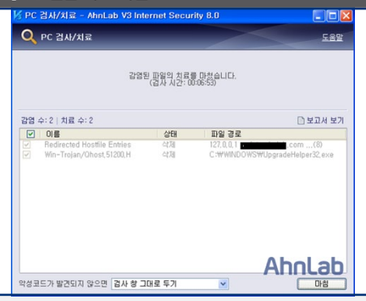
[그림 1-41] KISA 맞춤형 전용 백신 페이지

[그림 1-42] 기본 hosts 파일 내용, 변조된 hosts 파일 내용

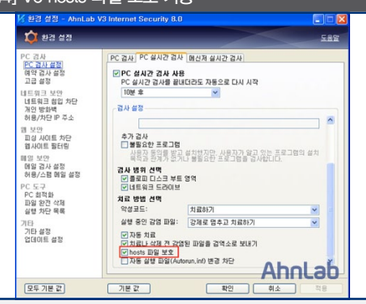


V3 제품은 빠른 검사나 수동 검사를 통해 변조된 hosts 파일을 진단·치료하는 기능이 포함되어 있어 전용 백신을 이용한 치료가 필요 없다. 또한, V3 Internet Security 8.0 제품은 hosts 파일 보호 기능을 옵션으로 제공하기 때문에 hosts 파일 변조를 원천 차단한다.

[그림 1-43] V3 진단·치료 화면



[그림 1-44] V3 hosts 파일 보호 기능



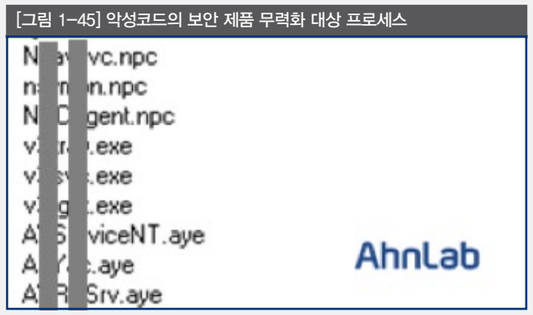
2011년 3·4 DDoS 공격에 이용된 악성코드도 이번에 이슈가 된 악성코드와 마찬가지로 hosts 파일을 변조하는 기능이 있어 보안 제품의 업데이트를 방해하였다. 당시 Redirected Hostfile Entries 진단명으로 변조된 Hosts 파일 내용을 치료하는 엔진이 배포되었다.

〈V3 제품군의 진단명〉
– Win-Trojan/Qhost.51200.H(2012.03.04.00)
– Redirected Hostfile Entries(2012.01.28.00)

보안 제품 동작을 방해하는 온라인 게임핵 변종

최근 온라인 게임핵 악성코드의 변종이 지속적으로 제작 및 유포되어 사용자들의 불편을 초래하고 있다. 이 악성코드는 감염된 시스템에 설치된 백신 제품의 동작을 방해한다.

[그림 1-45] 악성코드의 보안 제품 무력화 대상 프로세스



주요 생성 파일은 아래와 같으며 usbinckey.sys, cardctrl.exe 파일은 서비스로 등록된다.

[주요 생성 파일]
– C:₩WINDOWS₩system32₩drivers₩usbinckey.sys
– C:₩WINDOWS₩system32₩usbinckey.dll
– C:₩WINDOWS₩system32₩cardctrl.exe

드롭퍼에 의해 생성되어 서비스로 동작하는 루트킷(usbinckey.sys)은 자신과 usbinckey.dll 파일을 보호하며 악성코드가 생성한 서비스를 내리지 못하도록 방어한다. 또한, 해당 악성코드가 다운로드하는 파일에 의해 윈도우 시스템 정상 파일인 imm32.dll이 악성 파일로 교체된다.

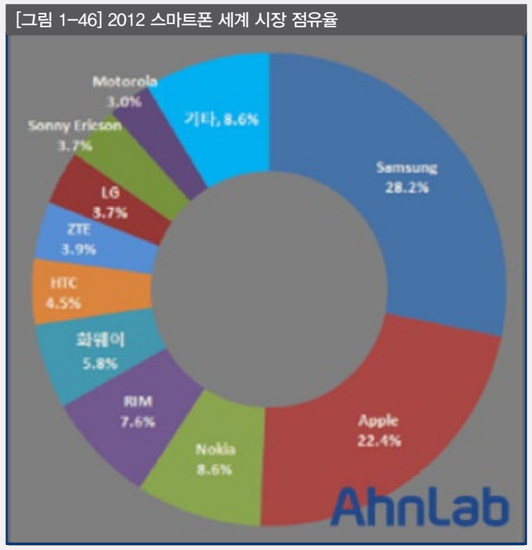
〈V3 제품군의 진단명〉
– Dropper/Win32.Rootkit
– Win-Trojan/Rootkit.7936.C
– Win-Trojan/Agent.75776.GA

Mac OS를 대상으로 하는 보안 위협의 증가

국내는 물론 전 세계 사용자들로부터 많은 사랑을 받고 있는 애플 제품들은 그동안 보안에 강력한 것으로 알려졌다. 하지만 최근 자바 취약점(CVE-2012-0507)을 악용한 Flashback 악성코드가 유포되어 55만 대의 Mac OS 사용자가 감염되는 등 악성코드 변종 및 해킹 기법이 나날이 증가하고 있다.

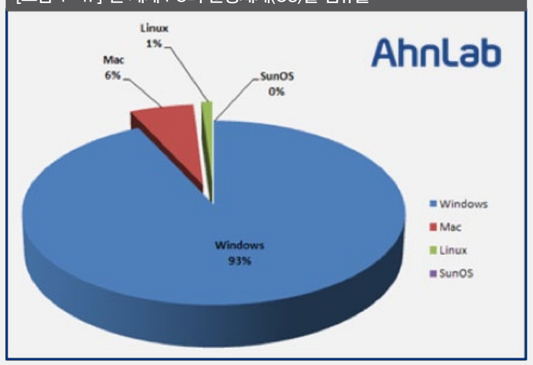
[그림 1-46]은 스마트폰 세계 시장 점유율로 삼성과 애플이 각각 50% 정도 점유하고 있다.

[그림 1-46] 2012 스마트폰 세계 시장 점유율



PC의 운영체제별 점유율은 [그림 1-47]과 같이 윈도우가 90% 이상을 차지하고 있다.

[그림 1-47] 전 세계 PC의 운영체제(OS)별 점유율



애플의 스마트폰이나 Mac OS는, 삼성이나 마이크로소프트에 뒤지긴 하지만, 상당한 시장 점유율을 보이고 있다.

[표 1-5]는 2012년 4월까지 애플 제품을 위협한 악성코드를 분류한 것이다.

[표 1-5] 애플(Mac) OS를 타깃으로 하는 악성코드

종류	설명
Flashback 악성코드	어도비 플래시 업데이트를 가장한 트로이목마로 2011년에 최초로 발견되었으며 SNS 등을 통해 유포된다. 최근 55만 대의 Mac 사용자가 이 악성코드에 감염되었다.
Sabpab 악성코드	MS 워드 취약점을 이용한 트로이목마로 이메일 첨부 파일 형태로 유포된다.
Tsunami Trojan	오래 전 리눅스에서 이용되었던 백도어 프로그램으로 IRC 기반의 분산 서비스 공격 클라이언트 프로그램이다.
OSX/Imuler-B	악의적인 목적으로 제작된 파일을 유명 모델의 사진인 것처럼 속여 실행을 유도하는 트로이목마다.
Trojan - Dropper:OSX.Revir.A	PDF 파일로 위장한 트로이목마로 원격 액세스할 수 있는 백도어를 포함하고 있으며, 이메일 첨부 파일 형태로 확산된다.
MacDefender Fake AV	Mac OS를 타깃으로 한 FakeAV(허위 백신)으로 결제를 유도하는 등의 악의적인 행위를 한다.
PDF Bug in Safari	Safari 웹 브라우저에서 PDF 파일을 표시할 때 발생할 수 있는 취약점으로, 공격에 성공하면 iPhone, iPad, iPod 기기에 대한 원격 제어가 가능하다.
Weyland-Yutani 로봇 키트	Mac OS를 겨냥한 악성코드 키트로 블랙 마켓을 통해 유통되고 있다.

애플(Mac) OS를 겨냥한 악성코드는 계속 증가하고 있다. 이는 Mac OS의 시장 점유율이 증가하면서 공격 대상이 된 것으로 판단된다. 사용자들은 Mac OS가 이제는 안전한 OS가 아님을 인지하고 보안 패치, MS 워드 및 플래시 플레이어, 자바 등의 응용 프로그램 패치를 항상 최신으로 유지하는 등의 각별한 주의가 필요하다.

