Security Trend

# ASEC REPORT

## VOL.65

May, 2015

AhnLab

# ASEC REPORT

**VOL.65** May, 2015

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

## 2015년 5월 보안 동향

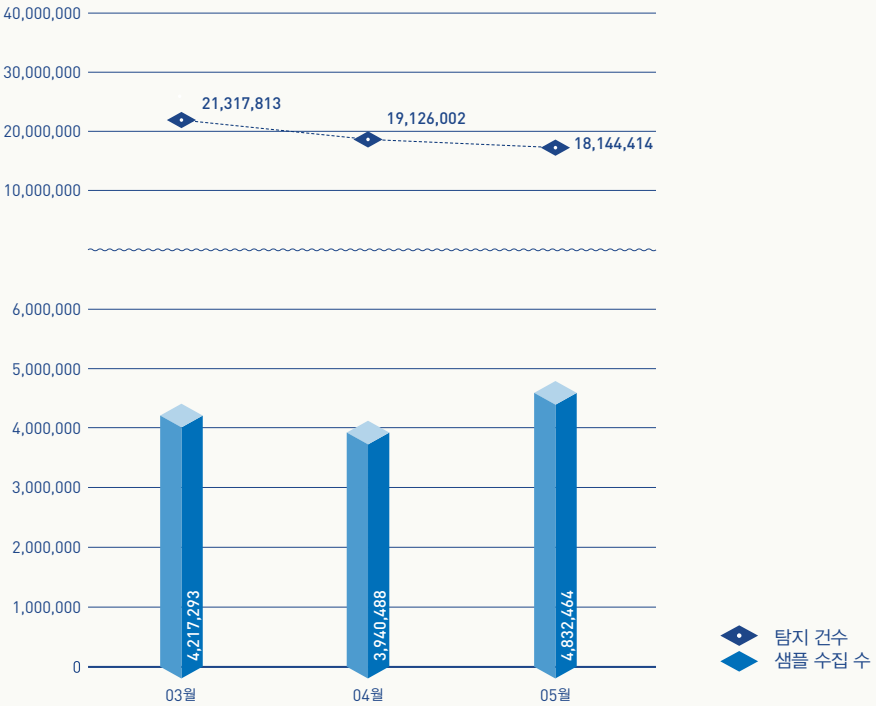
Table of Contents

# 1

# 보안 통계
# STATISTICS

# 01 악성코드 통계

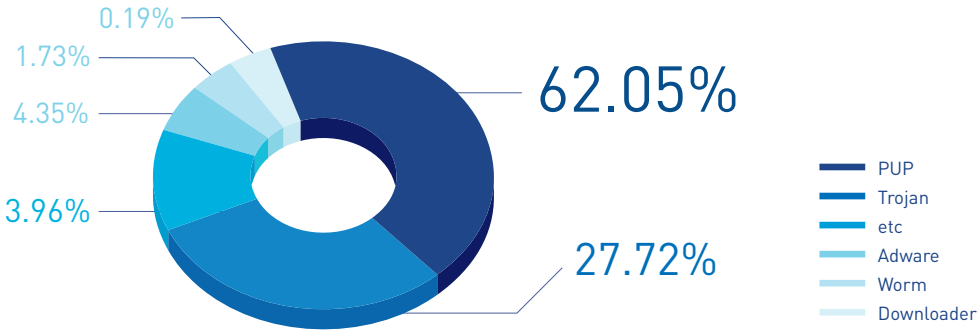
ASEC이 집계한 바에 따르면 2015년 5월 한 달간 탐지된 악성코드 수는 1,814만 4,414건이다. 이는 전월 1,912만 6,002건에 비해 98만 1,588건 감소한 수치다. 한편 5월에 수집된 악성코드 샘플 수는 483만 2,464건이다.




[그림 1-1] 악성코드 추이(2015년 3월 ~ 2015년 5월)

* '탐지 건수'란 고객이 사용 중인 V3 등 안랩의 제품이 탐지한 악성코드의 수를 의미하며, '샘플 수집 수'는 안랩이 자체적으로 수집한 전체 악성코드의 샘플 수를 의미한다.

[그림 1-2]는 2015년 5월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 62.05%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 27.72%, 애드웨어(Adware)가 4.35%로 그 뒤를 이었다.




[그림 1-2] 2015년 5월 주요 악성코드 유형

[표 1-1]은 5월 한 달간 가장 빈번하게 탐지된 악성코드 10건을 진단명 기준으로 정리한 것이다. PUP/Win32.BrowseFox가 총 215만 5,648건으로 가장 많이 탐지되었고, PUP/ Win32.MicroLab가 156만 3,164건으로 그 뒤를 이었다.

