# ASEC REPORT

VOL.29 | 2012.06

안랩 월간 보안 보고서

이 달의 보안 동향

모바일 악성코드 이슈

Disclosure to or reproduction
for others without the specific
written authorization of AhnLab
is prohibited.

Copyright (c) AhnLab, Inc.
All rights reserved.

AhnLab

**AhnLab Security Emergency response Center**

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.

## CONTENTS

# 1. 2012년 5월의 보안 동향

## 01. 악성코드 동향

### a. 악성코드 통계

#### 5월 악성코드 최다 20건

ASEC이 집계한 바에 따르면, 2012년 5월에 감염이 보고된 악성코드는 전체 1258만 9409건인 것으로 나타났다. 이는 지난 달의 1140만 9362건에 비해 118만 47건이 증가한 수치다([그림 1-1]). 이 중에서 가장 많이 보고된 악성코드는 Mov/Cve-2011-2140이었다. Trojan/Win32.Gen과 Trojan/Win32.adh이 그 다음으로 많이 보고됐으며, 최다 20건에 새로 포함된 악성코드는 총 7건 이었다([표 1-1]).


[그림 1-1] 월별 악성코드 감염 보고 건수 변화 추이



| 순위 | 등락 | 악성코드명 | 건수 | 비율 |
|---|---|---|---|---|
| 1 | NEW | Mov/Cve-2011-2140 | 1,651,649 | 27.1% |
| 2 | ▲1 | Trojan/Win32.Gen | 509,527 | 8.4% |
| 3 | ▼2 | Trojan/Win32.adh | 449,944 | 7.4% |
| 4 | ▲16 | ASD.PREVENTION | 365,613 | 6.0 |
| 5 | ▲1 | Trojan/Win32.bho | 355,377 | 5.8 |
| 6 | ▼1 | Textimage/Autorun | 341,125 | 5.6 |
| 7 | ▲2 | JS/Agent | 340,611 | 5.6% |
| 8 | — | Adware/Win32.korad | 288,587 | 4.7% |
| 9 | ▼5 | Malware/Win32.generic | 263,765 | 4.3% |
| 10 | NEW | Trojan/Win32.sasfis | 220,051 | 3.6% |
| 11 | NEW | Spyware/Win32.keylogger | 193,888 | 3.2% |
| 12 | NEW | Malware/Win32.suspicious | 160,370 | 2.6% |
| 13 | NEW | Adware/Win32.winagir | 157,828 | 2.6% |
| 14 | ▼3 | Als/Bursted | 138,792 | 2.3% |
| 15 | NEW | JS/Exploit | 135,294 | 2.2% |
| 16 | ▼14 | Mov/Cve-2012-0754 | 120,058 | 2.0% |
| 17 | ▼10 | Trojan/Win32.agent | 109,168 | 1.9% |
| 18 | ▼6 | Downloader/Win32.agent | 108,127 | 1.8% |
| 19 | ▼4 | Trojan/Win32.genome | 91,743 | 1.5% |
| 20 | NEW | RIPPER | 87,147 | 1.4% |
| | | | 6,088,664 | 100.0% |

[표 1-1] 2012년 5월 악성코드 최다 20건(감염 보고, 악성코드명 기준)

## 악성코드 대표진단명 감염보고 최다 20

[표 1-2]는 악성코드의 주요 동향을 파악하기 위하여 악성코드별 변종을 종합한 악성코드 대표진단명 최다 20건이다. 2012년 5월에는 Trojan/Win32가 총 225만 2906건으로 최다 20건 중 25.2%의 비율로 가장 빈번히 보고된 것으로 조사됐다. Mov/Cve-2011-21400이 165만 1649건, Adware/Win32가 76만 5660건으로 그 뒤를 이었다.

| 순위 | 등락 | 악성코드명 | 건수 | 비율 |
|---|---|---|---|---|
| 1 | — | Trojan/Win32 | 2,252,906 | 25.2% |
| 2 | NEW | Mov/Cve-2011-2140 | 1,651,649 | 18.5% |
| 3 | ▼1 | Adware/Win32 | 765,660 | 8.6% |
| 4 | ▼1 | Malware/Win32 | 458,425 | 5.1% |
| 5 | ▼1 | Win-Trojan/Agent | 380,512 | 4.3% |
| 6 | ▼1 | Downloader/Win32 | 370,945 | 4.2% |
| 7 | NEW | ASD | 365,613 | 4.1% |
| 8 | ▲7 | JS/Agent | 343,434 | 3.8% |
| 9 | — | Textimage/Autorun | 341,191 | 3.8% |
| 10 | ▲1 | Win-Adware/Korad | 263,556 | 3.0% |
| 11 | ▼4 | Win-Trojan/Downloader | 258,062 | 2.9% |
| 12 | ▼4 | Win-Trojan/Onlinegamehack | 233,060 | 2.6% |
| 13 | NEW | Spyware/Win32 | 218,524 | 2.4% |
| 14 | ▼1 | Win32/Conficker | 165,496 | 1.9% |
| 15 | NEW | Dropper/Win32 | 159,248 | 1.8% |
| 16 | ▲1 | Win-Trojan/Korad | 152,612 | 1.7% |
| 17 | ▼3 | Win32/Virut | 149,947 | 1.7% |
| 18 | ▲1 | Als/Bursted | 138,792 | 1.6% |
| 19 | NEW | JS/Exploit | 135,294 | 1.5% |
| 20 | ▼2 | Win32/Kido | 128,545 | 1.3% |
| | | | 8,933,471 | 100.0% |

[표 1-2] 악성코드 대표진단명 최다 20건



## 5월 신종 악성코드

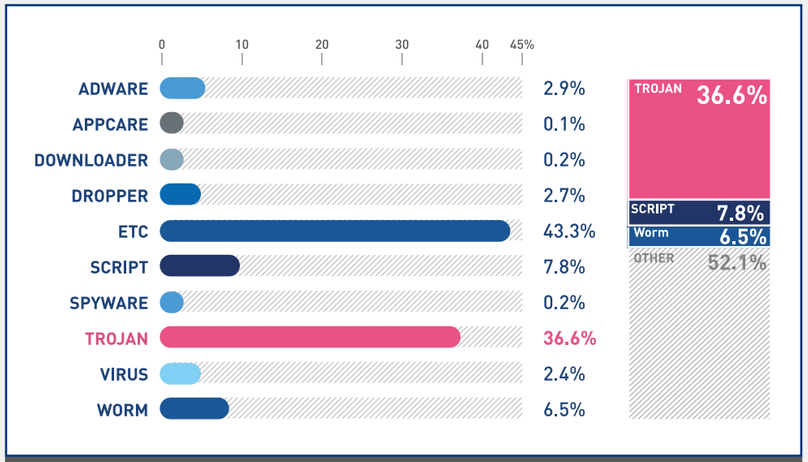
[표 1-3]은 5월에 신규로 접수된 악성코드 중 고객으로부터 감염이 보고된 최다 20건이다. 5월의 신종 악성코드는 Win-Trojan/Korad.311296이 5만 4464건으로 전체의 18.8%였으며, Win-Trojan/Downloader.303104.W가 1만 9554건으로 그 다음으로 많이 보고됐다.

| 순위 | 악성코드명 | 건수 | 비율 |
|---|---|---|---|
| 1 | Win-Trojan/Korad.311296 | 54,464 | 18.8% |
| 2 | Win-Trojan/Downloader.303104.W | 19,554 | 6.7% |
| 3 | Win-Trojan/Downloader.307200.V | 18,860 | 6.5% |
| 4 | Win-Adware/KorAd.405504 | 18,727 | 6.5% |
| 5 | Win-Trojan/Korad.309760 | 18,534 | 6.4% |
| 6 | Win-Trojan/Agent.274432.NE | 17,259 | 5.9% |
| 7 | Win-Adware/KorAd.307200.D | 14,574 | 5.0% |
| 8 | Win-Trojan/Korad.2120416 | 14,202 | 4.9% |
| 9 | Win-Trojan/Killav.35456 | 13,593 | 4.7% |
| 10 | Win-Adware/KorAd.303104.D | 12,781 | 4.4% |
| 11 | Win-Adware/KorAd.307200.B | 11,049 | 3.8% |
| 12 | Win-Trojan/Zegost.52736 | 10,478 | 3.6% |
| 13 | Win-Adware/KorAd.311296.D | 9,441 | 3.3% |
| 14 | Win-Adware/KorAd.138208 | 8,741 | 3.0% |
| 15 | Win-Trojan/Dload.229376 | 8,336 | 2.9% |
| 16 | Win-Adware/KorAd.303104.C | 8,267 | 2.8% |
| 17 | JS/Obfus | 8,249 | 2.8% |
| 18 | Win-Trojan/Downloader.297056 | 8,010 | 2.8% |
| 19 | Win-Adware/KorAd.303104.B | 7,614 | 2.6% |
| 20 | Win-Adware/BHO.KorAd.622592 | 7,445 | 2.6% |
| | | 290,178 | 100.0% |

[표 1-3] 5월 신종 악성코드 최다 20건

## 5월 악성코드 유형별 감염 보고

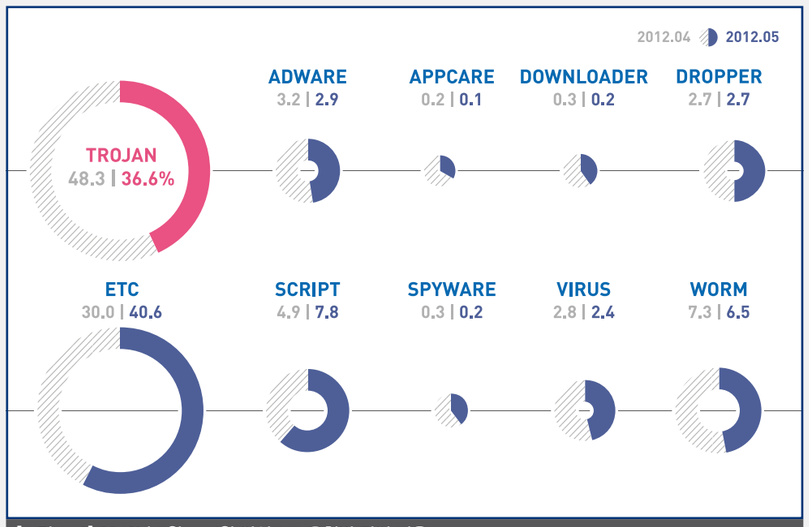
[그림 1-2]는 2012년 5월 한 달 동안 안랩 고객으로부터 감염이 보고된 악성코드의 유형별 비율을 집계한 결과다. 2012년 5월의 악성코드를 유형별로 살펴보면, 트로이목마(Trojan)가 36.6%, 스크립트(Script)가 7.8%, 웜(worm)이 6.5%인 것으로 나타났다.




[그림 1-2] 2012년 5월 악성코드 유형별 감염 비율

## 악성코드 유형별 감염보고 전월 비교

[그림 1-3]은 악성코드 유형별 감염 비율을 전월과 비교한 것이다. 스크립트가 전월에 비해 증가세를 보이고 있는 반면, 트로이목마, 웜, 애드웨어(Adware), 바이러스(Virus), 다운로더(Downloader), 스파이웨어(Spyware), 애프케어(Appcare) 계열들은 감소한 것을 볼 수 있다. 드롭퍼(Dropper) 계열은 전월 수준을 유지하였다.

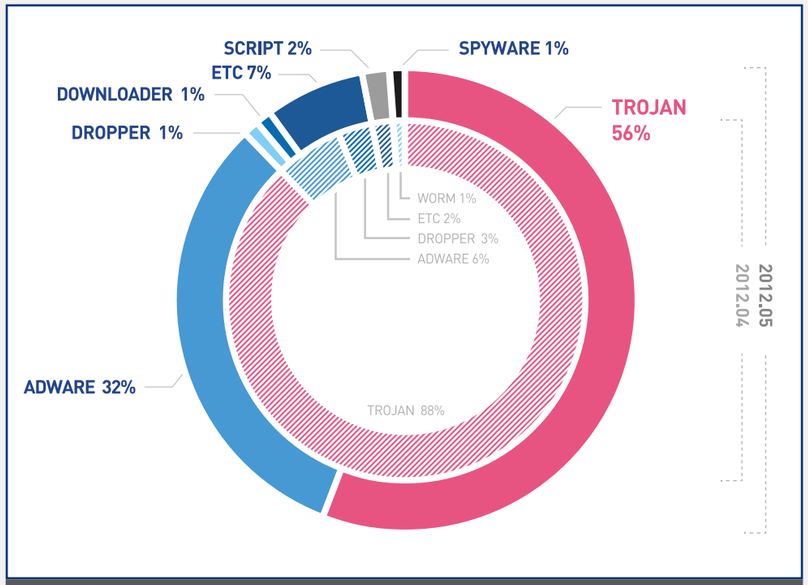



[그림 1-3] 2012년 5월 vs 4월 악성코드 유형별 감염 비율



## 신종 악성코드 유형별 분포

5월의 신종 악성코드를 유형별로 보면 트로이목마가 56%로 가장 많았고, 애드웨어가 32%, 스크립트가 2%였다.




