Security Trend

ASEC REPORT

VOL.73

January, 2016



AhnLab

ASEC REPORT

VOL.73 January, 2016

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.

2016년 1월 보안 동향

Table of Contents

1 보안 통계 STATISTICS

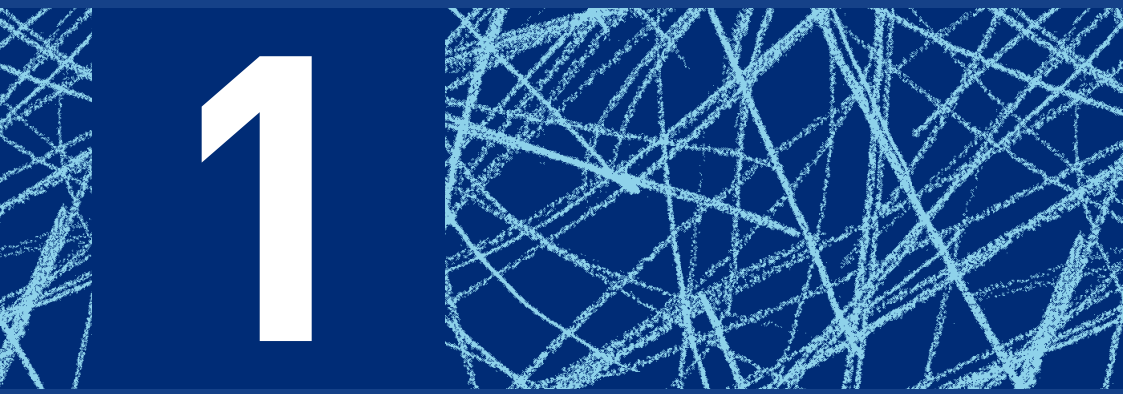
- **01** 악성코드 통계 4
- **02** 웹 통계 6
- **03** 모바일 통계 7

2 보안 이슈 SECURITY ISSUE

- **01** 한국 이어 일본까지, 파밍 악성코드 확산 10
- **02** 착신전환 노리는 안드로이드 악성 앱 12

3 악성코드 상세 분석 ANALYSIS IN-DEPTH

- 랜섬웨어 공격 기법의 다변화: 멀버타이징과 자바스크립트 16



1

보안 통계
STATISTICS

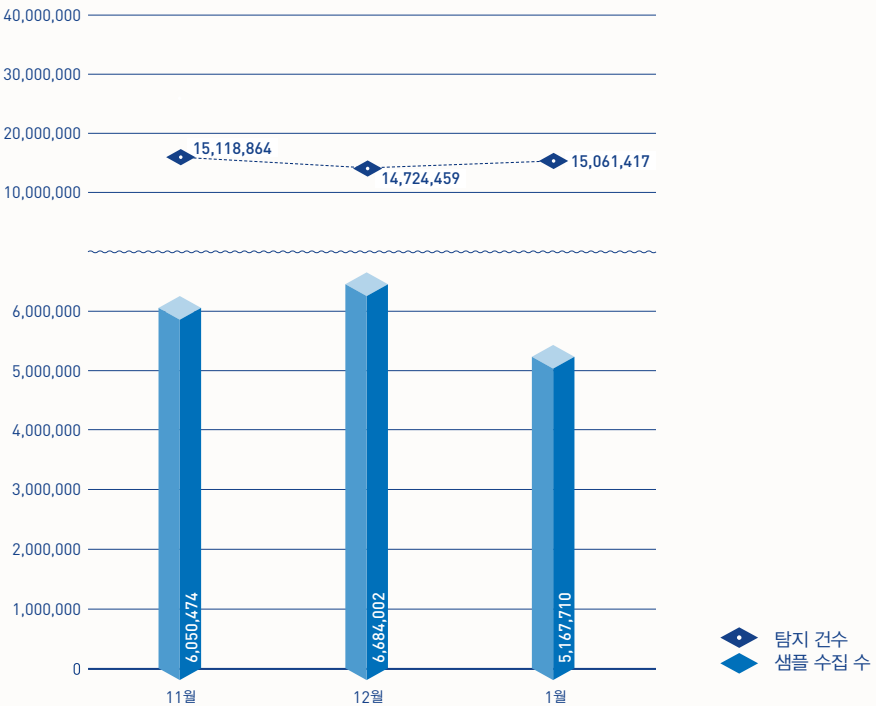
01 악성코드 통계

02 웹 통계

03 모바일 통계

01
악성코드 통계

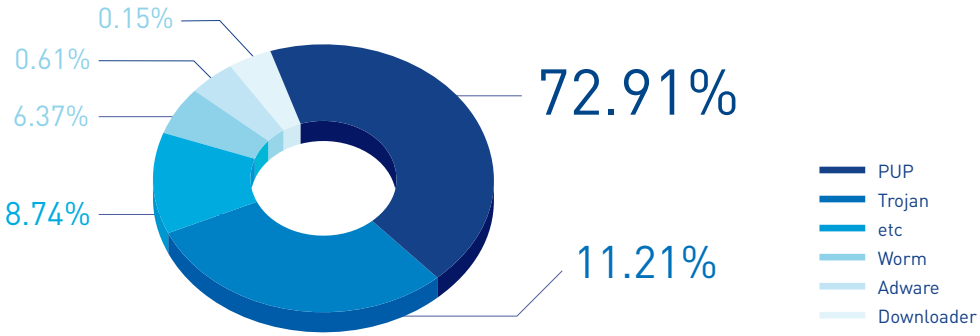
ASEC이 집계한 바에 따르면, 2016년 1월 한 달간 탐지된 악성코드 수는 1,506만 1,417건으로 나타났다. 이는 전월 1,472만 4,459건에 비해 33만 6,958건 증가한 수치다. 한편 1월에 수집된 악성코드 샘플 수는 516만 7,710건이다.