[표 1-1] 2015년 5월 악성코드 탐지 최다 10건(진단명 기준)

| 순위 | 악성코드 진단명 | 탐지 건수 |
|---|---|---|
| 1 | PUP/Win32.BrowseFox | 2,155,648 |
| 2 | PUP/Win32.MicroLab | 1,563,164 |
| 3 | PUP/Win32.MyWebSearch | 1,097,760 |
| 4 | PUP/Win32.Enumerate | 830,077 |
| 5 | PUP/Win32.Helper | 756,388 |
| 6 | PUP/Win32.MultiPlug | 437,970 |
| 7 | PUP/Win32.SubShop | 371,442 |
| 8 | PUP/Win32.WindowsTap | 362,236 |
| 9 | PUP/Win32.CloverPlus | 335,107 |
| 10 | PUP/Win32.WindViewer | 286,775 |

# 02
# 웹 통계

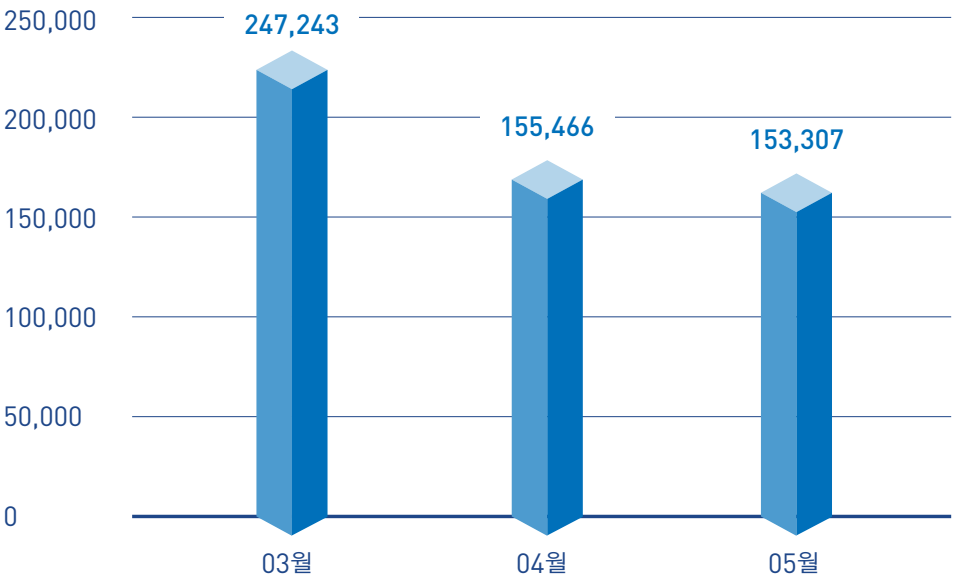
2015년 5월 악성코드 유포지로 악용된 도메인은 1,504개, URL은 1만 3,887개로 집계됐다. 또한 5월의 악성 도메인 및 URL 차단 건수는 총 572만 4,598건이다.


[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2015년 3월 ~ 2015년 5월)

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

# 03
# 모바일 통계

2015년 5월 한 달간 탐지된 모바일 악성코드는 15만 3,307건으로 집계됐다.




[그림 1-4] 모바일 악성코드 추이(2015년 3월 ~ 2015년 5월)

[표 1-2]는 5월 한 달간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. Android-PUP/SmsReg가 지난 4월에 이어 가장 많이 발견되었다.

[표 1-2] 2015년 5월 유형별 모바일 악성코드 탐지 상위 10건

| 순위 | 악성코드 진단명 | 탐지 건수 |
|---|---|---|
| 1 | Android-PUP/SmsReg | 64,697 |
| 2 | Android-PUP/Noico | 13,667 |
| 3 | Android-PUP/Zdpay | 11,222 |
| 4 | Android-Trojan/AutoSMS | 8,222 |
| 5 | Android-PUP/Airpush | 6,256 |
| 6 | Android-PUP/Dowgin | 5,668 |
| 7 | Android-Trojan/FakeInst | 3,565 |
| 8 | Android-PUP/SmsPay | 2,880 |
| 9 | Android-Trojan/SmsSpy | 2,389 |
| 10 | Android-PUP/Wapsx | 2,178 |

# 2

# 보안 이슈
# SECURITY ISSUE

# 01 입사 지원자로 위장해 기업 노리는 타깃 공격

TV 프로그램, 패션, 사용 언어마다 유행이 있듯이 악성코드도 유행이 있다. 2015년 스팸메일에 첨부된 악성코드는 '랜섬웨어 → Upatre → 랜섬웨어 → Upatre'로 반복되고 있다. 물론 최근 웹을 통해 유포된 드라이브 바이 다운로드(Drive-By-Download) 방식의 랜섬웨어는 기존에 첨부 파일로 유포되던 방식과 달라 많은 국내 사용자에게 피해를 주었다. 이러한 유행 속에서 특정 사용자를 목표로 하는 스팸메일이 가끔 발견되는데, 주로 문서 파일(hwp, doc)로 위장하고 있다는 것이 특징이다.

일반적으로 스팸메일은 사용자에게 의심을 주지 않으려고 제목과 내용이 간결하다. 하지만 최근 발견된 '이력서 지원으로 위장한 스팸메일'은 메일 수신자에게 신뢰를 주기 위해 지원동기나 포부 등 구체적인 내용을 담고 있다.

표 2-1 | 유포되고 있는 스팸메일

[발신자 / 유포되는 스팸메일 내용 중 일부]


[유포 내용 중 일부 1]

안녕하십니까? 제 이름은 ***이라고 합니다. **대학교 경영학과의 경영관리석사입니다. *** 앱에서 귀사의 채용정보를 봤어 메일을 보냈습니다. 병역필이고 올해 졸업할 것인데 귀사에 지원하려고 합니다.
저는 새로운 미래를 믿습니다.
/*중간생략*/
매일 공부를 게을리 하지 않고 더욱 큰 공헌을 하겠다고 다짐합니다.
첨부파일(이력서)을 참고하시기 바랍니다. 진심으로 감사합니다!


