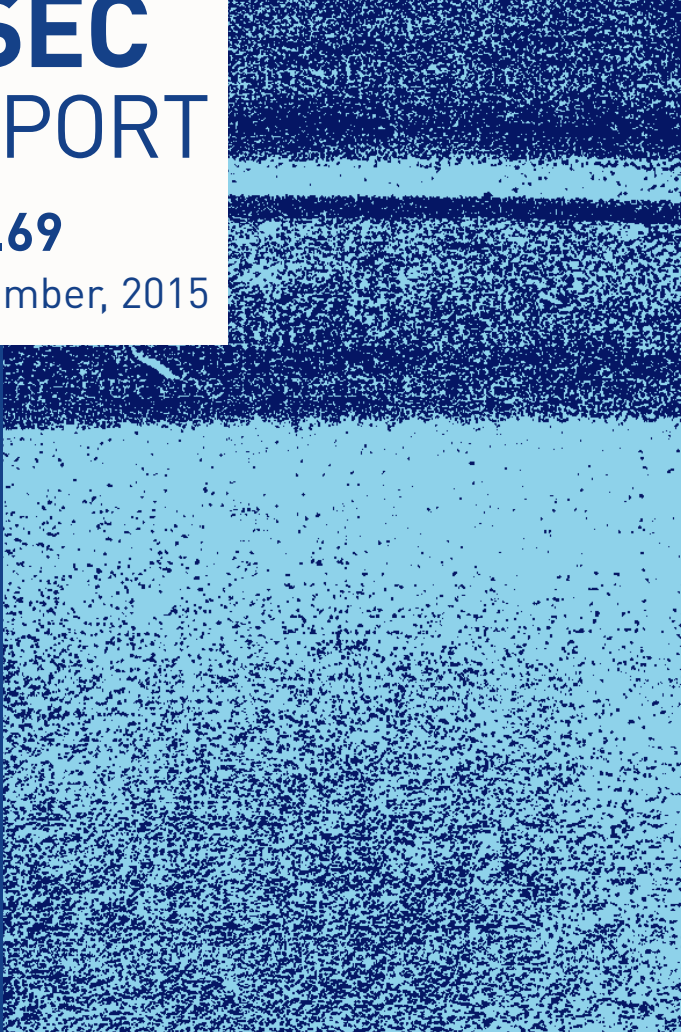


ASEC REPORT

VOL.69

September, 2015



ASEC REPORT

VOL.69 September, 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 9월 보안 동향

Table of Contents

1	01 악성코드 통계	4
보안 통계	02 웹 통계	6
STATISTICS	03 모바일 통계	7
2	01 게임 관련 불법 프로그램 속 악성코드	10
보안 이슈	02 금융은 튼튼하게 소비자는 행복하게	12
SECURITY ISSUE		
3	성인 음란물을 이용한 악성 앱	15
악성코드 상세 분석		
ANALYSIS IN-DEPTH		

1

보안 통계 STATISTICS

01 악성코드 통계

02 웹 통계

03 모바일 통계

보안 통계

01

악성코드 통계

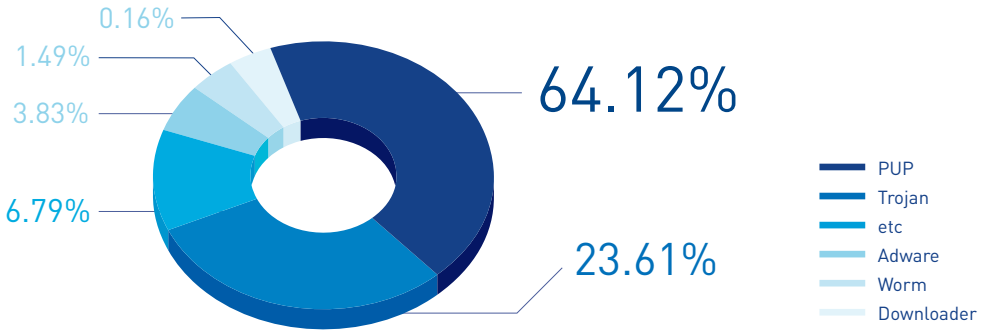
ASEC이 집계한 바에 따르면, 2015년 9월 한 달간 탐지된 악성코드 수는 1,520만 4,993건으로 나타났다. 이는 전월 1,786만 9,127건에 비해 266만 4,134건 감소한 수치다. 한편 9월에 수집된 악성코드 샘플 수는 731만 1,086건이다.