[그림 1-4] 신종 악성코드 유형별 분포

# 01. 악성코드 동향
## b. 악성코드 이슈

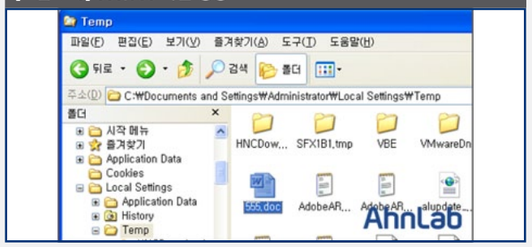
### 이력서로 위장한 악성코드

특정인의 이력서로 위장한 악성코드가 발견되었다. 이 악성코드는 MS 워드 아이콘을 사용하였지만 사실은 윈도우 실행 파일이다.

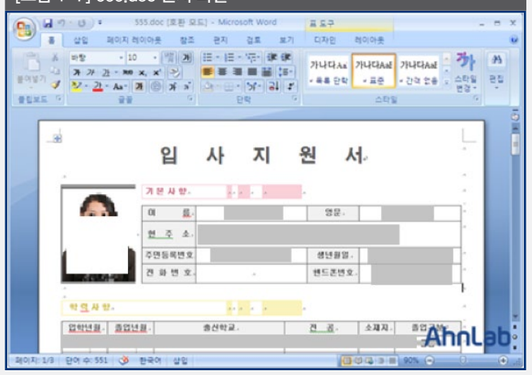
[그림 1-5] OOO이력서 악성코드


A. 해당 파일이 실행되면 정상적인 문서 파일이 열린 것처럼 555.doc 문서 파일이 로딩되며, 이때 악성코드가 함께 설치된다. [그림 1-7]은 악성코드 실행 후 로딩되는 문서 파일이다.

[그림 1-6] 555.doc 파일 생성

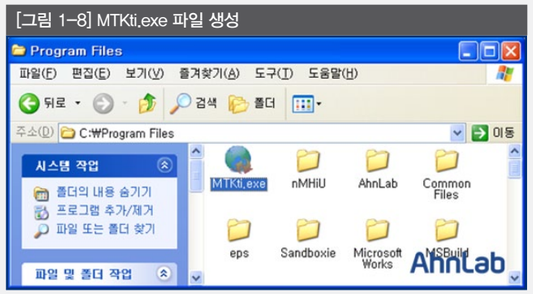



[그림 1-7] 555.doc 문서 파일

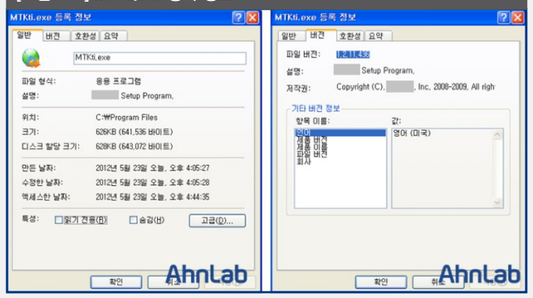



B. 문서 파일이 로딩될 때 백그라운드로 MTKti.exe 파일이 생성된다. MTKti.exe 파일은 정상 파일로 위장하기 위해 [그림 1-9]와 같이 허위로 작성된 V3 Lite 프로그램 등록 정보를 가지고 있다. 또한, 레지스트리에 등록되어 윈도우 시작 시 자동으로 실행된다.

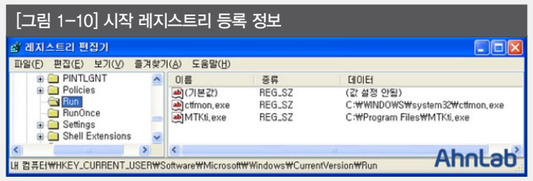
[그림 1-8] MTKti.exe 파일 생성




[그림 1-9] MTKti.exe 등록 정보



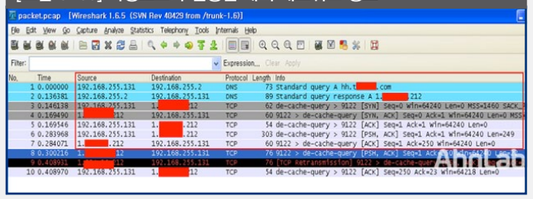

[그림 1-10] 시작 레지스트리 등록 정보




C. 악성코드가 실행되면 [그림 1-11]과 같이 'hh.toXX33.com(1.XXX.XX.212)' 서버에 접근을 시도한다.

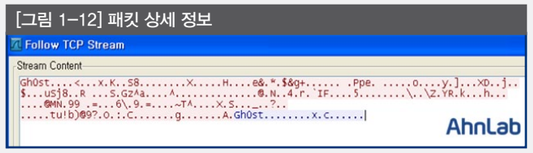


[그림 1-11] 악성코드가 실행될 때의 네트워크 정보

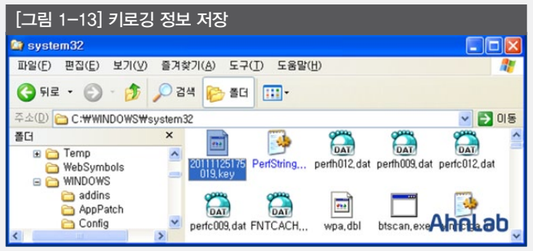



C&C 서버로 전송되는 271byte 패킷에서 Gh0st 문자열을 확인할 수가 있었다. 이것은 감염 시스템에서 키보드 입력 정보, 파일 업로드, 원격 제어 등의 기능을 수행하는 Ghost RAT 계열 악성코드로 추정된다. [그림 1-13]은 키로깅 정보가 저장된 파일이다.

[그림 1-12] 패킷 상세 정보




[그림 1-13] 키로깅 정보 저장



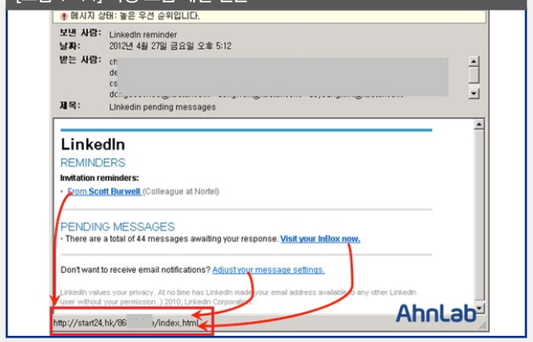

〈V3 제품군의 진단명〉

– Win-Trojan/Agent.1462272.R(2011.12.03.00)
– Win-Trojan/Agent.641536.F(2011.12.03.00)

### LinkedIn 스팸 메일을 위장한 악성코드 유포

LinkedIn 관련 메일로 위장하여 불특정 다수의 사람들에게 악성코드를 유포한 스팸 메일이 발견되었다.

[그림 1-14] 악성 스팸 메일 원문




[그림 1-14]는 미국의 business-related social networking site 업체인 LinkedIn(www.linkedin.com)으로 위장한 메일이다. LinkedIn에서 보내는 '대기중인 메시지가 있다'는 정상적인 알림 메시지로 꾸며 본문에 있는 링크를 클릭하도록 유도한다.

링크를 통해 연결되는 주소는 [그림 1-14]의 하단 URL과 같으며 정상적인 사이트 주소가 아닌 것을 확인할 수 있다. 해당 링크를 클릭하면 악성 스크립트가 포함된 사이트로 연결되어 악성코드에 감염된다. 현재 해당 링크 및 접속 IP가 유효하지는 않으나, 이와 유사한 형태로 사용자의 PC를 감염시키기 위한 시도는 계속될 것으로 예상되므로 사용자들의 주의가 요구된다.

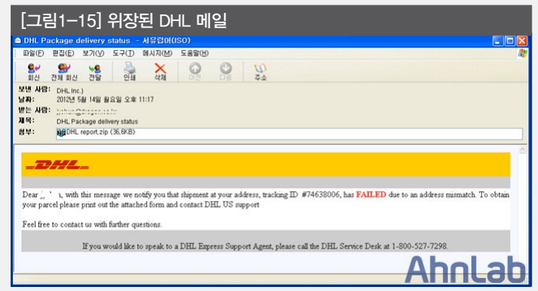
〈V3 제품군의 진단명〉

– Trojan/Win32.Zbot(2012.05.01.00)
– Trojan/Win32.Jorik

### DHL운송 메일로 위장한 악성코드

DHL 운송 메일로 위장한 스팸 메일을 이용하여 허위 백신 프로그램의 설치를 유도하는 악성코드가 지속적으로 유포되고 있다. 메일 본문에는 수신자에게 주소 불일치로 배송이 실패되었다는 내용과 함께, 첨부된 양식을 이용해서 DHL에 문의하라는 내용이 포함되어 있다.

[그림1-15] 위장된 DHL 메일




이 메일에 첨부된 DHL report.zip 압축 파일에 포함된 DHL report.exe 파일을 실행하면 자기 복제본을 랜덤한 이름으로 생성하고, 윈도우 방화벽을 우회하기 위해 해당 파일을 예외 프로그램으로 등록한다.

[ 파일 생성 ]

C:₩Documents and Settings₩All Users₩Local Settings₩Temp₩mswyyaa.com

또한, 시스템 시작 시 자동 실행되도록 레지스트리에 등록한 후 아래 URL에 접속을 시도한다.

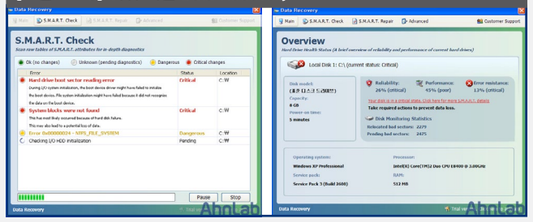
– 'http://www.update.microsoft.com'
– 'http://fro***oro.***/and/image.php'
– 'http://fok***ol.***/and/image.php'

– 'http://uaw***uro2012.***/and/image.php'
– 'http://lis***ujik.***/and/image.php'

'http://www.update.microsoft.com' 도메인은 악성코드 감염 후 네트워크 연결 상태를 확인하기 위해 접속하는 정상 URL이다. 허위 백신 프로그램이 다운로드되는 것으로 추정되는 URL로는 접속되지 않았다. 하지만 해당 악성코드에 감염된 시스템에서 수집한 파일을 실행하면 Data Recovery라는 허위 백신이 설치된다.

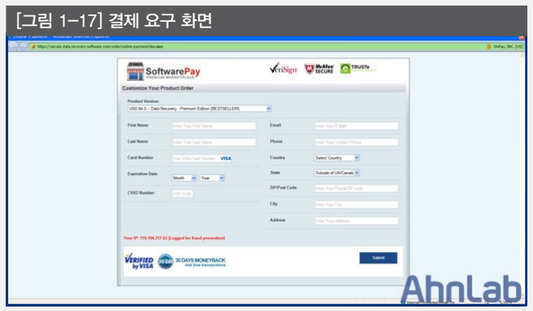
Data Recovery 프로그램이 실행되면 자동으로 시스템을 검사하고 허위 진단 내역을 보여준다.

[그림 1-16] 허위 백신 Data Recovery




결과 창에서 '치료'를 클릭하면 라이선스 등록을 위한 결제를 요구한다.

[그림 1-17] 결제 요구 화면




이 허위 백신에 감염되면 윈도우 시작 메뉴의 프로그램이나 바탕 화면에 등록된 바로 가기 파일을 삭제하거나 디스크 드라이브에 저장된 폴더 및 파일을 숨김 속성으로 변경하여, 사용자는 중요한 파일이 삭제된 것으로 오해할 수 있다. 또한, 시스템 설정(파일 실행 방해, 작업 관리자 및 다양한 시스템 유틸리티 실행 방해, 인터넷 옵션 변경 방해, 윈도우 방화벽 비활성화 등)을 변경하여 시스템 사용에 불편을 준다.