[유포 내용 중 일부 2]

안녕하십니까? 제 이름은 ***이라고 합니다. **대학교 컴퓨터학과 소프트웨어전공의 석사입니다. 병역필이고 올해 졸업할 것인데 귀사에 지원하려고 합니다.
고객가치를 최우선으로
/*중간생략*/
힘차게 노력하겠다고 다짐합니다.
첨부파일(이력서)을 참고하시기 바랍니다. 진심으로 감사합니다.

[표 2-1]과 같이 유포되고 있는 스팸메일에는 '이력서.rar' 파일이 첨부되어 있으며, 압축을 풀면 [그림 2-1]과 같이 워드파일 아이콘으로 위장한 실행 파일(.exe)을 확인할 수 있다.


그림 2-1 | '이력서.rar' 압축 해제 후의 파일

'이력서.rar' 파일을 실행하면 [표 2-2]의 경로에 파일을 생성하고 시작프로그램에 등록한다.

표 2-2 | 파일 생성 목록

| [파일 생성] |
| --- |
| C₩WINDOWS₩Temp₩wingt.dll |

표 2-3 | 시작프로그램 등록 정보

| [시작프로그램 등록] |
| --- |
| [레지스트리]<br>HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩SVC150508<br><br>[시작프로그램]<br>Wingtrundll32.exe C:₩WINDOWS₩Temp₩wingt.dll main |

드롭한 dll을 시작프로그램에 등록하고 나면 해당 악성코드는 바로 종료된다. 드롭된 dll은 부팅할 때마다 rundll32.exe에 로드되어 동작하며, 일정 주기로 스레드를 생성하고 C&C에 연결을 시도한다.

표 2-4 | 파일 생성 목록

| [네트워크 연결] |
| --- |
| 19*.**9.**0.*2:8095 k*.h***ip.com |

드롭된 dll이 C&C와 정상적으로 연결되면 특정 명령을 받아와 수행하는 백도어로 동작할 것으로 보인다.

최근 랜섬웨어와 어파트레(Upatre) 등으로 인해 스팸메일에 대한 경각심이 높아졌다. 하지만 위와 같이 스팸메일에 상세한 내용이 적혀있는 경우, 메일 수신자는 신뢰할 수 있는 메일이라고 판단하여 첨부 파일을 실행할 수도 있다. 따라서 확인되지 않은 발신자로부터 수신된 메일의 첨부 파일이나 의심스러운 파일은 실행 전 반드시 사용 중인 백신 프로그램으로 검사하고 실행하지 않는 것이 안전하다.

V3 제품군에서는 관련 악성코드를 다음과 같이 진단하고 있다.

**<V3 제품군의 진단명>**

Dropper/Win32.Adminuser (2015.05.12.02)
Trojan/Win32.Backdoor (2015.05.12.03)

# 02
# 유명 블로그를 악용한 익스플로잇 악성코드 유포

많은 사람들이 이용하는 유명 블로그에서 카이홍 익스플로잇(Caihong Exploit)을 이용한 악성코드가 유포되었다. 해당 악성 페이지는 이전 페이지의 주소를 확인하여 특정 포털 사이트에서 접속해야 악성코드 유포 사이트로 연결된다.

그림 2-2 | 이전 주소 확인 후 악성 페이지로 연결하는 자바스크립트

악성 페이지로 접속되는 URL은 카이홍(Caihong)이며 기존에 실버라이트 취약점(CVE-2013-0074)이 추가된 것이 특징이다.

그림 2-3 | 추가된 실버라이트 취약점 관련 코드

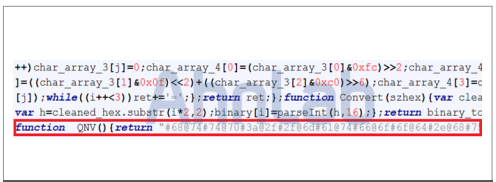


그림 2-4 | 실버라이트 취약점에서 복호화하여 사용하는 URL

해당 URL에서 특수문자를 제외하면 [그림 2-5]와 같이 URL주소가 나오며 해당 주소를 실버라이트 취약점의 셸코드에 붙여서 사용한다.

그림 2-5 | 특수문자를 제거한 다운로드 URL

그동안 실버라이트 취약점은 '리그 익스플로잇 킷(Rig Exploit Kit)'과 '앵글러 익스플로잇 킷(Angler Exploit Kit)'에서 사용했던 취약점이며 과거 카이홍 익스플로잇 킷에는 사용하지 않다가 이번에 추가되었다.

그 외 카이홍 킷은 해당 페이지에 접속하여 다운로드 및 실행되는 악성코드로, [표 2-5]와 같은 행위를 하는 전형적인 파밍 악성코드이다.

| 표 2-5 | 악성코드 행위 내역 | |
|---|---|---|
| [네트워크 연결] | C:₩windows₩syswow32.dll (Trojan/Win32.Banki.R135886) |
| [레지스트리 등록] | HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run₩systeo |
| [네트워크 통신] | users.qzone.qq.com/fcg-bin/cgi_get_*****ait.fcg?uins=**********?=67.***.***.29/ip.php?= |

이와같은 웹 익스플로잇 킷을 방어하는 가장 좋은 방법은 각종 애플리케이션의 업데이트를 꼼꼼히 하는 것이다. 또한 웹페이지 관리자나 블로그 관리자는 계정 비밀번호가 유출됐는지 반드시 확인하고 다른 보안 취약점은 없는지 세심하게 점검해야 한다.

