Security Trend

ASEC REPORT

VOL.60

December, 2014

AhnLab

ASEC REPORT

VOL.60 December, 2014

ASEC(AhnLab Security Emergency response Center)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 주식회사 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.

2014년 12월 보안 동향

Table of Contents

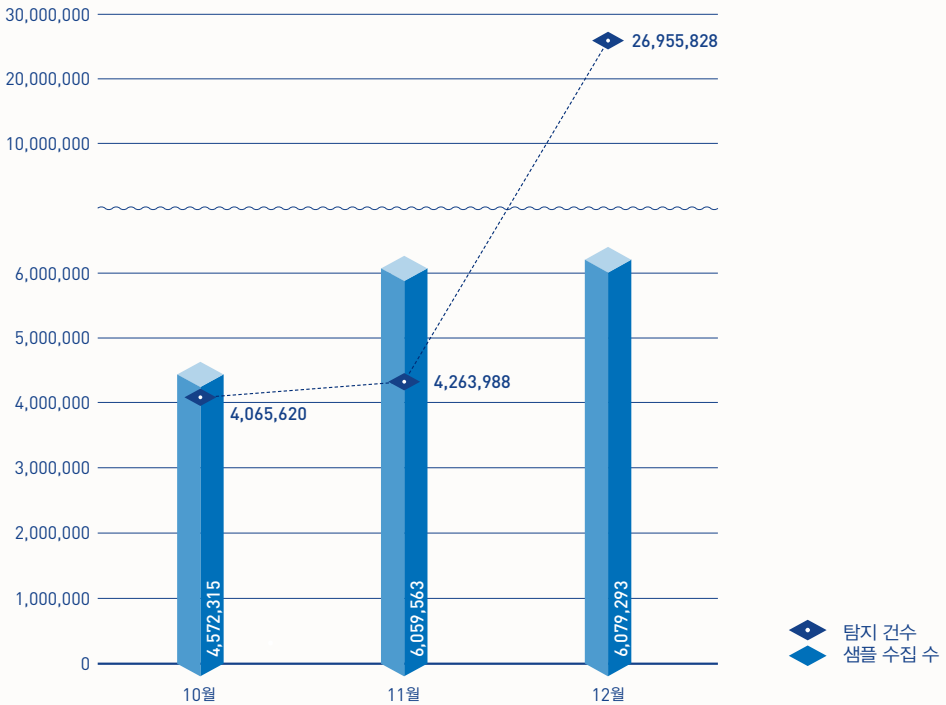
1

보안 통계
STATISTICS

01
악성코드 통계

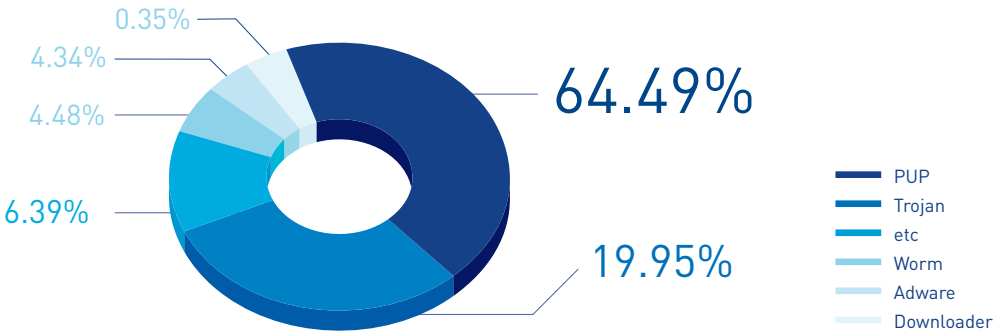
ASEC이 집계한 바에 따르면 2014년 12월 한달 간 탐지된 악성코드 수는 2,695만 5,828건이다. 이는 전월 426만 3,988건 보다 2,269만 1,840건 증가한 수치다. 한편 12월에 수집된 악성코드 샘플 수는 607만 9,293건이다.

[그림 1-1]에서 '탐지 건수'란 고객이 사용 중인 V3 등 안랩의 제품이 탐지한 악성코드의 수를 의미하며, '샘플 수집 수'는 안랩이 자체적으로 수집한 전체 악성코드의 샘플 수를 의미한다.



[그림 1-1] 악성코드 추이(2014년 10월 ~ 12월)

[그림 1-2]는 2014년 12월 한달 간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 64.49%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 19.95%, 웜(Warm)이 4.48%로 그 뒤를 이었다.



[그림 1-2] 2014년 12월 주요 악성코드 유형

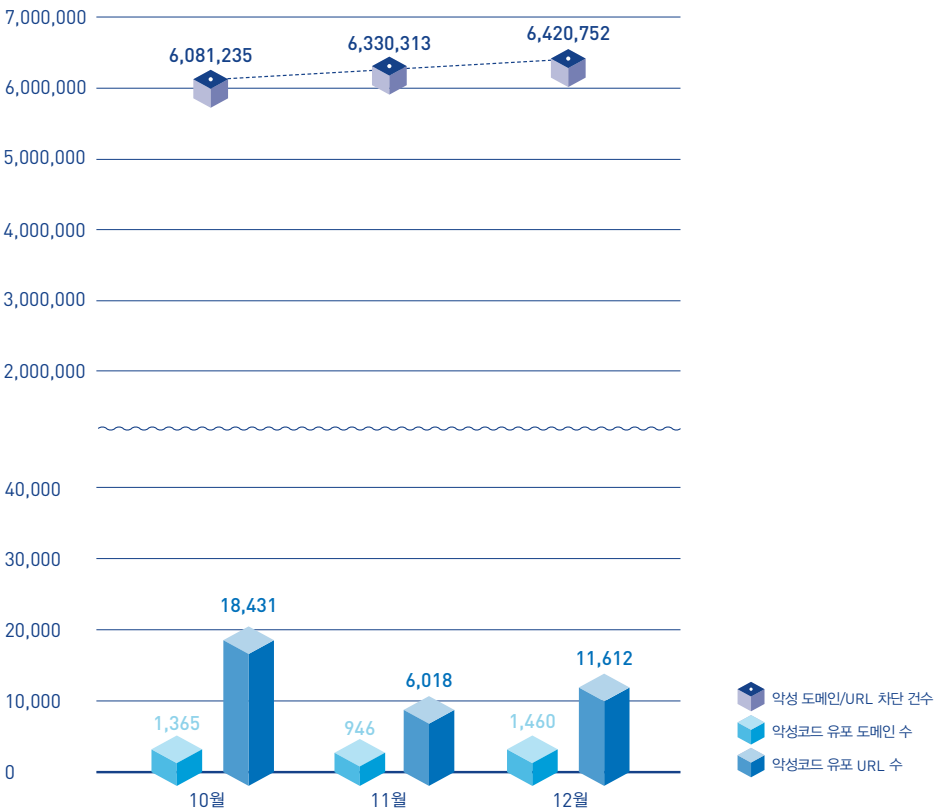
[표 1-1]은 12월 한 달간 가장 빈번하게 탐지된 악성코드 10건을 진단명 기준으로 정리한 것이다. PUP/Win32.IntClient가 총 155만 3,897건으로 가장 많이 탐지되었고, PUP/Win32.MyWebSearch가 111만 2,218건으로 그 뒤를 이었다.