[그림 1-1] 악성코드 추이(2015년 11월 ~ 2016년 1월)

* '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 2016년 1월 한 달간 유포된 악성코드를 주요 유형별로 집계한 결과이다. 불필요한 프로그램인 PUP(Potentially Unwanted Program)가 72.91%로 가장 높은 비중을 차지했고, 트로이목마(Trojan) 계열의 악성코드가 11.21%, 웜(Worm)이 6.37%의 비율로 그 뒤를 이었다.



[그림 1-2] 2016년 1월 주요 악성코드 유형

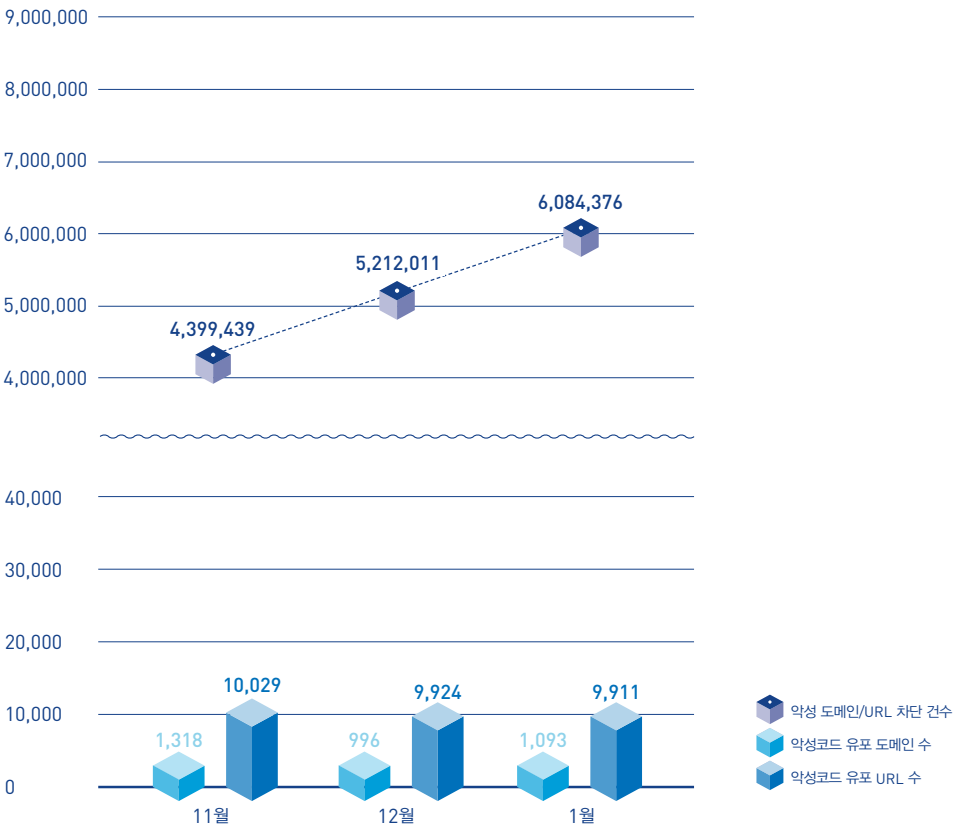
[표 1-1]은 1월 한 달간 탐지된 악성코드 중 PUP를 제외하고 가장 빈번하게 탐지된 10건을 진단명 기준으로 정리한 것이다. Trojan/Win32.Starter이 총 26만 6,240건으로 가장 많이 탐지되었고, Worm/Win32.IRCBot이 18만 5,225건으로 그 뒤를 이었다.

[표 1-1] 2016년 1월 악성코드 탐지 최다 10건(진단명 기준)

순위	악성코드 진단명	탐지 건수
1	Trojan/Win32.Starter	266,240
2	Worm/Win32.IRCBot	185,225
3	Malware/Win32.Generic	153,127
4	Trojan/Win32.Agent	142,804
5	Trojan/Win32.Neshta	108,677
6	Trojan/Win32.Banki	96,843
7	Trojan/Win32.Gen	86,134
8	Unwanted/Win32.HackTool	85,740
9	HackTool/Win32.Crack	71,105
10	Unwanted/Win32.Keygen	65,889

02
웹 통계

2016년 1월에 악성코드 유포지로 악용된 도메인은 1,093개, URL은 9,911개로 집계됐다([그림 1-3]). 또한 1월의 악성 도메인 및 URL 차단 건수는 총 608만 4,376건이다.

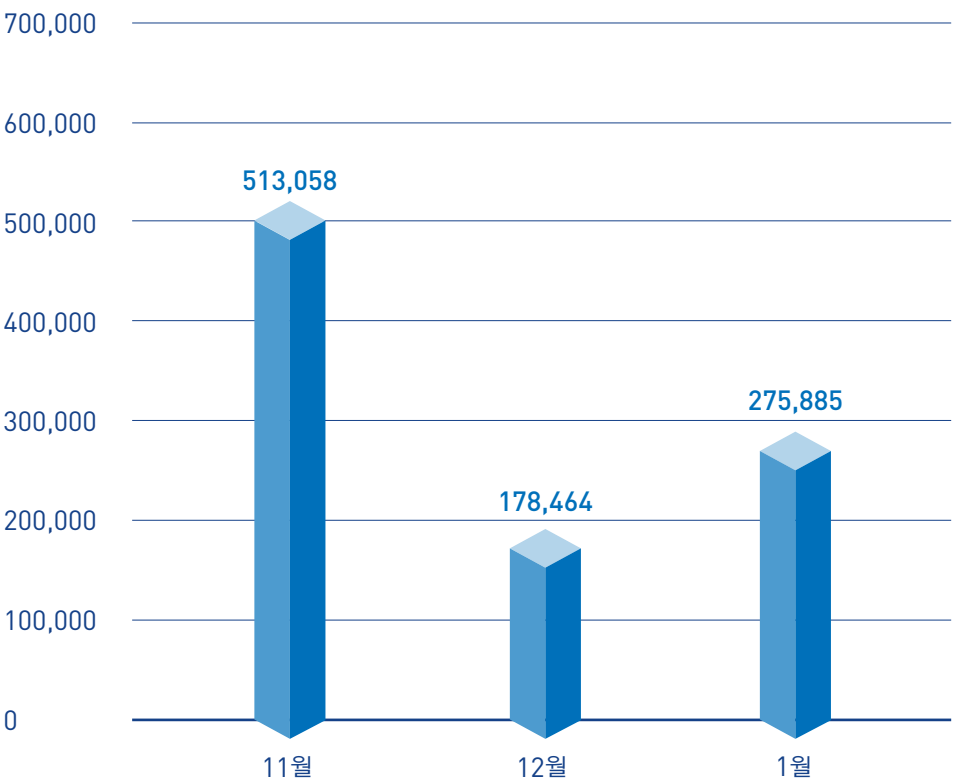


[그림 1-3] 악성코드 유포 도메인/URL 탐지 및 차단 건수(2015년 11월 ~ 2016년 1월)