[그림 1-1] 악성코드 추이(2015년 7월 ~ 2015년 9월)

* '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 9월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 64.12%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 23.61%, 애드웨어(Adware)가 3.83%의 비율로 그 뒤를 이었다.



[그림 1-2] 2015년 9월 주요 악성코드 유형

[표 1-1]은 9월 한 달간 탐지된 악성코드 중 PUP를 제외하고 가장 빈번하게 탐지된 10건을 진단명 기준으로 정리한 것이다. Trojan/Win32.Gen이 총 22만 4,589건으로 가장 많이 탐지되었고, Trojan/Win32.Starter가 15만 2,154건으로 그 뒤를 이었다.

[표 1-1] 2015년 9월 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	Trojan/Win32.Gen	224,589
2	Trojan/Win32.Starter	152,154
3	Trojan/Win32.Agent	95,593
4	Trojan/Win32.Banki	62,699
5	Unwanted/Win32.Exploit	60,256
6	Worm/Win32.IRCBot	50,232
7	Malware/Win32.Generic	44,228
8	Unwanted/Win32.Keygen	41,269
9	Trojan/Win32.Generic	40,447
10	HackTool/Win32.Crack	40,339

보안 통계

02
웹 통계

2015년 9월에 악성코드 유포지로 악용된 도메인은 1,258건, URL은 1만 457건으로 집계됐다([그림 1-3]). 또한 9월의 악성 도메인 및 URL 차단 건수는 총 412만 7,520건이다.



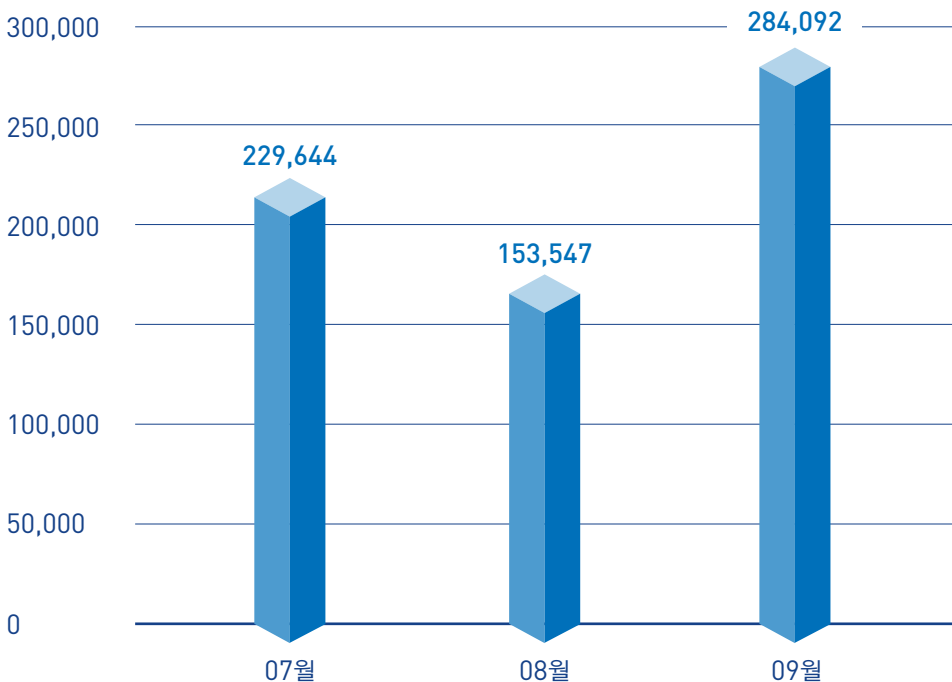
[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2015년 7월 ~ 2015년 9월)

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

03

모바일 통계

2015년 9월 한 달간 탐지된 모바일 악성코드는 28만 4,092건으로 나타났다.