〈V3 제품군의 진단명〉
– Win-Trojan/Jorik.49664.K(2012.05.16.00)
– Win-Trojan/Fakeav.278016.DJ(2012.05.16.00)

## ws2help.dll 파일을 패치하는 온라인게임핵 변종 악성코드

imm32.dll 파일이 아닌 ws2help.dll 파일을 패치하는 변종 온라인게임핵이 발견되었다.

[그림 1-18] 정상 ws2help.dll

```
719D1658: 7526          JNZ 719D1680
719D165A: E842000000    CALL 719D16A1
719D165F: 8B4508        MOV EAX,
```

[그림 1-18]은 정상 ws2help.dll 파일의 함수 호출 코드 부분으로, 악성코드에 감염되어 패치된 [그림 1-19]의 ws2help.dl과 비교해보면 함수 호출 주소가 변경된 것을 알 수 있다.

[그림 1-19] 패치된 ws2help.dll

```
719D1658: 7526          JNZ 719D1680
719D165A: E8D2360000    CALL 719D4D31
719D165F: 8B4508        MOV EAX,
```

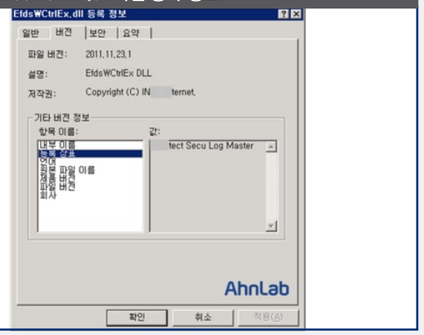
[그림 1-19]의 변경된 주소에는 [그림 1-20]의 코드가 삽입되어 있으며, 특정 모듈(DLL)명이 명시되어 있다.

[그림 1-20] 특정 섹션에 삽입된 코드

```
719D4D20  77 73 32 68 65 6C 70 2E  70 64 62 00 00 00 00 00  ws2help.pdb.....
719D4D30  26 60 02 C0 B8 00 00 00  00 E8 10 00 00 00 BF 77  &`.............w
719D4D40  1D 80 7C 83 C8 E0 FF D7  61 E9 53 C9 FF FF 0F 00  ..|.....a.S.....
719D4D50  C0 59 E8 E7 FF FF FF 45  66 64 73 57 43 74 72 6C  .Y.....EfdsWCtrl
719D4D60  45 78 2E 64 6C 6C 00 00  00 00 00 00 00 00 00 00  Ex.dll..........
```

코드상에서 확인되는 EfdsWCtrlEx.dll 파일이 악의적인 기능을 수행하는 온라인게임핵 악성코드이며, [그림 1-21]과 같이 특정 보안 제품의 파일인 것처럼 조작된 등록 정보를 가지고 있다.

[그림 1-21] EfdsWCtrlEx.dll 파일 등록 정보




〈V3 제품군의 진단명〉
– Win-Trojan/Patcher.107008(2012.05.06.00)
– Win-Trojan/Onlinegamehack.3146107(2012.05.06.00)
– Win-Trojan/Patched.19968.S(2012.05.06.00)
– Trojan/Win32.OnlineGameHack



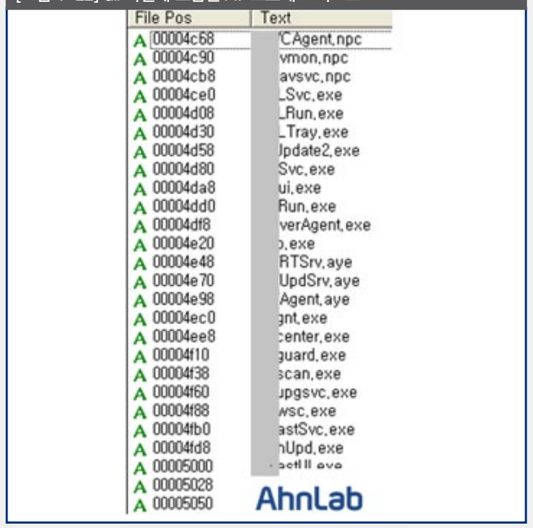
## AV Kill 기능을 가진 온라인게임핵 악성코드

윈도우 시스템 파일을 패치하는 악성 파일 이외에도 AV Kill 기능을 가진 다수의 파일을 생성하는 온라인게임핵 악성코드가 발견되었다. 다음은 드롭퍼에 의해 생성되는 파일 정보다.

– C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩A1.zip(ws2help.dll 백업 파일)
– C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩B1.zip(wshtcpip.dll 백업 파일)
– C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩Ceenieiyw.dll
– C:₩DOCUME~1₩ADMINI~1₩LOCALS~1₩Temp₩XHtd.dll
– C:₩WINDOWS₩system32₩wshtcpDQ.dll(wshtcpip.dll 정상 파일)
– C:₩WINDOWS₩system32₩wshtcpip.dll(악성 파일)

위의 윈도우 정상 파일을 패치하는 악성 파일 이외에도, %temp% 폴더 내에 다수의 dll 파일을 생성한다.

[그림 1-22] dll 파일에 포함된 AV 프로세스 리스트




해당 dll 파일은 AV Kill 기능과 특정 온라인 게임들의 사용자 계정을 탈취하는 기능이 있다. 이 dll 파일들은 5월 21일 이후 업데이트된 'v3_gamehackkill' 전용 백신에서 진단 및 치료가 가능하다.

〈V3 제품군의 진단명〉
– Trojan/Win32.Magania(2012.05.21.00)
– Trojan/Win32.OnlineGameHack(2012.05.21.00)

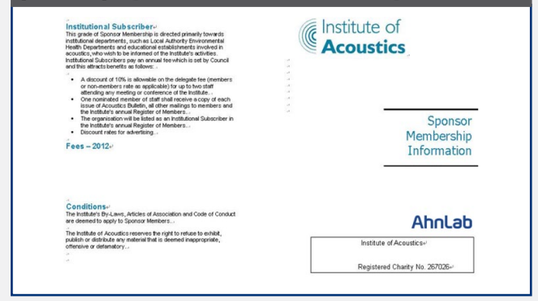
## 플래시 플레이어의 제로데이 취약점(CVE-2012-0779)을 이용하는 악성코드

어도비 플래시 플레이어의 제로데이 취약점(CVE-2012-0779)을 이용한 악성코드가 유포되었다. 어도비사는 악성코드 유포에 사용되는 보안 취약점에 대한 긴급 패치(Adobe Flash Player 11.2.202.235)를 배포하였다.

최근에 알려진 공격 형태는 DOC 문서 내에 보안에 취약한 SWF 파일이 특정 URL을 호출하고, 해당 사이트에 접속하는 과정에서 실행 파일 형태의 악성코드를 감염시키는 방식이다. 이와 유사한 형태의 공격이 지속적으로 보고되고 있으며 메일에 첨부된 DOC 문서 파일을 실행하도록 유도한다.

첨부 파일을 실행하면 [그림 1-23]과 같이 사용자를 속이기 위해 별도의 문서 파일을 보여준다.

[그림 1-23] 사용자를 속이기 위해 보여주는 문서 내용



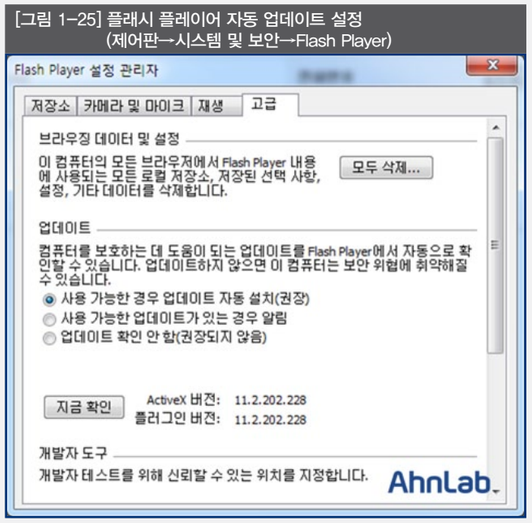

DOC 파일 내부에는 [그림 1-24]와 같이 특정 URL 정보가 들어있으며, 파일 실행 및 공격이 성공적으로 이루어지면 해당 사이트에 접속해 추가 악성코드를 다운로드하여 실행한다.

[그림 1-24] 플래시 취약점이 있는 URL 접속


설치된 악성코드는 부팅 시 자동으로 실행되기 위해 서비스에 자신을 등록하고, C&C 서버로 감염 정보를 전송한 후 공격자의 명령을 기다린다.

최근의 악성코드 유포 형태를 보면 OS 자체에 대한 공격보다는 서드파티 제품의 취약점을 이용하는 경우가 많으며, 어도비 플래시 플레이어는 악성코드 유포에 흔히 이용되고 있다. 이러한 제품은 보안 취약점이 자주 발견되고 업데이트 또한 빈번하게 이루어지므로, 업데이트가 자동 설치되도록 [그림 1-25]와 같이 설정할 것을 권장한다.

[그림 1-25] 플래시 플레이어 자동 업데이트 설정 (제어판→시스템 및 보안→Flash Player)

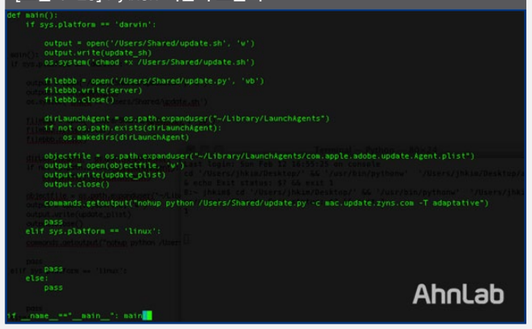



〈어도비 플래시 플레이어 최신 보안 패치 다운로드〉
– http://get.adobe.com/kr/flashplayer/

## Python으로 제작된 맥 악성코드

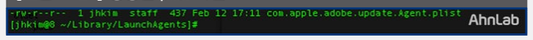
맥 OS X에 기본 설치되어 있는 Python 기반의 악성코드가 발견되었다. [그림 1-26]과 같이 Python으로 작성된 악성코드는 자바 취약점(CVE-2012-0507)을 이용하며, 맥 OS X 시스템이 맞는지 검사한 후에 설정된 경로에 파일들을 생성 및 실행한다.

[그림 1-26] Python 기반의 드롭퍼

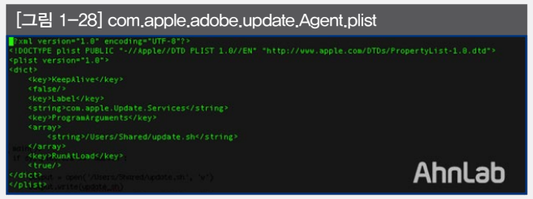



A. 시스템 시작 시 자동으로 실행하기 위해 [user]/Library/LaunchAgents/ 경로에 'com.apple.adobe.update.Agent.plist' 파일을 생성한다. 이 plist 파일은 update.sh 파일을 실행한다.

[그림 1-27] 생성된 plist 파일

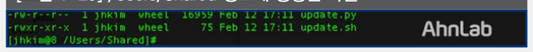



[그림 1-28] com.apple.adobe.update.Agent.plist

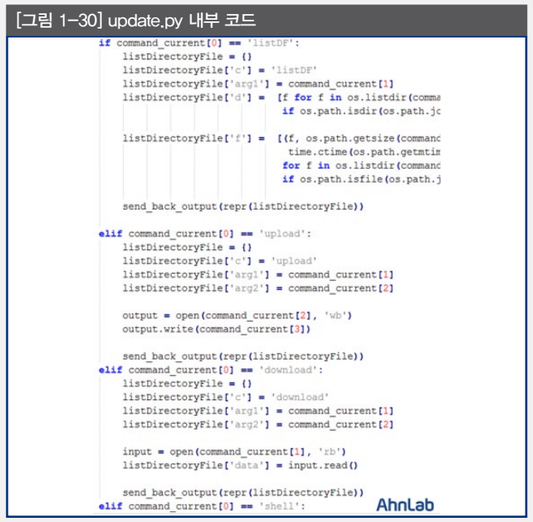



B. /Users/Shared/ 경로에 update.sh와 update.py 파일을 생성하는데, update.sh 파일에 의해 update.py 파일이 실행된다. 이 파일들은 백도어로 동작하며 파일을 유출하거나 공격자의 명령을 실행하는 등의 악성 행위를 수행한다.