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

03
모바일 통계

2016년 1월 한 달간 탐지된 모바일 악성코드는 27만 5,885건으로 나타났다.

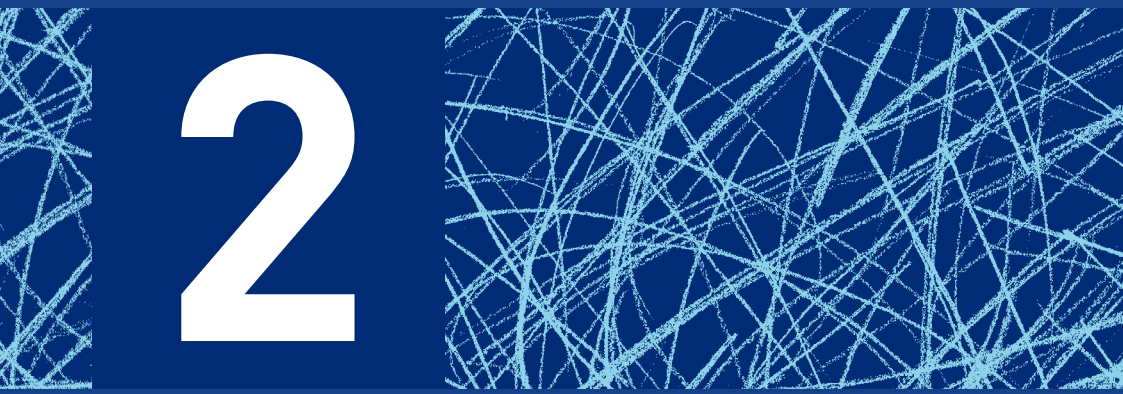


[그림 1-4] 모바일 악성코드 추이(2015년 11월 ~ 2016년 1월)

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

[표 1-2] 2016년 1월 유형별 모바일 악성코드 탐지 상위 10건

순위	악성코드 진단명	탐지 건수
1	Android-PUP/SmsReg	40,384
2	Android-PUP/SmsPay	35,866
3	Android-PUP/Noico	31,226
4	Android-Trojan/FakeInst	29,603
5	Android-Trojan/SmsSpy	9,151
6	Android-PUP/Chepa	8,621
7	Android-Trojan/Opfake	8,456
8	Android-PUP/Dowgin	7,519
9	Android-Trojan/Slocker	6,054
10	Android-Trojan/SmsSend	6,003



2

보안 이슈
SECURITY ISSUE

01 한국 이어 일본까지, 파밍 악성코드 확산

02 착신전환 노리는 안드로이드 악성 앱

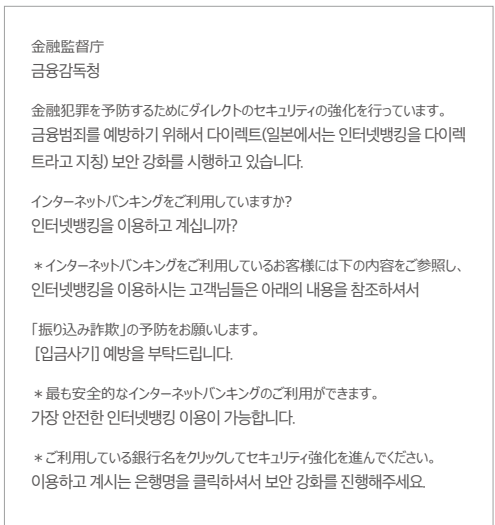
01 한국 이어 일본까지, 파밍 악성코드 확산

최근 일본의 주요 포털 사이트를 통해 일본 은행을 대상으로 하는 파밍 악성코드가 유포되었다. 일본에서 파밍 악성코드는 이미 보고된 바 있지만, 이번에 발견된 악성코드는 기존에 국내에서 유포된 파밍 악성코드와 연관성이 있는 것으로 확인됐다. 이로써 특정 그룹이 공격 대상으로 국내와 일본을 가리지 않고 악성코드를 제작하고 있는 것으로 추측된다. 관련 내용을 살펴보자.



그림 2-1 | 포털 사이트 접속 시 팝업창 발생 화면

해당 파밍 악성코드에 감염되면 [그림 2-1]과 같이 일본어로 된 팝업창이 발생하며, 상세 내용은 [그림 2-2]와 같다.



金融監督庁
금융감독청

金融犯罪を予防するためにダイレクトのセキュリティの強化を行っています。
금융범죄를 예방하기 위해서 다이렉트(일본에서는 인터넷뱅킹을 다이렉트라고 지칭) 보안 강화를 시행하고 있습니다.

インターネットバンキングをご利用していますか?
인터넷뱅킹을 이용하고 계십니까?

＊インターネットバンキングをご利用しているお客様には下の内容をご参照し、
인터넷뱅킹을 이용하시는 고객님들은 아래의 내용을 참조하셔서

「振り込み詐欺」の予防をお願いします。
[입금사기] 예방을 부탁드립니다.

＊最も安全的なインターネットバンキングのご利用ができます。
가장 안전한 인터넷뱅킹 이용이 가능합니다.

＊ご利用している銀行名をクリックしてセキュリティ強化を進んでください。
이용하고 계시는 은행명을 클릭하셔서 보안 강화를 진행해주세요.