윈도우 · Mac OS를 동시에 감염시키는 악성코드

최근 국외에서 'Invitation for Tibetan Films'라는 제목으로 유포된 악성 스팸 메일에서 [그림 1-48]과 같이 윈도우 · Mac OS에서 모두 동작하는 악성코드가 발견되었다.

[그림 1-48] 운영체제 비교 루틴

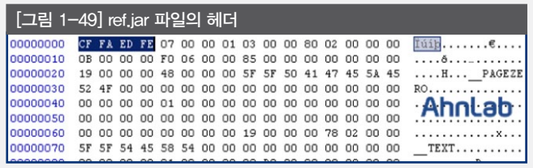
```
<script>
    var emb = document.createElement('applet');
    emb.setAttribute('name', 'applet');
    emb.setAttribute('width', '1');
    emb.setAttribute('height', '1');

    if (navigator.userAgent.indexOf('Win') != -1){
        emb.setAttribute('code', 'Func1.class');
        emb.setAttribute('archive', 'img.jar');
    }
    else if (navigator.userAgent.indexOf('Mac') != -1){
        emb.setAttribute('code', 'a.class');
        emb.setAttribute('archive', 'ref.jar')
    }
    document.body.appendChild(emb);
</script>
```

이 악성코드는 감염시킨 PC의 운영체제에 맞춰 아래의 파일들을 다운로드하고, 해당 파일들은 자바 취약점을 이용해 실행된다.

– 'file.***.**/v*******l/2*****R/img.jar' 〈— 윈도우에 사용되는 URL
– 'file.***.**/v*******l/2*****R//ref.jar' 〈— Mac OS에 사용되는 URL

img.jar 파일은 윈도우에서 실행 가능한 PE 파일 형태의 악성 파일을 가지고 있으며 ref.jar 파일은 Mac OS X에서 실행 가능한 파일 포맷의 악성 파일을 포함하고 있다.

[그림 1–49] ref.jar 파일의 헤더



과거 국내 패스트푸드 업체를 사칭해 유포된 악성 메일에서 OS를 구분하여 감염시키도록 작성된 코드가 발견됐었다. 하지만 실제로는 윈도우 대상 악성 파일을 다운로드하는 URL만 존재했다.

위 두 사례에서 보듯이 자바 취약점을 이용한 악성코드의 공격은 계속되고 있다. 이를 예방하기 위해서는 자바를 비활성화 상태로 설정하거나 보안 업데이트를 통해 최신 버전으로 유지해야 한다.

〈V3 제품군의 진단명〉

– Dropper/Agent.25088.CA
– MacOS_X/Olyx
– EXP/Cve–2011–3544
– JAVA/Cve–2012–0507

자바, MS 오피스 취약점을 이용하여 유포되는 Mac OS X 악성코드

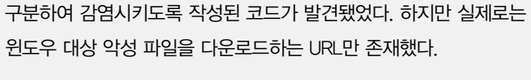
Sabpab 진단명으로 불리는 악성코드는 자바 취약점(CVE–2012–0507)과 MS 오피스 취약점(CVE–2009–0563)을 이용하여 사용자의 시스템을 감염시킨다.

A. 해당 악성코드는 사용자 계정의 Preferences 경로에 com.apple.PubSabAgent.pfile을 생성한다.

[그림1–50] 생성된 악성코드

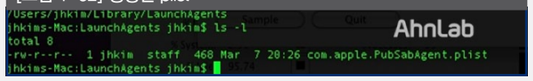
악성코드를 통해 생성된 파일은 Mac 실행 파일 포맷인 Mach–O 형태의 32bit 파일이다.

[그림 1–51] Mach–O 파일 포맷

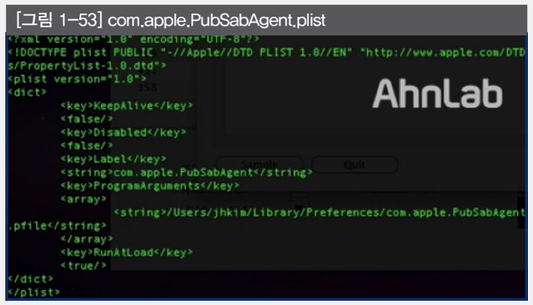


B. 악성코드를 지속적으로 실행하기 위해 사용자 계정의 LaunchAgents 경로에 com.apple.PubSabAgent.plist 파일을 생성한다.

[그림 1–52] 생성된 plist

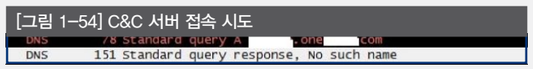


[그림 1–53] com.apple.PubSabAgent.plist



C. 해당 악성코드는 C&C 서버로부터 명령을 전달받아 악의적인 기능을 수행한다. 분석 당시에는 C&C 서버가 유효하지 않아 접속되지 않았다.

[그림 1–54] C&C 서버 접속 시도



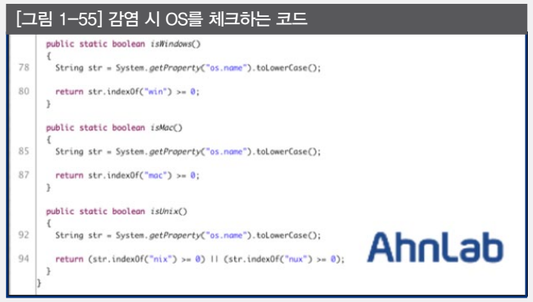
자바 및 MS 오피스 취약점을 이용한 Mac 악성코드가 지속적으로 발견되고 있으므로 최신 보안 패치의 설치가 필요하다.

티베트 NGO를 타깃으로 하는 Mac 악성코드

중국과 영토권 분쟁으로 이슈화되고 있는 티베트와 관련하여 티베트 NGOs(Non–Governmental Organizations)를 타깃으로 하는 악성코드가 유포되었다. 자바 취약점을 이용한(CVE–2011–3544) 이 악성코드는 C&C 서버와 통신하여 외부에서 전달된 명령을 수행한다.

Tibet.A는 Mac OS X뿐만 아니라 윈도우 등 다수의 운영체제를 감염시킬 수 있는 Cross–Platform 형태의 악성코드이다.

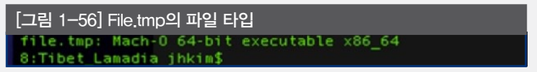
[그림 1–55] 감염 시 OS를 체크하는 코드



A. 자바 취약점을 이용한 index.jar 파일에 의해 실행된 file.tmp 파일은 자신의 복사본을 아래의 경로에 생성한다. File.tmp 또는 AudioServer 파일은 64bit로 컴파일된 실행 파일이다.

– /Library/Audio/Plug–Ins/AudioServer

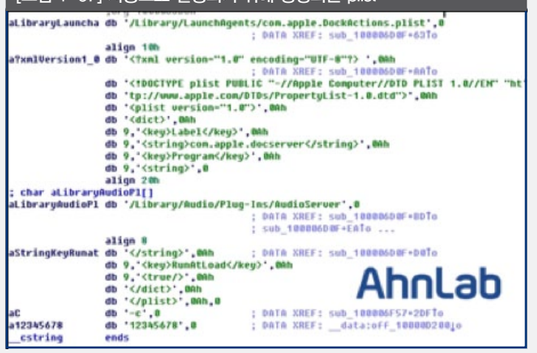
[그림 1–56] File.tmp의 파일 타입



B. 해당 악성코드는 시스템 시작 시 자동으로 실행되도록 아래의 경로에 plist 파일을 만들어둔다. 생성된 plist 파일을 통해 사용자가 로그인할 때마다 AudioServer 악성코드가 자동으로 실행된다.

– /Library/LaunchAgents/com.apple.dockActions.plist

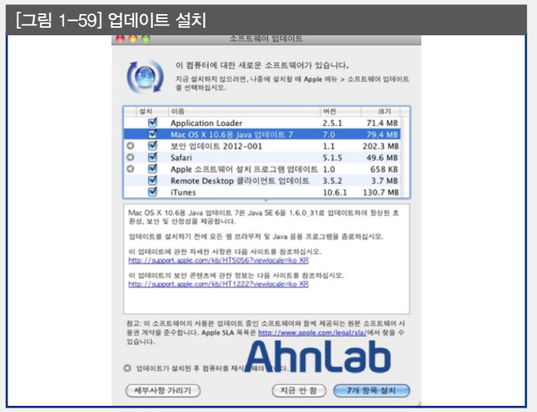
[그림 1–57] 자동으로 실행되기 위해 생성되는 plist



Mac OS X에서 자바 보안 패치를 업데이트하기 위해서는 상단 좌측의 애플 로고를 클릭한 후 '소프트웨어 업데이트…'를 클릭하여 업데이트 프로그램을 실행한다.