[그림 1-29] /Users/Shared 경로에 생성된 파일




[그림 1-30] update.py 내부 코드




최근에 발견된 맥 악성코드들은 대부분 자바 취약점을 이용하고 있다. 따라서 사용하고 있는 맥 시스템의 자바를 최신 버전으로 유지할 것을 권장한다.

## 프로그램 설치 화면 놓치지 마세요

컴퓨터를 사용하다 보면 설치한 기억이 없는 툴바 프로그램이 설치되어 있거나, 인터넷 시작 페이지가 바뀌고, 바탕 화면에 쇼핑몰 아이콘이 생성되어 있는 것을 볼 수 있다. 그 이유가 무엇일까?



일반적으로 무료로 배포되는 프로그램의 경우 프로그램 내에 광고를 삽입해 제작 비용을 충당한다. 또는 특정 기업에서 제작 비용을 지원받는 대신, 해당 기업의 프로그램이 추가 설치될 수 있도록 해주기도 한다.

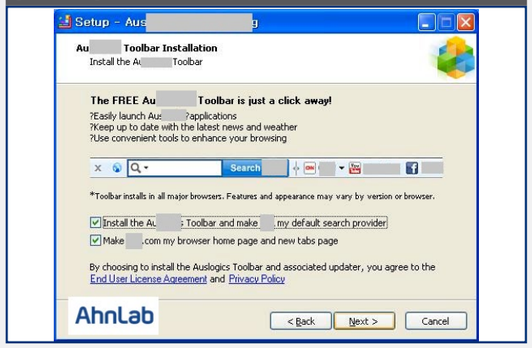
이러한 추가 프로그램들은 설치 과정 중에 사용자의 동의를 얻어야 한다. 하지만 대다수의 사용자들이 설치 동의 항목을 자세히 읽어보지도 않은 채 '다음' 버튼을 클릭한다. 무료 프로그램의 설치 과정만 꼼꼼히 살펴봐도 추가 프로그램의 설치를 사전에 예방할 수 있다.

몇 가지 프로그램을 통해 사례를 살펴보도록 한다.

### 1. 디스크 조각 모음 프로그램 Aus****** DiskDefrag

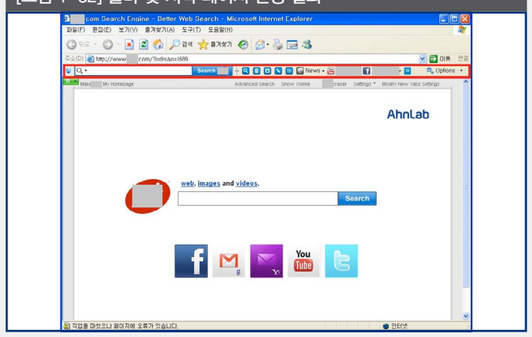
이 프로그램은 무료로 배포되는 디스크 조각 모음 프로그램으로, 설치 과정을 꼼꼼히 살펴보면 [그림 1-31]과 같은 화면을 볼 수 있다.

[그림 1-31] 프로그램 설치 과정 중 나타난 툴바 프로그램 설치 동의 화면




자세히 읽어보면 2개의 체크박스를 볼 수 있는데, 하나는 툴바 프로그램 설치의 동의 여부이고, 두 번째는 인터넷 시작 페이지의 변경 여부를 묻는 것이다. 해당 내용을 읽어보지 않고 'Next' 버튼을 누르면 [그림 1-32]와 같이 툴바 프로그램이 설치되고 인터넷 시작 페이지가 변경된다. 이때, 체크박스를 해제하면 해당 툴바는 설치되지 않고, 시작 페이지도 변경되지 않는다.

[그림 1-32] 툴바 및 시작 페이지 변경 결과




### 2. P2P 파일 공유 프로그램 u****ent

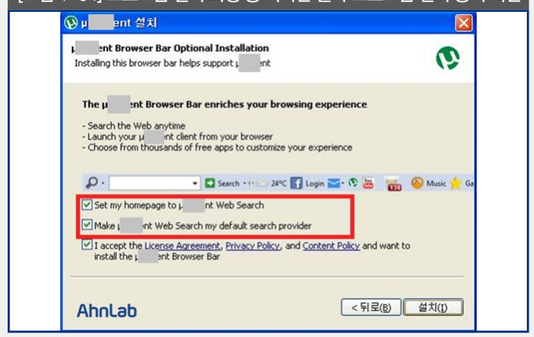
이 프로그램은 파일 공유를 위해 사용되는 P2P 프로그램 중에서 가장 광범위하게 사용되고 있다. 프로그램을 설치한 후 시드(Seed) 파일을 실행시켜 파일 공유 네트워크에 참가하는 방식으로 동작한다.

해당 프로그램은 설치 중 무료 음악 파일 다운로드 프로그램을 설치하도록 유도하는 화면을 보여준다. 이때, 설치 동의 항목을 체크 해제하지 않으면 설치가 끝난 후 해당 파일을 다운로드한다.

[그림 1-33] 설치 종료 후 무료 MP3 파일 다운로드 여부 결정

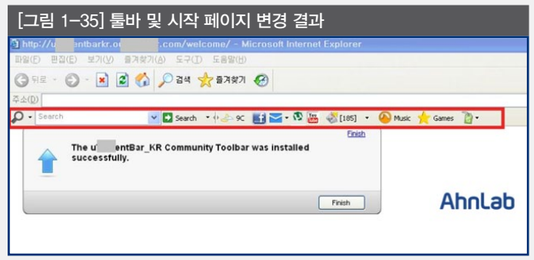

또한 사례 1과 같이 툴바 프로그램과 시작 페이지를 변경하는 메뉴가 나온다.

[그림 1-34] 프로그램 설치 과정 중 나타난 툴바 프로그램 설치 동의 화면




해당 부분을 체크 해제하지 않고 설치를 끝마치면 툴바 프로그램이 설치되고 시작 페이지도 변경된다.

[그림 1-35] 툴바 및 시작 페이지 변경 결과



이렇듯 유명한 무료 프로그램을 통해서 합법적으로 광고 프로그램들이 설치될 수 있다. 이러한 광고 프로그램들의 설치를 막기 위해서는 설치 과정 중 추가 프로그램 설치에 동의하지 않는 꼼꼼함이 필요하다.

### 어린이날에도 쉬지 않는 악성코드 제작자

국내에서 발견되는 악성코드의 상당수는 해킹된 웹 사이트를 통해서 주말에 집중적으로 유포된다. 때문에 악성코드에 대응해야 하는 보안 업체나 사이트 관리자들에게 주말은 악몽과 같다. 올해 어린이날에도 악성코드 제작자들은 평소와 같이 악성코드를 유포했다. 특히 이중에는 DDoS 공격을 수행하는 악성코드도 있었으나 다행히 큰 피해는 보고되지 않았다.

#### 1. DDoS 악성코드는 주말을 겨냥했다.

해당 악성코드의 분석 결과, 타임 스탬프가 최근임을 확인하였다. 이로 볼 때 어린이날과 겹친 주말에 웹 사이트의 관리가 소홀할 수 있다는 점을 노린 것으로 추정된다(타임 스탬프란 파일이 제작된 시간 정보를 가진 필드를 의미하며, 임의 조작이 가능하다).

#### 2. 어떤 기능이 있는가?

이번에 발견된 DDoS 악성코드는 기존의 악성코드들과 같이 C&C 서버에 접속하여 감염된 PC의 정보를 전송하고, 공격 대상 리스트를 받아와 DDoS 공격을 수행하는 기능이 있다.

[표 1-4] 메인 Thread의 기능

| Thread | C&C | 기능 |
|---|---|---|
| Thread 1 | XXXgame.5166.info:8080 | 감염 PC의 정보 전송 (PC의 CPU, Memory, OS 버전, System Language) |
| Thread 2 | XXXXmax6.XXgo.net:8108 | |
| Thread 3 | img.XXX7888.com:7066 | 공격 리스트 다운로드, DDoS |

C&C 서버 주소와 전송되는 감염 PC의 정보는 아래 루틴으로 암호화되어 있다.

[그림 1-36] 감염 PC 정보를 암호화하는 루틴

```
100071E8  |> /8B4424 08     /mov    eax, dword ptr [esp+8]
100071EC  |. |8ACA           |mov    cl, dl
100071EE  |. |03C6           |add    eax, esi
100071F0  |. |3208           |xor    cl, byte ptr [eax]
100071F2  |. |02CA           |add    cl, dl
100071F4  |. |46             |inc    esi
100071F5  |. |3B7424 0C      |cmp    esi, dword ptr [esp+C]
100071F9  |. |8808           |mov    byte ptr [eax], cl
100071FB  |.^\7C EB          \jl     short 100071E8
```

[표 1-4]의 Thread 3은 C&C 서버에 접속하여 공격 대상 리스트를 다운로드하고 하위에 다수의 Thread를 생성하여 다양한 DDoS 공격을 수행한다. 이를 정리해 보면 [표 1-5]와 같다.

[표 1-5] 하위 Thread와 DDoS 공격 방법

| Thread | 공격 형태 |
|---|---|
| Thread 1 ~ 3 | SynF Flood |
| Thread 4 ~ 5 | ICMP Flood |
| Thread 6 | UDP Flood |
| Thread 7 | UDP Small Flood |
| Thread 8 | TCP Flood |
| Thread 9 ~ 10 | Multi TCP Flood |
| Thread 11 | DNS Flood |
| Thread 12 | Game2Flood |
| Thread 13 ~ 15 | HttpGetFlood |
| Thread 16 | CC Attack |

분석 당시에는 해당 C&C 서버로 접속되지 않아 어떤 데이터를 받아오는지 확인할 수 없었지만 Thread 12의 Game2Flood를 수행할 것으로 추정되며, 이는 아래와 같은 형태의 공격이다.

[그림 1-37] Game2Flood의 공격 형태

```
.text:10001AA3   push    offset aGame2flood ; "Game2Flood"
.text:10001AA8   call    OutputDebugStringA

.text:10001AF2   jnz     loc_10018E0
.text:10001AF8   push    0              ; protocol
.text:10001AFA   push    1              ; type
.text:10001AFC   push    2              ; af
.text:10001AFE   call    socket

.text:10001B79   push    offset Format  ; "#%d<<<<<3@C<<<<<%d "
.text:10001B7E   push    eax            ; Dest
.text:10001B7F   call    sprintf

.text:10001B98   push    0              ; flags
.text:10001B9A   dec     ecx
.text:10001B9B   lea     eax, [ebp+buf]
.text:10001BA1   push    ecx            ; len
.text:10001BA2   push    eax            ; buf
.text:10001BA3   push    ebx            ; s
.text:10001BA4   call    send

.text:10001BC4   inc     [ebp+arg_0]
.text:10001BC7   cmp     [ebp+arg_0], 1964h ; Game2Flood 시 세번개수
```

〈V3 제품군의 진단명〉

– Win32/Ircbot.worm.52736(V3, 2012.05.07.00)

### 안드로이드 Notcompatible 악성코드 발견

PC 악성코드와 동일한 형태로, 해킹된 웹 사이트를 통해 유포되는 Android-Trojan/Notcompatible 악성코드가 발견되었다. 안드로이드 악성코드를 유포하는 웹 사이트는 PC에서 접속하면 "not found" 에러가 발생하지만 모바일(안드로이드) 기기를 사용하여 접속하면 특정 페이지로 리다이렉트 되어 악성코드(Update.apk)가 다운로드 된다.

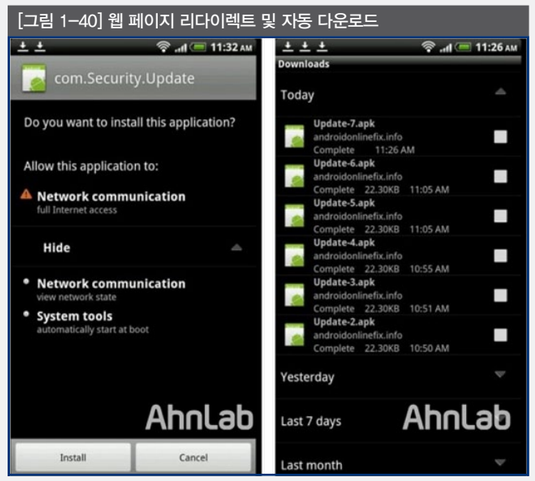
[그림 1-38]은 Notcompatible 악성코드를 유포하는 웹 사이트로, 웹 페이지 하단에 [그림 1-39]와같이 iframe 태그가 삽입되어 있다.