[그림 1-4] 모바일 악성코드 추이(2015년 7월 ~ 2015년 9월)

[표 1-2]는 9월 한 달간 탐지된 모바일 악성코드 유형 중 상위 10건을 정리한 것이다. Android-PUP/SmsPay가 가장 많이 발견되었다.

[표 1-2] 2015년 9월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsPay	98,592
2	Android-PUP/Noico	27,320
3	Android-PUP/SmsReg	22,747
4	Android-PUP/Chepa	16,922
5	Android-Trojan/FakeInst	16,527
6	Android-PUP/Dowgin	9,610
7	Android-Trojan/SmsSpy	6,874
8	Android-Trojan/SMSAgent	6,818
9	Android-PUP/Zdpay	6,316
10	Android-Trojan/Opfake	4,720

2

보안 이슈 SECURITY ISSUE

- 01 게임 관련 불법 프로그램 속 악성코드
- 02 금융은 튼튼하게 소비자는 행복하게

01

게임 관련 불법 프로그램 속 악성코드

문화체육관광부와 한국콘텐츠진흥원에서 진행한 설문조사에 따르면 한국인 10명 중 7명이 게임을 한 적이 있다고 답했다. 플랫폼별 이용률은 모바일 게임이 1위로 나타났으며 온라인 게임, PC용 패키지 게임이 그 뒤를 이었다. 설문조사 결과로 보아 우리나라 국민 대부분이 게임을 즐긴다는 사실을 알 수 있다. 이번에 소개할 악성코드는 게임 관련 불법 프로그램으로 위장하여 유포된 악성코드이다.



GTA_SA+120 Trainer.exe

그림 2-1 | 게임 관련 불법 프로그램으로 위장한 악성 파일

많은 게임 이용자들은 게임의 재미를 배가시키기 위해 게임 해크, 치트키, 매크로, 트레이너 프로그램과 같은 불법 프로그램을 설치한다. [그림 2-1]은 인기 게임인 Grand Theft Auto(이하 GTA)의 불법 프로그램이다. 해당 프로그램은 인터넷, 파일 공유 사이트에서 쉽게 다운로드할 수 있다.



그림 2-2 | 게임 관련 불법 프로그램

사용자가 실행한 불법 프로그램으로 위장한 악성 파일은 실제로 해당 게임의 불법 프로그램을 생성하고 실행시켜 사용자의 의심을 피한다.

악성 파일은 파일 생성, 레지스트리 값 수정, 네트워크 연결을 시도한다.

표 2-1 | 파일 생성 정보

[파일 생성 정보]

C:\Documents and ettings\Administrator\Application Data\0.exe
C:\Documents and Settings\Administrator\Application Data\1.exe
C:\WINDOWS\system32\huppug(랜덤명).exe

불법 프로그램으로 위장한 파일은 0.exe, 1.exe를 생성한다. 0.exe는 자가복제하여 %system32% 경로에 악성 파일을 생성한다. 1.exe는 [그림 2-2]에서 소개한 게임 해크 프로그램이다.

표 2-2 | 레지스트리 등록

[레지스트리 등록]

HKLM\SYSTEM\ControlSet001\Services\Nationaling
"ImagePath" = "C:\WINDOWS\system32\huppug.exe"
"DisplayName" = "Nationalbjf Instruments Domain Service"
"ObjectName" = "LocalSystem"

이렇게 생성된 악성 파일이 시스템을 다시 시작해도 반복 실행될 수 있도록 레지스트리 값을 수정하여 Nationaling이라는 이름의 서비스를 등록한다.