[그림 1–58] Mac OS X의 소프트웨어 업데이트

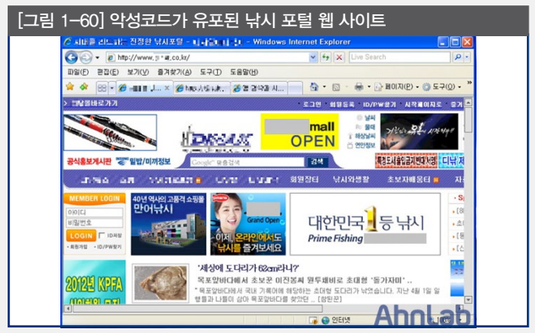
[그림 1–59] 업데이트 설치



낚시 포털 사이트를 통해 유포되는 온라인게임 계정 탈취 악성코드

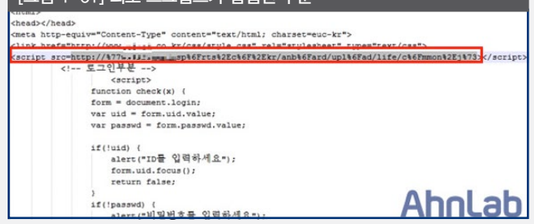
낚시 포털 사이트로 운영되고 있는 웹 사이트에서 온라인게임 계정을 탈취하는 악성코드가 유포되었다. 이 악성코드는 사용자의 온라인게임 계정 탈취를 목적으로 제작되었으며 감염된 OS에 따라 다른 파일이 생성된다.

[그림 1–60] 악성코드가 유포된 낚시 포털 웹 사이트

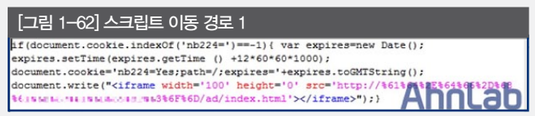


해당 웹 사이트에 방문하면 홈페이지에 삽입된 스크립트를 따라 차례로 또 다른 스크립트가 로딩된다.

[그림 1–61] 최초 스크립트가 삽입된 구문



[그림 1–62] 스크립트 이동 경로 1



악성코드 제작자는 웹 사이트에서 CVE–2010–0806 취약점을 이용해 악성코드를 유포하였다.

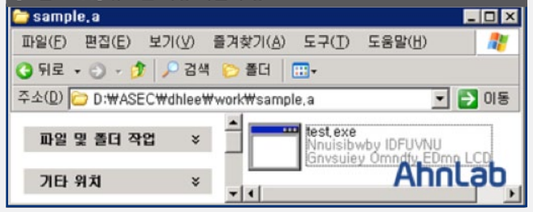
[그림 1–63] 스크립트 이동 경로 2

스크립트를 따라 최종적으로 유포되는 악성코드 경로와 파일명은 아래와 같다.

[그림 1-64] 유포지와 악성 파일

```
1  http://muma.df-l[illegible]me.com/test/test.exe
2  http://muma.df-l[illegible]me.com/test/tesx.exe
```

[그림 1-65] 유포된 악성 파일의 정보



이 악성코드에 감염되면 윈도우 XP는 ws2help.dll 시스템 파일이 변조되며 원본 파일은 ws2helpXP.dll로 백업된다. Windows 7은 C:₩Windows₩System32₩HlMYM.dll 파일이 생성된다. 이러한 웹 사이트에 삽입된 스크립트를 통해 악성코드에 감염되지 않도록 각 보안 패치를 설치해야 한다.

[표 1-6] 악성코드 유포에 자주 이용되는 취약점

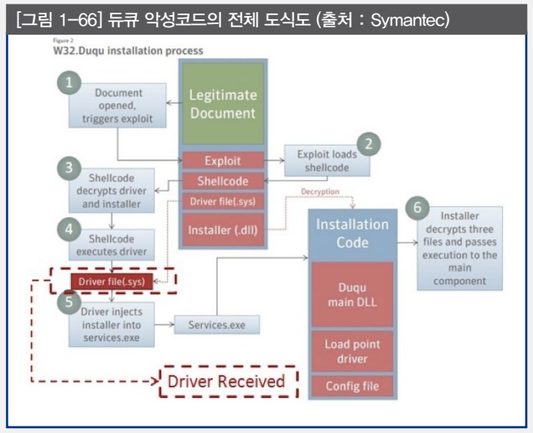
제목	URL
Windows OS	CVE-2010-0806 (MS10-018) CVE-2011-1255 (MS11-050) CVE-2012-0003 (MS12-004)
Adobe Flash Player	CVE-2012-0754 CVE-2011-2140 CVE-2011-2110 CVE-2011-0611
JAVA	CVE-2011-3544

스턱스넷 변형으로 알려진 듀큐 악성코드의 변형

현지 시각으로 2012년 3월 20일 시만텍에서 기업 블로그 〈New Duqu Sample Found in the Wild〉를 통해 스턱스넷(Stuxnet)의 변형으로 알려진 듀큐(Duqu) 악성코드의 변형이 발견되었음을 발표했다.

스턱스넷이 SCADA(Supervisory Control And Data Acquisition) 감염으로 원자력 발전소의 운영을 방해하려는 것과 달리, 듀큐는 감염된 시스템과 네트워크에서 정보를 수집하기 위한 목적으로 제작되었다. 이번에 발견된 듀큐의 변형은 시만텍에서 공개한 [그림 1-66]과 같이 붉은색 박스로 표기된 드라이버(.sys) 파일이다.

[그림 1-66] 듀큐 악성코드의 전체 도식도 (출처 : Symantec)



ASEC에서는 [그림 1-67] 파일의 Time Date Stamp를 통해 해당 파일이 2012년 2월 23일 생성된 것을 확인하였다. 이를 미루어 봤을 때 듀큐 제작자 또는 제작 그룹은 지속적으로 다른 변형들을 제작하여 유포하고 있는 것으로 추정된다.

[그림 1-67] 듀큐 변형의 제작 시간이 표기된 Time Data Stamp

pFile	Data	Description	Value
000000E4	014C	Machine	IMAGE_FILE_MACHINE_I386
000000E8	4F45D78A	Time Date Stamp	2012/02/23 06:07:06 UTC
000000F0	00000000	Number of Symbols	
000000F4	00E0	Size of Optional Header	
000000F6	0102	Characteristics	
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0100	IMAGE_FILE_32BIT_MACHINE

AhnLab

이러한 보안 위협에서 SCADA와 같은 산업 기반 시스템을 보호하기 위해서는 안티바이러스(Anti-Virus) 소프트웨어를 포함한 트러스라인(TrusLine)과 같은 산업용 시스템 전용 보안 솔루션을 사용하는 것이 효율적이다.

〈V3 제품군의 진단명〉
– Win-Trojan/Duqu.24320(V3, 2012.03.23.01)

스파이아이 공격 대상 기업들의 업종과 국가 분석

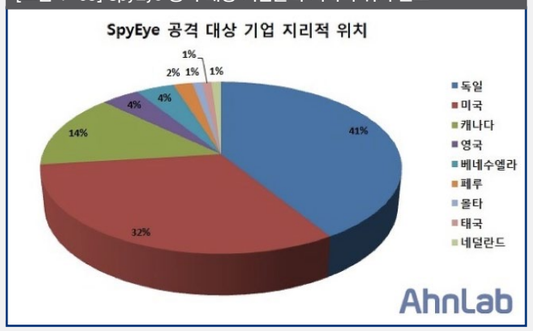
안랩은 2012년 4월 2일 '인터넷뱅킹 정보 탈취 악성코드 스파이아이 트렌드 발표'라는 보도자료를 배포하고 금전적인 목적으로 인터넷뱅킹 정보를 탈취하는 악성코드인 스파이아이(SpyEye)에 대해 경고하였다.

스파이아이는 툴킷(Toolkit)을 통해 악성코드를 제작할 때, 악성코드 제작자가 어떤 웹 사이트의 사용자 정보를 탈취할 것인지를 설정 파일을 통해 구성할 수 있다. ASEC에서는 2012년 1분기 동안 확보한 스파이아이 악성코드 샘플들을 대상으로 스파이아이가 어떠한 기업의 사용자 계정 정보와 암호를 노리는지 상세 분석하였다.

일반적으로 스파이아이는 악성코드가 첨부된 이메일 또는 취약한 웹 사이트 등을 통해 유포되므로 보안 제품을 사용하지 않거나 최신 엔진으로 업데이트하지 않은 사용자, 취약점이 존재하는 윈도우 운영체제 사용자들이 많이 감염되었다.