[그림 1-38] 안드로이드 악성코드 유포 사이트


[그림 1-39] 웹 페이지에 삽입된 악성 스크립트


해당 코드를 통해 특정 URL로 리다이렉트(hxxp://xxxroidonlinefix.info/fix1.php)되며, 이때 악성코드가 자동으로 다운로드된다. 이 악성 앱은 사용자가 수동으로 설치해야 하며 '알 수 없는 앱에 대해 설치' 항목을 허용하지 않으면 설치되지 않는다.

[그림 1-40] 웹 페이지 리다이렉트 및 자동 다운로드



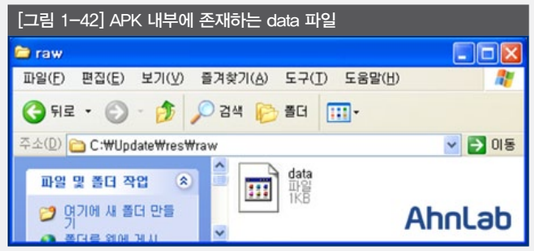

자동으로 다운로드된 Update.apk 파일이 설치되면 C&C 서버로 접근을 시도한다.

[그림 1-41] C&C서버 접근 시도

```
DNS     81 Standard query A notcompatibleapp.eu
DNS     97 Standard query response A 141.0.   .199
DNS     81 Standard query A notcompatibleapp.eu
DNS     97 Standard query response A 141.0.   .199
```

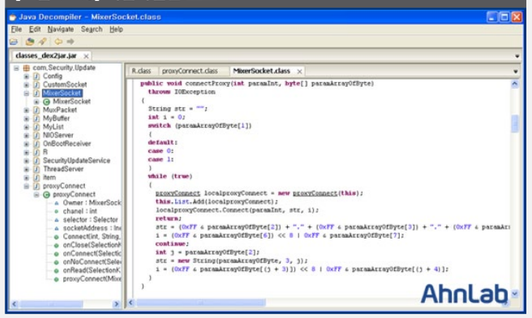
APK 파일 내부의 data 파일에 C&C 서버 정보가 암호화되어 저장되어 있다.

[그림 1-42] APK 내부에 존재하는 data 파일




악성코드에 감염된 단말기는 Proxy로 동작하며 연결된 C&C 서버를 통해 공격자의 명령을 수행할 것으로 추정된다.

[그림 1-43] 디컴파일된 코드



이 악성코드는 국내 특정 웹 사이트에서도 유포된 사례가 있다. [그림 1-44]는 국내 커뮤니티에 올라온 해당 악성코드와 관련된 글이다.

[그림 1-44] 국내 웹 사이트 악성코드 유포 발견


이번과 같이 해킹된 웹 사이트를 통해 안드로이드 악성코드가 계속해서 유포될 것으로 예상되므로 모바일 기기를 사용하여 웹 사이트를 방문하는 사용자들의 각별한 주의가 요구된다.

〈V3 제품군의 진단명〉
– Android-Trojan/Notcompatible

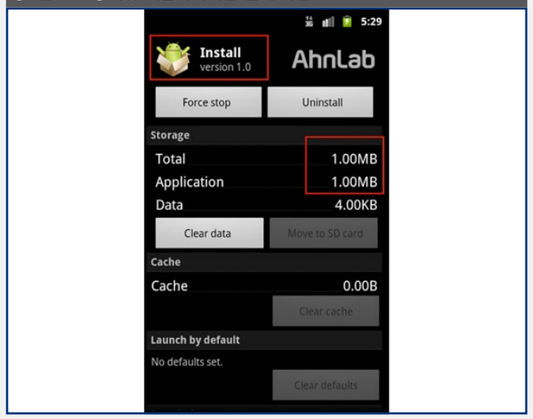
## 어도비 플래시 플레이어로 위장한 안드로이드 악성 앱

어도비에서 제공하는 안드로이드용 어도비 플래시 플레이어는 안드로이드에서 플래시(.swf)를 보기 위해 반드시 설치해야 하므로 사용자에게 꼭 필요한 앱 중 하나이다.
이러한 점을 이용한 가짜 플래시 플레이어가 러시아에서 발견되었다. 해당 악성 앱 제작자는 [그림 1-45]와 같이 플래시 플레이어의 모든 버전을 다운로드할 수 있다고 광고하며 악성 앱을 유포하고 있다.

[그림 1-45] 한국어로 번역된 악성 앱 유포 사이트

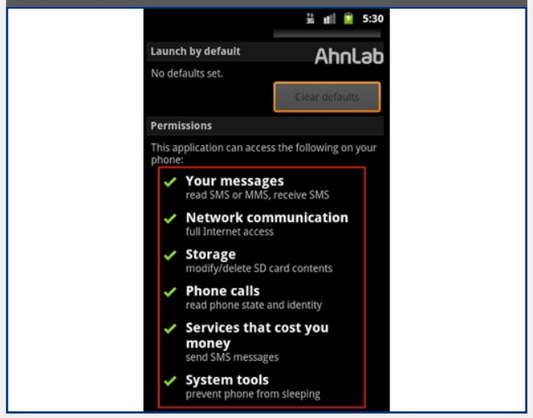

웹 페이지의 다운로드 링크를 클릭하면 악성 앱이 다운로드되고, 이를 설치하면 [그림 1-46]과 같이 'Install'이란 이름의 앱이 생성된다.

[그림 1-46] 악성 애플리케이션 설치 화면




이 악성 앱은 다수의 권한을 요구하는데 [그림 1-47]과 같이 '문자 관련 권한'과 '과금 서비스(Services that cost you money)'가 있다는 것에 주의해야 한다.

[그림 1-47] 악성 앱의 권한




이처럼 해당 앱은 유료 서비스(premium call) 문자를 발송하여 과금하는 것을 목적으로 제작되었다. 악성코드 제작자는 이러한 방법으로 이득을 취한다.

문자 과금과 관련된 코드를 보면 각 국가별로 문자 서비스 번호가 다르게 구분되어 있어 국가가 다르더라도 문자 과금이 가능하다.



[그림 1-48] 문자 과금 관련 코드 일부

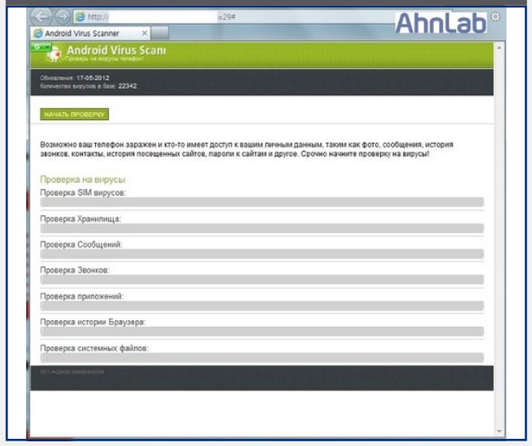
```
    str3 = str2;
    localObject = str1;
    NUMBERS = str2;
  }
  ArrayList localArrayList1 = new ArrayList();
  localArrayList1.add("4" + "0" + "2" + "6" + "2");
  localArrayList1.add("4" + "0" + "6" + "4" + "1");
  localArrayList1.add("4" + "0" + "9" + "7" + "3");
  localArrayList1.add("7" + "5" + "3" + "3" + "3");
  localArrayList1.add("7" + "5" + "4" + "2" + "1");
  localArrayList1.add("7" + "5" + "6" + "2" + "7");
  localArrayList1.add("7" + "5" + "8" + "5" + "1");
  localArrayList1.add("7" + "7" + "3" + "2" + "5");
  localArrayList1.add("7" + "7" + "5" + "9" + "3");
  localArrayList1.add("7" + "7" + "6" + "7" + "6");
  localArrayList1.add("7" + "8" + "1" + "1" + "3");
  localArrayList1.add("7" + "8" + "2" + "7" + "1");
  localArrayList1.add("7" + "8" + "3" + "4" + "4");
  localArrayList1.add("7" + "8" + "9" + "1" + "1");
  String str8 = Utils.getPref1(this.mContext, localArrayList1);
  ArrayList localArrayList2 = new ArrayList();
  localArrayList2.add("9" + "8" + "7" + "8" + "6" + "8");
  localArrayList2.add("9" + "0" + "0" + "9" + "7" + "6");
  localArrayList2.add("9" + "0" + "9" + "0" + "0" + "9");
  localArrayList2.add("9" + "0" + "5" + "4" + "3" + "2" + "0");
  localArrayList2.add("3" + "0" + "3" + "1" + "1" + "1");
  localArrayList2.add("3" + "0" + "0" + "2" + "3" + "4" + "5");
  localArrayList2.add("4" + "5" + "3" + "2" + "6" + "2");
  localArrayList2.add("4" + "5" + "4" + "1" + "7" + "1");
  localArrayList2.add("4" + "5" + "9" + "0" + "8" + "8");
  Utils.getPref2(this.mContext, localArrayList2);
  String str9 = "9" + "6" + "8" + "3";
  String str10 = "7" + "5" + "0" + "3" + "1";
  String str11 = "3" + "3" + "0" + "4";
  String str12 = "3" + "3" + "0" + "2";
  new StringBuilder(String.valueOf("1")).append("8").append("9").append("9").toString();
  new StringBuilder(String.valueOf("3")).append("3").append("3").append("2").toString();
  new StringBuilder(String.valueOf("3")).append("3").append("3").append("9").toString();
  String str13 = "5" + "7" + "6";
  String str14 = "8" + "9" + "8" + "7";
  String str15 = "7" + "0" + "0" + "1";
  String str16 = "7" + "2" + "5" + "0";
```

〈V3 제품군의 진단명〉
– Android-Trojan/Boxer

## 허위 안드로이드 모바일 백신 유포

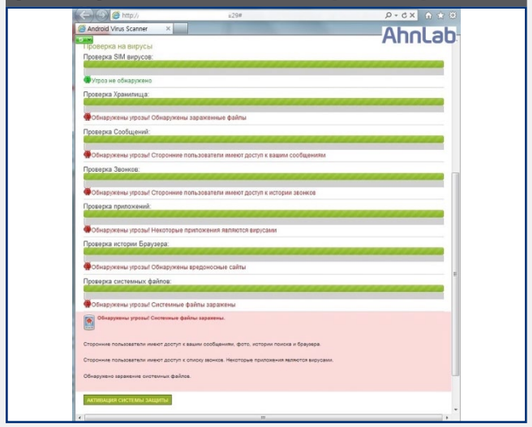
윈도우 운영체제 기반의 PC에 감염되었던 허위 백신들과 유사한 형태로 허위 안드로이드 모바일 백신을 유포하는 사례가 발견되었다. 이러한 허위 백신 형태의 악성코드는 최근 애플 맥 운영체제 사용자들이 증가함에 따라 맥 운영체제에서 동작하도록 제작되기도 한다. 이번에 발견된 안드로이드용 허위 백신은 [그림 1-49]와 같이 정상적인 보안 관련 웹 사이트로 위장하고 있다.

[그림 1-49] 허위 안드로이드 악성코드 스캐닝 웹 사이트




이 웹 사이트는 러시아어로 제작되었으며, 'SIM 검사', '저장소 검사'와 '시스템 파일 검사' 등의 항목을 보여줘 실제로 안드로이드 스마트폰의 보안 검사를 수행하는 것처럼 속이고 있다. 각 항목의 검사가 종료되면 [그림 1-50]과 같이 특정 항목을 붉은 색으로 표시해 악성코드에 감염된 것으로 위장하여 사용자가 VirusScanner.apk 파일을 설치하도록 유도한다.

[그림 1-50] 허위로 보여주는 안드로이드 악성코드 감염 정보들

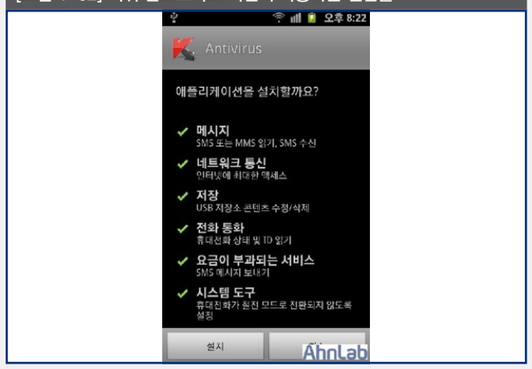



다운로드된 VirusScanner.apk를 설치하면 [그림 1-51]과 같이 러시아 보안 업체 카스퍼스키(Kaspersky)의 보안 제품과 동일한 아이콘이 생성된다.