그림 2-2 | 팝업창 상세 내용

팝업창의 내용을 보면, 은행 사칭 사이트로 연결을 유도하는 국내에서의 파밍 기법과 유사한 것을 확인할 수 있다. 상단의 로고 또한 금융감독원의 로고를 그대로 사용하고 있다. 팝업창에 연결되어 있는 은행 사칭 사이트로 접속하면, [그림 2-3]과 같이 각 사이트 별로 비밀번호, 사용자 계정 정보, 인증값 등의 금융 정보 입력을 요구하는 화면이 나타난다.

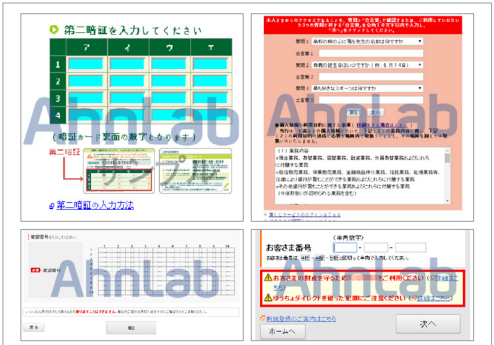


그림 2-3 | 은행 사이트별 금융 정보 입력 화면

이때 사용자가 금융 정보를 입력하면 [그림 2-4]와 같이 패킷을 통해 입력한 정보를 전송하는 것을 확인할 수 있다.

```
...t]....[....]....'.:POST /login/act/step2.php HTTP/1.1
Host:
Connection: Keep-alive
Content-Length: 223
Accept: application/json, text/javascript, */*; q=0.01
Origin:
X-Requested-with: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/47.0.2526.106 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: ko,en-US;q=0.8,en;q=0.6,ja;q=0.4
Cookie: fontStyle=undefined; s_cc=true; s_v1=[CS]v1|2B3E211E052AA01D-60000301A009F74(
[CE]; s_ppv1=http%253A%2F%                F52C%2C100%2C36%2C935%2C1920%2C
2C1080%2C1%2CP; s_fid=F78A33C2A9363B3-3AC11993F42B09FD; s_ppn=http%3A%2F%
2Fwww.                %2F; s_nr=1450984292389-New; s_pr3e=http%3A%2F%2F                ;
s_sq=                %3D%2526pid%253Dhttp%25253A%25252F%2525                %25252F%2526pidt%
253D1%2526odt%253Dhttp%25253A%25252F%2525                32flogin%25252Findex.php
2526ot%253DA; s_ppv=http%253A%2F%2Fw                %2F%2C100%2C36%2C2579%2C1920%2C892%
2C1920%2C1080%2C1%2CP; PHPSESSID=630ed6c288c2035e3a92019461d2c18

code%5B%5D=12&code%5B%5D=12&code%5B%5D=11&code%5B%5D=31&code%5B%
5D=12&code%5B%5D=45&code%5B%5D=11&code%5B%5D=12&code%5B%5D=46&code%5B%5D=11&code%5B%
5D=56&code%5B%5D=12&code%5B%5D=56&code%5B%5D=11&code%5B%5D=51HTTP/1.1 200 OK
```

```
POST /login/act/step3.php HTTP/1.1
Host:
Connection: Keep-alive
Content-Length: 557
Accept: application/json, text/javascript, */*
Origin: ht                :0
X-Requested-with: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/46.0.2490.86 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://                /login/question.php
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: PHPSESSID=3d2d446982aa641f7457626ade6fde8e;
LSESSIONID=jld1o64254gucc1KJxgg2D0LpF2Spn7cUO6kEXavFtPXO8UvMSB2Ss%3D;
___5043654=eyJzZCI6InVyWCWrZ5IGeyJUIjozLCJhIjpbW3siYiI6INSJ0VxOsInJbZCI6MC4yNzA4MTYy
MjkyODM4MDk2NnI9
question%5B%5D=%E9%AB%98%E6%A0%A1%E3%81%AE%E6%99%82%E3%81%AE%E5%BF%83%E3%81%AB%E6%AE%8B
%E3%82%8B%E5%85%88%E7%94%9F%E3%81%AE%E5%90%8D%E5%89%8D%E3%81%AF%E4%BD%95%E3%81%A7%E3%
81%99%E3%81%8B&question%5B%5D=%E6%AF%8D%E8%AA%9E%E3%81%AE%E8%A9%B1%E7%94%9F%E6%97%A5%
E3%81%AF%E3%81%84%E3%81%A4%E3%81%A7%E3%81%99%E3%81%8B+(+%E4%BE%8B+%3A+5+%E6%9C%88+1+4%
E6%97%A5%EF%BC%89&question%5B%5D=%E6%9C%80%E3%82%82%E5%A5%BD%E3%81%8D%E3%81%AA%E3%82%
B9%E3%83%9D%E3%83%BC%E3%83%84%E3%81%AF%E4%BD%95%E3%81%A7%E3%81%99%E3%81%8B&answer%5B%
5D=teo&answer%5B%5D=1010&answer%5B%5D=soccerHTTP/1.1 200 OK
```

그림 2-4 | 입력한 정보를 전송하는 패킷

이번 사례에서 발견된 일본의 파밍 악성코드는 국내에서 발견된 파밍 악성코드와 매우 유사하다. 유명 포털 사이트를 통해 은행 사칭 사이트로 연결을 유도하는 국내의 파밍 기법처럼 일본에서도 가장 많이 접속하는 포털 사이트를 통해서 은행 사칭 사이트로 접속하도록 하는 기법이 이용됐다. 현재 해당 악성코드를 유포한 유포지에서는 국내 은행을 대상으로 한 파밍 악성코드를 또 다시 유포하고 있다. 또한 해당 도메인은 과거에 PUP를 통한 악성코드 유포에 이용된 적이 있는 것으로 확인됐으므로 이에 따른 국내 사용자들의 각별한 주의가 필요하다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Agent (2015.12.25.08)

02
착신전환 노리는 안드로이드 악성 앱

안드로이드 폰을 겨냥한 해커들의 공격이 계속되면서 그 수법이 점점 고도화되고 있다. 이번에 발견된 안드로이드 악성코드는 사용자들이 모르는 사이에 스마트폰에 걸려온 전화가 다른 번호로 착신전환되도록 조작하고 있어 이에 따른 사용자들의 주의가 필요하다.