[표 1-1] 2014년 12월 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	PUP/Win32.IntClient	1,553,897
2	PUP/Win32.MyWebSearch	1,112,218
3	PUP/Win32.Helper	1,078,083
4	PUP/Win32.Generic	921,610
5	PUP/Win32.SubShop	856,453
6	PUP/Win32.BrowseFox	447,719
7	PUP/Win32.MicroLab	385,872
8	Trojan/Win32.Gen	344,095
9	PUP/Win32.CrossRider	319,729
10	PUP/Win32.savepop	300,509

02
웹 통계

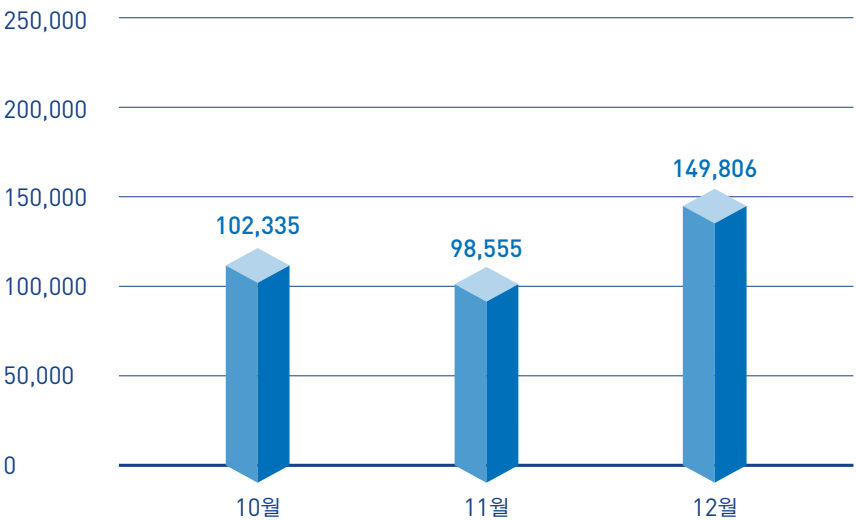
2014년 12월 악성코드 유포지로 악용된 도메인은 1,460개, URL은 1만 1,612개로 집계됐다. 또한 12월의 악성 도메인 및 URL 차단 건수는 총 642만 752건이다. 악성 도메인 및 URL 차단 건수는 PC 등 시스템이 악성코드 유포지로 악용된 웹사이트의 접속을 차단한 수이다.



[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2014년 10월 ~ 12월)

03
모바일 통계

2014년 12월 한달 간 탐지된 모바일 악성코드는 14만 9,806건으로 집계되었다.



[그림 1-4] 모바일 악성코드 추이(2014년 10월 ~ 12월)

[표 1-2]는 12월 한달 간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. 특히 Android-PUP/SmsReg가 지난달보다 2배 가량 증가한 4만 148건으로 집계되었다.

[표 1-2] 2014년 12월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsReg	40,148
2	Android-Trojan/FakeInst	19,920
3	Android-PUP/Dowgin	13,824
4	Android-Trojan/Opfake	7,226
5	Android-Trojan/Mseg	6,248
6	Android-Trojan/SmsSpy	3,578
7	Android-Trojan/SmsSend	3,247
8	Android-PUP/Noico	2,578
9	Android-Trojan/SMSAgent	2,531
10	Android-PUP/Airpush	2,311

2

보안 이슈
SECURITY ISSUE

01 악성코드 감염 통로로 이용되는 애드웨어와 PUP

최근 들어 온라인 게임핵(Online GameHack)의 재감염 사례가 자주 발견되고 있다. 백신을 통해 악성코드를 치료하더라도 재부팅 후 다시 감염되는 증상이 반복되었다. 보통 악성코드를 치료한 후 재부팅하여 악의적인 증상이 재발하는지 확인한다. 재부팅 후에도 악성코드가 여전히 동작하고 있다는 것은 추가적인 악성코드가 남아 있다는 의미이다. 하지만 이번 경우에는 온라인 게임핵을 유포하는 애드웨어(Adware)가 예약 작업에 등록되어 있어 지속적으로 재감염시키고 있었다.

그림 2-1 | 업데이트되는 파일의 아이콘

실제 유포 및 업데이트되는 파일의 아이콘은 [그림 2-1]과 같다. 업데이트 파일이 실행되면 [표 2-1]과 같은 파일이 생성된다.

표 2-1 | 온라인 게임핵 관련 생성 파일(상)/ 애드웨어 관련 생성 파일(하)

[파일 생성 정보]
C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩[영문&숫자].exe (온라인 게임핵 드롭퍼)
C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩A1.zip (ws2help.dll 정상 파일)
C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩B1.zip (wshtcpip.dll 정상 파일)
C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩C1.zip (version.dll 정상 파일)
C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩D1.zip (midimap.dll 정상 파일)
C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩yhsys₩doit.rar (손상된 PE)
C:₩WINDOWS₩system32₩drivers₩[영문&숫자].sys (온라인 게임핵 악성 파일)
C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩[영문&숫자].dll (온라인 게임핵 악성 파일)
C:₩WINDOWS₩system32₩midimap.dll (온라인 게임핵 악성 파일)
C:₩WINDOWS₩system32₩wshtcpip.dll (온라인 게임핵 악성 파일)
C:₩Program Files₩AdM***hing₩updater_temp.exe
C:₩Program Files₩AdM***hing₩admsys.exe
C:₩Documents and Settings₩Administrator₩Local Settings₩Temp₩1680₩adm***hing.dll
C:₩Documents and Settings₩Administrator₩Local Settings₩Temp₩2240₩windo***ab.dll
C:₩Documents and Settings₩Administrator₩Local Settings₩Temp₩4373₩AdM***hing.exe

updater_temp.exe 파일이 실행되면 C:₩DOCUME~1₩ADMINI~1₩LOCALS~1

₩Temp₩[영문&숫자].exe 경로에 파일을 생성한다. 이 파일은 [표 2-1]의 온라인 게임핵 관련 파일들을 생성하며 악의적인 행위를 한다. 또한 [표 2-2]의 사이트에서 파일을 받아와 실제 애드웨어 파일에 대한 설치와 업데이트도 이루어진다.

표 2-2 | 다운로드 되는 PUP 주소

[네트워크 정보]
http://down.adm***hing.co.kr/download/dna/adm***.exe
http://down.adm***hing.co.kr/download/dna/adm***hing.dll

현재는 증상이 나타나지 않지만 애드웨어 SSI 프로그램의 업데이트 과정에서 유포된 것으로 확인된다. 만약 비슷한 증상으로 지속적인 재감염 현상이 나타나면 [시작프로그램] →[예약작업]에서 해당 프로그램의 목록이 있는지 확인해야 한다.

이처럼 PUP(Potentially Unwanted Program)나 애드웨어에 의한 악성코드 유포는 다수 보고된 바 있다. 업데이트 서버는 단기간에 여러 PC에서 감염될 수 있는 만큼 제작사의 관리와 노력이 필요하다.

악성코드에 감염되었을 경우에는 [그림 2-2]와 같이 전용백신으로 악성코드를 치료한 후 애드웨어의 예약 작업 및 시작프로그램을 제거하거나 안랩의 V3 최신 엔진으로 정밀 검사를 하면 치료 가능하다.

그림 2-2 | 전용백신 치료 화면

요즘에는 인터넷에서 필요한 프로그램을 쉽게 구할 수 있다. 하지만 프로그램 구입과 설치 시 주의가 필요하다. 인터넷 자료실 사이트에서 내려받은 프로그램을 설치했을 뿐인데 원하지 않는 프로그램이 설치되었다. 이런 프로그램은 사용자 모르게 실행되는데 평소에는 아무런 행위를 하지 않는다. 그러다 사용자가 인터넷 익스플로러를 실행하면 광고 창을 띄워 사용자에게 불편을 준다.

그림 2-3 | 인터넷 익스플로러 사용 시 나타나는 광고창

원하지 않는 프로그램이 설치되는 원인은 사용자가 프로그램을 내려받고 설치하는 과정에서 확인할 수 있다. 사용자는 원하는 프로그램을 내려받기 위해 검색 사이트를 이용한다. 이 때 PUP 제작자들은 이 점을 노리고 실제 자료실 사이트와 유사한 사이트를 제작한다. 유사 자료실 사이트는 검색 사이트와 블로그 게시물의 광고에 노출되며, 사용자는 이러한 사이트를 실제 자료실 사이트로 착각한다.

그림 2-4 | 검색 사이트에 노출된 유사 자료실 사이트 링크

그림 2-5 | 블로그 게시물 광고에 노출된 유사 자료실 사이트 링크

그림 2-6 | 유사 사이트(상) / 포털 사이트의 자료실(하)

사용자를 속이는 것은 사이트에만 국한되지 않는다. 유사 자료실 사이트를 통해 내려받은 프로그램의 인터페이스는 포털 사이트의 다운로더와 비슷하게 제작되어 있어 사용자가 착각하기 쉽다.