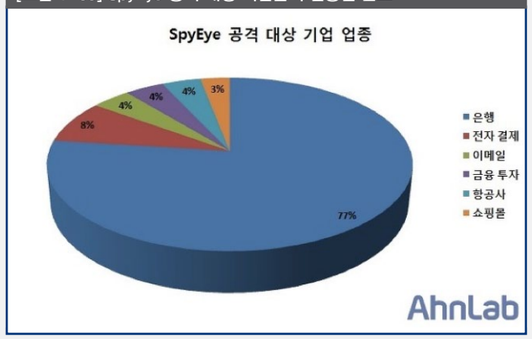
스파이아이가 생성하는 암호화된 설정 파일을 분석한 결과, 악성코드 제작자의 공격 대상이 되는 웹 사이트를 보유한 기업들의 지리적 위치는 [그림 1-68]과 같이 독일, 미국, 그리고 캐나다 순서로 금융업이 발달한 국가들에 집중되어 있었다.

[그림 1-68] SpyEye 공격 대상 기업들의 지리적 위치 분포



[그림 1-69]는 해당 악성코드의 공격 대상이 되는 웹 사이트를 보유한 기업들을 업종별로 분류한 것으로 대부분 온라인뱅킹을 지원하는 기업들에 집중되었으며, 전자 결제 서비스, 금융 투자 등의 순서로 나타났다.

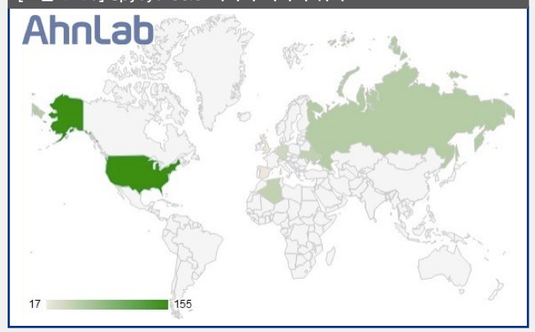
[그림 1-69] SpyEye 공격 대상 기업들의 업종별 분포



한 가지 특이한 사실은 스파이아이 제작자의 공격 대상이 되는 웹 사이트 중에는 온라인 항공권 구매 서비스를 제공하는 항공사도 포함되어 있다는 점이다.

안랩에서 운영하는 패킷 센터(Packet Center)의 구성 시스템인 SpyEYE C&C Tracking 시스템을 통해 분석한 결과, 스파이아이가 탈취한 사용자 계정 정보와 암호를 전송하는 C&C(Command and Control) 서버가 자리 잡고 있는 국가는 [그림 1-70]의 녹색 부분과 같다.

[그림 1-70] Spyeye C&C 서버의 지리적 위치



C&C 서버는 대부분 미국에 집중되어 있으며 그 외에 러시아와 우크라이나 순서로 많이 분포되어 있다. 이러한 C&C 서버 대부분이 해킹된 시스템 또는 관리가 소홀한 시스템에 설치되는 것으로 분석되었다. 다행스럽게도 스파이아이 제작자가 탈취를 노리는 웹 사이트들에는 한국 금융 기업들이 포함되어 있지 않다. 이는 과거 몇 년 전부터 진행되었던 보안 위협의 국지화 현상으로 해석할 수 있다. 그러나 외국 금융기관과 온라인뱅킹을 통해 거래하는 사용자들은 스파이아이 악성코드 감염 피해에 많은 주의를 기울일 필요가 있다.

01. 악성코드 동향
c. 모바일 악성코드 이슈

Another fake Angry birds

안드로이드 플랫폼이 큰 인기를 끌면서 모바일 기반의 악성코드 또한 활개치고 있다. 악성코드는 주로 인기 있는 앱으로 위장하여 사용자가 설치하게끔 유도하는데, 그 대상으로 빠지지 않고 이용되는 인기 게임 중 하나가 바로 'Angry Birds'다.

이번에 새롭게 발견된 악성코드 역시 유명 게임 Angry Birds로 위장하고 있다.

[그림1-71] 가짜 Angry Birds 아이콘

이 악성코드는 중국의 서드파티 마켓에서 처음 발견되었으며 [그림 1-71]과 같이 Angry Birds 게임으로 위장하고 있다. 중국의 서드파티 안드로이드 마켓의 규모는 우리나라보다 크고, 정품 앱을 불법으로 다운로드하기 위해 이용하는 경우가 많아 사용자들이 악성 앱에 노출되기 쉽다.

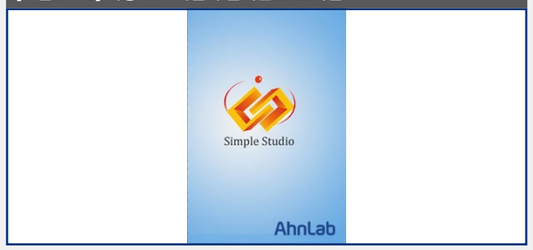
[그림 1-72] manifest에 나타나는 악성 서비스

해당 악성코드는 설치 시 'com.neworld.demo.UpdateCheck'라는 악성 서비스를 실행한다. 이 서비스는 앱의 assets 폴더에 저장된 그림 파일(mylogo.jpg)에 몰래 숨겨놓은 ELF 포맷의 악성 파일을 추가로 실행하여 아래와 같은 악의적인 동작을 지속적으로 수행한다.

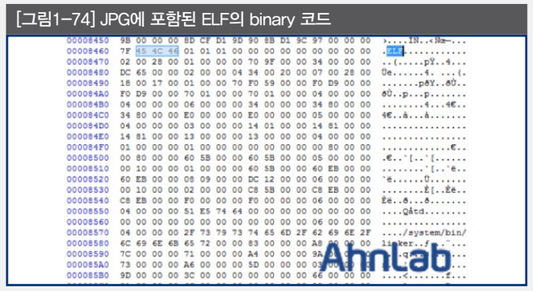
– 사용자 스마트폰 정보 탈취
– 강제 루팅 시도
– C&C 서버와 통신하며 명령 수행(예 : 프로그램 설치)

〈V3 제품군의 진단명〉
– Android-Exploit/Rootor.TC

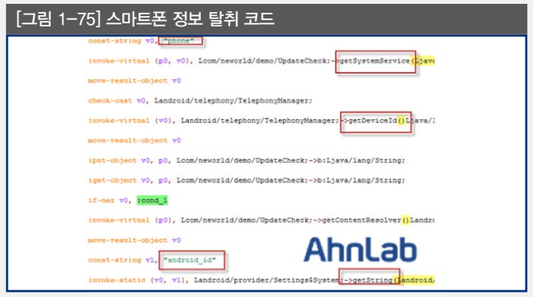
[그림 1-73] 악성 ELF 파일이 숨겨진 JPG 파일



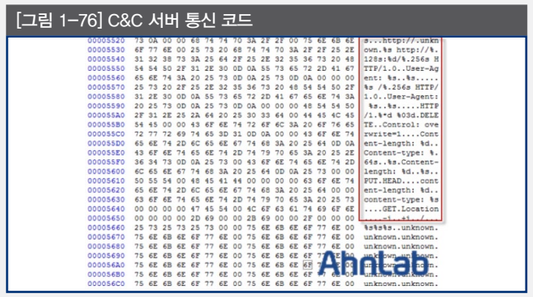
[그림1-74] JPG에 포함된 ELF의 binary 코드



[그림 1-75] 스마트폰 정보 탈취 코드



[그림 1-76] C&C 서버 통신 코드



01. 악성코드 동향
d. 악성코드 분석 특집

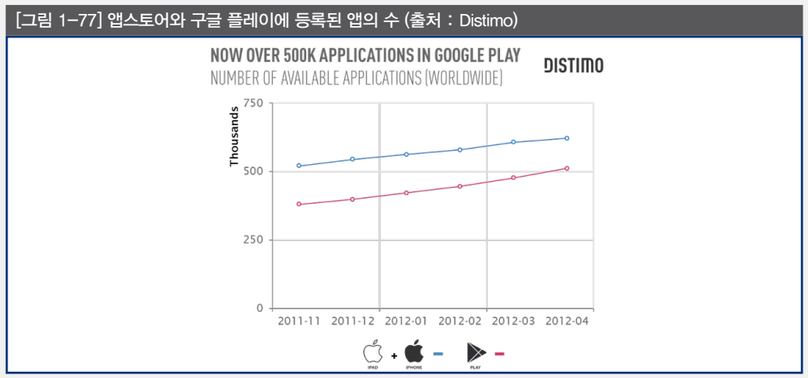
불필요한 옵션 사용으로 발생할 수 있는 스마트폰 보안 위협과 대응

이번 호에서는 사용자에게 불필요한 설정을 한 안드로이드 스마트폰을 PC에 연결할 때 발생할 수 있는 보안 문제를 예상하고 그에 대한 예방책을 제시한다.

1. 수많은 앱과 다양한 설치 방법

스마트폰의 활성화를 주도하는 것은 다양한 앱이라 해도 과언이 아니다. [그림 1-77]은 Distimo에서 확인한 구글 플레이 스토어와 애플 앱스토어에 등록된 앱의 수다.