다음 사례는 안드로이드 악성 앱이 플래시 플레이어 프로그램( )으로 위장하고 있는 경우다. 설치 과정부터 면밀히 살펴보자. 해당 앱은 [그림 2-5]에서 보이는 것과 같이 설치 시에 메시지 접근 및 전송, 전화번호 자동 연결 등을 수행할 권한을 부여받는다.

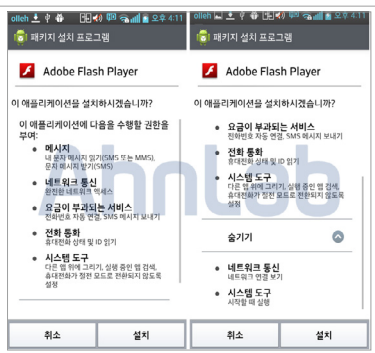


그림 2-5 | 악성 앱 설치 과정 (1)

악성 앱 설치가 완료되면 플래시 플레이어와 동일한 아이콘이 생성되며, 해당 앱을 실행하면 아이콘은 삭제된다. 이 때 겉으로는 아이콘이 삭제되어 앱이 삭제된 것처럼 보이지만, 실제로는 스마트폰 내부적으로 동작하고 있다. 이후 악성 앱은 휴대폰 관리자 권한을 획득하기 위하여 [그림 2-6]과 같이 사용자에게 활성화를 요구한다.

최근 발견되는 대다수의 악성 안드로이드 앱은 이처럼 휴대폰 관리자 권한을 요구한다. 하지만 사용자가 이를 한 번 활성화한 이후 다시 원래 상태로 돌아가는 것은 어렵다. 그 이유는 악성 앱이 스스로를 보호하기 위해 활성화를 해제하지 못하도록 방해하기 때문이다. 사용자가 활성화 해제를 시도하면, 스마트폰이 다른 화면으로 넘어가지 않고 활성화 화면만 팝업되도록 설계되어 있다.



그림 2-6 | 악성 앱 설치 과정 (2)

휴대폰 관리자 활성화까지 마친 악성 앱이 동작하면, 스마트폰의 여러 가지 정보를 우선 수집하여 특정 서버로 전송한다.

- 스마트폰 전화번호
- 국가 정보
- IMEI(국제 단말기 식별 번호)
- 스마트폰 모델명
- 설치되어 있는 앱의 패키지명
- 스마트폰 운영체제 버전 정보
- 스마트폰에 저장된 메시지 내용(받은 날짜, 받은 내용, 보낸 사람 전화번호)

악성 앱의 APK 파일을 디컴파일하여 내부 코드를 살펴보면 [그림 2-7]과 같이 스마트폰 정보를 탈취하고 이를 전송하도록 설계되어 있는 것을 확인할 수 있다. Sender 및 MessagesContentSender 등의 클래스를 이용하여 스마트폰 정보를 수집한 다음 hxxp://5ynxwc4k4gw44an.biz:8448 서버로 전송한다.

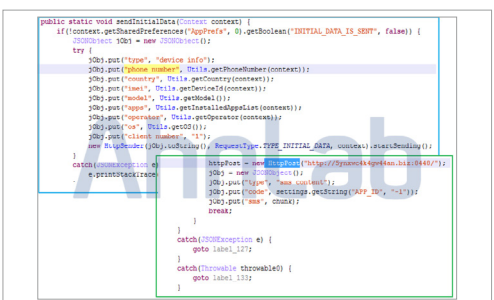


그림 2-7 | 스마트폰 정보를 탈취하고 전송하는 코드 일부

탈취한 정보를 서버로 전송하는 것 이외에도 해당 악성 앱에는 명령을 받아 착신전환 서비스를 실행하는 코드가 존재한다. 서비스 코드의 명령은 다음과 같다.

- *21*전환대상 번호# // 착신전환 설정
- #21# // 착신전환 해제



그림 2-8 | 착신전환 코드 일부

이러한 서비스 코드는 아시아 태평양 지역에서 사용되고 있는 것으로 알려져 있다. 하지만 국내에서는 착신전환 서비스가 유료 서비스로 차단돼 있으므로, 악성 앱에서 사용하는 서비스 코드가 동작할 수 없다. 또한 국내에서는 '*21'이 아닌 '*71' 서비스 코드를 주로 이용하고 있다.

실제로 악성 앱에서 하드코딩된 서비스 코드 '*21'을 사용하면 국내 스마트폰에서는 [그림 2-9]와 같은 오류가 발생한다.



그림 2-9 | 국내 스마트폰의 서비스 코드 오류 화면

한편, 해외 스마트폰에서 서비스 코드를 입력하면 [그림 2-10]과 같이 착신전환 성공 메시지를 확인할 수 있다.