[그림 1-51] 러시아 보안 제품과 동일한 아이콘 생성

설치 과정에서 해당 허위 백신은 [그림 1-52]의 권한들이 사용됨을 사용자에게 보여준다.

[그림 1-52] 허위 안드로이드 백신이 사용하는 권한들



설치된 허위 백신은 사용을 위해 요금을 지불해야 하는, 금전적인 목적으로 제작된 안드로이드 악성코드이다. 향후 이러한 허위 백신 형태의 안드로이드 악성코드가 지속적으로 등장할 것으로 예상된다.

〈V3 제품군의 진단명〉
– Android–Trojan/FakeAV
– Android–Trojan/FakeAV.B

### 허위 유명 안드로이드 앱 배포 웹 사이트

안드로이드 운영체제에서 동작하는 유명 게임들을 배포하는 것처럼 위장하여 악성코드를 유포하는 웹 사이트를 발견했다.

[그림 1–53] 유명 게임을 배포하는 것으로 위장한 웹 사이트


이 웹 사이트들은 모두 러시아어로 제작되었으며, 안드로이드 운영체제에서 설치 가능한 APK 파일들을 다운로드하도록 유도한다.

구글은 안드로이드 앱 스토어에서 악성코드가 유포되는 것을 막기 위해 사전 심사를 강화하였고, 많은 사람들이 방문하는 서드파티 앱 스토어에는 사용자의 평판이 존재한다. 악성코드 제작자는 이를 회피하기 위하여 별도의 허위 웹 사이트를 제작한 것으로 보인다.

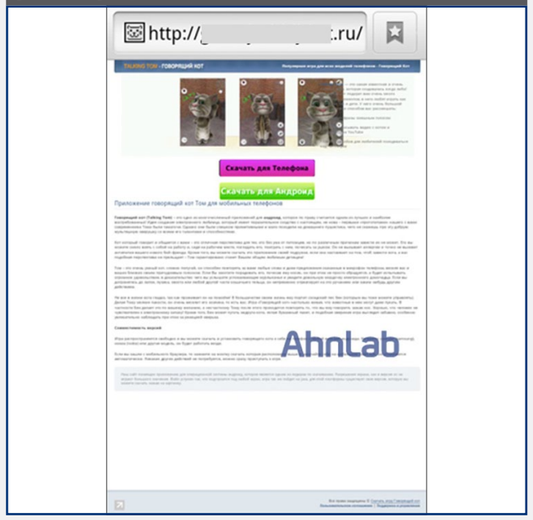
이처럼 허위로 제작된 안드로이드 마켓은 2012년 3월에 발견 사례가 있었다. 안드로이드 사용자들은 구글에서 직접 운영하는 앱 스토어나 통신사에서 운영하는 신뢰할 수 있는 앱 스토어에서만 앱을 다운로드하여 설치하는 것이 바람직하다.

〈V3 제품군의 진단명〉
– Android–Trojan/Boxer.KX

### Talking Tom Cat 사이트로 위장한 앱 사이트를 통해 유포되는 악성코드

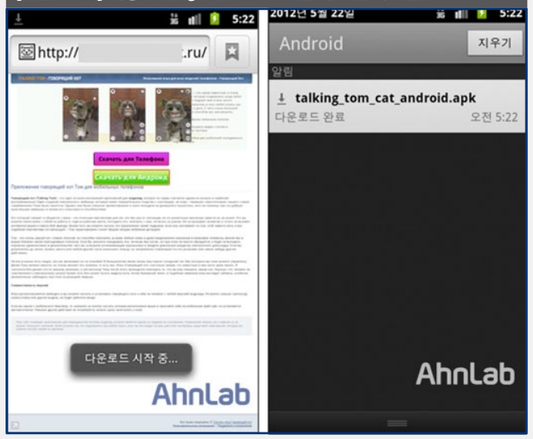
러시아에서 운영 중인 허위 '말하는 고양이(Talking Tom Cat)' 사이트에서 유료 서비스 문자를 발송하여 금전적인 피해를 발생시키는 안드로이드 악성코드가 발견되었다.

[그림 1–54] 악성코드 유포 사이트




이 웹 사이트는 러시아어로 제작되었으며 연결된 앱 설치 버튼을 누르면 talking_tom_cat_android.apk 파일이 다운로드된다.

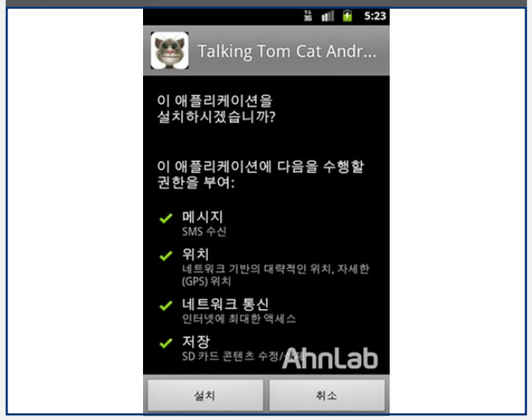
[그림 1–55] 악성 Talking Tom Cat 안드로이드 앱 다운로드




악성 앱의 설치 화면을 보면 [그림 1–56]과 같이 SMS 수신, 발신 권한을 요구한다.

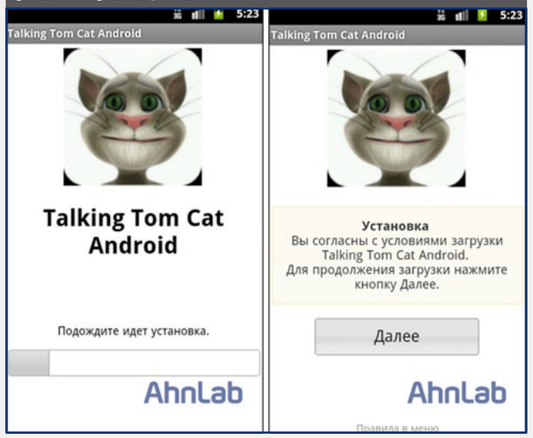


[그림 1–56] 권한 정보



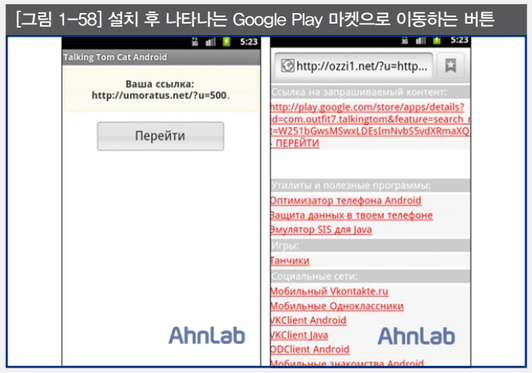

해당 앱이 설치되면 정상적으로 실행되는 것처럼 사용자에게 보여주며 내부적으로는 유료 서비스 문자를 발송한다.

[그림 1–57] 앱 실행 화면



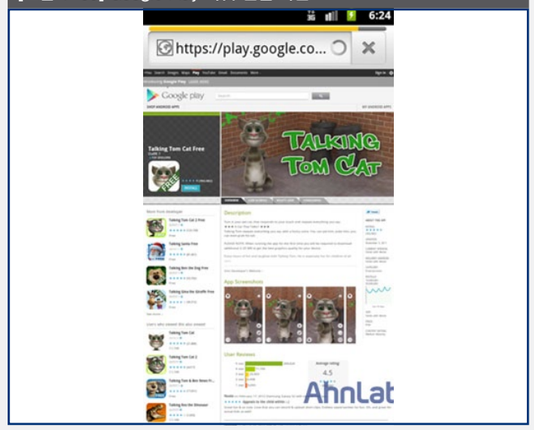

앱 설치 화면이 지나간 뒤 화면에 나타난 버튼을 누르면 Google Play 마켓 링크가 있는 페이지로 이동한다.

[그림 1–58] 설치 후 나타나는 Google Play 마켓으로 이동하는 버튼




Google Play 마켓으로 연결된 링크를 클릭하면 말하는 고양이 페이지로 이동한다. 연결된 화면에서 알 수 있지만 정식 버전은 마켓에서 무료로 사용할 수 있으며, 아이콘에 FREE 문구가 표시된다.

[그림 1–59] Google Play 마켓 연결 화면



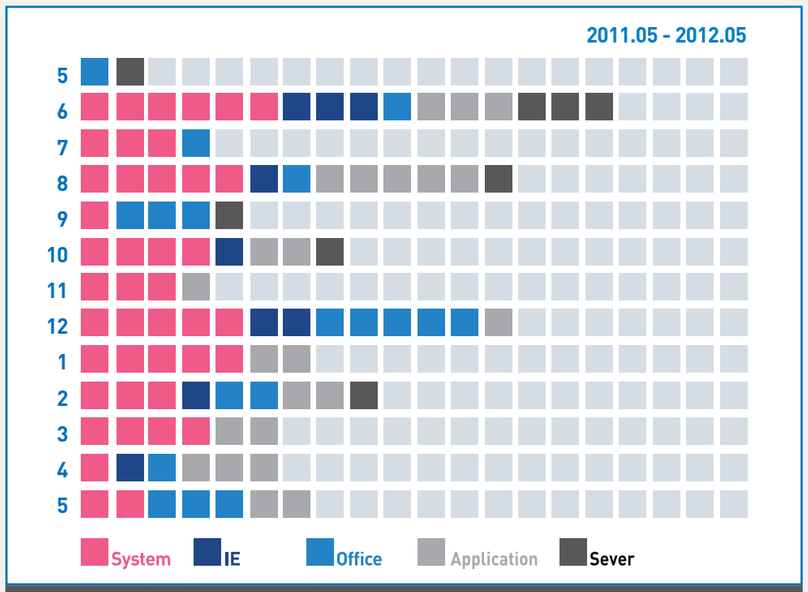

앱을 불법으로 받기 위해 사용하는 가짜 앱 마켓(서드파티 마켓)에서 악성코드를 유포하는 사례가 계속해서 보고되고 있다. 사용자들은 애플리케이션 설치 시 구글 앱 스토어나 통신사에서 운영하는 앱 스토어와 같이 신뢰할 수 있는 마켓을 이용하고 권한 정보를 자세히 확인하는 등의 주의가 필요하다.

〈V3 제품군의 진단명〉
– Android–Trojan/ DJY(2012.05.23)

## 02. 보안 동향
### a. 보안 통계

#### 5월 마이크로소프트 보안 업데이트 현황

마이크로소프트가 발표한 보안 업데이트는 긴급 3건, 중요 4건이다.




[그림 2-1] 공격 대상 기준별 MS 보안 업데이트

| 위험도 | 취약점 |
|---|---|
| 긴급 | MS12-029 Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점 |
| 긴급 | MS12-030 Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점 |
| 긴급 | MS12-031 Microsoft Visio Viewer의 취약점으로 인한 원격 코드 실행 문제점 |
| 중요 | MS12-032 TCP/IP의 취약점으로 인한 권한 상승 문제점 |
| 중요 | MS12-033 Windows Partition Manager의 취약점으로 인한 권한 상승 문제점 |
| 중요 | MS12-034 Microsoft Office, Windows, .NET Framework, Silverlight 대상 통합 보안 업데이트 |
| 중요 | MS12-035 .NET Framework의 취약점으로 인한 원격 코드 실행 문제점 |

[표 2-1] 2012년 5월 주요 MS 보안 업데이트



## 02. 보안 동향
### b. 보안 이슈

#### 어도비 플래시 플레이어 CVE-2012-0779 취약점 발견

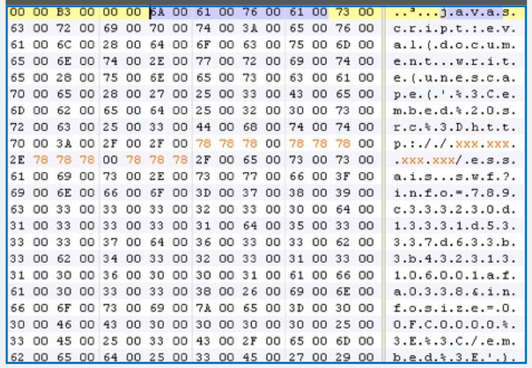
5월 초 어도비사는 플래시 플레이어 취약점인 CVE-2012-0779에 대한 보안 업데이트를 공지하였고, 다수의 블로그에서 실제 취약점을 이용한 공격 사례들이 보고되기도 하였다. 이번 취약점은 RTMP(Real Time Messaging Protocol) 프로토콜을 처리하는 과정에서 발생하는 취약점으로, RTMP는 오디오, 비디오 및 기타 데이터를 플래시 플레이어와 서버 사이에서 스트리밍할 때 사용하기 위한 어도비의 독자적인 통신 규약이다.

