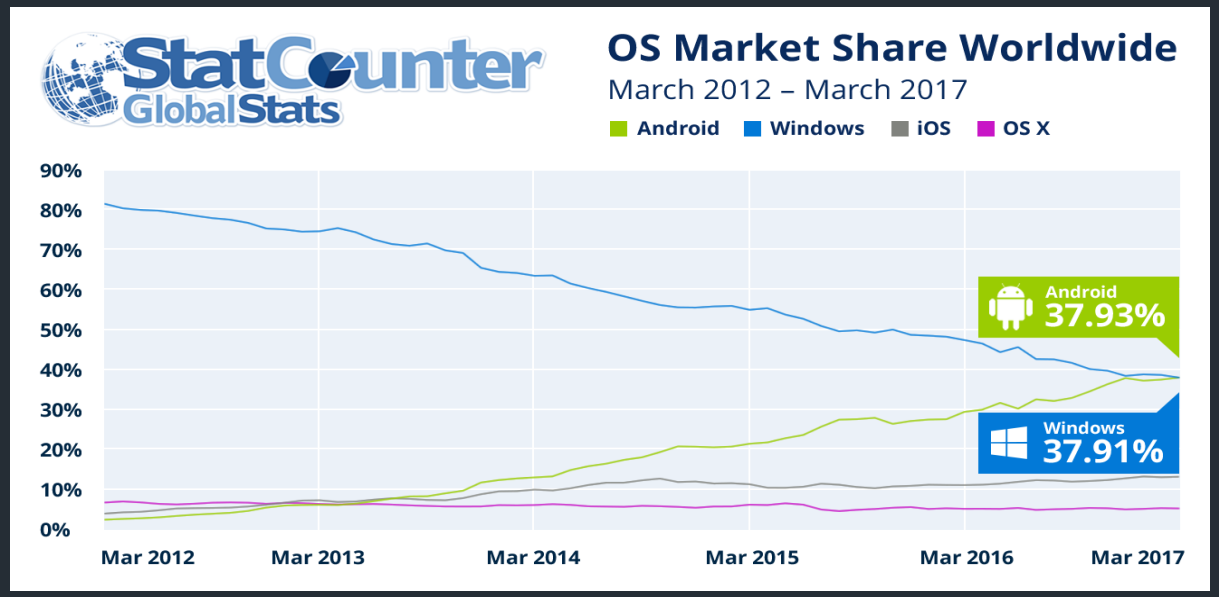
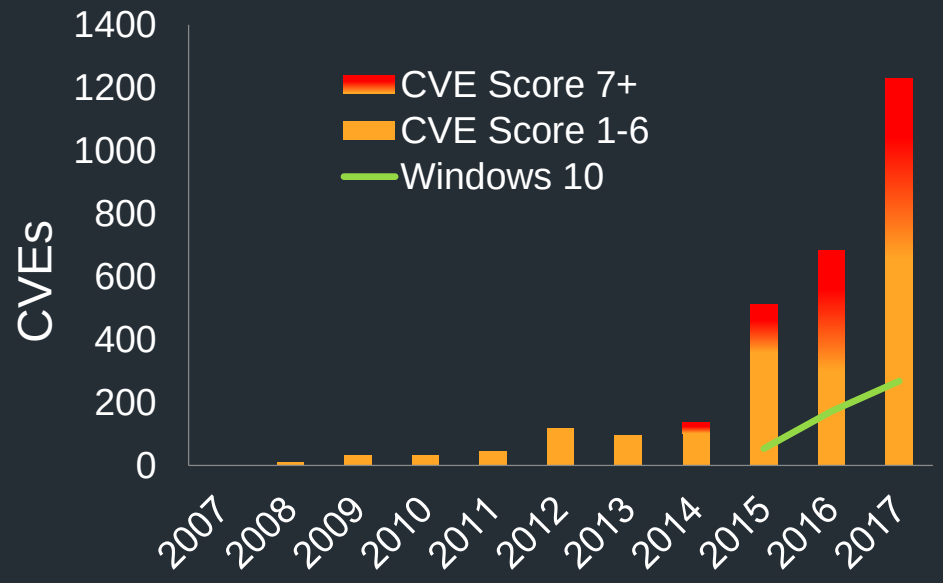
모바일을 향한 실제 위협 및 대응 방안

엔시큐어㈜
손장군 이사 (sohn.jg@ensecure.co.kr)

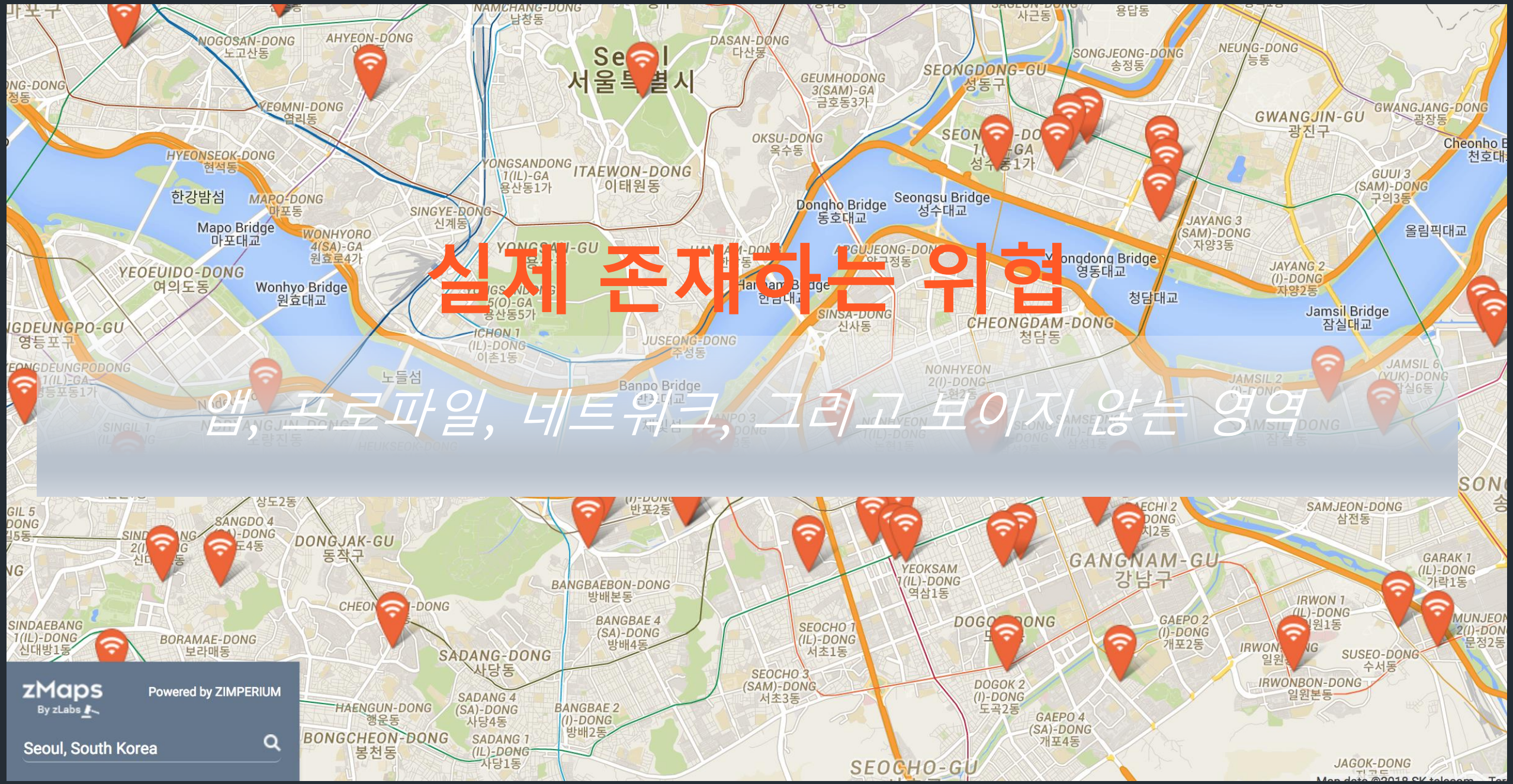
2019.06.13

증가하는 모바일 사용 → 취약한 모바일 OS





Source: CVE.Mitre.org.
CVEDetails.com: Android and iOS CVEs


실제 존재하는 위협
앱, 프로파일, 네트워크, 그리고 보이지 않는 영역
zMaps
By zLabs
Powered by ZIMPERIUM
Seoul, South Korea