그림 2-7 | 가짜 전용 다운로드 프로그램(상) / 포털 자료실의 프로그램 다운로더(하)

[그림 2-8]의 전용 다운로드 프로그램의 실행 화면을 보자. 우측 하단에 '체크박스'와 함께 '프로그램명'이 기재되어 있다. 이렇게 체크박스에 체크된 프로그램은 '다운로드' 버튼을 누를 때 사용자가 인지할 수 없도록 설치된다.

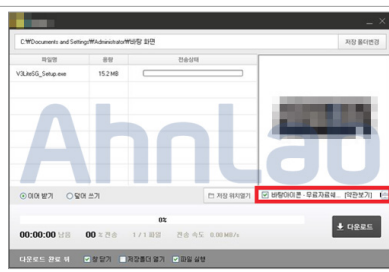


그림 2-8 | 가짜 전용 다운로드 프로그램

또한 원하지 않게 설치되는 불필요한 프로그램은 육안으로는 잘 보이지 않는 사용자 동의 및 약관을 포함하고 있다.

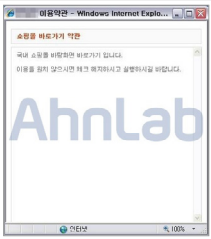


그림 2-9 | 부실한 이용약관

[그림 2-8]과 같이 다운로드 버튼을 클릭하면 네트워크를 통해 실제 프로그램의 설치 파일을 다운로드한다. 다운로드가 완료되면 프로그램 설치 화면이 나타난다.

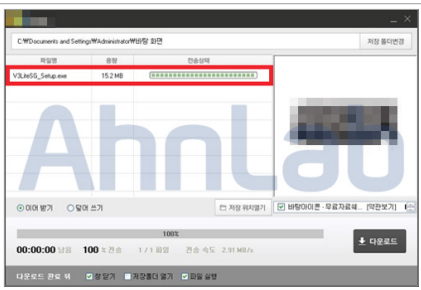


그림 2-10 | 실제 프로그램의 설치 파일 다운로드

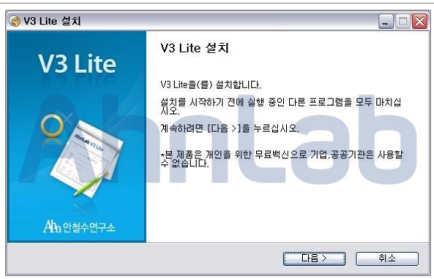


그림 2-11 | 실제 프로그램의 설치 화면

이와 함께 네트워크를 통해 불필요한 프로그램의 설치 파일을 다운로드한다. 실제 프로그램의 설치 화면이 나타나기 때문에 사용자는 불필요한 프로그램이 함께 설치되는 것을 인지하기 어렵다.

표 2-3 | 네트워크 연결 정보

[네트워크 연결 정보]
http://uti*****.com/down2/Ssetup.exe
http://file.topinf*****.com/dst/TopToolN_TN06.exe
http://down.searc*****.co.kr/distribute/SLslenska/searchlike.exe
http://uti*****.com/down2/install.exe
http://sub.sma***.co.kr/opapp/raonmedia/app/download/smartweb_silent.exe
http://down.pop*****.co.kr/download/PoppinSearch_p_hinst.exe
http://m.bt*****.com/fdwn/NE010/bt_neo1.exe
http://down.microop*****.com/app/pn/mopop_p08_inst.exe
http://app.koreanke*****.com/INST/ELT10/wd_id01.exe
http://update.medi*******.co.kr/bin/OffManagerSetup.DA.03.exe
http://file.targetke*****.co.kr/app/newiniweblink/P061/weblinkup.exe
http://down.luck*****.net/lucky08/luckyinstall.exe
http://down.*****ansupport.com/down/adInstall_wms007.exe
http://his*****.or.kr/aaa/windowadvertisement_codenemo16.exe
http://file.m***.co.kr/app/windowstab/WindowsTabSetup_utilbada.exe
http://yo*****.com/ins/part05_setup.exe
http://up1.po*****.co.kr/etcApp/smartbar/XecureSetup.exe

다운로드된 설치 파일은 자동으로 실행되어 [표 2-4]의 경로에 파일을 생성하며 [프로그램 추가/제거]에 설치된 프로그램을 등록한다. 이렇게 생성된 파일은 시스템에 광고 팝업창을 표시하여 사용자에게 불편을 준다.

표 2-4 | 생성된 파일 경로

[파일 경로]
C:₩OffManager
C:₩Program Files₩KoreanKeyword
C:₩Program Files₩PoppinSearch
C:₩Program Files₩sharebox_barcon
C:₩Program Files₩TopToolN
C:₩Program Files₩SmartWeb
C:₩Program Files₩SpaceAD
C:₩Program Files₩WindowAdvertisement
C:₩Program Files₩XecrueCrossWeb
C:₩Documents and Settings₩Administrator₩Local Settings₩Application Data₩apps
C:₩Documents and Settings₩Administrator₩Local Settings₩Application Data₩searchlike
C:₩Documents and Settings₩Administrator₩Local Settings₩Application Data₩windowstab
C:₩Documents and Settings₩Administrator₩Local Settings₩Application Data₩wiseman
C:₩Documents and Settings₩Administrator₩Local Settings₩Application Data₩weblink
C:₩Documents and Settings₩Administrator₩Local Settings₩Application Data₩Windows BT Icons
C:₩Documents and Settings₩Administrator₩Application Data₩luckytool
C:₩Documents and Settings₩Administrator₩Application Data₩MOpop

그림 2-12 | [프로그램 추가/제거]에 등록된 원하지 않는 프로그램

사용자가 원하지 않게 설치되는 불필요한 프로그램은 광고를 통한 금전 이득을 목적으로 이용된다. 프로그램 제작자는 목적 달성을 위해 다수 사용자에게 광고를 노출해야 수익을 얻을 수 있다.

그러려면 프로그램 제작자는 많은 사용자가 설치할 수 있도록 인기 있는 프로그램의 설치 파일로 위장하여 배포해야 한다. 주 목적이 금전 이득인 만큼 프로그램에 대한 보안 관리는 허술할 수밖에 없다. 이러한 프로그램은 악성코드 제작자에 의해 악성코드 감염 통로로 악용될 수 있으며 2차 피해로 이어질 수 있으므로 주의가 필요하다.

[불필요한 프로그램 설치 예방법]

1. 프로그램 설치 화면을 주의 깊게 확인한다.
원하지 않게 설치되는 불필요한 프로그램은 육안으로 식별하기 어려운 부분에 프로그램명과 사용자 동의 여부를 표기하기 때문에 프로그램 설치 전 충분히 확인해볼 필요가 있다.

2. 블로그 게시물 또는 광고를 통해 연결되는 사이트의 파일은 다운로드하지 않는다.
블로그 게시물의 파일 또는 광고를 통해 연결되는 사이트의 파일로 위장하는 방법도 불필요한 프로그램 제작자들이 사용하는 방법 중 하나이다.

3. 가능한 신뢰할 수 있는 사이트를 이용한다.
프로그램의 제작사 홈페이지를 이용한다.

한편, V3 제품군에서는 관련 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Simda (2014.12.08.00)
Trojan/Win32.NSAnti (2014.12.08.00)
Trojan/Win32.OnlineGameHack (2014.12.11.00)
PUP/Win32.WindowTab (2014.05.28.04)
Adware/Win32.CloverPlus (2014.11.26.00)외 다수

02
국제 화물 배송업체 메일로 위장한 악성코드…가짜 백신 설치 주의!

최근 '알뜰 쇼핑족'이 늘면서 국내보다 가격이 저렴한 수입 제품을 해외 사이트에서 직접 구매하는 '직구' 이용자가 증하고 있다. 해외에서 제품이 배송되다 보니 주로 국제 화물 배송업체(FedEx, DHL, UPS 등)를 이용한다. 이 과정에서 국제 화물 배송업체의 메일로 위장한 악성코드 유포가 과거부터 꾸준히 발생하고 있다. 해외 직구 증가에 따른 악성코드 감염 피해도 늘어날 전망이다.