V3 제품군에서는 관련 악성코드를 다음과 같이 진단하고 있다.

**<V3 제품군의 진단명>**

Trojan/Win32.Kazy (2015.05.26.01)
Trojan/Win32.Banki (2015.05.26.04)

# 03 최신 사이버 금융 사기 동향

경찰청 사이버안전국에 따르면 지난해 사이버 금융 범죄로 인한 피해액은 약 600억 원으로 추산된다. 사이버 금융 범죄의 대표적인 수법은 '파밍(Pharming)'과 '스미싱(Smishing)'이다.

'파밍(Pharming)'은 사용자의 컴퓨터에 악성코드를 감염시킨 다음 사용자가 은행사이트에 접속하면 피싱 사이트로 연결되도록 조작해 금융정보를 빼내는 공격 방법이다. 파밍 공격은 이제 조금은 식상해서 피해가 별로 없을 것 같지만, 2013년 3,218건에서 2014년 7,107건으로 2배 이상 증가했다.

이러한 파밍 공격이 어떠한 방법으로 컴퓨터에 악성코드를 감염시키며, 피해자를 속이기 위해 어떻게 변화해 왔는지 알아보자.

파밍 악성코드는 파일을 실행하거나 프로그램을 설치하는 등의 행위를 하지 않는다. 사이트에 접속만 해도 악성코드를 감염시키는 '드라이브-바이 다운로드(Drive-by-download) 방식'을 통해 유포된다.

파밍 악성코드 유포자는 짧은 시간 동안 많은 사용자에게 악성코드를 유포하려고 한다. 주로 주중보다 인터넷 사용이 많은 주말에 집중적으로 파밍 공격을 한다. 공격 방법은 인터넷 사용자들이 자주 이용하는 뉴스, 블로그, 파일공유, 쇼핑, 교육, 여행, 건강 사이트 등 분야를 가리지 않고 악의적인 코드를 삽입하여 악성코드의 다운로드 및 실행을 유도한다.

파밍 악성코드에 감염된 후, 주요 포털 사이트 및 금융 사이트에 접속하면 [그림 2-6]과 같이 금융감독원을 사칭한 팝업창을 볼 수 있다. [그림 2-6]의 첫 번째는 현재 사용되고 있는 금융감독원 사칭 팝업창으로, '옥션정보유출 사건'이라는 문구를 삽입하여 사용자를 현혹한다.


그림 2-6 | 금융감독원 사칭 팝업창 유형

파밍 악성코드를 유포하는 조직은 위와 같이 사칭하는 기관과 경고 문구 변경으로 꾸준히 사용자를 속이기 위해 변화하고 있다. 또한, 지난해와 비교하여 기존에 존재하지 않는 금융사이트를 추가하여 많은 사용자에게 공격을 목표로 하고 있다.

게다가 사칭 팝업창을 통해 연결되는 금융정보 탈취 페이지는 한국인터넷진흥원이나 금융민원센터 사이트와 유사하게 제작되므로 사용자가 구별하기 어렵다.

[그림 2-7]은 한국인터넷진흥원(KISA)의 웹사이트를 모방하여 만든 금융정보를 탈취하는 페이지이다.


그림 2-7 | 한국인터넷진흥원 사칭 페이지

[그림 2-8]은 금융민원센터의 사이트를 모방하여 만든 금융정보 탈취 페이지이다.

그림 2-8 | 정상 금융민원센터 페이지(위) / 금융민원센터 사칭 페이지(아래)

[그림 2-9]는 최근에 발견된 한국인터넷진흥원(KISA) 웹사이트를 모방하여 만든 금융정보 탈취 페이지이다. 기존 사칭 페이지보다 정교하게 제작되었다.


그림 2-9 | 정상 한국인터넷진흥원 페이지(위) / 한국인터넷진흥원 사칭 페이지(아래)

이처럼 파밍 공격은 점점 더 교묘하게 진화하고 있다. 파밍 공격 예방을 위해서는 보안 업데이트를 설치하여 드라이브-바이 다운로드(Drive-By-Download) 공격을 막고, 백신 제품의 엔진을 최신으로 유지하는 등 사용자자의 올바른 보안 습관이 필요하다.

V3 제품군에서는 관련 악성코드를 다음과 같이 진단하고 있다.

**<V3 제품군의 진단명>**

Win-Trojan/Qhost.28672.G (2014.05.12.00)
Win-Trojan/Banki.29184 (2014.04.28.00)
Trojan/Win32.Kryptik (2015.03.04.00)
Trojan/Win32.Yakes (2015.03.04.01)
Trojan/Win32.Banki (2015.04.14.00)
Trojan/Win32.Injector (2015.05.06.01)
Win-Trojan/Malpacked5.Gen (2015.05.07.01)