L6-7 – APPLICATION + PRESENTATION

Data

L5 – SESSION

Keys

L4 – TRANSPORT

Segment, Datagram

L3 – NETWORK

Packet

L2 – MAC / DATA LINK

Frame

L1 – PHSYICAL

Bit

APPS

- AV/Malware (Ransomware, Trojans, Adware, Spyware)
- Access Abuse (Unsecured Apps and Privacy Risk)
- Repackaged Apps
- 3rd Party Lib / Back Door
- Time Bombs
- Download & Execute

USER

- Social Engineering
- Lack of Security Awareness
- False sense of security

BROWSER, EMAIL

- Known Browser CVEs
- Attachments (PDF, DOC,XLS)
- Spear phishing Emails
- Session Hijacking
- Man In The Browser
- Fake SSL Certificates (SSL Decryption)
- SSL Stripping

MULTIMEDIA

- Stagefright (24 CVEs)
- 11+ Threat Vectors (MMS, Browser, Downloads, Email, Facebook App, Gallery, etc.)
- Ransomware

SMS, MMS

- Spear phishing SMS
- Malicious MMS
- Stagefright (24 CVEs)

CONTAINERS

- Unlocked Containers
- VPN, Micro VPN

RECON SCANS

- IPv4, IPv6 Scans
- TCP, UDP Scans
- ARP Scans

OS / KERNEL

- OS Exploits
- Kernel Exploits
- Malicious Profiles (iOS)
- Network Configuration Attacks (DNS, Proxy, Gateway)
- Over The Air (OTA) updates (like Swift Key)
- Remote Device Management
- Shared Lib Injection
- Persistent File System Modifications

WIFI

- Rogue AP
- ARP MITM
- ICMP Redirect
- ICMP Double Direct
- SSL Striping
- Session Hijacking
- Fake SSL Certificates

NFC, BLUETOOTH

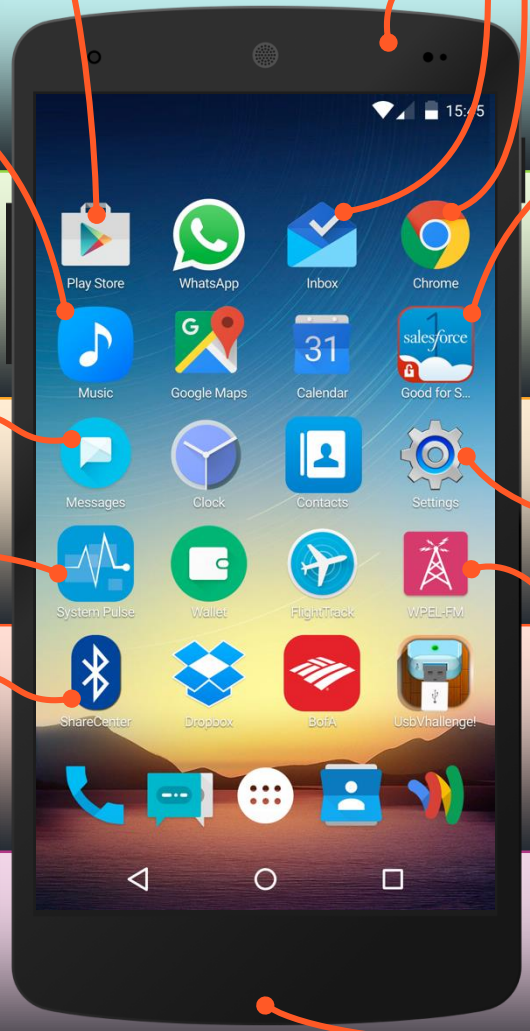
- NFC Proxy
- Malicious Bluetooth

RADIO

- Rogue Cell tower / Femtocell
- MITM
- Location Tracking

USB

- Malicious Chargers
- Juice Jacking
- Key Loggers
- Shared Lib Injection
- Unsecured Memory Cards



Application

Network

Device

안티바이러스로 충분 한가?

AV에서의 악성 앱 식별은 대부분 시그니처가 있어야 작동

This Dirty Cow Exploit found in Over 1,200 Android Apps

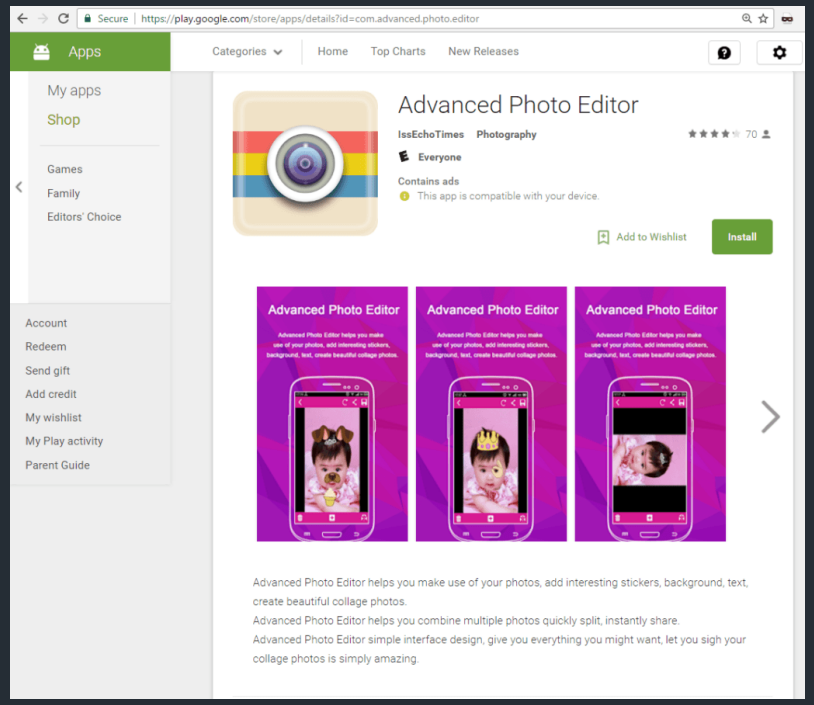
Security researchers from SfyLabs have now discovered a new Android banking Trojan that is being rented on many dark websites for $500 per month, SfyLabs' researcher Han Sahin told The Hacker News.

During the quarter, there were 5.68 million notifications about attempted malware infections to steal money from users via online access to bank accounts.