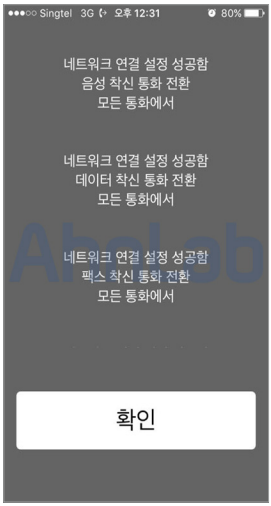


그림 2-10 | 해외 스마트폰에서 서비스 코드 입력 성공 화면

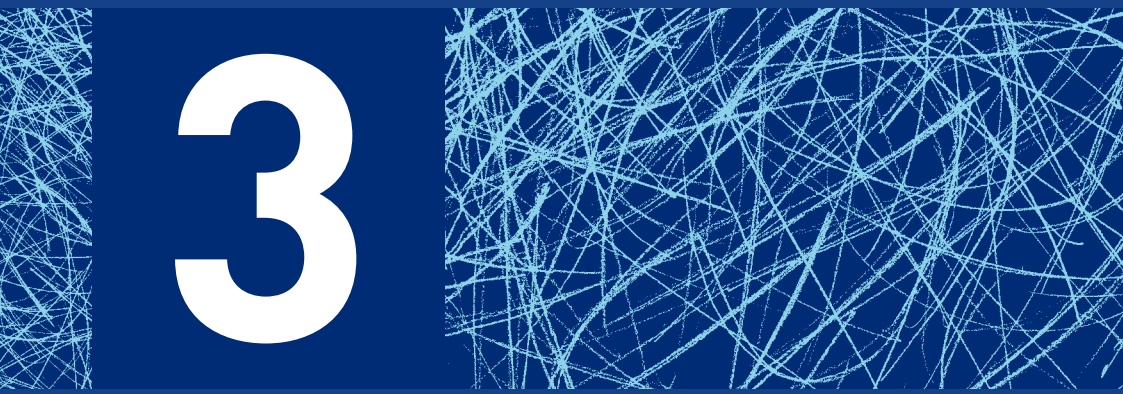
위 사례에서 볼 수 있듯 사용자가 다운로드한 악성 안드로이드 앱은 사용자 모르게 스마트폰을 다른 번호로 착신전환시킬 수 있다. 문제는 이와 같은 악성 행위가 착신전환에서 끝나는 것이 아니라, 더 나아가 착신전환 기능을 악용한 각종 금융 범죄로 발전될 수 있다는 점이다. 착신전환된 전화로 인증서를 발급하거나, OTP 인증 등 금융 거래에 필요한 인증 절차를 우회하여 추가 피해를 발생시킬 것으로 추정되므로 사용자의 각별한 주의가 필요하다.

이와 같은 피해를 예방하기 위해서 앱은 공식 마켓에서 다운로드 받아 설치하는 것이 상대적으로 안전하지만, 공식 마켓에도 악성 앱이 등록되어 있을 수 있어 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 설치는 하지 않도록 주의해야 한다. 또한 세계 1위의 모바일 전용 보안 앱(V3 모바일 등)이나 스미싱 탐지 앱(안랩 안전한 문자 등)을 설치하고, 자동 업데이트 설정으로 항상 최신 엔진을 유지하여 보다안전한 스마트폰 환경을 만들어야 한다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Android-Trojan/Slocker



3

악성코드 상세 분석
ANALYSIS-IN-DEPTH

랜섬웨어 공격 기법의 다변화: 멀버타이징과 자바스크립트

랜섬웨어 공격 기법의 다변화: 멀버타이징과 자바스크립트

사례 1) 멀버타이징을 이용한 랜섬웨어

2016년에도 랜섬웨어 유포는 계속되고 있다. 랜섬웨어는 사용자 컴퓨터의 문서, 그림 파일 등을 암호화하여 돈을 요구하는 악성코드다. 최근에는 애드웨어를 이용한 멀버타이징(Malvertising) 기법, 스팸 메일을 이용한 기법 등 랜섬웨어의 유포 방식이 점차 다양해지고 있다.

먼저 멀버타이징을 이용한 공격 기법을 살펴보자. 멀버타이징(Malvertising)이란 악성코드(Malware)와 광고(Advertising)의 합성어다.

즉, 멀버타이징 공격 기법은 인터넷 사이트에 삽입되는 광고를 이용하여 악성코드를 유포하는 방법을 뜻한다. 이러한 랜섬웨어 유포 방법은 짧은 시간 동안 다수의 사용자에게 악성코드를 유포할 수 있으며, 광고 서비스에 삽입되어 있어 백신으로부터의 탐지 회피에도 용이하다는 점이 특징이다.

이번에 소개할 멀버타이징 사례에서는 불필요한 프로그램(Potentially Unwanted Program, PUP)에 의해 접속한 광고 서비스 사이트에 악성코드가 삽입되어 있는 형태다.

불필요한 프로그램(이하 PUP)은 유틸리티 소프트웨어나 불법 인증 프로그램을 설치할 경우 함께 설치되는데, [그림 3-1]에서는 날씨 정보 제공 프로그램으로 위장한 것을 확인할 수 있다.

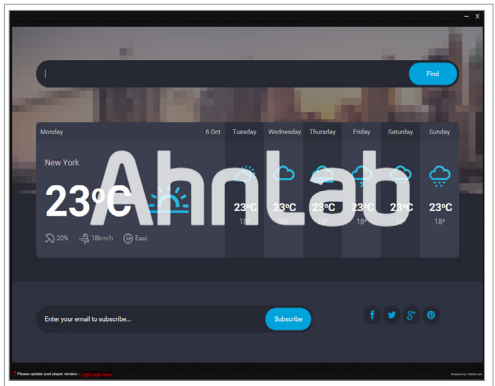


그림 3-1 | 날씨 정보 프로그램으로 위장한 불필요한 프로그램(PUP)

날씨 정보 프로그램으로 위장한 PUP는 다음 [표 3-1]과 같이 레지스트리 정보를 등록한다.

표 3-1 | 레지스트리 정보

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WindoWeather -> "C:\Program Files\WindoWeather\WindoWeather.exe" (시작프로그램 등록)

이후 [그림 3-2]에서 확인된 바와 같이 C&C 서버에 시스템의 정보(운영체제 정보, 네트워크 정보, 시스템

에 설치된 백신 제품 정보)를 전송한다.



그림 3-2 | C&C 서버에 전송되는 정보

C&C 서버와 통신이 완료되면, [그림 3-3]에서처럼 PUP가 명령 프롬프트를 통해 백그라운드 상태로 실행된다. 따라서 사용자는 PUP가 실행 중인 상태를 인지하기 어렵다.

