Review of Web and Mobile Threats

Presented by: Goh, Su Gim (Security Advisor, APAC)

Twitter: @sugimgoh

F-Secure


WE ARE
F-SECURE
F-Secure.

F-Secure.

OVER 26 YEARS OF DIGITAL SECURITY EXPERIENCE

F-Secure


F-Secure Labs Kuala Lumpur


TRESTON

250,000

Number of samples per day

F-Secure

9,000

Number of Android samples per day

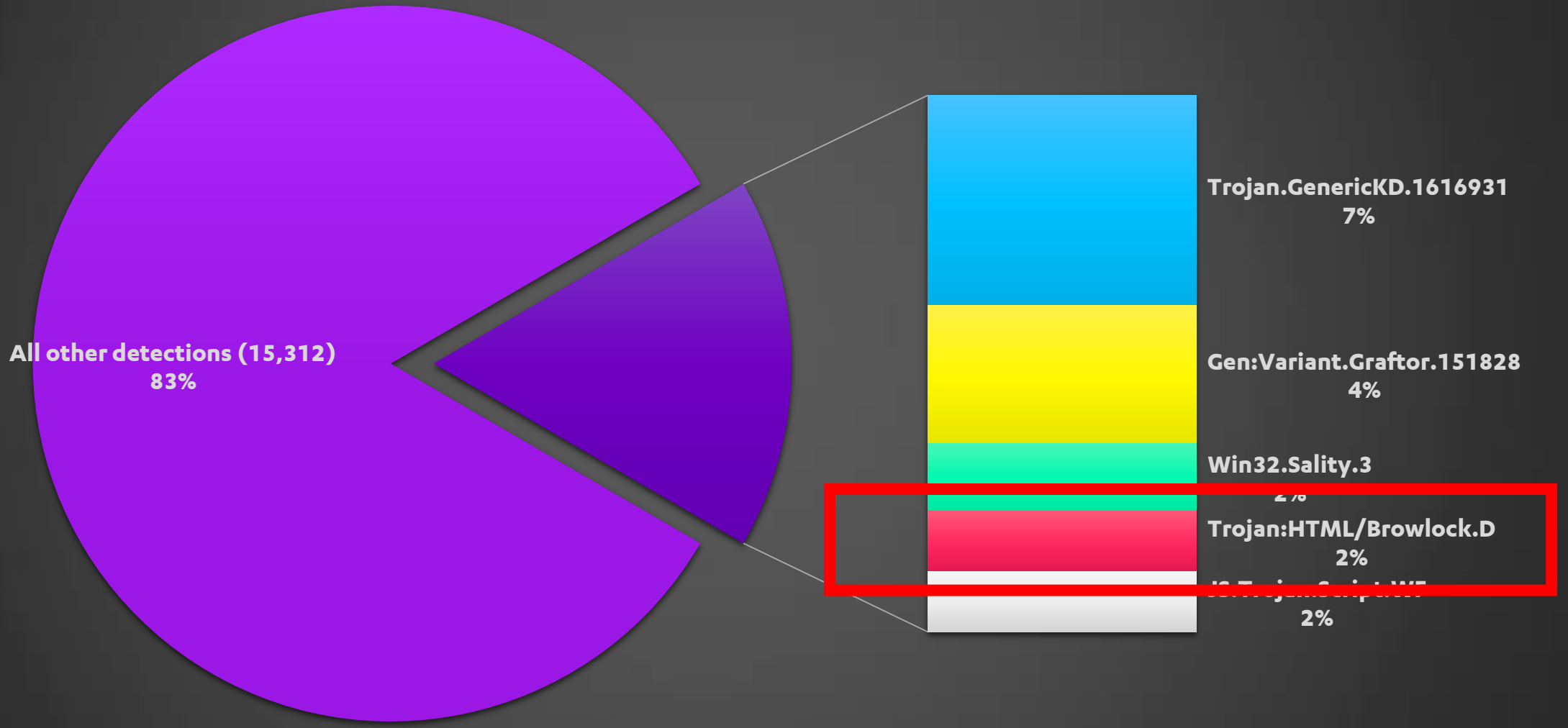
2,500,000,000

Online reputation queries per day

F-Secure

Hong Kong Threat Landscape 2014

Top 5 Malware Detections in Hong Kong 2014
(as % of all malware detections)



Police Themed Ransomware hits Hong Kong!

EUROPOL

EUROPEAN CYBERCRIME CENTRE

All activities of this computer have been recorded. All your file

Your IP:

[redacted]

COUNTRY	CITY
United Kingdom	Maidstone

REGION

England

All activities of this computer have been recorded.
All your files are encrypted.

ATTENTI

All your files are encrypted to prev
Due to violations of the law, your
because of at least one o

1. You have been subjected to violation of C
using or distributing copyrighted contents suc
found in your browser's temporary files and y
Section 8, Clause 8 of the Criminal Code of the
Article 1, Section 8, Cause 8 of the Criminal Co
or a deprivation of liberty of two to eight years.
2. You have been viewing or distributing pro
photos and such, were found in browser's tempo
Thus, you are violating article 202 of the Crimi
Criminal Code states a deprivation of liberty of f
3. Illegal access has been initiated from your
may be infected with malware, thus you are viol
Computer. Article 210 of the Criminal Code dec
of liberty of four to nine years.
Pursuant to the amendment of the Criminal Coc
infringement (if it is a first time offence) may be
fine.