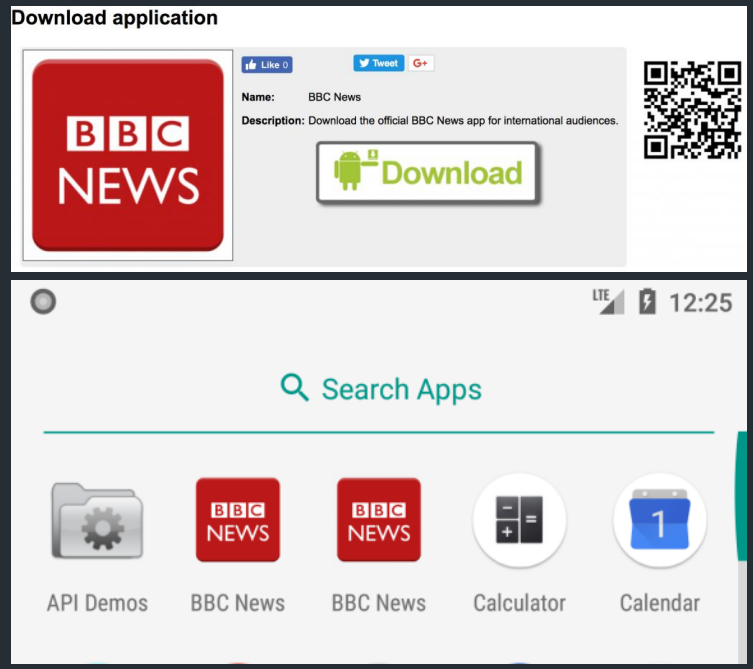
Between the two incidents, the malware family has been downloaded between 6 million and 21 million times, Check Point said citing Google Play data.

“사용자 교육”이 답인가??

많은 보안 전문가 들이 사용자에 대한 보안 교육을 통해 많은 문제가 감소 할 것이라 말하지만.....



공식 구글 앱 스토어의 Trojan.AndroidOS.Ztorg.bp



가짜 BBC 뉴스 앱 배포를 통한 공격

모바일 위협은 명확하고 대단히 위험

- 2017년 Apple과 Google은 보안 패치 수 발표[1]
- 2/3의 모바일 디바이스가 취약한 OS에서 작동[2]
- 10%의 디바이스가 “man-in-the-middle” 공격을 경험[2]
- 2019 년까지 모바일 악성 코드는 전체 악성 코드의 1/3에 달할 것[3]

1. CVE.Mitre.org. CVEDetails.com: Android and iOS CVEs
2. Zimperium Global Threat Intelligence, 3Q 2017
3. Market Guide for Mobile Threat Defense Solutions, Gartner, 22 August 2017, ID: G00314969

실존하는 타깃 공격들...

Russian rogue cell sites, spy drones target NATO troop smartphones, says report

- Moscow's smartphone campaign targeted at least 4,000 NATO troops in Eastern Europe, including U.S. soldiers, according to the Wall Street Journal.
- Russia wants troop numbers on NATO bases, and the hacking into soldiers' personal smartphones allows them to keep tabs on force strength.
- Drones with surveillance equipment as well as rogue access points on the ground give Russia the capability to track or hijack smartphones.

Jeff Daniels | @jeffdanielsca

Published 4:06 PM ET Wed, 4 Oct 2017 | Updated 4:42 PM ET Wed, 4 Oct 2017

CNBC

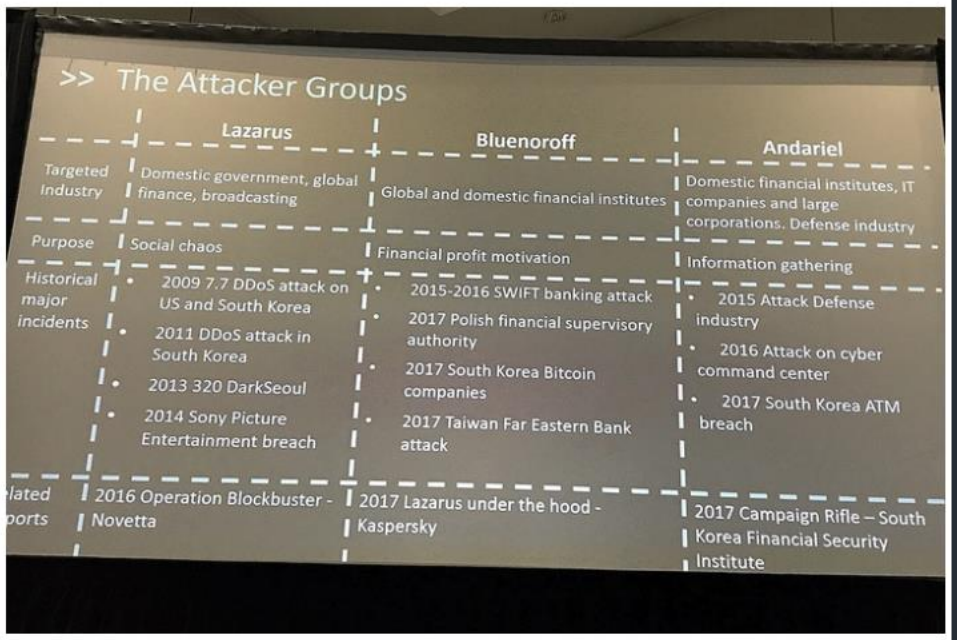
Petras Malukas | AFP | Getty Images

eWEEK

North Korea-Backed Lazarus Group Takes Aim at Android Security

By: Sean Michael Kerner | November 20, 2017

McAfee discovers new mobile malware that is linked to the same group that was behind the attack on Sony Pictures and the recent WannaCry ransomware worm.