# 3

# 악성코드 상세 분석
# ANALYSIS-IN-DEPTH

최신 모바일 랜섬웨어 앱 및 대응 방안

# 최신 모바일 랜섬웨어 앱 및 대응 방안

최근 국내 사용자들을 노린 '크립토락커(CryptoLocker)'라는 랜섬웨어가 크게 이슈가 된 바 있다. 랜섬웨어(Ransomware)는 컴퓨터의 데이터를 암호화하여 사용을 제한하고 데이터 복구를 조건으로 금품을 요구하는 방식이다. 랜섬웨어에 감염되면 사용자는 중요한 데이터를 사용할 수 없게 될 뿐만 아니라 공격자의 요구에 따라 비용을 지불한다 하더라도 데이터가 복구된다는 보장이 없어 큰 피해를 입게 된다. 이러한 랜섬웨어는 주로 PC 사용자가 대상이었지만 이제 PC 못지 않게 스마트폰도 랜섬웨어 공격자들에게 매력적인 대상이 되고 있다. 스마트폰의 사용자 수도 PC 사용자 수에 못지 않을뿐더러 스마트폰에도 수많은 개인정보와 중요한 데이터가 저장되어 있기 때문이다.

다행스럽게도 아직 국내 사용자를 대상으로 하는 모바일 랜섬웨어 애플리케이션은 발견되지 않았지만, 해외에서는 이미 다양한 종류의 모바일 랜섬웨어 애플리케이션이 나타나고 있다. 현재 안드로이드 운영체제 기반의 스마트폰을 대상으로 하는 모바일 랜섬웨어는 주로 정상적인 단말기 이용을 불가능하게 하거나 데이터를 암호화하는 방식이다.

이에 이 보고서에서는 안드로이드 랜섬웨어인 'Android-Trojan/Koler', 'Android-Trojan/Simplelock', 'Android-Trojan/Slocker'에 대해 알아보고 랜섬웨어에 감염되었을 때 해결 방법을 살펴본다.

## 1. 주요 모바일 랜섬웨어 애플리케이션

### 1.1. FBI를 사칭하는 모바일 랜섬웨어 Android-Trojan/Koler

Android-Trojan/Koler는 아동 음란물을 이용하는 랜섬웨어 애플리케이션으로, 주로 'PornDroid'라는 애플리케이션 이름으로 위장하여 사용자들을 현혹시킨다. 'Videos'나 'Sex Tube'등의 이름을 쓰기도 한다.

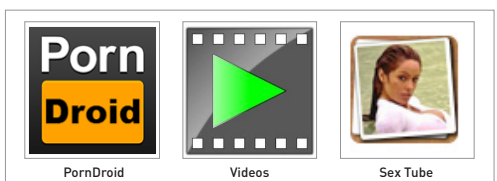



그림 3-1 | Android-Trojan/Koler가 주로 사용하는 허위 아이콘

이 글에서는 허위 애플리케이션인 'PornDroid'를 중심으로 Android-Trojan/Koler 랜섬웨어 애플리케이션에 대해 살펴본다. 해당 랜섬웨어 애플리케이션은 설치 완료와 동시에 동작을 시작하며 'Package installation'이라는 제목의 화면을 출력한다. 이때 구글을 사칭하여 설치 과정의 일부인 것처럼 사용자를 속여 기기 관리자 등록을 유도하고 카

메라 기능을 이용해 사진 촬영을 한다. 이렇게 촬영된 사진은 사용자에게 몸값(ransom), 즉 금전을 요구할 때 사용된다.

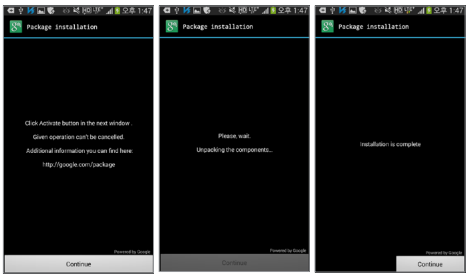



그림 3-2 | 정상적인 설치 과정으로 위장하여 악성 행위 수행

설치 후 일정 시간이 지나면 이 악성 애플리케이션은 단말기의 기본 잠금화면을 해제하고 자신의 화면을 항상 최상위에 나타나게 함으로써 사용자가 정상적으로 단말기를 이용하지 못하게 한다. 홈 키를 비롯한 다른 버튼들의 입력도 동작하지 않거나 랜섬웨어가 출력한 화면에 의해 입력 결과가 확인되지 않는다.

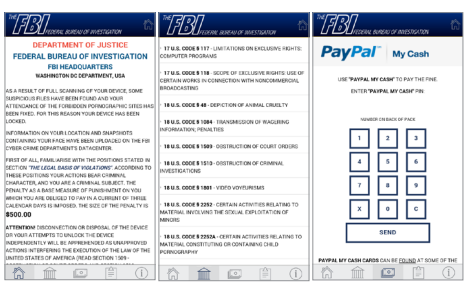



그림 3-3 | FBI를 사칭한 경고 화면

해당 악성 애플리케이션이 강제로 나타나게 하는 화면에는 [그림 3-3]과 같이 FBI를 사칭하며 '사용자가 아동 음란물을 이용했기 때문에 단말기 사용을 제한했고 벌금으로 일정 금액을 지급하라'는 내용을 담고 있다. 이러한 경고 문구와 함께 사용자 단말기에서 저장된 연락처 정보를 읽어와 화면에 출력하거나 웹 브라우저 방문 기록을 출력한다.


그림 3-4 | 촬영된 사용자의 사진과 함께 음란물 이미지를 출력

또 단말기의 전면 카메라로 촬영한 사진을 함께 보여준다. 사용자의 모습과 음란물 이미지를 함께 출력시키고 있다.