[그림 1-77] 앱스토어와 구글 플레이에 등록된 앱의 수 (출처 : Distimo)



앱을 스마트폰에 설치하는 방법은 OS별로 조금씩 다르다. 아이폰은 탈옥(Jail Break)을 제외하면 기본적으로 앱스토어를 통해 모든 앱을 설치한다. 반면 안드로이드는 서드파티 마켓을 허용하는 정책 때문에 스마트폰 제작사나 통신사 등에서 운영하는 마켓을 포함하여 수많은 마켓에서 앱을 배포하며, 설치하는 방법 또한 다양하다.

안드로이드 스마트폰 사용자들은 앱을 설치하기 위해 주로 기본 설치돼 있는 삼성 Apps, 구글 Play 스토어를 실행하거나 인터넷 마켓을 이용한다. 또는 인터넷이나 토렌트 등을 이용하여 필요한 앱을 다운로드할 수 있는데, 이 경우 스마트폰을 PC에 연결해야 한다.

PC에 스마트폰을 연결해 앱을 설치하는 방법은 다시 두 가지로 나눌 수 있다. 첫 번째는 USB 드라이버 모드로 연결해 APK 파일을 스마트폰으로 직접 복사한 후 스마트폰에서 설치하는 것이다. USB 드라이버 모드로 스마트폰을 연결하면 스마트폰의 저장소는 USB 저장소와 같은 기능을 한다. 이렇게 복사된 설치 파일은 안드로이드 OS의 인스톨매니저를 통해 설치할 수 있다. 두 번째 방법은 스마트폰을 PC에 연결한 후 PC에서 ADB 명령어를 이용해 설치하는 것이다.

PC를 이용해 다운로드한 안드로이드용 앱은 APK 확장자를 가진다.

2. ADB를 이용한 앱 설치

이 방법은 앱을 간편하게 설치할 수 있지만, 설치되는 앱이 스마트폰의 어떤 기능을 활용하는지 사용자에게 보여주는 권한 확인 프로세스를 건너뛰게 된다(설치되는 앱이 동작하는 데 필요한 권한을 사용자에게 보여주는 것은 안드로이드의 보안 기능 중 하나다).[1]

ADB를 이용해 안드로이드 스마트폰에 앱을 설치하기 위해서는 안드로이드의 설정 중 ‘USB 디버깅’, ‘알 수 없는 소스’ 두 항목이 허용 상태여야 한다.

3. 알 수 없는 소스 허용

인증서는 인증된 프로그램만 설치할 수 있도록 하는 안드로이드 OS의 또 다른 보안 기능이다. 인증된 프로그램이란 구글의 공식 마켓인 Play 스토어에서 배포되는 앱을 말한다. 하지만 서드파티 마켓을 허용하는 안드로이드의 특성상 안드로이드 스마트폰 사용자는 대부분 알 수 없는 소스 사용을 허용하고 있다. 각 통신사나 스마트폰 제조사에서 제공한 앱을 설치하기 위해서는 반드시 알 수 없는 소스를 허용해야 하기 때문이다.

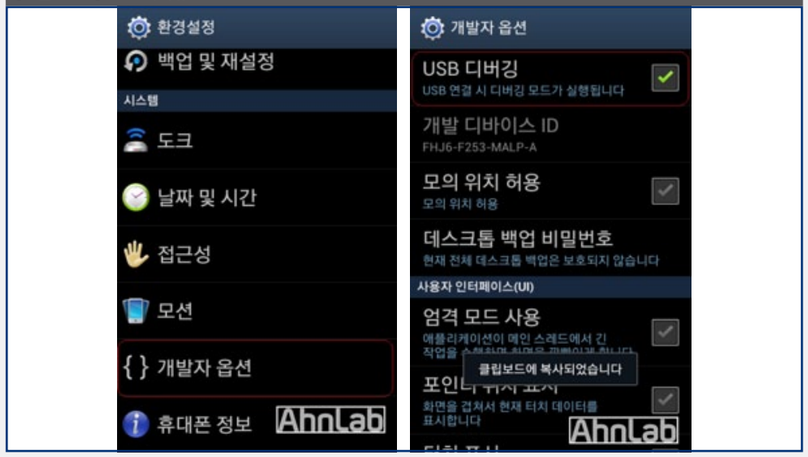
[그림 1-78] 알 수 없는 소스

[1] 안드로이드의 보안 기능 http://www.ibm.com/developerworks/kr/library/x-androidsecurity/

4. USB 디버깅

USB 디버깅은 안드로이드에서 동작하는 앱을 테스트할 때 사용하는 기능이다. 사용자가 USB 디버깅을 선택하면 안드로이드 스마트폰의 ADB 데몬이 활성화된다. ADB를 이용해 할 수 있는 일은 다음과 같다.

[그림 1-79] USB 디버깅



ADB(Android Debug Bridge) : ADB는 다양한 명령어를 통해 안드로이드 운영체제를 사용하는 기기를 제어할 수 있도록 해준다. [그림 1-80]은 ADB 1.0.25 버전에서 사용 가능한 옵션 중 일부다(자세한 내용은 안드로이드 개발자 사이트에서 확인할 수 있다).[2]

[그림 1-80] ADB 명령 옵션

```
Android Debug Bridge version 1.0.25
-----------------------------------------생략-----------------------------------------
 devices                        - list all connected devices
 connect <host>:<port>          - connect to a device via TCP/IP
 disconnect <host>:<port>       - disconnect from a TCP/IP device

device commands:
 adb push <local> <remote>      - copy file/dir to device
 adb pull <remote> <local>      - copy file/dir from device
 adb sync [ <directory> ]       - copy host->device only if changed (see 'adb help all')
 adb shell                      - run remote shell interactively
 adb shell <command>            - run remote shell command
 adb emu <command>              - run emulator console command
 adb logcat [ <filter-spec> ]   - View device log
 adb forward <local> <remote>   - forward socket connections
                                  forward specs are one of:
                                    tcp:<port>
                                    localabstract:<unix domain socket name>
                                    localreserved:<unix domain socket name>
                                    localfilesystem:<unix domain socket name>
                                    dev:<character device name>
                                    jdwp:<process pid> (remote only)
 adb jdwp                       - list PIDs of processes hosting a JDWP transport
 adb install [-l] [-r] <file>   - push this package file to the device and install it
                                  ('-l' means forward-lock the app)
                                  ('-r' means reinstall the app, keeping its data)
 adb uninstall [-k] <package>   - remove this app package from the device
                                  ('-k' means keep the data and cache directories)
-----------------------------------------생략-----------------------------------------
```

[2] 안드로이드 개발자 사이트 http://developer.android.com/guide/developing/tools/adb.html

디바이스 옵션은 ADB 서버가 인식한 스마트폰과 에뮬레이터의 목록을 보여주는 기능을 한다. 셸 옵션은 지정한 스마트폰 시스템의 셸에 연결해 프롬프트를 띄운다. 이 셸은 리눅스 셸과 유사하며 안드로이드에서 지원하는 간단한 명령을 통해 연결된 스마트폰을 탐색하고 수정할 수 있다. 인스톨, 언인스톨 옵션은 앱을 설치하거나 삭제할 때 이용되는 명령이다. 이런 ADB의 다양한 기능은 개발의 편의성을 제공하기 위한 안드로이드 OS의 도구다.

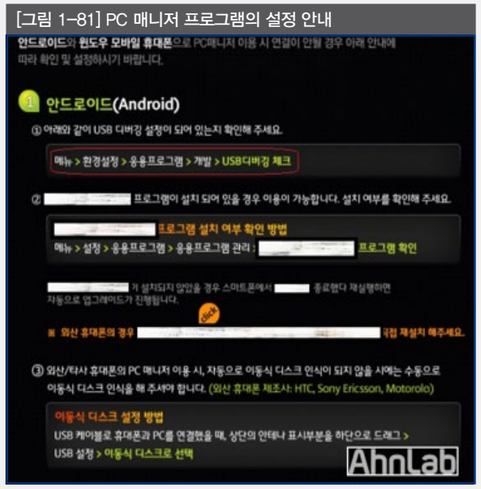
이렇듯 개발자에게 유용한 기능인 USB 디버깅 설정을 많은 사용자가 활성화하는 이유는 무엇일까?

5. 왜 USB 디버깅의 활성화가 필요한가?

USB 디버깅은 스마트폰 루팅 시 필요한 기능이다. 루팅(Rooting)은 OS나 앱에 존재하는 취약점을 이용해 관리자 권한을 획득하는 것을 의미한다. 일부 스마트폰 사용자들은 바탕 화면을 바꾸거나 통신사나 스마트폰 제작사에서 임의로 포함한 앱을 제거하고 싶어한다. 또는 아직 자신의 스마트폰에 적용되지 않은 최신 버전의 운영체제로 업그레이드하려 한다. 이럴 때 필요한 것이 관리자 권한이다.