모바일 위협

공격의 발판을 위한 목표

Device Attacks

표적 공격을 위한 주요 메커니즘

Network Attacks

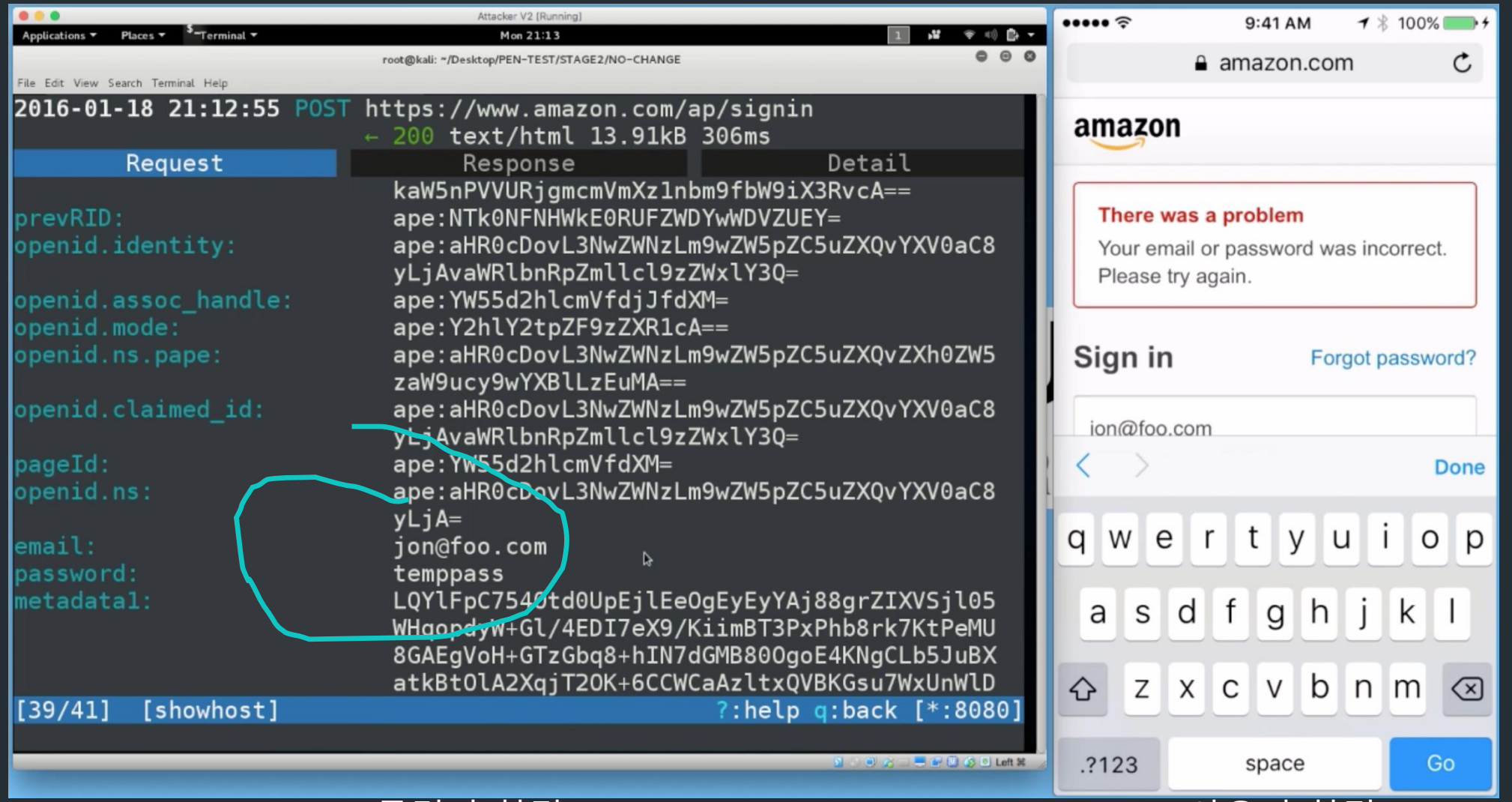
불특정 다수에 대한 악성코드 배포

Phishing Sites

불특정 다수에 대한 불법 광고 및 위협

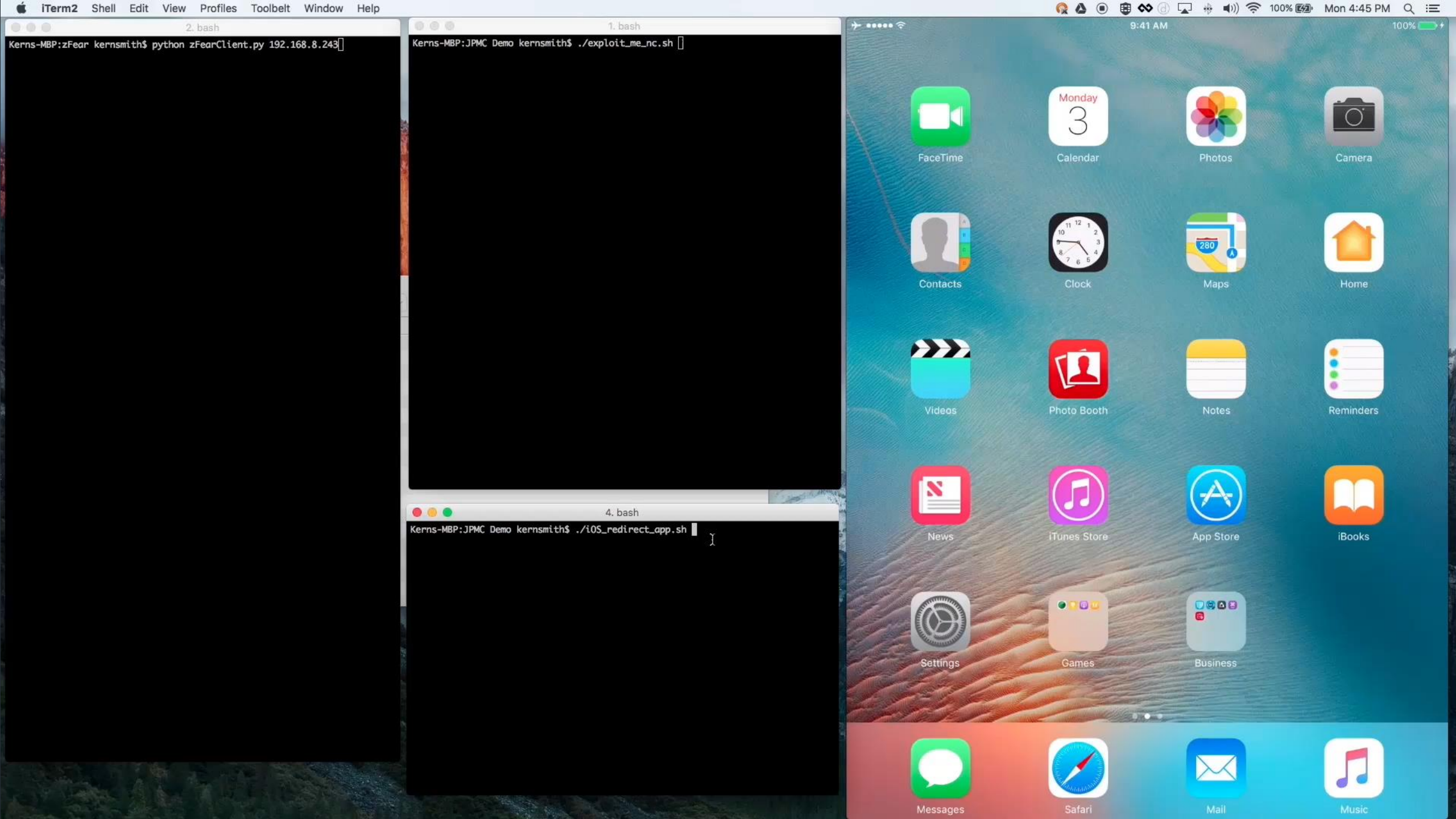
Malicious & Leaky Apps

네트워크 공격을 통한 장치 공격 (Man-in-the-Middle 예시) - 자격증명 탈취



공격자 화면

사용자 화면


iTerm2 Shell Edit View Profiles Toolbelt Window Help
100% Mon 4:45 PM
2. bash
Kerns-MBP:zFear kernsmith$ python zFearClient.py 192.168.8.243
1. bash
Kerns-MBP:JPMC Demo kernsmith$ ./exploit_me_nc.sh
4. bash
Kerns-MBP:JPMC Demo kernsmith$ ./iOS_redirect_app.sh
9:41 AM
100%
FaceTime
Calendar
Monday
3
Photos
Camera
Contacts
Clock
Maps
280
Home
Videos
Photo Booth
Notes
Reminders
News
iTunes Store
App Store
iBooks
Settings
Games
Business
Messages
Safari
Mail
Music

기기에 대한 공격은 앱에 대한 공격과 동일

(텔레그람 예 - 메모리를 통해 채팅 메시지보기)