자극하는 콘텐츠는 악성코드 유포에 사용되는 단골 소재인 만큼 사용자는 불법 콘텐츠 및 유료 콘텐츠의 불법 다운로드를 자제해야 한다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Win-Trojan/Malpacked5.Gen (2015.09.19.00)

Dropper/Win32.Agent (2015.09.24.09)

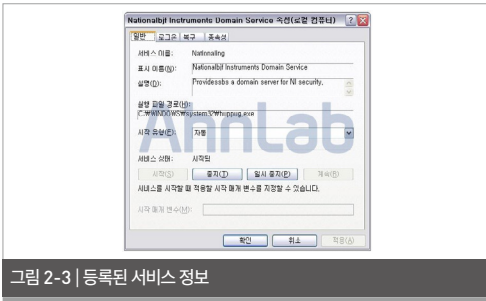


그림 2-3 | 등록된 서비스 정보

악성코드는 다음 IP 주소와 네트워크 연결을 시도한다.

표 2-3 | 네트워크 연결

[네트워크 연결]

2*1.2**1*8.**5:1**6

2*1.2**1*8.**5:5**0

분석 당시에는 사이트로 연결되지 않았으나 연결된 후에는 악성파일 다운로드, 개인 정보 탈취와 같은 추가 악성 행위가 이뤄질 수 있다.

이번 사례에 소개한 악성 파일은 인기 게임의 불법 프로그램으로 위장하여 유포됐다. 실제로 정상 파일을 생성하여 실행시키기 때문에 사용자들은 다운로드한 파일이 악성 파일이라는 사실을 인지하기 어렵다.

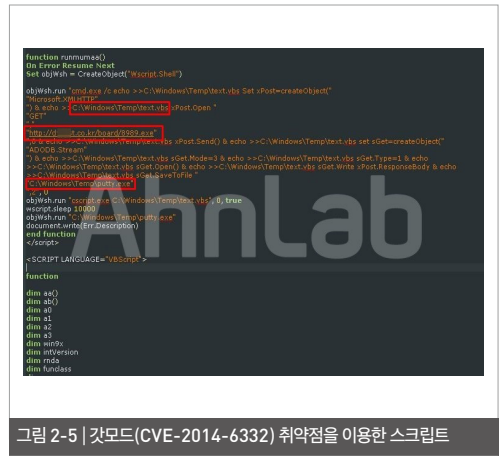
최근 불법 소프트웨어 크랙, 제품 번호 생성 프로그램으로 위장하여 실제 프로그램과 악성 파일을 동시에 유포하는 사례가 부쩍 증가했다. 사용자의 호기심을

02

금융은 튼튼하게 소비자는 행복하게

‘금융은 튼튼하게, 소비자는 행복하게 금융감독원 이 약속합니다.’ 라는 메시지는 금융감독원을 위장한 악성코드의 거짓말이다. 악성코드는 ‘전자금융사기 예방 서비스’를 가입하도록 권하여 이를 통해 사용자의 금융정보를 탈취한다. 이러한 파밍 악성코드는 3년 새 50배가 늘었으며 2014년에는 그 피해 금액이 256억원이라고 하니, 사용자의 각별한 주의가 필요하다. 이번에 소개할 파밍 악성코드는 갓모드(GodMode, CVE-2014-6332) 취약점을 통해 유도되었다.

를 변경하여 VBScript를 수행하는 취약점이다. 따라서 해당 취약점이 패치되지 않은 웹 브라우저에서 악성 스크립트가 삽입된 사이트에 접속하면 즉시 악성코드에 감염된다.



[그림 2-5]의 스크립트를 보면 갓모드(CVE-2014-6332) 취약점이 사용된 것을 확인할 수 있다. 이 취약점을 통해 악성 VBScript를 수행하여 악성 행위를 한다.

일반적으로는 보안상의 이유로 웹 브라우저가 VBScript를 사용하지 못하도록 행위를 제한한다. 이러한 제한은 내부의 safemode 플래그를 통해 구현되어 있다. 갓모드는 바로 이 safemode 플래그

표 2-4 | 파일 생성 정보

[파일 생성 정보]

```
create C:\WINDOWS\TEMP\text.vbs
```

VBS 파일을 생성한 다음 이를 실행하여 네트워크 연결을 통해 악성파일을 다운로드한다.

표 2-5 | 네트워크 연결

[네트워크 연결]

110.45.146.68 (http://d****t.co.kr/board/8989.exe)

위 네트워크 연결을 통해 다운로드한 악성 파일은 %temp% 경로에 putty.exe라는 이름으로 변경된다.