## 1.2. 파일을 암호화하는 모바일 랜섬웨어 Android-Trojan/Simplelocker

Android-Trojan/Simplelocker는 단말기에 저장된 파일을 암호화하여 사용하지 못하게 하는 랜섬웨어다. 단말기의 외부 저장소에 있는 특정 파일들을 암호화한 후 원본 파일을 삭제하여 사용자가 데이터를 이용하지 못하도록 한다.

그림 3-5 | Android-Trojan/Simplelocker가 사용하는 허위 아이콘

주로 플래시 플레이어(Flash Player)를 사칭하며, 이와 유사한 아이콘과 이름으로 VideoPlayer라는 이름을 사용하기도 한다. 해당 랜섬웨어 애플리케이션의 기능을 살펴보면, 서버와 문자 메시지 또는 http를 이용해 통신하며 C&C 통신 기능을 갖고 있다. 해당 악성 애플리케이션을 설치하면 기기 관리자 권한을 요구하며, 설치 후 실행하려 해도 애플리케이션 화면이 나타나지 않는다.

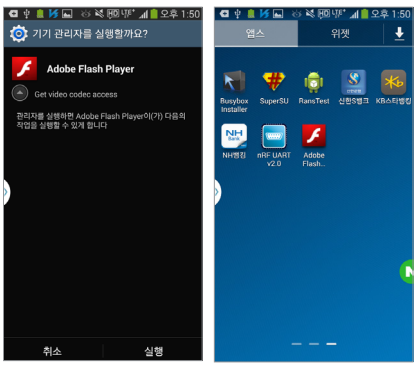



그림 3-6 | 기기 관리자 권한을 요구하는 악성 앱

이어 해당 애플리케이션은 단말기에 있는 파일에 대한 암호화 작업을 시작한다. 암호화에 사용하는 키 값은 코드 내부에 포함되어 있다. 코드 내부에 있는 문자열을 SHA-256으로 해시하고 해당 값을 이용해 비밀 키를 생성한다. 파일을 생성한 키로 암호화하고 확장자를 .enc로 변경 후 원본 파일을 삭제한다.

해당 애플리케이션이 암호화를 시도하는 데이터는 외부 저장소의 jepg, jpg, png, bmp, gif, pdf, doc, docx, txt, avi, mkv, 3gp, mp4 등의 확장자를 가진 파일들이다.

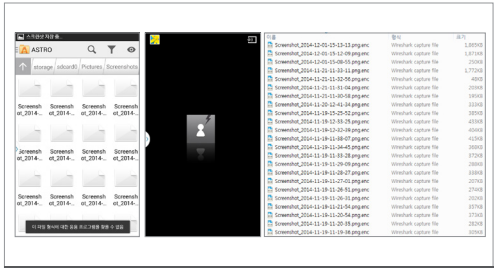


그림 3-7 | 악성 애플리케이션에 의해 암호화된 데이터

## 1.3. 러시아 스마트폰 사용자를 노린 모바일 랜섬웨어 Android-Trojan/Slocker

대부분 영어를 사용한 랜섬웨어와 달리 Android-Trojan/Slocker는 러시아어로 된 안내 문구를 출력하는 랜섬웨어 애플리케이션이다. 데이터를 암호화하는 기능은 없으며 단말기에 항상 자신의 화면을 최상단에 보이게 하는 방식으로 정상적인 단말기 이용을 제한한다.

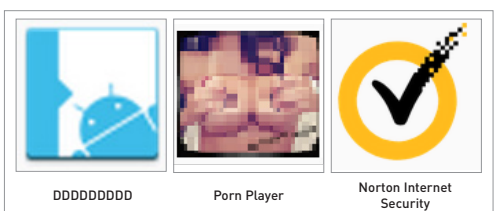



그림 3-8 | Android-Trojan/Slocker가 주로 사용하는 허위 아이콘

Android-Trojan/Slocker는 주로 보안 애플리케이션을 사칭하거나 플래시 플레이어 등의 이름을 사용하기도 한다. 최근에는 성인 애플리케이션으로 위장해 Porn Player라는 이름을 주로 사용하고 있으며, DDDDDDDDD, AAAAAAAAA 등의 알파벳을 이용한 이름을 쓰기도 한다.

이 중에서 'DDDDDDDDD'라는 이름의 애플리케이

션을 살펴보자.

해당 악성 애플리케이션은 설치 시 다른 악성 애플리케이션들과 마찬가지로 기기 관리자 권한을 요구하는데, 그 중에서도 안드로이드 시스템 보안과 관련된 권한을 요구한다.

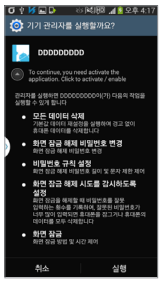



그림 3-9 | 안드로이드 시스템 보안과 관련된 기기 관리자 권한 요구

기기 관리자 권한을 허용하면 잠시 후 [그림 3-10]과 같이 러시아어로 된 화면이 나타난다. 사용자에게 일정 비용을 지불하면 잠금을 해제하겠다는 내용을 보여주며 비용 지불 방법에 대해 상세하게 설명하고 있다. 이후 이 화면은 항상 단말기 최상단에 위치하며 다른 화면이나 버튼 등을 수행할 때 나타나는 모든 창을 가려 정상적인 단말기 이용을 불가능하게 한다.