User Screen

```
+ cache4.db
0031d30: 4f88 0568 8e24 b428 4305 c8d7 a2de a803  O..h.$.(C.......
0031d40: b836 810c aa16 f71a f942 cca8 6e2c 344f  .6.......B..n,40
```

```
+ 79a61000-79abb000.dump
0056cb0: 0908 046c 0808 0111 9881 f600 0000 0054  ...l...........T
0056cc0: ba91 14f8 5555 5500 0000 0092 cbfc ff00  ....UUU.........
0056cd0: 0000 00bf 7f6e 026d bcb1 9d44 8de7 0414  .....n.m...D....
0056ce0: 91ba 5404 576f 6f66 0000 0020 63ed 3d00  ..T.Woof... c.=.
0056cf0: 0000 00ff 58ff ffff ffff fff9 cb93 0b00  ....X...........
0056d00: 0609 0804 810c 0908 0111 9881 f600 0000  ................
0056d10: 0054 ba91 01f8 5555 5503 0000 0093 cbfc  .T....UUU.......
0056d20: ff00 0000 0044 8de7 046d bcb1 9dbf 7f6e  .....D...m.....n
0056d30: 0201 91ba 5416 4e6f 7453 6f45 6e63 7279  ....T.NotSoEncry
0056d40: 7074 6564 496e 4d65 6d6f 7279 0020 63ed  ptedInMemory. c.
0056d50: 3d00 0000 00ff 4bff ffff ffff fff9 cba8  =.....K.........
0056d60: 0a00 0609 0804 7408 0801 1198 81f6 0000  ......t.........
0056d70: 0000 54ba 8a38 f855 5555 0100 0000 a8cb  ..T..8.UUU......
0056d80: fcff 0000 0000 bf7f 6e02 6dbc b19d 448d  ........n.m...D.
0056d90: e704 388a ba54 0854 616d 6261 6c75 6c00  ..8..T.Tambalul.
0056da0: 0000 2063 ed3d 0000 0000 ff4b ffff ffff  .. c.=.....K....
0056db0: ffff f9cb a90a 0006 0908 0474 0908 0111  ...........t....
0056dc0: 9881 f600 0000 0054 ba8a 22f8 5555 5503  .......T.."UUU.
0056dd0: 0000 00a9 cbfc ff00 0000 0044 8de7 046d  ...........D...m
0056de0: bcb1 9dbf 7f6e 0222 8aba 5408 436f 6f6b  .....n."..T.Cook
0056df0: 6965 646f 0000 0020 63ed 3d00 0000 00ff  iedo... c.=.....
0056e00: 4bff ffff ffff fff9 cbaa 0a00 0609 0804  K...............
0056e10: 7409 0801 1198 81f6 0000 0000 54ba 8a1d  t...........T...
0056e20: f855 5555 0300 0000 aacb fcff 0000 0000  .UUU............
0056e30: 448d e704 6dbc b19d bf7f 6e02 1d8a ba54  D...m.....n....T
0056e40: 0953 686c 6f6f 6b69 646f 0000 2063 ed3d  .Shlookido.. c.=
0056e50: 0000 0000 ff47 ffff ffff ffff f9cb ab0a  .....G..........
0056e60: 0006 0908 046c 0808 0111 9881 f600 0000  .....l..........
0056e70: 0054 ba86 93f8 5555 5501 0000 00ab cbfc  .T....UUU.......
0056e80: ff00 0000 00bf 7f6e 026d bcb1 9d44 8de7  .......n.m...D..
0056e90: 0493 86ba 5404 5465 7874 0000 0020 63ed  ....T.Text... c.
```

```
0a 0006  mh.G..........
00 0054  ...l..........T
fc ff00  ....UUU.......
e7 0414  .....n.m...D....
ed 3d00  ..T.Woof... c.=.
93 0b00  ....X..........
00 0000  ................
93 cbfc  .T....UUU.......
bf 7f6e  .....D...m.....n
63 7279  ....T.NotSoEncry
20 63ed  ptedInMemory. c.
f9 cba8  =.....K.........
f6 0000  ......t.........
00 a8cb  ..T..8.UUU......
9d 448d  ........n.m...D.
75 6c00  ..8..T.Tambalul.
ff ffff  .. c.=.....K....
08 0111  ...........t....
55 5503  .......T.."UUU.
e7 046d  ...........D...m
6f 6f6b  .....n."..T.Cook
00 00ff  iedo... c.=.....
09 0804  K...............
ba 8a1d  t...........T...
00 0000  .UUU............
8a ba54  D...m.....n....T
63 ed3d  .Shlookido.. c.=
cb ab0a  .....G..........
00 0000  .....l..........
ab cbfc  .T....UUU.......
44 8de7  .......n.m...D..
20 63ed  ....T.Text... c.
f9 cbac  =.....K.........
```

Attacker Screen

해법은 존재 한다

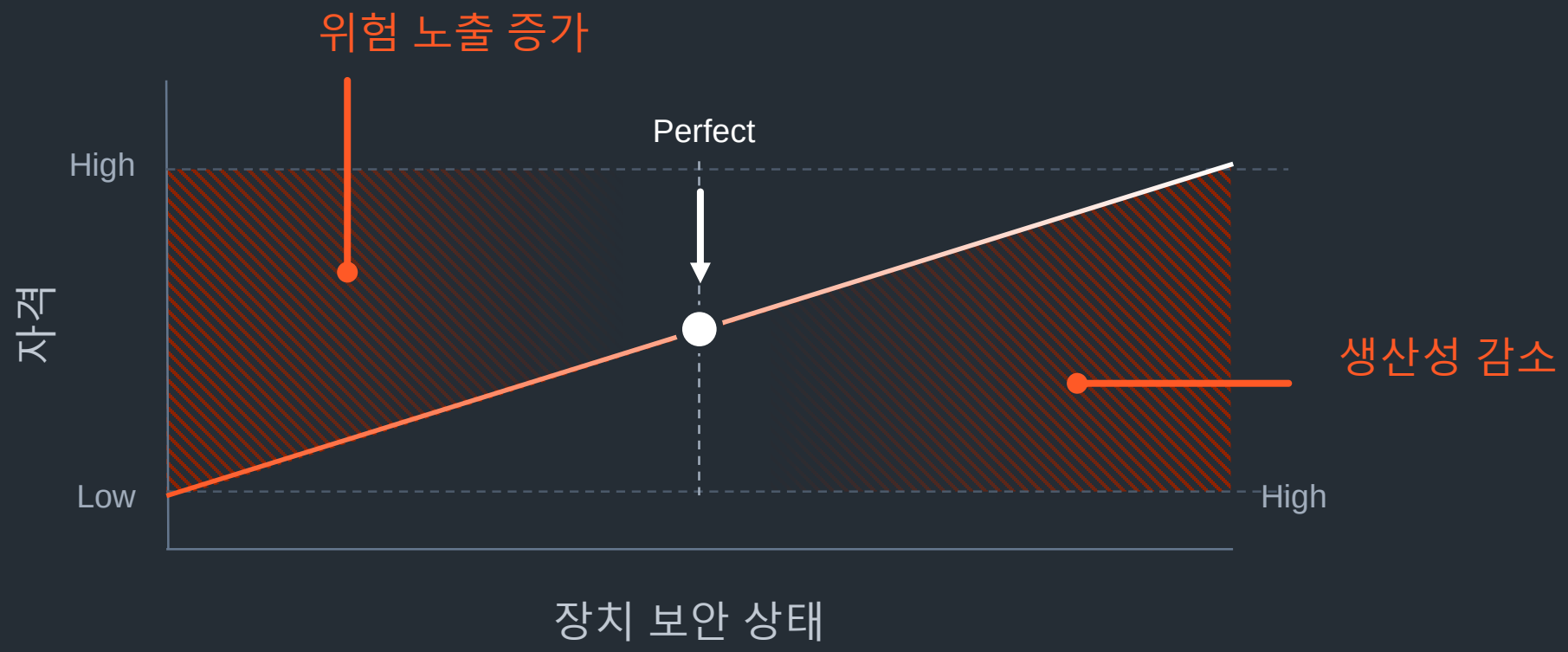
Mobile MTD

ZIMPERIUM®
MOBILE THREAT DEFENSE

두 가지 핵심 요소

1. *정책에 근거한 위협 관리*
2. *능동적 위협 방어*

1. 가용성과 보안성을 확보한 위협 관리



2. 능동적인 위협 방어

모바일을 위해 설계된 특허 받은 탐지 엔진

z9™ 탐지 엔진은 머신러닝을 통해 **실시간, 온디바이스** 로
알려지거나 알려지지 않은 모든 위협을 탐지 합니다.