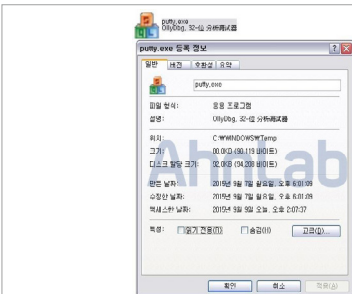


그림 2-6 | 악성 파일 속성 화면

텔넷 접속 프로그램인 PuTTY로 위장하기 위해 악성 파일의 이름을 putty.exe로 수정한 것으로 추정된다. 해당 악성 파일은 사용자에게 금융정보를 요구하는 파밍 악성코드이다. 사용자가 해당 프로그램을 실행하면 추가 악성 파일 생성, 호스트 파일 변조 등의 악성 행위를 한다.



그림 2-7 | 변경된 호스트 파일

악성코드에 감염된 PC로 포털사이트에 접속하면 [그림 2-4]에서 보았던 팝업 창이 나타난다. 그 다음 전자금융사기 예방 서비스 가입 절차로 위장하여 사용자에게 개인 정보 및 계좌 번호, 보안카드 일련 번호, OTP 번호 등을 입력하도록 유도한다. 입력 받은 정보를 이용하여 사용자의 계좌에 있는 돈을 탈취하는 것이 파밍 악성코드의 목적이다.

이번에 소개한 파밍 악성코드는 이미 보안 패치로 해결된 것MODE 취약점을 통해 다운로드 됐다. 따라서 보안 패치가 된 인터넷 익스플로러에서는 악성 스크립트가 삽입된 사이트에 방문하더라도 악성코드에 감염되지 않는다. 악성코드로 인한 금전적 피해를 예방하려면 소프트웨어를 최신으로 업데이트하고, 출처가 불분명한 페이지 방문을 자제해야 한다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

VBS/Downloader (2015.09.08.00)
Trojan/Win32.Banki (2015.09.08.01)
Trojan/Win32.Qghost (2015.09.10.00)

3

악성코드 상세 분석 ANALYSIS-IN-DEPTH

성인 음란물을 이용한 악성 앱

회원 가입 과정은 다음과 같은 정보를 요구하고 있다.



그림 3-4 | 성인 사이트 회원 가입 화면

주목할 만한 점은 회원 가입 과정에서 “인증 코드”를 요구하고 있는데, 이 인증 코드를 발급받기 위해서는 해당 사이트에서 제공하는 앱을 설치해야 한다는 점이다. 앱 다운로드를 다음 페이지에서 제공하고 있다.



그림 3-5 | 인증 코드 발급을 위한 앱 다운로드 유도

성인 사이트에서는 인증 코드 발급을 위해 앱을 다운로드 받을 수 있도록 링크와 QR 코드를 제공하고 있다. 해당 악성 앱을 다운로드 받아 스마트폰에 설치하면 [그림 3-6]에서 보이는 것처럼 하트형 아이콘이 생성되며, 홈페이지에서 요구하는 인증 코드를 발급받을 수 있다.



그림 3-6 | 성인 사이트에서 배포 중인 악성 앱

겉으로 보기에는 단순히 인증 코드만 발급되는 것처럼 보이지만, 악성 앱은 사용자 모르게 사용자 정보를 탈취하고 있다. 이 악성 앱은 MainActivity 클래스와 UploadService 클래스를 통하여 다음 정보를 홍콩에 위치한 서버로 전송한다.