이러한 형태의 악성코드 유포와 관련하여 한동안 국내에서 잠잠했던 가짜 백신(FakeAV)류의 악성코드 감염 피해 사례가 발견되었다.

[그림 2-13]과 같이 페덱스(FedEx)로 위장한 메일이 수신되었으며, 첨부 파일을 실행한 후 악성코드에 감염되었다는 피해 사례가 한 개인 블로그에서 확인되었다.

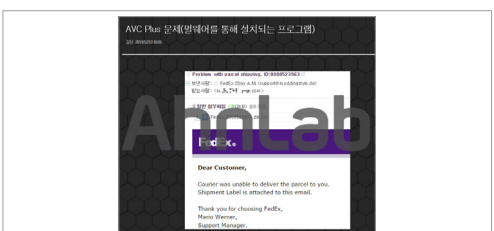


그림 2-13 | 수신된 메일 내용 출처 : http://niafilmuh.tistory.com/23

해당 피해 사례와 유사한 악성코드를 확인해보자. [그림 2-14]와 같이 첨부 파일은 압축되어 있었으며 압축을 해제한 결과 문서 파일의 확장자(.doc)로 위장한 스크립트(.js) 파일로 확인되었다.

그림 2-14 | 파일 확장자 확인

해당 스크립트 파일은 난독화되어 있으며 실행 시 설정된 URL에서 추가로 악성코드 다운로드를 통해 감염된다.

그림 2-15 | 스크립트 난독화 해제 전/후

[그림 2-15]의 URL을 통해 추가로 파일이 정상적으로 다운로드되면 악성코드에 감염되고 [그림 2-16]과 같은 메시지가 출력된다.

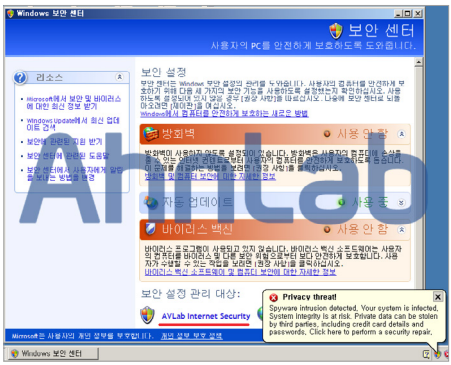


그림 2-16 | 보안 센터 및 허위 위협 탐지 알림

이는 트레이 알림을 통해 허위 시스템 감염 알림창이 뜨고 보안 센터를 띄워 가짜 백신의 실행을 유도하려는 의도로 보인다.

가짜 백신은 허용된 파일(ThumbnailExtractionHost.exe, rundll32.exe, dllhost.exe, searchprotocolhost.exe, wuauclt.exe, explorer.exe) 이외의 실행파일 실행 시 [그림 2-17]과 같이 감염된 프로그램이라는 메시지나 [그림 2-18]과 같이 '시스템 검사 결과 악성코드가 다수 발견되었다'는 허위 메시지를 띄운다. 이와 함께 인터넷 브라우저를 실행한 후 사이트에 접속하면 [그림 2-19]와 같이 허위 메시지를 띄워 가짜 백신 실행 및 결제 페이지로 유도한다.

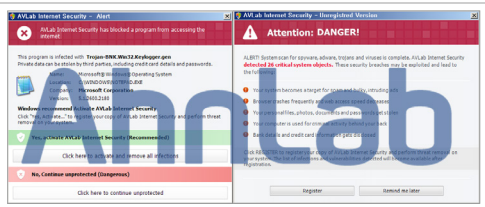


그림 2-17 | 허위 감염 알림창

그림 2-18 | 인터넷 창을 통한 허위 감염 메시지

그림 2-19 | 결제 안내 페이지

[그림 2-20]과 같이 가짜 백신은 'AVLab Internet Security'라는 이름으로 실행되었다. 다른 사례를 보면 'AVC Plus XP Antivirus 2015', 'AVC Plus' 등의 이름으로 실행되는 것이 확인된다.

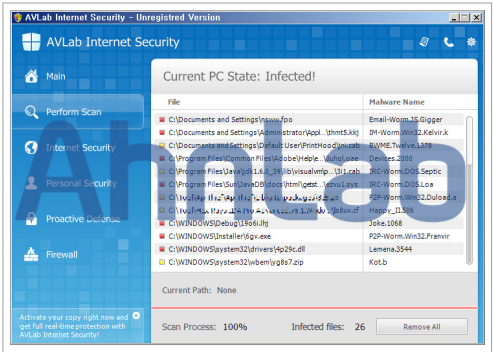


그림 2-20 | 가짜 백신 실행 화면

이러한 가짜 백신(허위 백신)은 낯설지 않지만 한동안 국내에서 피해 사례가 거의 발견되지 않다가 최근 피해 사례가 다시 발견됨에 따라 이에 대한 정보를 파악하고 피해 예방을 위한 노력이 필요하다.

스팸 메일을 통한 악성코드 유포는 여전히 계속되고 있다. 스팸 메일에 첨부(또는 링크)되는 파일, 혹은 첨부된 파일을 통해 추가로 다운로드되는 파일에 따라 감염되는 악성코드의 형태는 달라질 수 있다. 최근에는 소위 APT(Advanced Persistent Threat, 지능형 지속 위협) 공격의 수단으로 자주 이용되고 있다.

이러한 형태의 악성코드 유포는 이미 익숙한 형태이다. 이를 인지하고 출처가 불분명하거나 확인되지 않은 내용의 메일이나 조금이라도 의심스러운 메일에 대해서는 주의가 필요하다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

JS/Downloader (2014.12.18.00)

HTML/Cryptic (2014.12.18.00)

Trojan/Win32.Necurs (2014.12.18.00)

Trojan/Win32.Agent (2014.12.18.00)

Trojan/Win32.XPack (2014.12.17.01)

Trojan/Win32.MDA (2014.12.18.00)

3

악성코드 상세분석
ANALYSIS-IN-DEPTH

금융 정보 탈취형 악성코드의 보이지 않는 특징

금융 정보 탈취형 악성코드의 보이지 않는 특징

취약한 웹사이트를 통해 감염되는 파밍 악성코드의 행위 분석

취약한 웹사이트를 통한 악성코드 유포는 오래 전부터 발견되었지만, 현재에도 유포가 활발하게 진행되고 있다. 이 글에서 소개하는 침해 사이트를 통해 유포되는 악성코드는 정상적인 웹사이트에 악성 스크립트를 삽입하는 방식을 이용하기 때문에 일반 사용자는 인식하기 어렵다.

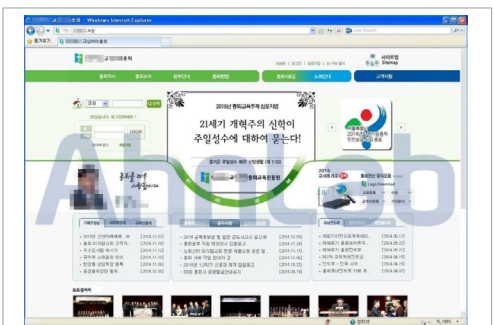


그림 3-1 | 침해 사이트

지금부터 사용자가 사이트에 접속했을 때 악성코드가 어떻게 감염되는지 그 과정을 살펴보자. 우선 사용자가 침해 사이트 페이지에 접근하면 악성 스크립트가 삽입된 사이트로 리다이렉트(redirect)되어 악성코드가 다운로드 및 실행된다.

표 3-1 | 침해 사이트에서 접근하는 사이트 목록

URL
http://ju**u.com
http://www.pensio******.com
http://www.******nsoo.co.kr

이 때 침해 사이트의 악성코드 유포 경유지를 살펴보면 [그림 3-2]와 같다.