Device Attacks

Network Attacks

Phishing Sites

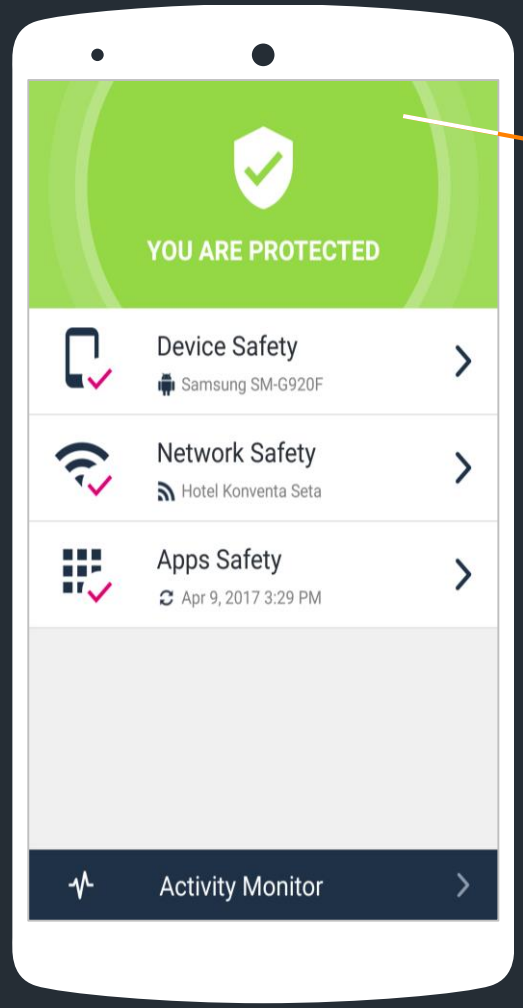
Malicious Apps

zIPS – 기업과 BYO 디바이스 보호

Always-on

제로데이 탐지

iOS & Android 지원



낮은 배터리, 메모리 소모

디바이스, 애플리케이션, 네트워크 보호

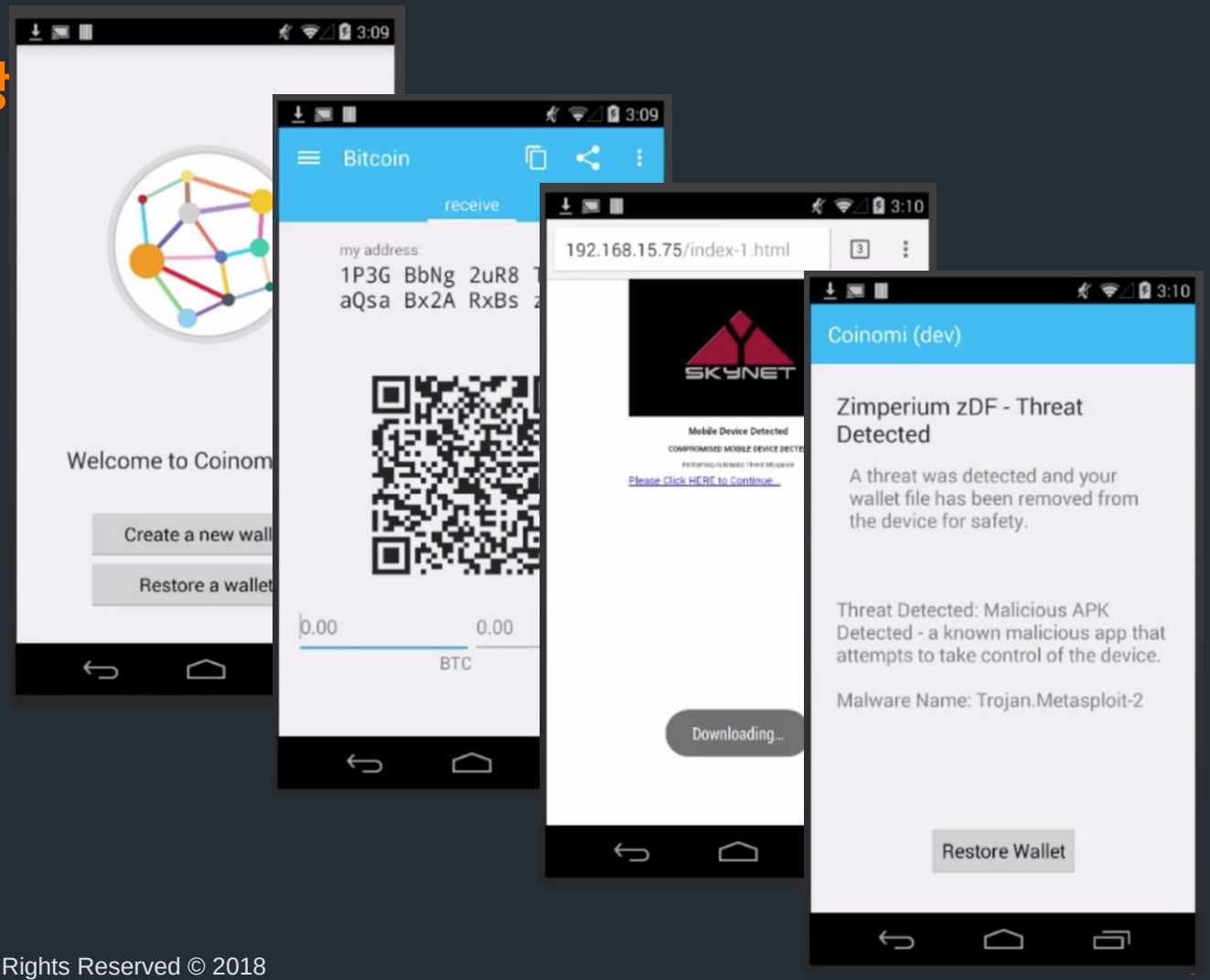
사용자 모드에서의 작동

zIAP – 인앱 보호

앱에 세계 정상급 보안을 구현하는 가장 빠른 방법

- Z9의 DNA 위협 검출 기능
- 일반적인 오용 탐지.

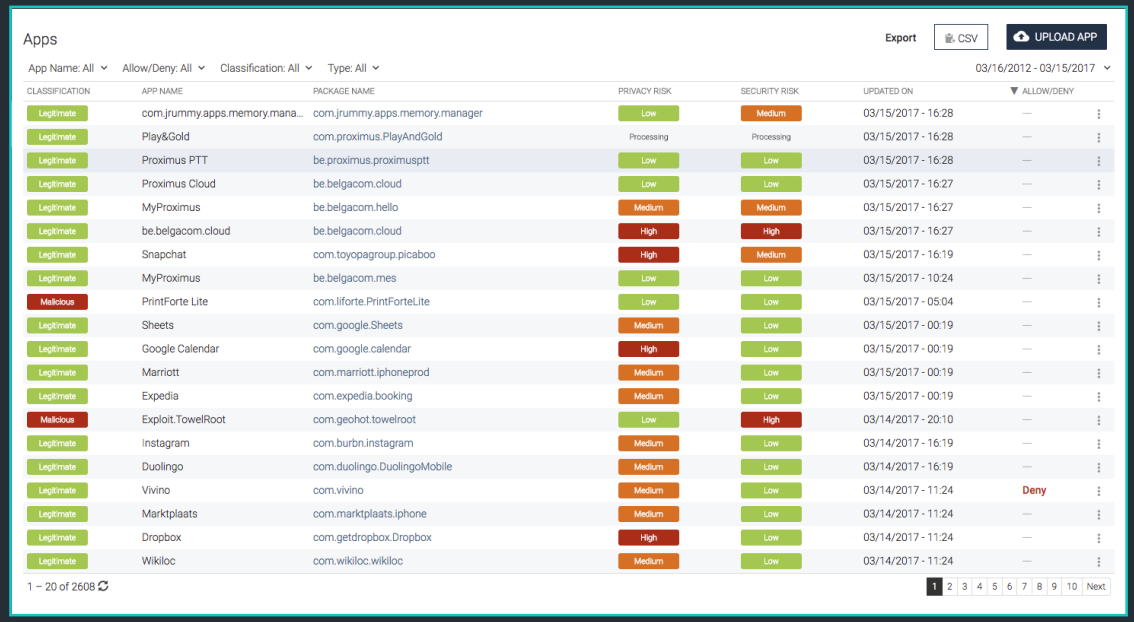
  예) 탈옥, 루팅 탐지
- 해커에 의한 정교한 공격 탐지 :
  - 데이터 탈취
  - 키스트로크 로깅
  - 네트워크 연결 하이제킹
  - 앱의 메모리와 파일 읽기
  - 프라이버시 위협