또 다른 이유는 많은 사용자가 사용하는 마켓의 PC 매니저 프로그램이나 특정 앱을 설치하기 위해서다. 각 제작사나 통신사는 다양한 이름으로 자사의 앱 마켓을 운영하고 있다. 다양한 앱 마켓에서는 사용자 편의를 위해 PC 매니저 프로그램을 제공한다. 매니저 프로그램은 스마트폰 사용자의 PC에 설치되어 스마트폰에 저장된 데이터를 추출하거나 자신의 마켓에서 구매한 앱을 스마트폰에 손쉽게 설치하도록 도와주는 기능을 제공한다. 이러한 매니저 프로그램 중 일부가 USB 디버깅을 활성화할 것을 권장하기도 한다.

[그림 1-81] PC 매니저 프로그램의 설정 안내



[그림 1-82] USB 디버깅 해제 경고

일부 안드로이드 스마트폰은 해당 기능의 비활성화를 시도할 때 특정 앱을 사용할 수 없다는 경고 메시지를 노출해 사용자가 USB 디버깅 기능을 비활성화하지 않도록 유도한다.

이외에도 여러 가지 이유로 안드로이드 스마트폰 사용자들은 알 수 없는 소스를 허용하고 USB 디버깅의 활성화를 유지한다. USB 디버깅이 활성화된 상태로 스마트폰을 PC에 연결하면 사용자의 의도와 상관없이 ADB 데몬이 활성화되어 스마트폰이 보안 위협에 노출될 수 있다.

6. USB 디버깅이 활성화된 경우 발생할 수 있는 문제

PC에 감염된 악성코드가 ADB의 기능을 악용하는 것은 어렵지 않다. 스마트폰이 PC에 연결되는 것을 감지한 후 ADB의 옵션 중 일부를 이용한다면 손쉽게 설치된 프로그램 목록을 확인하고, 필요하다면 백신과 같은 보안 앱을 삭제할 수도 있다. 또 특정 앱을 조회 후 삭제하고 악의적인 기능을 포함하도록 리패키징[3] 한 악성코드를 설치할 수 있어 사용자는 자신의 스마트폰에 설치된 앱이 변조된 것을 알기 어렵다.

7. 가능한 위협과 대응

PC에 연결된 스마트폰으로 사용자가 인지하지 못한 사이에 설치된 악성코드는 저장된 연락처 정보를 읽어 외부로 유출하거나 사용자의 스마트폰을 이용해 광고 SMS를 발송하는 등 휴대전화와 PC에서 행할 수 있는 다양한 악의적인 행위를 할 수 있다.

이런 유형의 보안 위협에서 벗어날 수 있는 방법은 간단하다.

– USB 디버깅 설정은 필요한 경우에만 활성화하고 사용이 완료됐을 때는 반드시 비활성화한다.

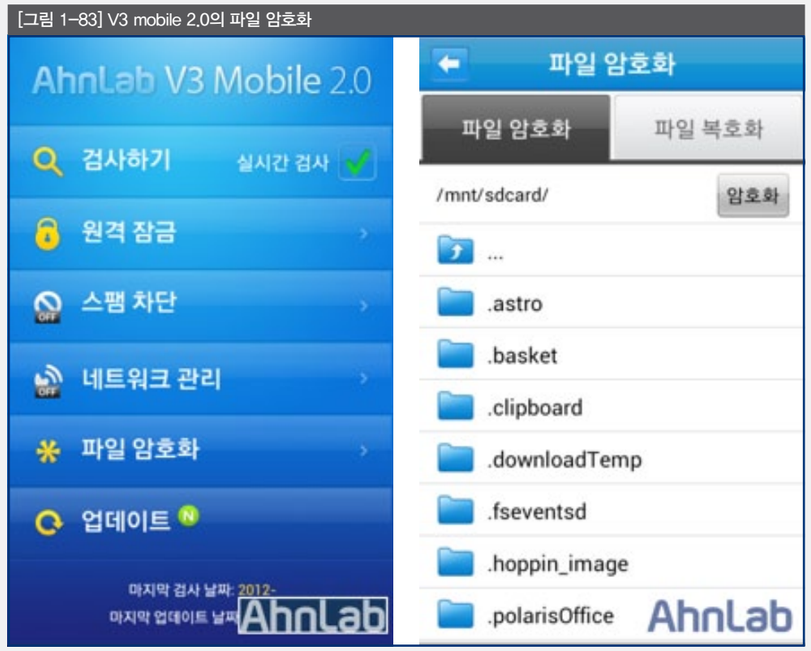
– 많은 사람이 사용하는 PC방이나 도서관에서는 스마트폰을 연결하지 않는다.

– 스마트폰에 앱을 설치할 때는 유명한 마켓을 이용하고, 다운로드한 프로그램을 설치할 때에는 반드시 권한을 확인해 비정상적인 권한이 없는지 확인한다.

– 비밀번호와 같은 중요한 정보는 되도록 스마트폰 내에 저장하지 않아야 하지만, 꼭 저장해야 할 때는 별도의 프로그램을 이용하여 암호화한다.

– 모바일 백신 프로그램과 같은 보안 앱을 활용해 혹시 모르는 악성 앱의 피해를 예방한다.

[그림 1-83] V3 mobile 2.0의 파일 암호화

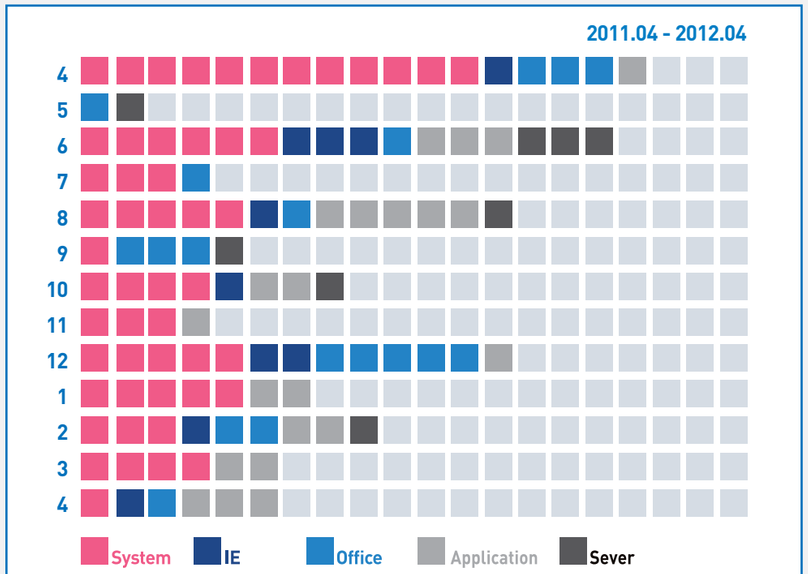


[3] 안드로이드 악성코드는 어떻게 만들어지는가? – ASEC Report 2012 4월호
http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=19269

02. 보안 동향
a. 보안 통계

4월 마이크로소프트 보안 업데이트 현황

마이크로소프트가 발표한 보안 업데이트는 긴급 4건, 중요 2건의 총 6건이다. 원격에서 코드 실행이 가능한 취약점은 MS12-026을 제외한 5건으로, 그 중 MS12-027은 이미 관련 공격 코드가 공개된 만큼 주의가 필요하다.



[그림 2-1] 공격 대상 기준별 MS 보안 업데이트

위험도	취약점
긴급	인터넷 익스플로러 보안 업데이트 누적(MS12-023)
긴급	윈도우의 취약점으로 인한 원격 코드 실행 문제점(MS12-024)
긴급	.NET Framework의 취약점으로 인한 원격 코드 실행 문제점(MS12-025)
긴급	Windows Common Controls의 취약점으로 인한 원격 코드 실행 문제점(MS12-027)
중요	Forefront Unified Access Gateway (UAG)의 취약점으로 인한 정보 공개 허용 문제점 (MS12-026)
중요	MS 오피스의 취약점으로 인한 원격 코드 실행 문제점(MS12-028)

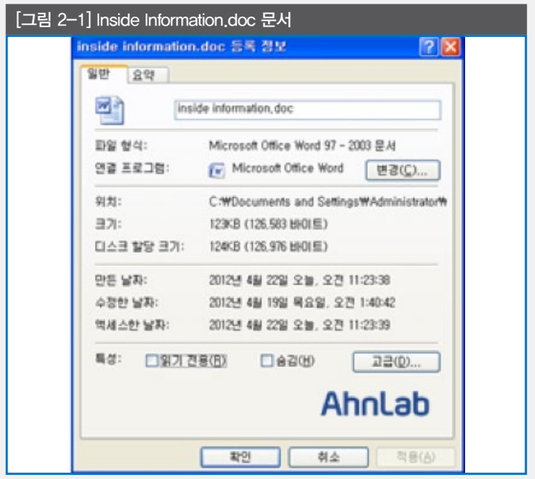
[표 2-1] 2012년 4월 MS 주요 보안 업데이트

02. 보안 동향
b. 보안 이슈

윈도우 공용 컨트롤 취약점(CVE-2012-0158)을 악용하는 문서

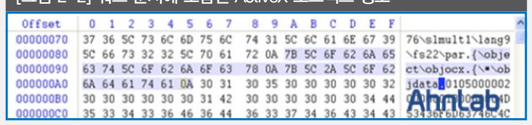
2012년 4월, MS가 발표한 6건의 보안 업데이트 가운데 윈도우 공용 컨트롤의 취약점(CVE-2012-0158)을 악용하는 RTF 형식의 문서 파일이 발견되었다. 이번에 발견된 악성 문서 파일은 2010년에 발표된 MS 워드 취약점(CVE-2010-3333)과 유사하게 제작됐으며, 이메일에 워드 문서가 첨부된 형태로 유포되었다.