그림 3-2 | 악성코드 유포 경유지

침해 사이트에는 공격자가 삽입한 스크립트가 존재하고 있으며 난독화되어 있다.

표 3-2 | 침해 사이트에서 로드하는 파일에 삽입된 스크립트 일부

복호화된 스크립트
"<iframe src=http://ju***.com/S**r/i**ex.h**l width=0 height=0></iframe>"

위의 [그림 3-2]의 침해 사이트 중 가장 마지막에 접근하는 사이트로부터 최종적으로 'v3c.exe' 파일이 다운로드된다. [그림 3-2]와 같이 다운로드된 파일은 파밍 악성코드로, 실행되면 DNS(도메인 네임 시스템)를 변조하거나 악성코드 자신이 DNS 역할을 한다. 해당 악성코드의 상세 행위를 살펴보면 [그림 3-3]과 같다.

그림 3-3 | 다운로드된 악성코드

악성코드가 실행되면 [표 3-3]과 같이 파일을 추가로 생성한다.

표 3-3 | 생성된 파일

파일 생성 정보
C:₩inst.exe
C:₩Documents and Settings₩Administrator₩Local Settings₩Temporary Internet Files₩Content.IE5₩0B290PAN₩cgi_personal_card[1]
C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩f91d6992fc2a47e9f9cb3ef9d27bf73f.zip

이 가운데 inst.exe 파일은 [표 3-4]와 같이 레지스트리에 등록한다.

표 3-4 | 레지스트리 등록

Key	Value
HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run₩syotom	"C:₩inst.exe"
HKLM₩SYSTEM₩ControlSet001₩Services₩SharedAccess₩Parameters₩FirewallPolicy₩StandardProfile₩AuthorizedApplications₩List₩C:₩inst.exe	"C:₩inst.exe:*:Enabled:Sevsl"
HKCU₩Software₩Microsoft₩Internet Explorer₩Main₩Start Page	"www.naver.com"

[그림 3-4]와 같이 악성코드는 시작프로그램에 inst.exe를 등록하여 윈도 시작 시마다 자동 실행시킨다. 또한 윈도 방화벽에 예외로 등록하여 방화벽을 우회한다. 추가로, 인터넷 익스플로러의 시작페이지를 수정하여 사용자가 인터넷을 사용할 경우 파밍 사이트로 자동 연결하도록 유도한다.

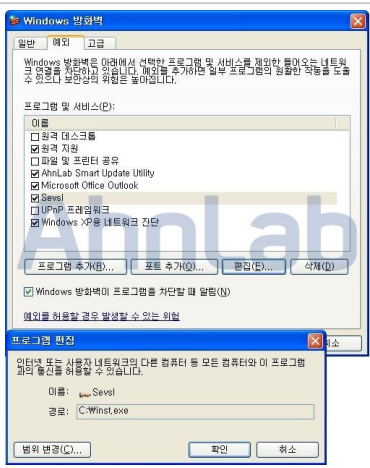


그림 3-4 | 윈도 방화벽에 예외 처리된 악성코드

그림 3-5 | IE 시작페이지 변경 전(상)/ 후(하)

이 악성코드가 추가 생성하는 cgi_personal_card 파일은 특정 사이트로 접근하며, 파밍에서 사용될 서버의 IP를 확인하는데 사용된다. [표 3-5]는 cgi_personal_card 파일의 내용이다.

표 3-5 | cgi_personal_card 파일 내용

```
_Callback(
{"uin":305***6108,
"qzone":0,
"intimacyScore":0,
"nickname":"***.178.**.**6",
"realname":"",
"smartname":"",
"friendship":0,
"isFriend":0,
"bitmap":"08009c8002000101",
"avatarUrl":"http://q***o1.st**e.qq.com/**one/30***46108/305***6108/100"});
```

악성코드에 감염되면 계속해서 특정 사이트로 접근하여 cgi_personal_card 파일을 생성한다. 이렇게 공격자의 IP를 가져온 후 악성코드는 사용자 PC에서 공인인증서를 탈취하고 PC의 정보를 전송한다.

표 3-6 | PC에 저장되는 공인인증서 위치

운영체제	NPKI 폴더 경로
Windows XP	C:₩Program Files₩NPKI
Win7 이상	C:₩Users₩[사용자계정]₩AppData₩LocalLow₩NPKI

위의 [표 3-6]의 경로에 NPKI 폴더가 있을 경우, [표 3-7]의 위치로 복사하고 Temp 폴더에 zip 파일을 생성하여 [그림 3-6]과 같이 공격자의 서버로 전송한다.

표 3-7 | 복사된 공인인증서 위치

운영체제	NPKI 폴더의 복사된 경로
Windows XP	C:₩Documents and Settings₩Administrator₩Local Settings₩Temp₩Hs_₩Pf₩NPKI
Win7 이상	C:₩Users₩[사용자계정]₩AppData₩Local₩Temp₩Hs_₩Appdata₩NPKI

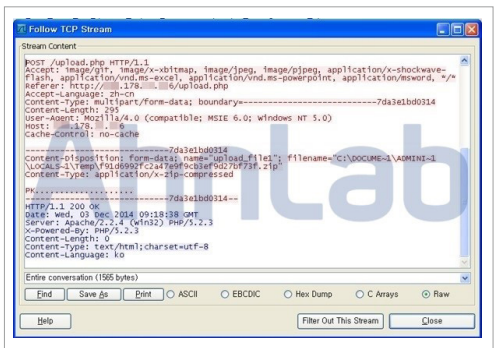


그림 3-6 | 압축된 공인인증서 전송

표 3-8 | 맥 주소(MAC Address) 정보를 가져오는 함수

```
Function MACAddress()
Dim mc,mo
    Set mc=GetObject("Winmgmts:").InstancesOf("Win32_NetworkAdapterConfiguration")
  For Each mo In mc
     If mo.IPEnabled=True Then
        MACAddress= mo.MacAddress
        Exit For
     End If
  Next
End Function
```

또한 [표 3-8]과 같이 함수를 통해 맥 주소의 정보를 가져와 공격자의 서버로 전송한다.

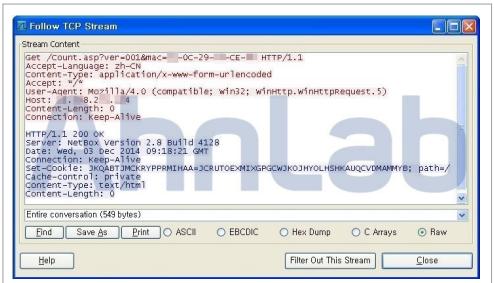


그림 3-7 | 맥 주소 정보 전송

이 경우 맥 주소를 전송하는 IP로 접속하면 [그림 3-8]과 같이 비밀번호(P/W)를 입력하는 창이 나타난다. [그림 3-7]의 Count.asp에서 확인할 수 있듯이 감염된 사용자의 카운팅 및 정보 수집 페이지로 추정된다.

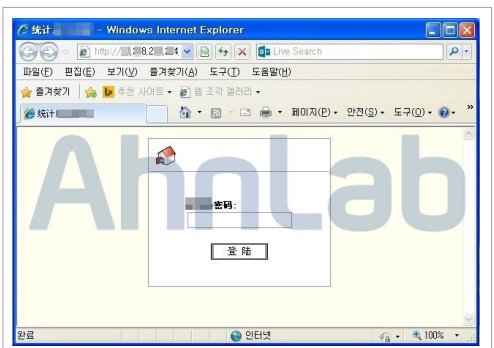


그림 3-8 | 맥 주소를 전송하는 페이지

또한 이 악성코드는 PC의 DNS를 [그림 3-9]와 같이 127.0.0.1 / 8.8.8.8로 변조한다.

그림 3-9 | 맥 정보 및 DNS 정보/ DNS 변경 전(상)과 후(하)

[그림 3-9]에서 이 악성코드가 DNS를 변조하는 이유는 호스트(hosts) 파일을 변조하여 파밍 사이트로 연결하는 것이 아닌, 로컬호스트(127.0.0.1)로 루프백(loopback)을 하여 악성코드가 IP를 변조한 후 공격자가 제작한 파밍 사이트로 접속하도록 하기 위해서이다.