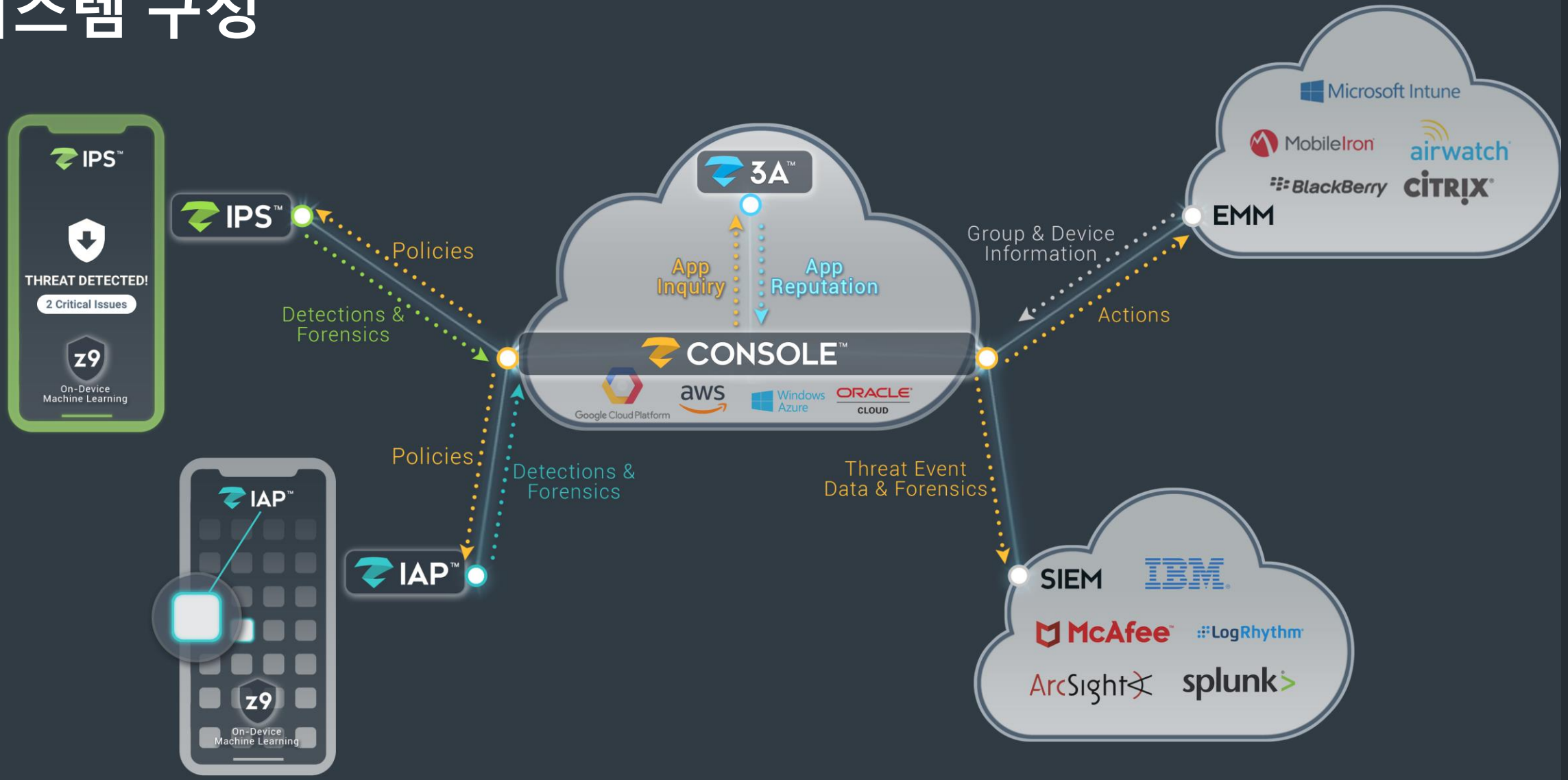
z3A™ – 고 수준 앱 분석

- 머신러닝과 인공지능을 통해 앱 분석
- 사용자에게 설치된 앱 또는 배포전 앱에 대한 보안과 프라이버시 위협 분석
- Android와 iOS 앱을 분석하는 고성능 클라우드
- 딥 앱 분석 및 포렌식
  - Content – 앱 코드
  - Intent – 앱이 수행하는 행동
  - Context – 도메인, 인증서, 공유코드, 네트워크 통신 등
- 명확하고 실행 가능한 정보
  - 앱 별 요약 및 상세 분석 보고서