- 스마트폰 전화번호
- 악성 앱 설치 이후 수신되는 문자 메시지(사용자가 탈취당한 메시지는 메시지함에서 확인이 불가능하며, 메시지를 탈취당한 사실을 사용자가 인지할 수 없음)
- 공인인증서

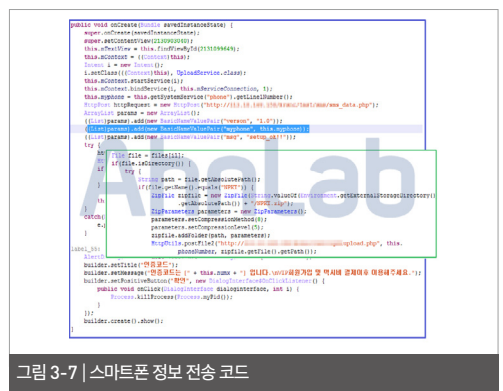
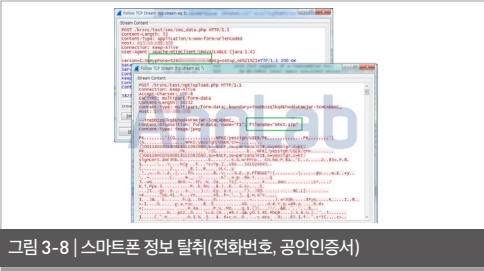
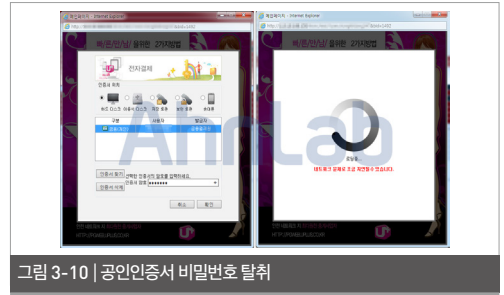


그림 3-7 | 스마트폰 정보 전송 코드

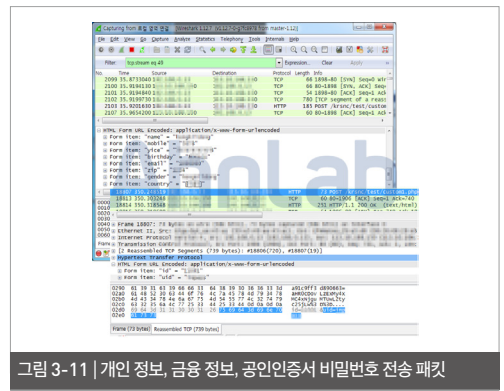
실제 전송되는 네트워크 패킷을 모니터링하면 다음과 같은 과정으로 전송되는 것을 확인할 수 있다.



한 가지 특이한 점은, 공인인증서 비밀번호를 탈취하는 과정에서는 존재하지 않는 인증서를 마치 존재하는 것처럼 보여준다는 점이다. 이는 사용자가 입력한 내용을 참조하여 공인인증서가 존재하는 것처럼 보여줌으로써 의심을 피하려고 한 것으로 추정된다. 하지만 모든 정보를 입력하고 “확인” 버튼을 누르면 ‘로딩 중’ 화면이 나타나며 더 이상 진행은 되지 않는다.



네트워크 패킷을 통해 전송되는 과정을 살펴보면 다음과 같이 구분자를 통해 사용자의 개인 정보 및 금융 정보와 공인인증서 비밀번호를 전송하고 있다는 사실을 확인할 수 있다.



이렇게 탈취한 정보들은 모두 홍콩에 위치한 서버로 전송된다.

이렇게 단순히 스마트폰 전화번호와 공인인증서만 탈취해서는 금전적 이익을 얻기는 어렵기 때문에 악성코드 제작자는 홈페이지를 통해 추가로 사용자의 개인 정보 및 금융 정보와 공인인증서 비밀번호를 수집한다.

홈페이지를 통해 비용을 결제하는 과정에서 사용자가 입력한 정보를 수집한다. 수집한 정보는 스마트폰에서 탈취한 정보와 마찬가지로 홍콩에 위치한 서버로 전송된다. 수집하는 정보는 다음과 같다.