[그림 2-2] 취약점 발생 코드(AC)

```
public function 75(param1:String) : void
{
        this.70 = new NetConnection();
        var _loc_2:String = "rtmp://";
        var _loc_3:String = "/TSGeneralSetting";
        var _loc_4:* = _loc_2 + param1 + _loc_3;
        this.70.connect(_loc_4);
        this.70.call("systemMemoryCall", this.71, "argc");
        return;
}// end function
```

이번에 보고된 실제 취약점 악용 사례는 기존과 동일하게 단독 플래시 파일이 아닌 MS 오피스(워드) 파일을 공격의 매체로 삼았다. 다만 워드 파일을 악용하는 방법의 차이가 있으며 플래시 파일(swf)을 직접 문서에 삽입하는 방식이 아닌, 다음과 같이 스크립트 객체를 삽입하여 간접적으로 플래시 파일을 호출하는 방식을 사용하였다.

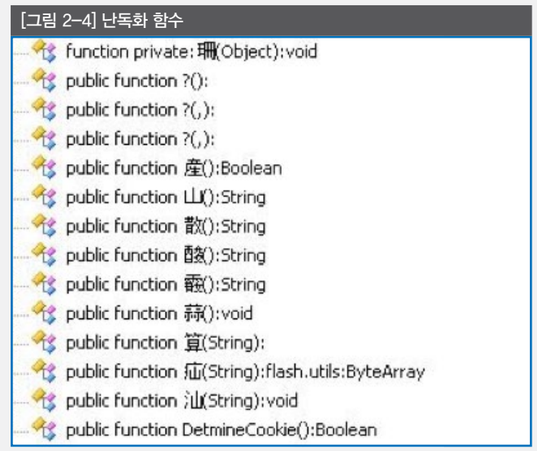
[그림 2-3] 워드 파일 일부



최근 악성 플래시 파일들에 대한 탐지 · 진단 기술이 발달하면서, 이를 우회하려는 공격자들의 기술 또한 다양해지고 있다. 이번 사례에서도 다음과 같은 다수의 우회 방법들이 발견되었다.

– doSWF 툴을 사용한 파일 암호화
– Class/Variable/Function 이름 난독화(한자 사용)
– 외부 파라미터를 통한 정보 전달(info=, infosize=)

[그림 2-4] 난독화 함수




과거 CVE-2012-0754 MP4 파일 취약점을 비롯하여, 최근 집중 타깃(Target)이 되고 있는 플래시 플레이어 내부 엔진과 관련된 다양한 취약점들이 연이어 발견되고 있다. 따라서, MS 제품군뿐만 아니라 어도비 제품을 비롯한 서드파티 제품군의 보안 업데이트도 잊지 말아야 할 것이다.

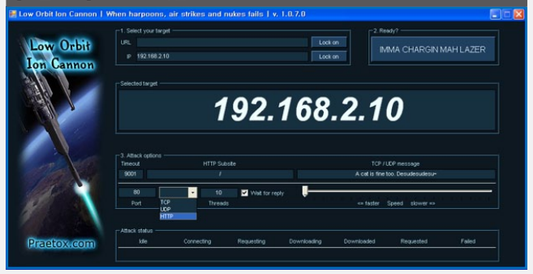
#### 'LOIC' 툴을 이용한 DDoS 공격 주의!

5월 25일을 기점으로 'WikiBoat'라는 새로운 핵티비스트 그룹에 의해, Apple, Bank of America, British Telecom, Bank of China 등 세계적인 대형기관에 대한 DDoS 공격이 계획 중이라는 사실이 알려졌다. 수많은 공격자들이 LOIC(Low Orbit Ion Canon)라는 공격 툴을 내려 받아 공격에 참여할 것이라고 밝혔으며, 해당 툴은 SANS가 예

고한 6월 16일 ’ 이란(Iran)’ 웹 사이트 DDoS 공격에도 이용될 예정이다.

Low Orbit Ion Canon(LOIC)는 최초로 Praetox Technologies에 의해서 개발되어 지금은 오픈 소스인 네트워크 부하(stress) 테스트 및 DoS 공격에 쓰이고 있는 툴이다.

[그림 2-5] LOIC UI 화면




해당 툴은 TCP, UDP, HTTP flooding 종류를 선택하고, 타겟 경로(subsite), 포트, 스레드, 속도(speed) 등을 조절할 수 있는 별도의 옵션을 제공한다.

UDP/TCP flooding 공격은, 디폴트로 TCP/UDP message(사용자 변경 가능) 문자열을 페이로드 데이터로 사용하여 대량의 패킷을 발생한다. HTTP flooding 공격은, 다음과 같이 일반적인 HTTP 헤더와 구별되는 3개의 연속적인 뉴라인(NewLine) 문자를 포함하는 HTTP GET 패킷을 대량으로 발생한다.

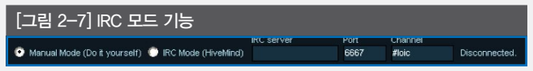
[그림 2-6] HTTP Flooding 패킷

```
Hypertext Transfer Protocol
  GET / HTTP/1.0\r\n
    [Expert Info (Chat/Sequence): GET / HTTP/1.0\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.0
    \r\n
Hypertext Transfer Protocol
    \r\n

0000  00 0c 29 12 90 8e 00 0c  29 a6 b0 7d 08 00 45 00   ..).... )..}..E.
0010  00 3c 5f 1d 40 00 80 06  e9 40 c0 a8 98 88 c0 a8   .<_.@... .@......
0020  98 84 08 bb 00 50 42 25  0d 78 0e a3 4c 22 50 18   .....PB% .x..L"P.
0030  ff ff 5e 43 00 00 47 45  54 20 2f 20 48 54 54 50   ..^C..GE T / HTTP
0040  2f 31 2e 30 0d 0a 0d 0a  0d 0a                     /1.0.... ..
```

특히, 상위 버전의 LOIC(V 1.1)에서는 Internet Relay Chat(IRC) 모드가 존재하여, 원격으로 IRC 채널에 접속하여 대상(target) 정보 및 설정들을 전달받아 수행할 수 있는, 더욱 진화된 기능도 지원한다.

[그림 2-7] IRC 모드 기능



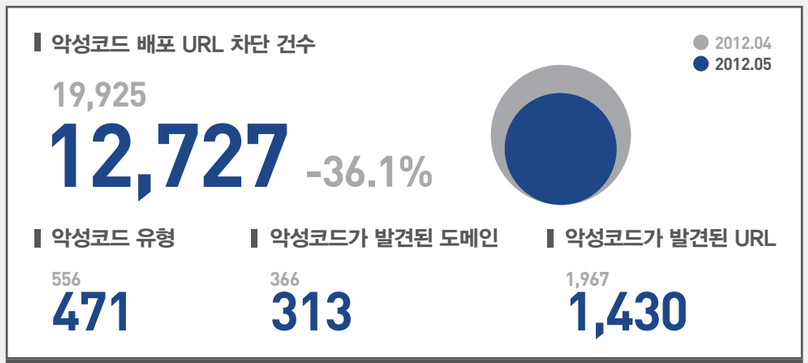

LOIC 툴에서 발생되는 트래픽들은 일반적인 DDoS 방어 장비에서 제공하는 threshold 기반이나 디폴트 설정의 경우 콘텐츠 기반 차단 방식으로도 어느 정도의 차단이 가능하다. 그러나, 공격은 하나의 공격 클라이언트가 아닌 수많은 클라이언트를 통해 대량의 DDoS 트래픽이 발생하는 만큼 DDoS 모니터링에 더 주의를 기울일 필요가 있다.



## 03. 웹 보안 동향
### a. 웹 보안 통계

### 웹사이트 악성 코드 동향

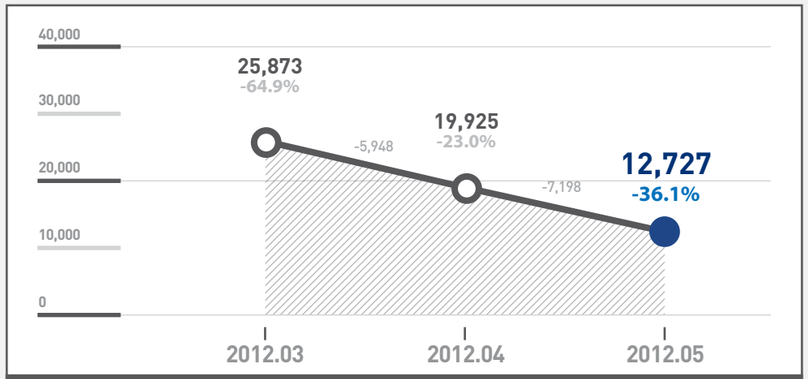
안랩의 웹 브라우저 보안 서비스인 사이트가드(SiteGuard)를 활용한 웹 사이트 보안 통계 자료에 의하면, 2012년 5월 악성코드를 배포하는 웹 사이트를 차단한 건수는 총 1만 2727건이었다. 악성코드 유형은 471종, 악성코드가 발견된 도메인은 313개, 악성코드가 발견된 URL은 1430개였다. 이는 2012년 4월과 비교할 때 전반적으로 다소 감소한 수치이다.




[표 3-1] 웹 사이트 악성코드 동향

### 월별 악성코드 배포 URL 차단 건수

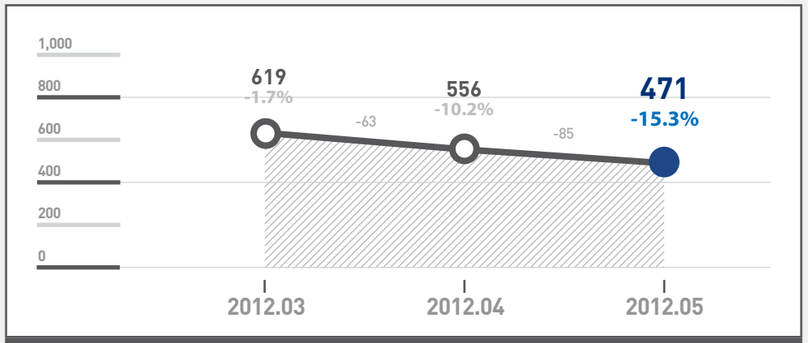
2012년 5월 악성코드 배포 웹 사이트 URL 접근에 대한 차단 건수는 지난달 1만 9925건에 비해 36% 감소한 1만 2727건이었다.




[그림 3-1] 월별 악성코드 배포 URL 차단 건수 변화 추이

## 월별 악성코드 유형

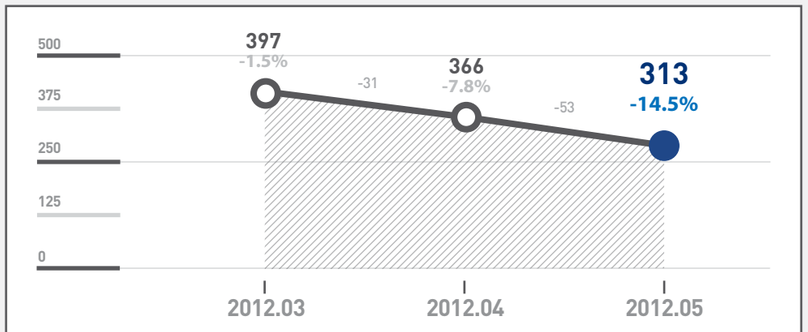
2012년 5월의 악성코드 유형은 전달의 556건에 비해 15% 줄어든 471건이었다.




[그림 3-2] 월별 악성코드 유형 수 변화 추이

## 월별 악성코드가 발견된 도메인

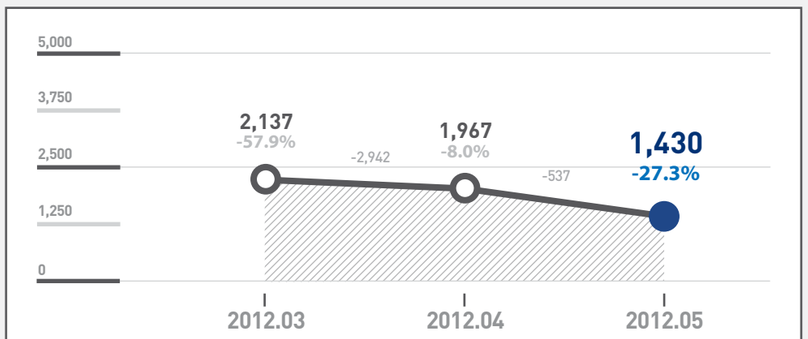
2012년 5월 악성코드가 발견된 도메인은 313건으로 2012년 4월의 366건에 비해 14% 감소했다.