또한 이 악성코드는 변조에 사용할 URL 목록을 암호화된 상태로 가지고 있다. 여기에서 보조 DNS가 8.8.8.8로 설정되는 이유는 악성코드가 DNS 역할을 하지만, 파밍이 목적이기 때문에 그에 해당하는 URL만 가지고 있다. 그 외 다른 사이트는 정상적으로 사용하도록 하기 위해 구글의 DNS인 8.8.8.8로 설정하는 것이다.

이 악성코드에 의해 파밍에 사용되는 URL은 [표 3-9]와 같다.

표 3-9 | 파밍에 사용되는 URL

k****r.com	***p.i**.co.**
www.k****r.com	***ank.i**.co.**
nk.k*r.com	***nh**.com
*mo**y.k****r.com	www.***nh**.com
H**ab***.com	***king.***nh**.com
www.h**ab***.com	***bank.***nh**.com
open.h**ab***.com	***ghy**.com
k**c.co.**	www.***ghy**.com
www.k**c.co.**	***king.***ghy**.com
s.kco.**	**z.***ghy**.com
k**.co.**	**te.c**
www.k**.co.**	***er.c**
***nk.k**.co.**	www.***er.c**
***ine.k**.co.**	**um.n**
***n.k**.co.**	www.**um.n**
rib.com	***ma**.n**
www.***rib***.com	www.***ma**.n**
u.***rib***.com	**sa.k****r.com
b.*rib***.com	**sa.***ghu**.com
stb.**.kr	**sa.***nh**.com
www.***stb***.**.kr	**sa.***rib***.com
k.co.	**sa.**k.co.**
www.**k.co.**	**sa.***stb***.**.kr

이렇게 악성코드에 감염된 PC의 사용자가 인터넷 익스플로러를 실행하면 [그림 3-10]과 같이 파밍 사이트로 연결된다.

그림 3-10 | 파밍 사이트

사용자는 정상 사이트에 접속하더라도 해당 사이트가 침해 사고를 당했다면 악성코드에 감염될 가능성이 있다.

취약한 웹사이트를 통한 악성코드 유포 과정

2014년에는 리그(Rig), 스위트 오렌지(Sweet Orange), 뉴클리어(Nuclear) 등 다양한 웹 익스플로잇 킷(Exploit Kit)이 등장하면서, 취약한 웹사이트를 악용한 악성코드 유포가 급증하였다. 특히 지금까지 파밍 악성코드 유포에 주로 사용되었던 '공다 익스플로잇 킷 & 카이홍 익스플로잇 킷(Gongda Exploit Kit & Caihong Exploit Kit)' 형태에서 최근에는 '카이홍 익스플로잇 킷 & 갓모드(Caihong Exploit Kit & God Mode)'로 유포 형태가 변화되어 시선이 집중되고 있다.

갓모드 취약점을 이용한 악성코드 유포는 2014년 11월에 등장하였으며, 이후 12월에 '카이홍 & 갓모드'를 이용한 파밍 악성코드 유포가 급증하고 있어 일반 사용자들의 주의가 필요한 시점이다.

최근에 파밍 악성코드 유포로 탐지된 종교 관련 웹사이트의 URL Tree는 [표 3-10]과 같다.

표 3-10 | 웹사이트 URL Tree

순서	URL
Root	http://on***.com
1	http://on***.com/Create***** - 해당 사이트 하위 페이지에서 공통적으로 사용되는 스크립트 파일 <script type="te AhnLab pt" src="http://images.on****.com/Comm****_js/YUtil.js">

1 - 1	http://images.on***.com/Com***_js/YUtil.js - 다른 경로의 YUtil.js로 이동
1 - 2	http://crm.born*******.com/ad/s/YUtil.js - 정상코드가 작성되어 있으나 최하단에 iframe 삽입 : hg.gif
2	http://www.is****lplus.com/xml/hg.gif - iframe 삽입 : han.html
3	http://www.is*********.com/xml/han.html - iframe 삽입 : index.html / count[감염수] 체크
4	http://sol***ul.com/upload/ta**/b/index.html - **Caihong** /ww.html (CVE-2011-2140에 해당될 경우)

→ 난독화된 index.html 복호화 후 (아래)

- 사용된 취약점:
CVE-2013-0422, CVE-2012-4681, CVE-2011-3544, CVE-2013-0634, CVE-2011-2140

4 - PE	http://www.oi**s.co.kr/***a/log/log.exe - PC내 취약점 존재할 경우 파밍 악성코드 감염
5	http://sol***ul.com/upload/ta**/b/main.html - **God Mode**
5 - PE	http://www.oi**s.co.kr/***a/log/log.exe - PC내 취약점 존재할 경우 파밍 악성코드 감염

[그림 3-11]과 같이 갓모드 공격에 해당하는 main.html의 중반부에는 카이홍(Caihong)으로 난독화되어 있으며, 하단에는 VB스크립트 코드가 존재한다. VB스크립트는 난독화된 코드를 복호화하고 취약점 CVE-2014-6332를 악용하여 최종 명령을 실행한다.

그림 3-11 | main.html 중 카이홍으로 난독화된 부분

그림 3-12 | 1차 복호화된 카이홍 코드 중 일부

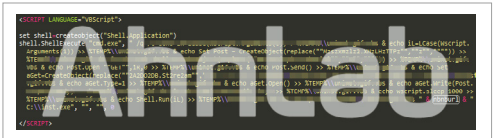


그림 3-13 | 최종 복호화된 실행 코드

갓모드 공격의 CVE-2014-6332(윈도 OLE 자동화 배열 원격 코드 실행 취약점)는 윈도와 인터넷 익스플로러를 사용하는 대부분의 환경(윈도 95이상, IE 3~11)에서 동작할 수 있어 그 영향도가 매우 크다.

갓모드 공격은 IE가 VB스크립트 엔진을 포함하는 점을 악용하는 것으로, 공격자는 VB스크립트를 통해 시스템 명령을 실행할 수 있는 권한을 획득하여 VB스크립트를 실행, 사용자 PC에 악성코드를 감염시킨다.

해당 악성코드의 상세한 동작 정보는 위에서 먼저 살펴본 침해 사이트의 악성코드 행위와 유사하다.

그림 3-14 | 악성코드 감염 후 포털 접속 및 배너 클릭 시 나타나는 화면

CVE-2014-6332 취약점에 대한 패치는 2014년 11월에 제공되었으나, 최신 보안 업데이트를 진행하지 않은 경우에는 갓모드 기법을 통해 누구나 쉽게 악성코드에 감염될 수 있어 매우 치명적이다.

인터넷은 정보의 바다이기도 하지만, 그만큼 악성코드 또한 많이 배포되고 있어 사용자들은 주의를 기울여 사용할 필요가 있다.

이러한 파밍 악성코드 감염을 예방하기 위해서는 보안업데이트를 꼼꼼히 확인하고, 설치한 백신 제품의 엔진을 최신 버전으로 유지하는 사용자의 올바른 습관이 선행되어야 한다.

갓모드 공격과 안랩 MDS에서의 DICA 진단 방식의 자세한 내용은 안랩 홈페이지 보안 이슈에서 확인할 수 있다.

http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=1&menu_dist=2&seq=23225&dir_group_dist=0

V3 제품군에서는 관련 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Banker (2014.12.18.00)

HTML/Cryptic (2014.12.18.00)

Trojan/Win32.StartPage (2014.12.03.02)

4

연간 위협 동향

ANNUAL REPORT

2014년 보안 위협 동향

2014년 보안 위협, 영역과 경계를 파괴하다

2015년 보안 위협 전망

2015년 보안 위협 키워드, '다변화·고도화·타깃화'

2014 보안 위협, 영역과 경계를 파괴하다

연초 대규모 개인정보 유출부터 연말 공공기관 해킹까지 2014년은 사회 전반에 걸쳐 '정보 보안(보호)'이 핫이슈가 된 해였다. 특히 개인정보 유출 사건 • 사고는 거의 매달 발생했다고 해도 과언이 아닐 정도로, 안전행정부 발표 자료에 따르면 2014년 상반기에만 5,300만 명의 개인정보 8,600만 여건이 유출된 것으로 추정된다. 그야말로 '보안 위협'이 개인과 기업을 넘나들며 사회적 • 국가적 피해를 야기하고 있다.