- 은행 이름
- 계좌번호
- 비밀번호
- 예금주
- 주민등록번호
- 계정 정보(아이디/비밀번호)
- 공인인증서 비밀번호





그림 3-12 | 탈취한 정보가 전송되는 서버의 위치

성인 사이트를 사칭해 악성코드를 유포한 이번 사례는 전체적으로 발전된 형태이나 세부적으로는 여전히 허술한 면도 보인다. 홈페이지 회원 가입 과정에서 스마트폰 앱의 설치를 통한 인증 과정과 공인인증서 탈취 과정은 자연스럽게 유도했지만, 전체적인 결재 진행 과정을 보면 다른 악성코드에 비해 정보 수집 방식이 다소 비효율적이고 일부 설정들은 면밀하지 못했다. 그러나 사용자가 주의를 기울이지 않는다면 이러한 과정에 의해서도 금전적 피해를 입을 수 있다는 점을 유의하자.

사례2)

음란물을 이용한 악성 랜섬웨어 앱



그림 3-13 | 악성 랜섬웨어 앱 아이콘

악성 랜섬웨어 앱은 [그림3-13]과 같이 음란물 앱으로 위장한다. 이 앱은 일반적인 악성 랜섬웨어 앱과는 달리 스마트폰 내부 파일을 암호화하지는 않는다.

대신 사용자의 스마트폰 사용에 제약을 준다. 설치된 앱은 스마트폰 시작 시 자동으로 실행되며, 악성 랜섬웨어 앱이 실행하는 화면만을 출력하여 사용자의 스

마트폰 제어를 불가능하게 만든다. 악성 랜섬웨어 앱을 제거하기 위해서 공격자는 일정 금액을 요구한다.

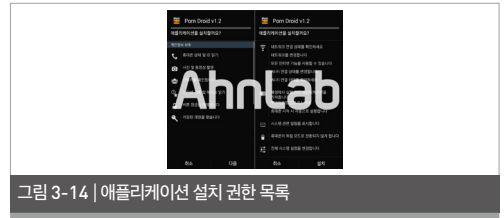


그림 3-14 | 애플리케이션 설치 권한 목록

해당 앱은 [그림 3-14]와 같은 권한을 요구한다. 일반적인 동영상 시청 앱에 필요하지 않은 버튼 잠금, 배경에서 실행 중인 앱 제어, 전체 시스템 설정 변경과 같은 권한을 획득하고자 한다. 추가로 스마트폰의 저장된 개인 정보와 시스템 정보를 이용하는 권한도 요구한다.

요구하는 권한을 악성 랜섬웨어 앱의 내부 설정 파일을 통해 자세히 확인해보면 다음과 같다.

표 3-1 | Androidmanifest.xml

```
<uses-permission android:name="android.permission.DISABLE_KEYGUARD"/>
<uses-permission android:name="com.android.browser.permission.READ_HISTORY_BOOKMARKS"/>
<uses-permission android:name="com.sec.android.app.sbrowser.operatorbookmarks.permission.READ_HISTORY_BOOKMARKS"/>
<uses-permission android:name="android.permission.RESTART_PACKAGES"/>
<uses-permission android:name="android.permission.CAMERA"/>
<uses-permission android:name="android.permission.GET_TASKS"/>
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.WRITE_SETTINGS"/>
<uses-permission android:name="android.permission.KILL_BACKGROUND_PROCESSES"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
```

요구하는 권한에는 “android.permission.SYSTEM_ALERT_WINDOW”가 존재한다. 해당 권한은 스마트폰의 잠금 화면을 포함한 모든 화면을 무시하고 자신이 출력한 화면을 표시할 수 있게 하는 권한이다.

따라서 악성 랜섬웨어 앱이 이 권한을 획득할 경우, 사용자의 스마트폰에는 악성 앱이 의도하는 화면만 보이게 된다.

악성 랜섬웨어 앱의 설치 버튼을 클릭하면 [그림 3-15]와 같이 앱 설치 과정이 출력된다. 이는 실제 앱 설치 과정이 아니라 악성 랜섬웨어 앱의 실행 화면이다.