[그림 3-3] 월별 악성코드가 발견된 도메인 수 변화 추이

## 월별 악성코드가 발견된 URL

2012년 5월 악성코드가 발견된 URL은 전월의 1967건에 비해 27% 감소한 1430건이었다.




[그림 3-4] 월별 악성코드가 발견된 URL

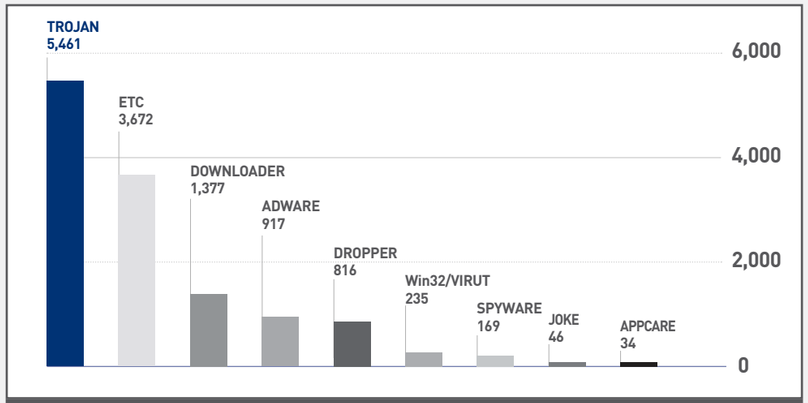


## 악성코드 유형별 배포 수

악성코드 유형별 배포 수를 보면 트로이목마가 5461건/42.9%로 가장 많았고, 다운로더가 1377건/10.8%인 것으로 조사됐다. 악성코드 배포 최다 10건 중에서 Trojan/Win32.HDC가 996건으로 가장 많았고 Downloader.Win32.Korad가 755건으로 그 뒤를 이었다.

| 유형 | 건수 | 비율 |
|---|---|---|
| **TROJAN** | **5,461** | **42.9%** |
| DOWNLOADER | 1,377 | 10.8% |
| ADWARE | 917 | 7.2% |
| DROPPER | 816 | 6.4% |
| Win32/VIRUT | 235 | 1.8% |
| SPYWARE | 169 | 1.3% |
| JOKE | 46 | 0.4% |
| APPCARE | 34 | 0.3% |
| ETC | 3,672 | 28.9% |
| | **12,727** | **100.0%** |

[표 3-2] 악성코드 유형별 배포 수




[그림 3-5] 악성코드 유형별 배포 수

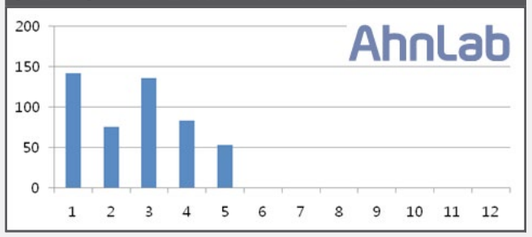
| 순위 | 등락 | 악성코드명 | 건수 | 비율 |
|---|---|---|---|---|
| **1** | **▲4** | **Trojan/Win32.HDC** | **996** | **18.7%** |
| 2 | — | Downloader/Win32.Korad | 755 | 14.2% |
| 3 | ▲4 | ALS/Bursted | 630 | 11.8% |
| 4 | NEW | ALS/Qfas | 458 | 8.6% |
| 5 | ▼1 | Downloader/Win32.Totoran | 454 | 8.5% |
| 6 | NEW | Trojan/Win32.SendMail | 449 | 8.4% |
| 7 | ▲1 | Unwanted/Win32.WinKeyfinder | 434 | 8.2% |
| 8 | ▼2 | Trojan/Win32.ADH | 430 | 8.1% |
| 9 | ▲1 | Unwanted/Win32.WinKeygen | 400 | 7.5% |
| 10 | ▼7 | Dropper/Small.Gen | 319 | 6.0% |
| | | | **5,325** | **100.0%** |

[표 3-3] 악성코드 배포 최다 10건

## 03. 웹 보안 동향
### b. 웹 보안 이슈

### 2012년 5월 침해 사이트 현황

[그림 3-6] 2012년 4월 악성코드 유포 목적의 침해 사이트 현황




[그림 3-6]은 악성코드 유포를 목적으로 하는 침해 사고가 발생했던 사이트들의 월별 현황이다. 3월 이후로 계속 감소하고 있는데, 이는 기존에 악성코드를 유포했던 P2P 사이트들에서 악성코드 유포가 감소했기 때문인 것으로 분석된다.

### 침해 사이트를 통해서 유포된 악성코드 최다 10건

[표 3-4] 2012년 4월 악성코드 최다 10건

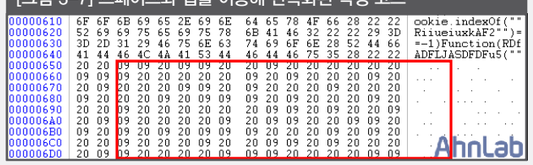
| 순위 | 악성코드명 | 건수 |
|---|---|---|
| 1 | **Win-Trojan/Onlinegamehack.45568.AB** | **25** |
| 2 | Dropper/Onlinegamehack.128845 | 21 |
| 3 | Win-Trojan/Onlinegamehack.102912.AY | 19 |
| 4 | Dropper/Onlinegamehack.36965 | 19 |
| 5 | Win-Trojan/Patched.102912 | 18 |
| 6 | Dropper/Win32.OnlineGameHack | 18 |
| 7 | Win-Trojan/Patched.102912 | 18 |
| 8 | Win-Trojan/Onlinegamehack.102912.AY | 18 |
| 9 | Win-Trojan/Onlinegamehack.101888.AY | 18 |
| 10 | Win-Trojan/Onlinegamehack.92672.DK | 17 |

[표 3-4]는 5월 한 달 동안 가장 많은 사이트를 통해서 유포되었던 악성코드 최다 10건이다. 가장 많이 유포된 Win-Trojan/Onlinegamehack.45568.AB(이하 Onlinegamehack.54784.BC)는 25개의 국내 웹 사이트(언론사 21, 취업 포털 2, 종교 1, 기타 1)를 통해 유포되었다.

특정 언론사의 경우 상위 도메인을 기준으로 서비스별로 여러 개의 하위 도메인이 존재하였고, 각 하위 도메인별로 각각 다른 페이지에 악성코드를 다운로드하는 주소가 삽입되어 있었다. 각 서브 도메인의 페이지에 삽입된 악성 스크립트 코드는 [그림 3-7]과 같이 '스페이스와 탭을 이용한 자바스크립트 난독화'에서 다뤘던 형태이다.

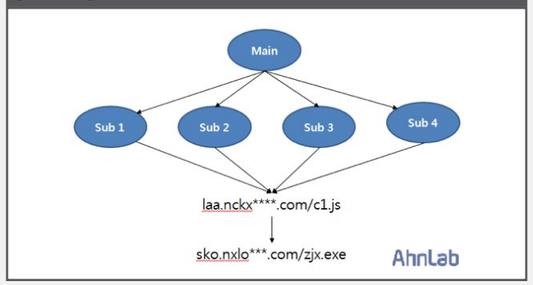
- **스페이스와 탭을 이용한 자바스크립트 난독화 출현**: http://asec.ahnlab.com/767

[그림 3-7] 스페이스와 탭을 이용해 난독화된 악성 코드




하지만 최종적으로 다운로드되는 악성코드의 주소는 [그림 3-8]과 같이 모두 동일하였다.

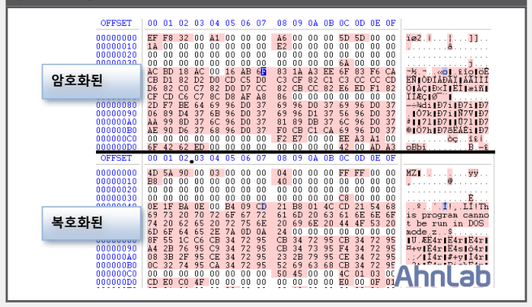
[그림 3-8] 침해된 사이트의 구조와 삽입된 악성코드의 다운로드 주소




일반적으로 최종 다운로드되는 파일은 [그림 3-9]와 같이 백신의 진단을 회피하도록 실행 불가 파일 형태로 유포된다. 이후 셸 코드에 의해서 복호화되어 온라인게임핵 악성코드가 실행된다.



[그림 3-9] 복호화 전/후의 악성코드

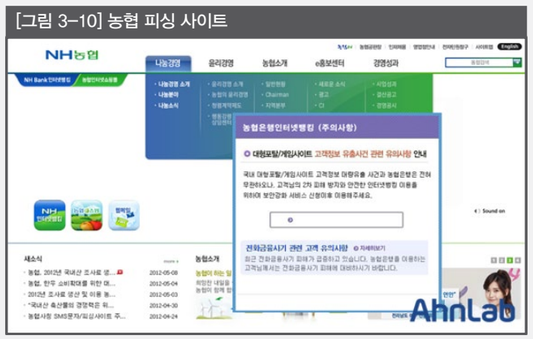



### 꾸준히 발견되는 농협 피싱 사이트

국내 주요 금융기관을 대상으로 하는 피싱 사이트들이 크게 증가하고 있는 가운데 농협 피싱 사이트가 발견되었다. 실제 사이트와 유사하게 제작되었으며, 문자 메시지를 발송하여 접속을 유도하고 있어 사용자들의 주의가 요구된다.

[그림 3-1-]은 농협 피싱 사이트의 화면이다. 금전적 이유를 목적으로 제작된 피싱 사이트는 실제 농협 사이트와 구분할 수 없을 정도로 정교하게 제작되었다.

[그림 3-10] 농협 피싱 사이트



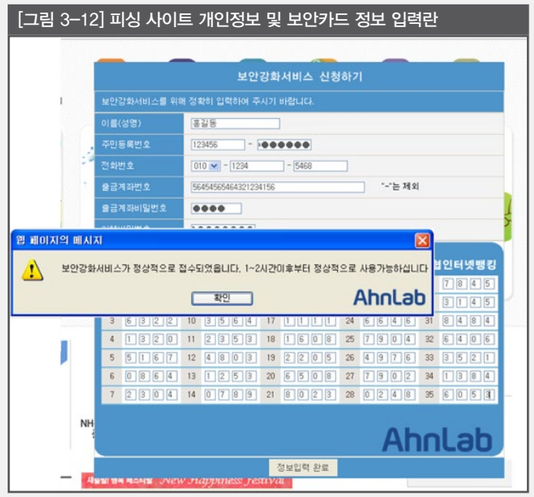

이 사이트는 '보안 강화 서비스 신청하기' 이외의 부분은 클릭할 수 없도록 만들어졌다. 이를 통해 개인정보 수집 페이지로 사용자들의 접속을 유도하여 개인 정보 및 보안 카드 정보를 요구한다.

[그림 3-11] 실제 농협 사이트


이러한 피싱 사이트가 꾸준히 발견되는 이유는 실제로 많은 피해자가 피싱 사이트에 현혹되기 때문이다. 보이스피싱과 연계한 신종 사례도 발견되었다.

소중한 정보를 보호하기 위해서는 수신된 문자 메시지를 통해 금융기관 접속을 유도하거나 보안카드와 같은 금융 정보 입력을 요구할 때 각별히 조심해야 한다.

[그림 3-12] 피싱 사이트 개인정보 및 보안카드 정보 입력란



VOL. 29
ASEC REPORT Contributors

집필진
책임 연구원 심 선 영
선임 연구원 안 창 용
선임 연구원 이 도 현
선임 연구원 장 영 준
주임 연구원 문 영 조

참여연구원 ASEC 연구원
SiteGuard 연구원

편집장
선임 연구원 안 형 봉

편집인 안랩 세일즈마케팅팀

디자인 안랩 UX디자인팀

감 수
전 무 조 시 행

발행처 주식회사 안랩
경기도 성남시 분당구
삼평동 673
(경기도 성남시 분당구
판교역로 220)
T. 031-722-8000
F. 031-722-8901

Disclosure to or reproduction
for others without the specific
written authorization of AhnLab is
prohibited.

Copyright (c) AhnLab, Inc.
All rights reserved.