2014년의 주요 보안 이슈는 ▲스마트폰 보안 위협 ▲인터넷 뱅킹을 노린 파밍 악성코드 ▲공격 경로의 다양화 ▲POS(Point-of-Sales) 시스템 해킹 ▲ 다수의 오픈소스 취약점 등장 등으로 요약할 수 있다. 스마트폰, POS 시스템, 오픈소스 등의 키워드에서 볼 수 있는 것처럼 지난 한해 보안 위협은 다양한 플랫폼(platform)으로 확대되었다.

1. 스마트폰으로 확대되는 보안 위협

지금까지 주로 PC 환경에서 자주 등장했던 보안 위협이 2014년에는 스마트폰 환경으로 옮겨가는 한편 본격적으로 모바일 환경에 특화된 보안 위협이 대거 등장했다.

우선 '랜섬웨어(Ransomeware)'가 PC에 이어 스마트폰으로 확산됐다. 사용자의 데이터를 볼모로 금전을 요구하는 랜섬웨어는 지난 한해 동안 PC와 스마트폰 등 플랫폼을 가리지 않고 꾸준히 발견됐다. 해외에서는 FBI를 사칭한 조직이 스마트폰 사용자들을 노리고 유포한 랜섬웨어인 '심플로커(SimpleLocker)'로 실질적인 피해가 발생하기도 했다.

PC를 노리던 이른바 '몸캠피싱'도 스마트폰으로 확대되기도 했다. 몸캠피싱이란 화상채팅 등을 통해 음란 행위를 하는 것을 뜻하는 '몸캠'과 사용자를 허위 사이트 또는 프로그램으로 유도하는, 즉 낚는 것을 뜻하는 '피싱'의 합성어다. 스마트폰 상에서의 몸캠피싱 기법은, 공격자가 스마트폰 채팅 애플리케이션을 이용해 음란 화상 채팅을 유도하여 사용자의 얼굴과 알몸 등을 동영상으로 녹화하는 한편 악성 앱 설치를 유도해 스마트폰 내 주소록을 탈취하는 방식이다. 이후 공격자는 수집한 주소록에 있는 사용자의 지인에게 몸캠 동영상을 전송한다고 협박하며 금전을 요구한다.

'스미싱(Smishing)'이라는 스마트폰에 특화된 보안 위협이 사회 전반의 화두로 떠올랐다. 문자메시지

(SMS)와 피싱(Phishing)의 합성어인 스미싱은 악성코드의 유형과 문구 측면에서 더욱 진화했다. 기존에는 소액결제를 노렸으나 최근에는 인터넷 뱅킹에 필요한 금융 정보를 노리는 악성코드를 사용하는 등 더 큰 금전적 피해를 야기하고 있다. 사용자를 현혹하는 스미싱 문구 또한 '택배', '청첩장/돌잔치/생일 초대장', '예비군/민방위' 등을 사칭하는 사례가 지속적으로 발견되는 가운데 층간 소음, 분리수거 위반, 쓰레기 무단투기 등 실생활에서 쉽게 경험할 수 있는 민원을 사칭한 이른바 '생활 밀착형' 스미싱이 등장했다.

이처럼 스마트폰을 노리는 보안 위협이 심화되는 가운데 주요 정보를 스마트폰에 저장하는 빈도가 높아지는 만큼 각별한 주의가 필요하며, 특히 출처가 불분명한 스마트폰 앱을 다운로드할 시에는 더욱 유의해야 한다.

2. 인터넷 뱅킹을 노린 파밍 악성코드, '메모리 해킹'까지

2013년 이후 인터넷 뱅킹 정보를 노리는 '파밍(Pharming)' 악성코드의 피해가 이어졌고 2014년에는 더욱 심화되는 양상을 보였다.

기존 파밍 악성코드는 PC의 호스트 파일을 변조해 가짜 인터넷 뱅킹 사이트로 유도하는 방식이었다. 2014년에는 인터넷 도메인네임시스템(DNS) 정보를 담고 있는 메모리를 변조해 사용자가 가짜 사이트로 이동하는 것을 더욱 인지하기 어렵게 하는 방식이 등장했다. 또한 정상 사이트에 방문했어도 이체거래 과정에서 금융거래정보 등을 실시간 변조하기 위해 인터넷 뱅킹 모듈의 메모리 영역을 해킹하는 형태까지 진화했다. 인터넷 뱅킹의 메모리 해킹이란 컴퓨터의 메모리에 있는 수취인의 계좌번호, 송금액을 변조하거나 보안카드 비밀번호를 탈취한 후 돈을 빼돌리는 새로운 해킹 방식이다. 정상적인 인터넷 뱅킹 사이트에 접속하더라도 이체거래 과정에서 금융거래 정보 등을 실시간 위 • 변조하는 것이 특징이다.

이처럼 인터넷 뱅킹을 노리는 공격 기법이 갈수록 사용자가 인지하기 어렵게 진화하고 있어 사용자 및 기관의 주의가 요구된다.

3. 공격 경로의 다양화

기존의 취약점 공격은 악용하는 프로그램이 한정적이었다. 그러나 공격 대상이 확대됨에 따라, 특히 특정 타깃을 노리는 맞춤형 공격이 자행되면서 공격에 사용되는 프로그램, 즉 공격 경로도 다양화되고 있다.

2014년은 이메일, 전자결재, DRM(Digital Rights Management, 디지털콘텐츠 저작권 보호 기술), 그룹웨어, 암호화 솔루션 등 다양한 프로그램의 취약점을 이용해 악성코드 제작이 증가함과 동시에 이들 프로그램을 공격 경로로 이용하는 복합적인 형태의 공격이 빈번하게 포착됐다. 대표적으로 문서 프로그램의 취약점을 이용한 MBR 파괴 악성코드를 이메일의 첨부 파일 형태로 전송한 사례가 있었다. 또는 특정 프로그램의 구동과 관련된 정상 파일을 악성 파일로 교체해 악성코드를 배포하는 사례도 발견됐다. 많은 기업들이 보안에 노력을 기울이고 있음에도 불구하고 이러한 고도화된 형태의 공격으로 악성코드

에 감염된 프로그램이 고객에게 피해를 줄 수 있어 더욱 주의가 필요하다.

4. POS(Point-of-Sales) 시스템 해킹

국내외를 막론하고 지난 2014년에는 POS 단말기를 해킹해 중요 거래정보를 빼내고, 이 정보로 부당거래를 일으킨 피해가 빈번히 발생했다.

해외의 경우, 2013년 말 미국 내 대형 유통사의 POS 시스템이 해킹 당해 7천만 명 이상의 개인정보가 유출된 사건을 시작으로 2014년에는 세계 곳곳에서 백화점 • 식당 등의 POS 시스템이 해킹 당해 신용카드 정보가 유출된 사례가 지속적으로 보고됐다. 국내에서도 POS 시스템 공급 업체의 서버를 해킹해 정상 파일을 악성 파일로 교체하는 방식을 이용한 공격 사례가 발견되기도 했다.

사실 보안 전문가들은 수년 전부터 POS 시스템 보안에 대한 우려를 제기해왔다. 최근 가시적인 피해가 발생함에 따라 관련 업계 및 기업들의 POS 시스템 보안 방안 마련이 시급해지고 있다.

5. 다수의 오픈소스 취약점 등장

지금까지는 MS 오피스, 어도비, 오라클 등 다수의 개인과 기관이 사용하고 있는 프로그램들에서 취약점이 발견되는 경우가 대부분이었다. 그러나 2014년에는 특정 조직이나 시스템에서 사용하는 오픈소스 프로그램과 관련된 심각한 취약점이 발견돼 전 세계적으로 큰 충격을 주었다. '하트블리드(Heartbleed)'와 '쉘쇼크(ShellShock)' 등이 그것이다. '하트블리드'는 전 세계 웹사이트에서 대다수가 사용하는 오픈SSL(Open Secure Socket Layer)에서 발견된 취약점으로, 웹 서비스 및 모바일 비즈니스에 잠재적인 위협이 되고 있다.