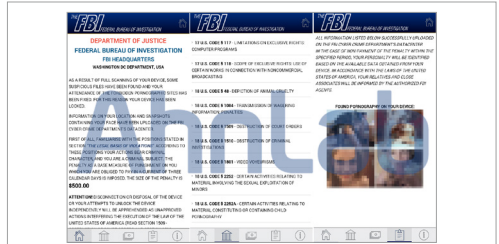


그림 3-16 | 악성 랜섬웨어 앱 실행 화면

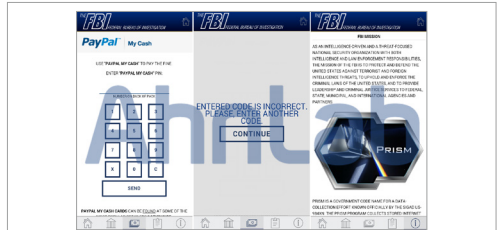


그림 3-17 | 악성 앱 실행 화면

악성 랜섬웨어 앱이 실행되면, [그림 3-17]과 같은 화면이 출력된다. FBI를 사칭하며, 아동 음란물 시청과 스마트폰 잠금 해제를 빌미로 돈을 요구한다.



그림 3-18 | 카메라 촬영 코드

위조된 설치 과정 화면에는 구글 아이콘과 화면 우측 하단에 “Powered by Google” 문구를 삽입하여 사용자를 속이려 한다.

이를 인지하지 못한 사용자가 화면 하단의 “Continue” 버튼을 클릭할 경우 악성 랜섬웨어 앱은 “안드로이드 기기 관리자 권한(Android Device Manager)”을 획득한다. 기기 관리자 권한을 획득하게 되면, 해당 권한을 제거하기 전에는 악성 랜섬웨어 앱의 삭제가 불가능하다.

또한, 악성 랜섬웨어 앱은 스마트폰의 전면 카메라 기능을 이용하여 스마트폰 이용자의 모습을 촬영한다. 촬영된 사진은 사용자를 협박하기 위해 앱 화면에 함께 출력시킨다.

스마트폰 화면 조작을 할 수 없기 때문에 사용자가 스마트폰을 다시 시작하면 더욱 난감한 상황이 발생한다. [그림3-19]와 같이 스마트폰의 PIN 번호를 변경

하여 스마트폰을 잠금 상태로 만드는 것이다.



요즘은 PC보다 스마트폰을 이용하는 경우가 많아졌다. 스마트폰 가입자의 증가와 더불어 악성 앱 역시 증가했다. 따라서 앱은 공식 마켓에서 다운로드하여 설치하는 것이 상대적으로 안전하지만, 공식 마켓에도 악성 앱이 등록되어 있을 수 있으므로 평판 정보를 확인하고 설치하는 습관을 가져야 한다. 무심코 문자에 포함된 URL을 클릭하다 보면 악성 앱이 설치될 수도 있기 때문에 안전성이 확인되지 않은 URL 및 앱은 설치하지 않도록 주의해야 한다. 또한, 모바일 전용 보안 앱(V3 모바일 등)이나 스미싱 탐지 앱(안랩 안전한 문자 등)을 설치하고, 자동 업데이트 설정으로 항상 최신 엔진을 설치하여 스마트폰 환경을 안전하게 유지해야 한다.

이전의 악성 랜섬웨어 앱은 스마트폰 안전 모드로 다시 시작할 경우, 해당 앱을 삭제할 수 있었다. 하지만 이번 악성 랜섬웨어 앱의 경우 시스템에서 사용하는 PIN 번호를 이용하여 스마트폰을 잠그기 때문에 해당 PIN 번호를 풀지 못할 경우 스마트폰 제어가 불가능하다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Android-Trojan/Lovet

Android-Trojan/Koler

만약 스마트폰이 루팅되지 않았으면 유일한 해결 방법은 스마트폰 공장 초기화뿐이다. 공장 초기화를 진행할 경우 PIN 번호뿐만 아니라 스마트폰의 모든 자료가 삭제된다. 따라서 소중한 개인 정보를 지키려면 출처가 정확하지 않은 앱 설치에 대해 주의해야 한다.

AhnLab

ASEC REPORT VOL.69 September, 2015

집필	안랩 시큐리티대응센터 (ASEC)	발행처	주식회사 안랩
편집	안랩 콘텐츠기획팀		경기도 성남시 분당구 판교역로 220
디자인	안랩 디자인팀		T. 031-722-8000
			F. 031-722-8901

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