z3A
Advanced App Analysis



시스템 구성



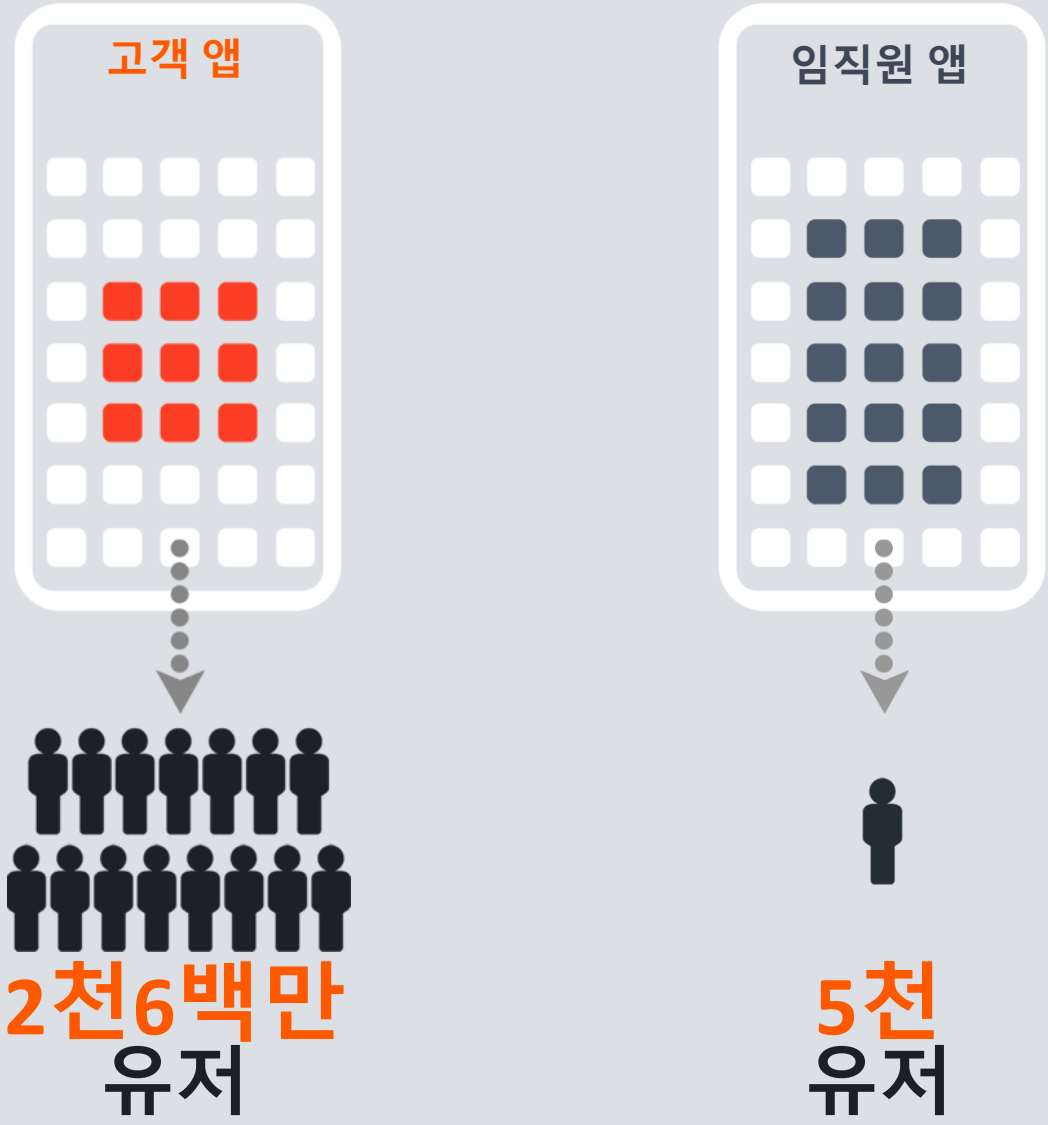
실제 사례

Mobile MTD

MTD 적용 30일 후

zIAP™

호주 대형 은행
모바일 앱



zIAP ™ 천만 단위의 디바이스 에서 천만 단위의 위협과 공격 탐지

900K
위협

1,433
NETWORKS

276K
DEVICES

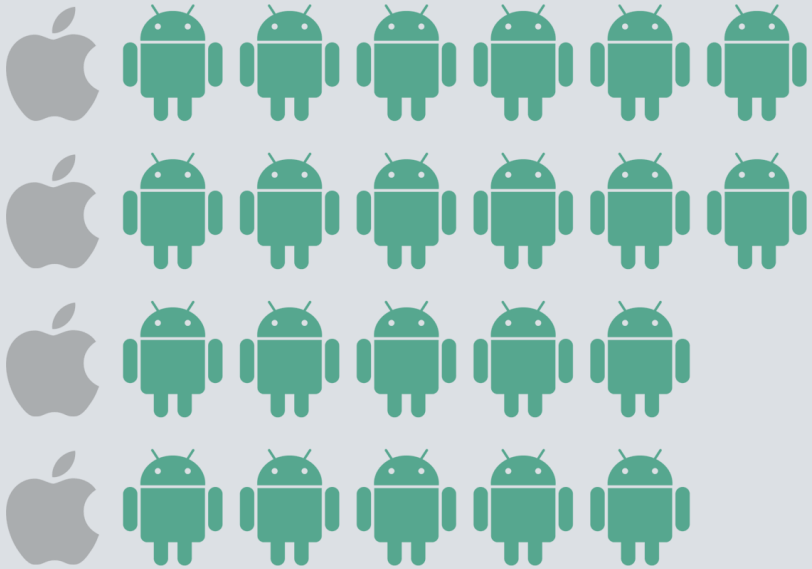
495K
DEVICES

166K
DEVICES

공격된
디바이스

4K

22K



2만6천

은행은 잠재적인 공격에 대한
가시성을 확보

$1.1 BILLION

계좌

80% 의 공격이 기기 손상을 목표로 함

사용자 기기에 대한 침해 위협

21,000

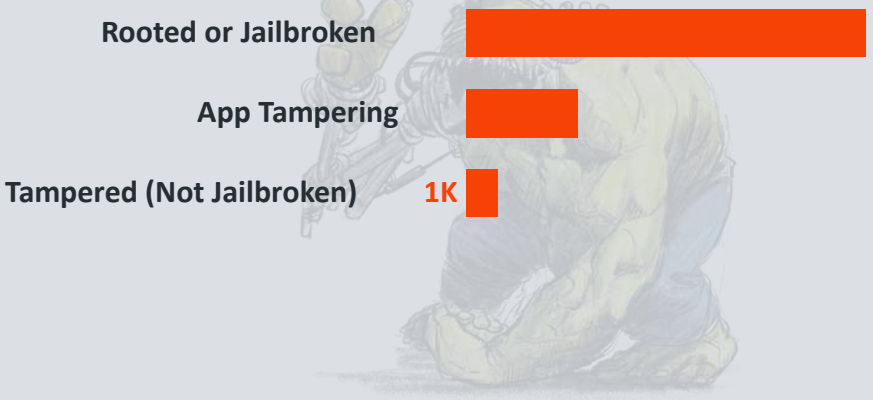
손상된 네트워크 위협

3,000

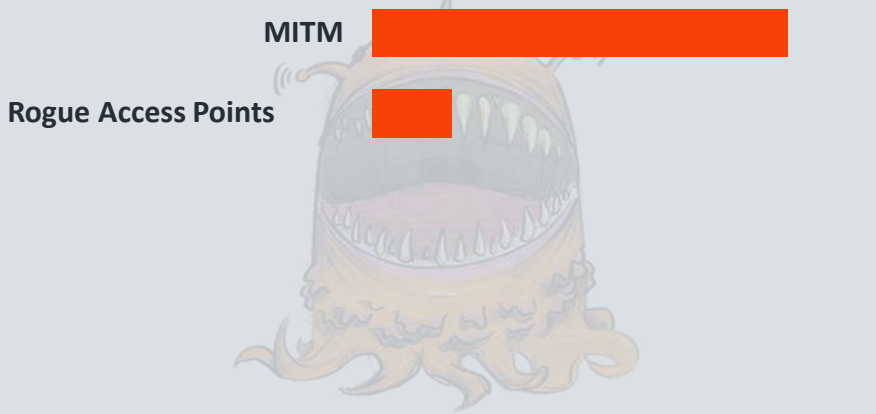
악성앱에 의한 위협

2,000

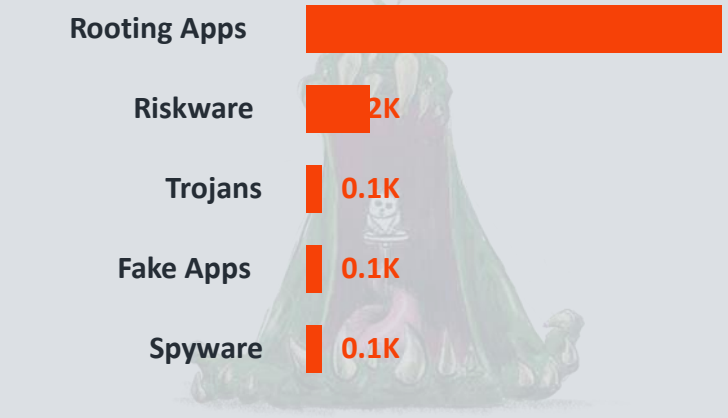
DEVICE ATTACKS



NETWORK ATTACKS



MALICIOUS APPS



감사합니다

https://www.ensecure.co.kr/