이른바 '쉘쇼크'로 불리는 배쉬(Bash) 취약점은 대부분의 서버 OS로 사용되는 유닉스 및 리눅스와 관련된 취약점으로, 이를 통해 공격자가 원하는 코드를 손쉽게 실행할 수 있어 심각한 위협으로 대두되었다. 프로그램 자체의 취약점뿐만 아니라 리눅스 계열 시스템에서 동작하는 웜까지 등장하면서 보안 위협의 범위가 오픈소스 프로그램까지 크게 확장되었다.

2015년 보안 위협 키워드, '다변화·고도화·타깃화'

최근 영역과 경계를 허물기 시작한 보안 위협은 2015년에 더욱 다변화되고 고도화될 것으로 보인다. 또한 2014년 연말의 국내외 주요 해킹 사례와 같은 타깃 공격이 더욱 거세질 것으로 전망된다. 다변화 • 고도화 • 타깃화의 키워드를 중심으로 예측 가능한 2015년 보안 위협은 ▲모바일 결제 및 인터넷 뱅킹 공격 심화 ▲공격 대상별 맞춤형 악성코드 유포와 동작 방식의 진화 ▲POS 시스템 보안 위협 본격화 ▲오픈소스 취약점 공격 및 타깃 공격을 통한 정보 유출 가속화 ▲IoT 보안 위협 등이다.

1. 모바일 결제 및 인터넷 뱅킹 공격 심화

모바일 금융 서비스가 단순 '모바일 뱅킹'에서 '모바일 결제시장'으로 그 영역과 규모가 크게 확장되고 있다. LG경제연구원에 따르면 매년 30~40%씩 성장해 2017년 800조 원에 가까운 금액이 모바일 기기를 통해 결제될 것으로 전망된다. 또한 글로벌 시장조사기관 가트너는 2016년 모바일 거래액이 6,169억 달러, 이용자 수는 4억 4,793만 명, 거래 건수로는 209억 건에 달할 것으로 추정했다.

모바일 결제가 확대됨에 따라 이를 노리는 보안 위협 또한 증가하리라는 것은 명약관화다. 2012년 소액 결제 서비스 관련 모바일 악성코드가 발견된 이후 모바일 뱅킹을 노리는 악성코드는 지속적으로 발견되고 있다. 향후 모바일 결제와 관련해 각종 피해를 유발하는 알려지지 않은 악성코드가 대량 등장할 것으로 예상되는 만큼 관련 서비스 제공 업체와 사용자의 각별한 주의가 요구된다.

한편 2015년에도 다양한 웹 익스플로잇 툴킷(Web Exploit Toolkit)을 이용한 '뱅킹 악성코드' 유포가 급증할 것으로 보인다. 웹 익스플로잇 툴킷은 다수의 취약점을 악용해 사용자 PC에 악성코드를 감염시키는 공격 코드를 만드는데 쓰인다. 메모리해킹 및 파밍뿐만 아니라 각 은행의 거래 시스템에 최적화된 악성코드가 등장할 가능성이 있으며 은행권 이외에도 카드사, 증권사 등 금융권 전반에 걸쳐 유사한 피해 사례가 등장할 것으로 예상된다.

2. 공격 대상별 맞춤형 악성코드 유포와 동작 방식의 진화

올해는 타깃형 악성코드의 증가와 함께 악성코드의 유포 및 동작 방식 또한 더욱 진화할 것으로 예측된다. 예를 들어 연말이나 연초 등 특정한 시기에 이메일 제목뿐만 아니라 첨부 문서 자체의 내용 또한 송년회 초대 또는 새해 인사 등의 내용으로 보이도록 교묘

하게 제작하여 사용자의 의심을 따돌리는 것 등이다. 또한 최근에는 시스템에서 오랫동안 은닉하는 악성코드가 주로 등장했다면 앞으로는 은닉한 상태에서 머무는 것이 아니라 수시로 은밀히 변형을 업데이트하여 보안 제품의 탐지를 효과적으로 피하는 등 동작 방식 또한 점차 진화하는 양상을 보일 전망이다.

이 밖에도 불특정 다수를 대상으로 유포되는 악성코드들이 양적으로도 뚜렷하게 증가하는 추세를 보이고 있다. 블랙마켓에서 판매되는 악성코드 자동 생성기나 익스플로잇 킷 등이 이러한 추세를 더욱 가속화할 것으로 보인다.

3. POS 시스템 보안 위협 본격화

최근 POS 시스템(Point Of Sales System) 해킹이 지속적으로 발생하면서 업체들이 보안을 강화하고 있지만 이를 뛰어넘는 다양한 방식의 공격이 등장할 것으로 예상된다. POS 시스템 제작 업체를 노리는 해킹 시도 또한 증가할 것으로 보인다.

국내외에서 POS 시스템 해킹이 증가함에 따라 보안 기능이 강화된 신용카드 결제 방식으로 전환을 서두르고 있다. 그러나 시스템과 신용카드를 모두 교체하기까지는 수년의 시간과 막대한 비용이 소요될 것으로 예상돼 당분간 POS 시스템에 대한 보안 위협은 지속될 것으로 보인다.

4. 오픈소스 취약점 공격 및 타깃 공격을 통한 정보 유출 가속화

오픈소스 프로그램들의 새로운 취약점이 등장할 것으로 예상된다. 2014년에 연이어 확인된 주요 오픈소스 프로그램의 취약점들은 예상되는 피해 범위가 심각해 하트블리드(Heartbleed), 쉘쇼크(ShellShock)로 표현되기도 했다. 오픈소스의 특성상 지속적인 개선이 가능해 상대적으로 안전한 것으로 알려졌던 프로그램에서 새로운 취약점이 잇따라 발생함에 따라 기업과 관련 업계의 대응 방안이 요구된다.

한편 지능형 지속 위협 APT(Advanced Persistent Threat)와 같은 타깃 공격이 꾸준히 증가할 것으로 보인다. 공격 대상 또한 다양한 산업군 및 국가기관으로 확대되고 기업기밀, 금융정보, 군사안보 정보 등을 목표로 하는 타깃 공격이 심화될 전망이다. 유출된 정보를 범죄에 악용하는 사례 또한 더욱 증가할 것으로 예측된다. 아울러 최근 정치, 사회적으로 국가 간 이해관계가 첨예하게 대립됨에 따라 사이버 전을 통한 정보 유출 시도는 더욱 격화될 전망이다.

5. IoT 보안 위협의 증가

사물인터넷 IoT(Internet of Things) 기술의 개발 및 발전으로 IoT 시장이 지속적으로 성장하면서 이와 관련된 보안 위협이 등장할 것으로 예상된다.

지금까지 사물인터넷에 대한 주요 이슈는 관련 기술 개발과 IoT 플랫폼 표준화 작업이었으나 향후 사물인터넷 기술의 표준화와 함께 관련 시장이 급격히 확대될 것으로 보인다. 우리 주변의 모든 사물이 인터넷을 통해 정보를 주고받고 연결되어 있다는 것은 이 모든 사물이 사이버 범죄자들의 공격 대상이 될 수 있다는 것을 의미한다. IoT 기기는 종류와 성능 또한 다양해 기존의 보안 기능을 적용하기 어렵다. 또한 대부분 무선 네트워크를 통한 통신이 이루어지기 때문에 무선 공유기 등 무선 네트워크 보안 위협이 증가할 것으로 보인다.

AhnLab

ASEC REPORT

VOL.60
December, 2014

집필 안랩 시큐리티대응센터 (ASEC)
편집 안랩 콘텐츠기획팀
디자인 안랩 UX디자인팀

발행처 주식회사 안랩
경기도 성남시 분당구 판교역로 220
T. 031-722-8000
F. 031-722-8901