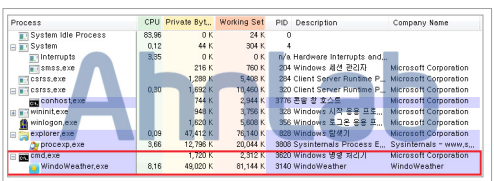


그림 3-3 | 명령 프롬프트 명령을 통해서 실행된 PUP

백그라운드 상태로 실행된 PUP는 다시 C&C 서버와 통신하여 광고 서비스를 위한 데이터 정보를 수신한다.



그림 3-4 | 광고 팝업창을 생성하기 위한 스크립트 정보

이후 사용자의 인터넷 브라우저 사용 여부를 확인하고, [표 3-2]의 명령어를 실행하여 해당 브라우저를 이용한 광고 팝업창을 생성한다.

표 3-2 | 광고 팝업창 생성 명령어

```
cmd /c start iexplore.exe "광고 사이트 Redirect URL"
cmd /c start iexplore.exe –noframemerging "광고 사이트 Redirect URL"
```

명령어가 실행되면 [그림 3-5]와 같이 다수의 팝업창이 동시에 생성되며, 이렇게 연결된 사이트에서는 또 다른 프로그램의 설치를 유도한다.



그림 3-5 | 생성된 광고 팝업창



그림 3-6 | 브라우저 프레임이 제거된 광고 팝업창

연결된 광고 사이트에는 다음 [표 3-3]과 같이 악성코드를 유포하는 사이트가 존재하는 것을 확인할 수 있다.

표 3-3 | 네트워크 연결 정보

www.adnet****per********.com/****cpm.php
-sa*****buy.com/l****r.html
-dsf.*********.net/?w3aKdriZJRnGC4A=l3SKfPrfJxzFGMS
Ub-nJDa9BMEXCRQLPh4SGhKrXCJ... (Exploit Kit)

또한 [그림 3-7]과 같이 접속한 사이트 내부에는 악성 스크립트가 삽입되어 있어, 만약 사용자의 시스템에 취약점이 존재할 경우 악성코드에 감염되게 된다.

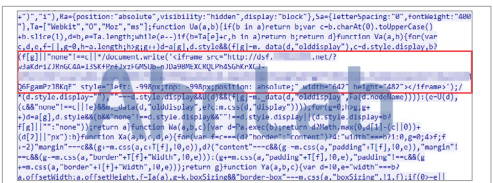


그림 3-7 | 사이트 내부에 삽입된 악성 스크립트



그림 3-8 | 랜섬웨어(TeslaCrypt 3.0) 경고창

랜섬웨어에 감염된 사용자의 PC에서는 [그림 3-8]과 같은 경고창을 확인할 수 있다. 이번 사례에서 확인한 PUP와 광고 서비스 사이트를 이용한 멀버타이징 기법은 사용자의 인터넷 환경에 깊숙히 침투해 있음을 알 수 있다. 또한 해당 기법은 악성코드가 광고 서비스에 삽입되어 있기 때문에 백신으로부터의 탐지를 회피할 수 있어 사용자의 각별한 주의가 필요하다.

따라서 평소 랜섬웨어 감염을 예방하기 위해서는 보안 업데이트(운영체제, 웹 브라우저, 자바, 플래시 플레이어)를 최신 버전으로 설치하여 드라이브-바이-다운로드(Drive-by-download) 공격을 방어하고, 불필요한 프로그램은 설치하지 않는 것을 권장한다. 또한 백신 제품의 엔진을 항상 최신으로 유지하는 사용자의 올바른 습관이 필요하다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

Trojan/Win32.Teslacrypt
Trojan/Win32.CryptoWall
Trojan/Win32.CryptoLocker
PUP/Win32.Amonetiz

사례 2) 자바스크립트를 이용한 랜섬웨어

랜섬웨어는 사용자 시스템의 파일을 암호화해서 정상적으로 사용하지 못하도록 하고 이를 빌미로 추적이 어려운 전자 화폐를 통한 금액 지불을 요구하는 악성코드다. 개인 및 기업을 막론하고 중요한 문서나 파

일이 암호화되었을 경우 치명적인 피해를 입을 수 있기 때문에 각별한 주의가 필요하다. 초창기 랜섬웨어는 스팸 메일에 실행 파일을 첨부한 형식으로 많이 유포되었으나, 최근에는 취약한 웹 사이트를 이용하거나 첨부 파일의 형식을 바꾸는 등 다양한 방법을 통해 유포가 이루어지고 있다. 이번에는 자바스크립트를 이용한 사례를 살펴보자.

1. 스팸 메일의 첨부 파일에 포함된 자바스크립트

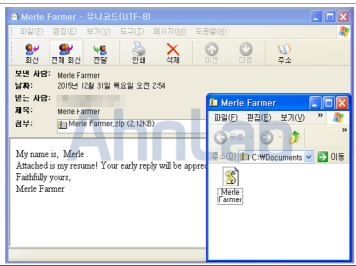


그림 3-9 | 스팸 메일에 첨부된 자바스크립트

스팸 메일을 통한 악성코드 유포가 빈번하게 이뤄짐에 따라 메일에 실행 파일이 첨부되어 있을 경우, 보안 장비나 애플리케이션에서 이를 사전에 경고하고 차단하는 시스템들이 많이 도입되었다. 이에 따라 랜섬웨어는 실행 파일을 스팸 메일에 첨부하는 방식을 벗어나 자바스크립트 파일을 통해 악성코드를 다운로드하도록 유포 방식을 변화했다.

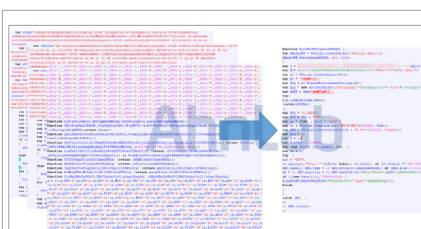


그림 3-10 | 난독화 스크립트

[그림 3-10]과 같이 스팸 메일에 첨부된 자바스크립트는 난독화되어 있다. 파일에 따라 유형은 조금씩 다르지만 해당 스크립트를 실행하면 추가 유포지에서 랜섬웨어를 다운로드하고 사용자 PC를 감염시켜 [그림 3-11]과 같은 화면을 출력한다.