그림 3-10 | 일정 시간 내에 일정 금액을 지불하라고 요구하는 내용의 러시아어 화면

## 2. 모바일 랜섬웨어 애플리케이션 제거 방법

모바일 랜섬웨어에 감염되었을 때 제거 방법을 알아보자. 앞서 살펴본 대부분의 안드로이드 랜섬웨어 애플리케이션은 자신의 화면을 항상 최상단에 출력하여 다른 화면을 가리는 방식으로 정상적인 스마트폰 사용을 방해한다. 특히 단말기를 재부팅하더라도 다시 랜섬웨어 화면이 나타나며 정상 애플리케이션과 같은 방법으로는 제거할 수 없다. 이 경우, ▲안전모드를 통한 제거 ▲ADB를 이용한 제거 등 대표적으로 두 가지 방법을 이용할 수 있다.

### 2.1. 안전모드 부팅을 통한 제거

단순한 랜섬웨어의 경우, 안전모드 부팅을 통해 제거할 수 있다. 안전모드로 부팅 시 단말기의 기본 시스템 애플리케이션을 제외한 다른 애플리케이션은 동작하지 않게 된다. 랜섬웨어 애플리케이션도 시스템 애플리케이션이 아니므로 안전모드로 부팅하면 동작하지 않는다.

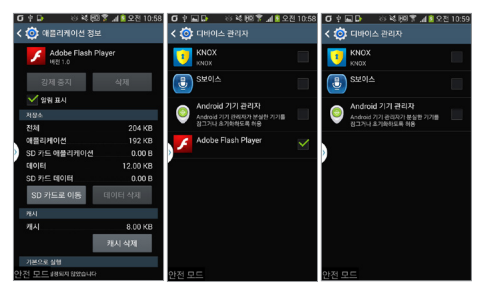



그림 3-11 | 안전모드 부팅을 통한 기기 관리자 권한 해제

이때 기기 관리자 권한을 가지고 있는 애플리케이션의 경우 삭제되지 않는다. 따라서 이 경우에는 기기 관리자 권한을 해제한 후, 악성 애플리케이션 제거를

진행한다.

그러나 일부 랜섬웨어 애플리케이션은 사용자가 기기 관리자 권한을 해제하려 할 경우 다시 자신의 화면을 출력시켜 단말기 사용을 제한하여 애플리케이션 제거를 방해한다.

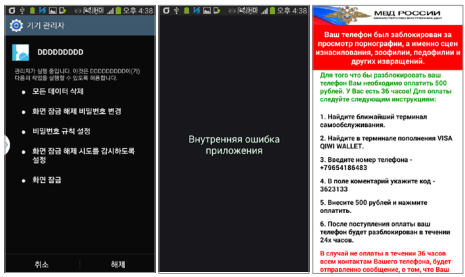



그림 3-12 | 기기 관리자 권한 해제를 방해하는 랜섬웨어 Android-Trojan/Slocker

이처럼 안전모드를 이용한 랜섬웨어 애플리케이션 제거가 불가능할 경우, ADB를 이용해서 랜섬웨어 애플리케이션의 동작을 중지시키고 제거를 진행해야 한다.

## 2.2. ADB를 이용한 제거

ADB(Android Debug Bridge)는 안드로이드 기기와 통신할 수 있는 도구다. ADB를 이용해 애플리케이션 설치 및 제거, 셸 명령어 실행, 시스템 로드 등을 확인할 수 있다. ADB를 통해 PC와 단말기를 연결해 랜섬웨어 애플리케이션의 동작을 중지하고 제거한다.

① USB 디버깅 활성화

ADB를 사용하기 위해서는 먼저 PC에 안드로이드 SDK를 설치해야 한다. 그리고 단말기에서 USB 디버깅 설정을 활성화해야 한다. 랜섬웨어에 감염된 상태라면 단말기를 종료하고 안전모드로 재부팅한 다음 진행한다.


그림 3-13 | USB 디버깅 모드 활성화

② 디바이스 확인 및 ADB 연결

USB로 PC와 스마트폰 단말기를 연결하고 명령 프롬프트를 실행하여 안드로이드 SDK 폴더 아래 Platform-tools로 이동한다. 여기에 adb 유틸리티가 있다.

adb devices 명령어로 ADB 서버가 인식한 단말기 목록을 확인한다.

```
C:₩Users₩Jeonggeun₩android-sdks₩platform-tools>adb devices
List of devices attached
3fceb27f        device
```

그림 3-14 | ADB 서버가 인식한 단말기 정보

연결된 단말기 정보가 나오지 않는다면 단말기 드라이버가 설치되어있는지 확인한다. 그리고 'adb shell' 명령어로 연결한다.

```
C:₩Users₩Jeonggeun₩android-sdks₩platform-tools>adb shell
shell@hltekt:/ $
```

그림 3-15 | ADB를 이용한 연결

③ 랜섬웨어 애플리케이션 패키지명 확인

제거를 방해하는 랜섬웨어 애플리케이션을 종료하려면 애플리케이션 패키지명을 확인해야 한다. 'am kill-all' 명령어를 사용하면 실행 중인 모든 애플리케이션을 종료할 수 있지만, 애플리케이션 삭제를 위한 시스템 창도 종료된다. 따라서 랜섬웨어 애플리케이션만 종료하는 것이 필요하다.