[그림 2-1] Inside Information.doc 문서



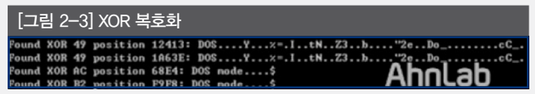
윈도우 공용 컨트롤 MSCOMCTL ActiveX Control 취약점(CVE-2012-0158)을 악용하는 워드 문서에는 ActiveX 오브젝트가 포함되어 있다.

[그림 2-2] 워드 문서에 포함된 ActiveX 오브젝트 정보



분석 당시 해당 워드 문서가 정상적으로 실행되지 않아 문서 내용과 생성 파일에 대한 정보를 파악하는 데 어려움이 있었지만, 특정 XOR 키로 복호화하여 문서를 통해 드롭되는 악성코드 및 워드 파일에 대한 정보를 확인할 수 있었다.

[그림 2-3] XOR 복호화



복호화한 워드 문서 파일에서 다음과 같은 실행 파일 헤더(MZ)가 확인된다.

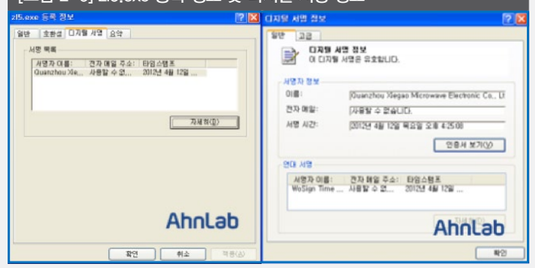
[그림 2-4] 문서 내부에 포함된 악성 파일

실행 파일(PE)과 함께 생성되는 워드 문서 정보를 확인할 수 있다.

[그림 2-5] 문서 내부에 포함된 워드 문서

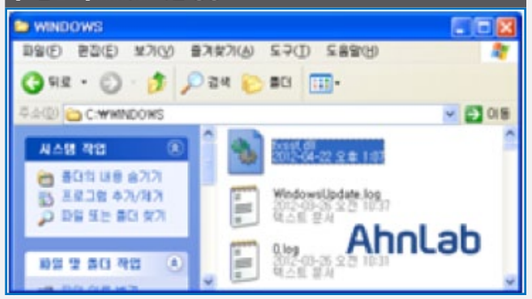
워드 문서에 의해 생성되는 zl5.exe 악성코드 파일은 확인 당시에 유효한 디지털 서명을 사용 중이었다.

[그림 2-6] zl5.exe 등록 정보 및 디지털 서명 정보



zl5.exe 악성코드가 실행되면 windows 폴더에 fxsst.dll 파일을 생성한다.

[그림 2-7] fxsst.dll 파일 생성



악성코드는 특정 도메인으로 접근을 시도하지만 4월 현재 정상적으로 연결되지 않는다.

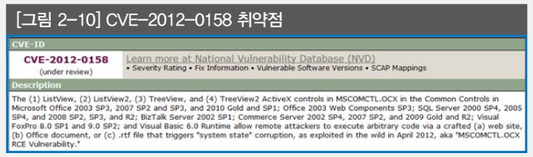
[그림 2-8] 네트워크 연결 시도

악성코드가 접근을 시도하는 IP 주소는 미국과 중국 IP로 확인된다.

[그림2-9] 일부 접속 IP 정보

악성코드 유포에 사용된 취약점은 MS 오피스, Visual FoxPro, Commerce Server, BizTalk Server, SQL Server와 같은 윈도우 제품에 영향을 미친다. 또한, 침해된 웹 사이트로 방문을 유도하거나 MS 오피스 문서 파일, RTF 형식으로 제작된 악성 파일을 이메일에 첨부하는 형태로 악성코드 유포가 가능하며, 최신 취약점을 이용한 악성코드 유포가 계속될 것으로 예상되므로 사용자들은 신속히 MS 보안 패치를 설치해야 한다.

[그림 2-10] CVE-2012-0158 취약점



〈V3 제품군의 진단명〉

– Exploit/Cve-2012-0158(2012.04.21.00)

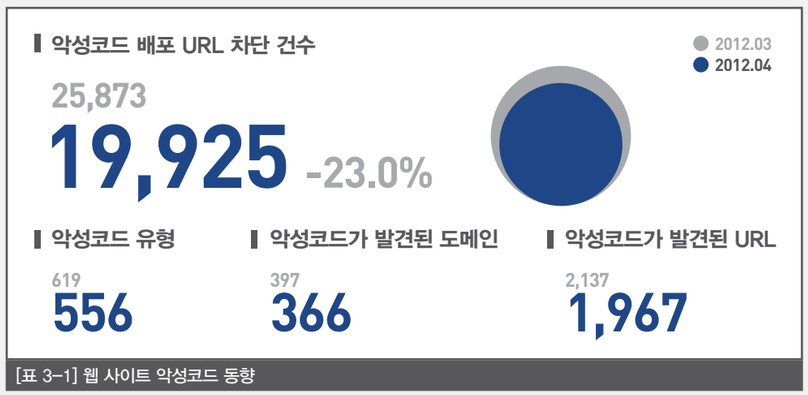
– Win-Trojan/Etchfro.99839(2012.04.21.00)

– Win-Trojan/Geddel.11176(2012.04.21.00)

03. 웹 보안 동향
a. 웹 보안 통계

웹사이트 악성 코드 동향

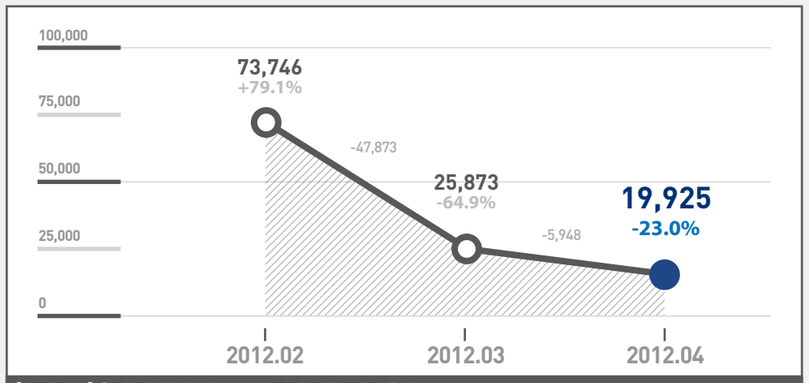
안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 의하면, 2012년 4월 악성코드를 배포하는 웹 사이트를 차단한 건수는 총 1만 9925건이었다. 악성코드 유형은 556종, 악성코드가 발견된 도메인은 366개, 악성코드가 발견된 URL은 1967개였다. 이는 2012년 3월과 비교할 때 전반적으로 다소 감소한 수치이다.



[표 3-1] 웹 사이트 악성코드 동향

월별 악성코드 배포 URL 차단 건수

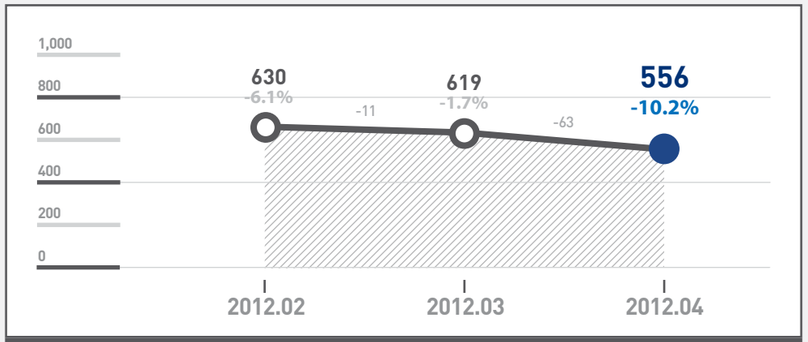
2012년 4월 악성코드 배포 웹 사이트 URL 접근에 대한 차단 건수는 지난 달 2만 5873건에 비해 23% 감소한 1만 9925건이었다.