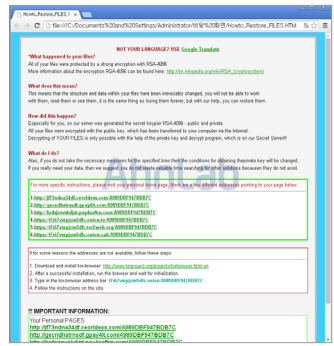


그림 3-11 | Teslacrypt 감염 화면

2. 자바스크립트 코드로 작성된 Ransom32

EMSISOFT에 의해 자바스크립트로 작성된 랜섬웨어, Ransom32가 공개되었다. 해당 악성코드는 윈도우 실행 파일(exe)로 보이나 사실은 [그림 3-12]와 같이 SFX(Self-extracting archive) 기능을 이용한 압축 파일이며, 실행 시 TEMP 경로에 자동으로 압축이 풀리고 내부 chrome.exe가 실행된다.

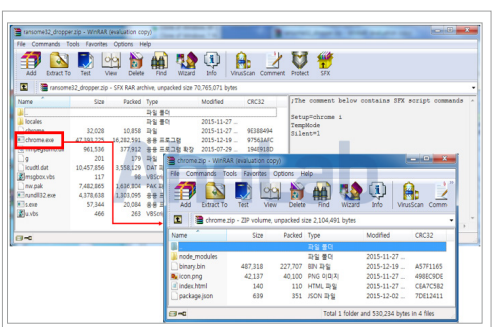


그림 3-12 | SFX로 압축된 랜섬웨어

chrome.exe는 NW.js를 이용하였으며, 내부에는 악성 행위에 필요한 파일들이 패키징되어 있다. NW.js는 HTML과 JavaScript를 이용한 애플리케이션 개발 프레임워크로, [그림 3-13]과 같이 index.html 파일을 통해 자바스크립트로 작성된 바이너리를 실행한다.

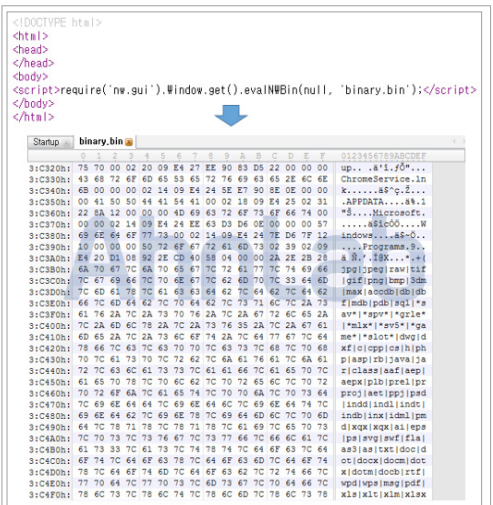


그림 3-13 | 자바스크립트 바이너리 실행

Ransom32가 암호화하는 데이터의 확장자는 [표 3-4]와 같다.

표 3-4 | 감염 확장자

jpg|jpeg|raw|tif|gif|png|bmp|3dm|max|accdb|db|dbf|mdb|pdb|sql|*sav*|*spv*|*grle*|*mlx*|*sv5*|*game*|*slot*|dwg|dxf|c|cpp|cs|h|php|asp|rb|java|jar|class|aaf|aep|aepx|plb|prel|prproj|aet|ppj|psd|indd|indl|indt|indb|inx|idml|pmd|xqx|xqx|ai|eps|ps|svg|swf|fla|as3|as|txt|doc|dot|docx|docm|dotx|dotm|docb|rtf|wpd|wps|msg|pdf|xls|xlt|xlm|xlsx|xlsm|xltx|xltm|xlsb|xla|xlam|xll|xlw|ppt|pot|pps|pptx|pptm|potx|potm|ppam|ppsx|ppsm|sldx|sldm|wav|mp3|aif|iff|m3u|m4u|mid|mpa|wma|ra|avi|mov|mp4|3gp|mpeg|3g2|asf|asx|flv|mpg|wmv|vob|m3u8|csv|efx|sdf|vcf|xml|ses|dat

Ransom32에 감염된 사용자 PC에서는 [그림 3-14]와 같은 화면을 확인할 수 있다.

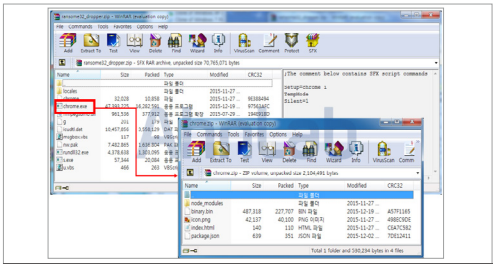


그림 3-14 | Ransom32 감염 화면

이처럼 불특정 다수를 대상으로 한 랜섬웨어의 공격은 2016년에도 지속될 것으로 보이며, 더욱 고도화될 것으로 예측된다. 더 나아가 랜섬웨어의 공격 범위는 PC를 넘어 스마트폰, 웨어러블 기기 등으로 점차 확대되어 사용자들을 위협할 전망이다. 또한 암호화 알고리즘을 사용하여 데이터를 암호화하기 때문에 복구 키를 알지 못하면 사실상 데이터 복구가 불가능하다. 따라서 랜섬웨어에 대한 위협을 완전히 벗어나기 위해서는 최신 백신을 유지하는 것 이외에도 보안 의식 강화를 통한 중요 데이터의 백업이 중요하다.

V3 제품에서는 해당 악성코드를 다음과 같이 진단하고 있다.

<V3 제품군의 진단명>

JS/Downloader (2015.12.31.08)
JS/Downloader (2015.12.31.08)
JS/Downloader (2015.11.06.06)
Trojan/Win32.Teslacrypt (2015.12.18.03)
Trojan/Win32.Ransom32 (2016.01.06.01)
Dropper/Win32.Ransom32 (2016.01.06.00)

AhnLab

ASEC REPORT

VOL.73
January, 2016

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

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.

© 2016 AhnLab, Inc. All rights reserved.