우선 안전모드 상태에서 기기 관리자 해제 등 제거 과정을 진행하다가 랜섬웨어 애플리케이션이 다시 동작하면 ADB를 통해 'dumpsys activity activities | grep –i run' 명령어를 입력한다. 이를 통해 [그림 3-16]과 같이 현재 단말기에서 실행 중인 애플리케이션의 액티비티 목록을 확인할 수 있다.

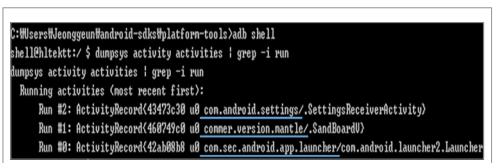



그림 3-16 | 동작 중인 안드로이드 액티비티 스택

[그림 3-16]에서 'com.android.settings', 'commer.version.mantle', 'com.sec.android.app.launcher'는 패키지 명으로, 해당 패키지명을 가진 액티비티들이 동작 중이라는 뜻이다. 이제 'am force-stop <패키지명>' 명령어로 패키지명을 입력해 현재 동작 중인 애플리케이션을 중지시키면 랜섬웨어 애플리케이션의 패키지명을 정확히 확인할 수 있다.


그림 3-17 | 패키지명 'commer.version.mantle'를 가진 애플리케이션 중지 명령어


그림 3-18 | 'am force-stop commer.version.mantle' 명령어로 종료된 랜섬웨어

'am force-stop commer.version.mantle' 명령어로 commer.version.mantle 패키지명을 가진 애플리케이션을 중지하면 단말기에서 동작 중이던 랜섬웨어 애플리케이션이 종료된다. 이를 통해 현재 단말기에 설치된 랜섬웨어 애플리케이션 패키지명이 'commer.version.mantle'인 것을 알 수 있다.

④ 랜섬웨어 애플리케이션 종료 후 제거

기기 관리자 해제를 방해하는 랜섬웨어 애플리케이션 제거를 진행한다. 우선 기기 관리자 등록을 해제한다. 이 글에서는 Android-Trojan/Slocker 랜섬웨어를 삭제하는 방법을 살펴본다.

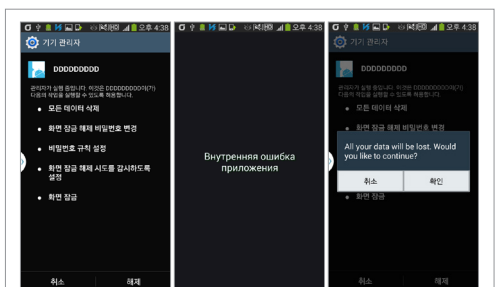



그림 3-19 | 기기 관리자 해제를 방해하는 랜섬웨어 애플리케이션 동작 중지

기기 관리자 해제를 시도하면 랜섬웨어 애플리케이션 화면이 다시 나타난다. 이때 ADB에서 'am force-stop <패키지명>' 명령어로 애플리케이션 동작을 중지한다. 여기에서는 'am force-stop commer.version.mantle' 명령어를 입력한다. 해당 명령어로 랜섬웨어 애플리케이션 창이 사라지면 계속해서 기기 관리자 해제 과정을 진행하면 된다. 중간에 다시 랜섬웨어 화면이 나타날 경우, 같은 방법으로 악성 애플리케이션을 중지시키며 제거 과정을 진행한다.

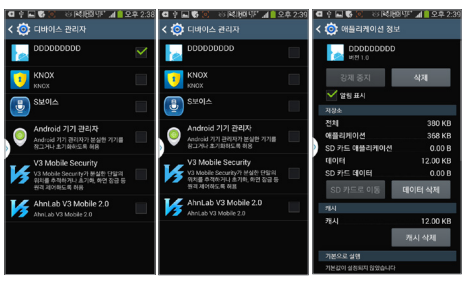



그림 3-20 | ]모바일 랜섬웨어 애플리케이션 제거

기기 관리자 등록을 해제하면 랜섬웨어 애플리케이션의 제거가 가능해지므로 이후 해당 애플리케이션의 삭제를 진행한다. 데이터를 암호화 하는 랜섬웨어 애플리케이션의 경우에는 랜섬웨어 애플리케이션을 백업하고 애플리케이션에서 키를 추출해 복원할 수 있는 방법도 있다.

지금까지 주요 안드로이드 랜섬웨어 애플리케이션과 제거 방법에 대해 살펴보았다. 랜섬웨어는 한번 설치되면 제거하기 어렵고 데이터를 암호화하는 랜섬웨어는 중요한 데이터를 잃을 수도 있다. 또 국내 스마트폰 사용자들을 대상으로 하는 랜섬웨어도 등장할 가능성이 높은 만큼 사용자의 각별한 주의가 필요하다. 대부분의 악성 애플리케이션은 유명 애플리케이션을 사칭하는 경우가 많은 만큼 사용자가 속기 쉽지만 애플리케이션을 설치하기 전에 평판 정보 등을 반드시 확인하고 출처가 불분명한 애플리케이션은 설치하지 않도록 주의해야 한다. 또한, V3 Mobile 등 모바일 백신 프로그램을 이용해 평상시 스마트폰의 감염 여부를 확인하는 것이 바람직하다.

AhnLab

# ASEC REPORT

VOL.65
May, 2015

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

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