[그림 3-1] 월별 악성코드 배포 URL 차단 건수 변화 추이

월별 악성코드 유형

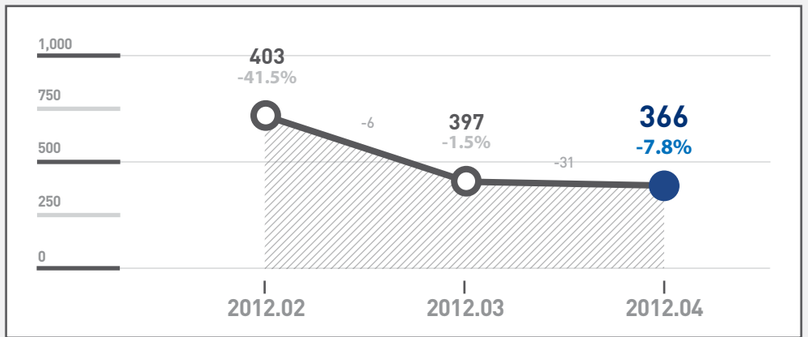
2012년 4월의 악성코드 유형은 전달의 619건에 비해 10% 줄어든 556종이었다.



[그림 3-2] 월별 악성코드 유형 수 변화 추이

월별 악성코드가 발견된 도메인

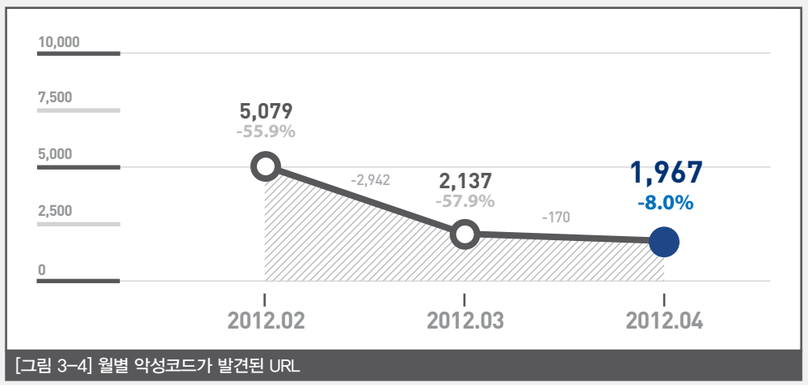
2012년 4월 악성코드가 발견된 도메인은 366건으로 2012년 3월의 397건에 비해 8% 감소했다.



[그림 3-3] 월별 악성코드가 발견된 도메인 수 변화 추이

월별 악성코드가 발견된 URL

2012년 4월 악성코드가 발견된 URL은 전월의 2137건에 비해 8% 감소한 1967건이다.



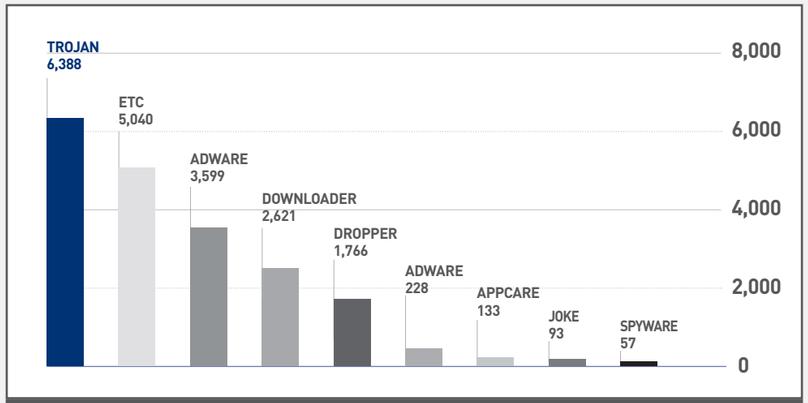
[그림 3-4] 월별 악성코드가 발견된 URL

악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면 트로이목마가 6388건/32.1%로 가장 많았고, 애드웨어가 3599건/18.1%인 것으로 조사됐다. 악성코드 배포 최다 10건 중에서 Win-Adware/ToolBar.Cashon.308224가 1754건으로 가장 많았고 Downloader/Win32.Korad가 1255건으로 그 뒤를 이었다.

유형	건수	비율
TROJAN	**6,388**	**32.1%**
ADWARE	3,599	18.1%
DOWNLOADER	2,621	13.2%
DROPPER	1,766	8.9%
Win32/VIRUT	228	1.1%
APPCARE	133	0.7%
JOKE	93	0.5%
SPYWARE	57	0.3%
ETC	5,040	25.1%
	19,925	**100.0%**

[표 3-2] 악성코드 유형별 배포 수



[그림 4-8] 2012년 1분기 악성코드 유형별 배포 수

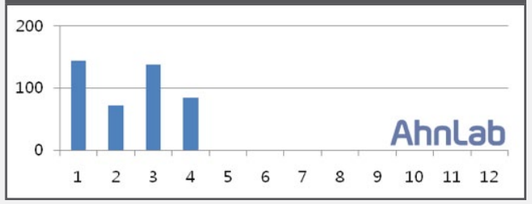
순위	등락	악성코드명	건수	비율
1	**—**	**Win-Adware/ToolBar.Cashon.308224**	**1,754**	**20.6%**
2	▲1	Downloader/Win32.Korad	1,255	14.7%
3	▼1	Dropper/Small.Gen	961	11.3%
4	▲1	Downloader/Win32.Totoran	845	9.9%
5	▲4	Trojan/Win32.HDC	680	8.0%
6	NEW	Trojan/Win32.ADH	679	8.0%
7	NEW	ALS/Bursted	675	7.9%
8	—	Unwanted/Win32.WinKeyfinder	574	6.7%
9	▼3	Adware/Win32.KorAd	570	6.6%
10	▼3	Unwanted/Win32.WinKeygen	542	6.3%
			8,535	**100.0%**

[표 3-3] 악성코드 배포 최다 10건

03. 웹 보안 동향
b. 웹 보안 이슈

2012년 4월 침해 사이트 현황

[그림 3-6] 2012년 4월 악성코드 유포 목적의 침해 사이트 현황



[그림 3-6]은 악성코드 유포를 목적으로 하는 침해 사고가 발생했던 사이트의 현황이다. 전월보다 감소했지만 사이트 유형별에서는 P2P 사이트를 통한 악성코드 유포가 소폭 상승하였다.

침해 사이트를 통해서 유포된 악성코드 최다 10건

[표 3-4]는 4월 한 달 동안 가장 많은 사이트를 통해서 유포되었던 악성코드 최다 10건이다. 가장 많이 유포된 Win-Trojan/Onlinegamehack.54784.BC(이하 Onlinegamehack.54784.BC)는 20개의 국내 웹 사이트를 통해서 유포되었다.

[표 3-4] 2012년 4월 악성코드 최다 10건

순위	악성코드명	건수
1	**Win-Trojan/Onlinegamehack.54784.BC**	**20**
2	Win-Trojan/Onlinegamehack.102400.DX	20
3	Win-Trojan/Onlinegamehack.212992.S	15
4	Win-Trojan/Onlinegamehack.53248.KA	15
5	Win-Trojan/Onlinegamehack.140493.B	14
6	Win-Trojan/Onlinegamehack.112640.P	12
7	Win-Trojan/Onlinegamehack.38912.BJ	12
8	Win-Trojan/Onlinegamehack.38400.BA	11
9	Win-Trojan/Onlinegamehack.73216.AI	11
10	Win-Trojan/Agent.9344.L	10

3월에 48개의 사이트에서 유포되었던 Win-Trojan/Patched.64512.B는 언론사 〉 P2P & 웹하드 〉 기타 순이나, 4월에 가장 많이 유포된 Onlinegamehack.54784.BC의 경우 언론사를 통한 유포가 대폭 감소하면서 P2P & 웹하드 〉 언론사 & 기타 순으로 바뀌었다.

[표 3-4]의 가장 많이 유포된 Onlinegamehack.54784.BC의 유포 사이트 구성을 자세히 살펴보면 P2P & 웹하드를 통한 유포는 3월과 거의 비슷하지만 4월의 경우 언론사를 통한 유포가 급감하면서 상대적으로 P2P & 웹하드를 통한 유포가 많았던 것처럼 보일 수 있다. 단 Onlinegamehack.54784.BC만을 기준으로 본 것으로 실제 다양한 악성코드의 종합적인 유포 비율에서 언론사 사이트가 차지한 비율은 3월과 거의 동일 하였다.

VOL. 28
ASEC REPORT Contributors

집필진
선임 연구원 강 동 현
선임 연구원 안 창 용
선임 연구원 장 영 준
주임 연구원 문 영 조
주임 연구원 박 정 우
연구원 김 재 홍

참여연구원 ASEC 연구원
SiteGuard 연구원

편집장
선임 연구원 안 형 봉

편집인 안랩 세일즈마케팅팀

디자인 안랩 UX디자인팀

감 수
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