To unlock your computer and avoid other legal
release fee of £200, payable through Ukash (you
the code). You can buy the card at any store or g

Find the nearest epay or payzone location.
Go to any location with a PayPoint or Payzone termina
Ask for Ukash: 200.00GBP (one voucher code)

Please note: Fine can only be paid within 12 hours
pay the fine is lost forever. All your PC data will be
initiated against you if the fine will not be paid!

Ukash available from Payzone terminals around UK

Use the store locator to find your nearest outlet

Exchange your money for a unique Ukash code

Use the code to pay fine.

Ukash It's eMoney.

Get Ukash wherever you see the Paypoint sign

Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

Royal Canadian Mounted Police

All activities of this computer have been recorded. All your files are encrypted.

Your IP:

[redacted]

COUNTRY	CITY
Canada	Montreal

REGION

Quebec

All activities of this computer have been recorded
All your files are encrypted.

ATTENTION!

All your files are encrypted to prevent their distribution and use.
Due to violations of the law, your browser has been blocked
because of at least one of the reasons below.

1. You have been subjected to violation of Copyright and Related Rights Law and illegally using or distributing copyrighted contents such as Video, Music or and Software (files were found in your browser's temporary files and your documents), thus conflicting with Article 1, Section 8, Clause 8 of the Criminal Code of the Canada.
Article 1, Section 8, Cause 8 of the Criminal Code states a fine or two hundred minimal wages or a deprivation of liberty of two to eight years.

2. You have been viewing or distributing prohibited Pornographic contents: Child Porno photos and such, were found in browser's temporary files and your documents.
Thus, you are violating article 202 of the Criminal Code of the Canada. Article 202 of the Criminal Code states a deprivation of liberty of four to twelve years.

3. Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected with malware, thus you are violating the law of Neglectful Use of your Personal Computer. Article 210 of the Criminal Code declares a fine of up to 50,000 CAD and/or deprivation of liberty of four to nine years.
Pursuant to the amendment of the Criminal Code of the Canada of May 28, 2011, this law infringement (if it is a first time offence) may be considered as conditional in case you pay the fine.

To unlock your computer and avoid other legal consequences, you are obliged to pay a release fee of 150 CAD, payable through Ukash (you must purchase the Ukash card and enter the code). You can buy the card at many stores or gas stations, nationwide.

Find the nearest Ukash location.
Go to any location where you can buy Ukash.
Ask for Ukash: 150.00 CAD

paid within 12 hours. As soon as 12 hours expire, the possibility to pay the fine is lost forever. All your PC data will be detained and criminal's procedure will be initiated against you if the fine will not be paid!

Canada Post / Postes Canada

Esso GAS

Use the store locator to find your nearest outlet

Exchange your money for a unique Ukash code

Use the code to pay fine.

Ukash It's eMoney.

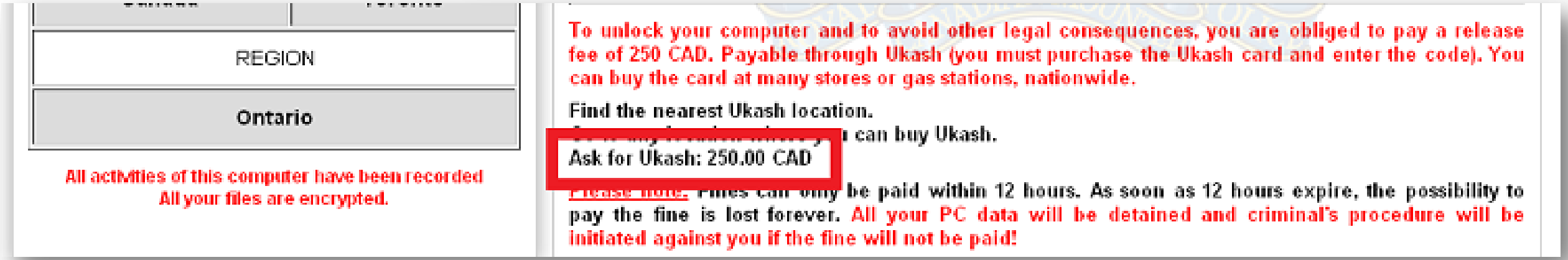
Code (Digits only)

Enter the UKASH code

1 2 3 4 5 6 7 8 9 0 Clear

F-Secure.

http://europol.europe.eu.france.id657546456-3999456674[redacted]com//	AS44050 Petersburg Internet Network LLC	91.220.131.193
http://politie.nl.id657546456-3999456674.[redacted]com//	AS44050 Petersburg Internet Network LLC	91.220.131.193
http://fbi.gov.id657546456-3999456674[redacted]com//	AS44050 Petersburg Internet Network LLC	91.220.131.193



F-Secure

中国新闻网 M.CHINANEWS.COM 客户端下载

D-Link云路由存漏洞或泄露网银密码 1分钟攻破

2015年04月16日 03:27 新京报

前日，专家演示显示，最快用时1分钟便攻破存在漏洞的D-Link路由器后台。

D-Link云路由存漏洞可能泄露网银密码

涉及17个型号产品；友讯集团在英文官网发布其中四个型号路由器的补

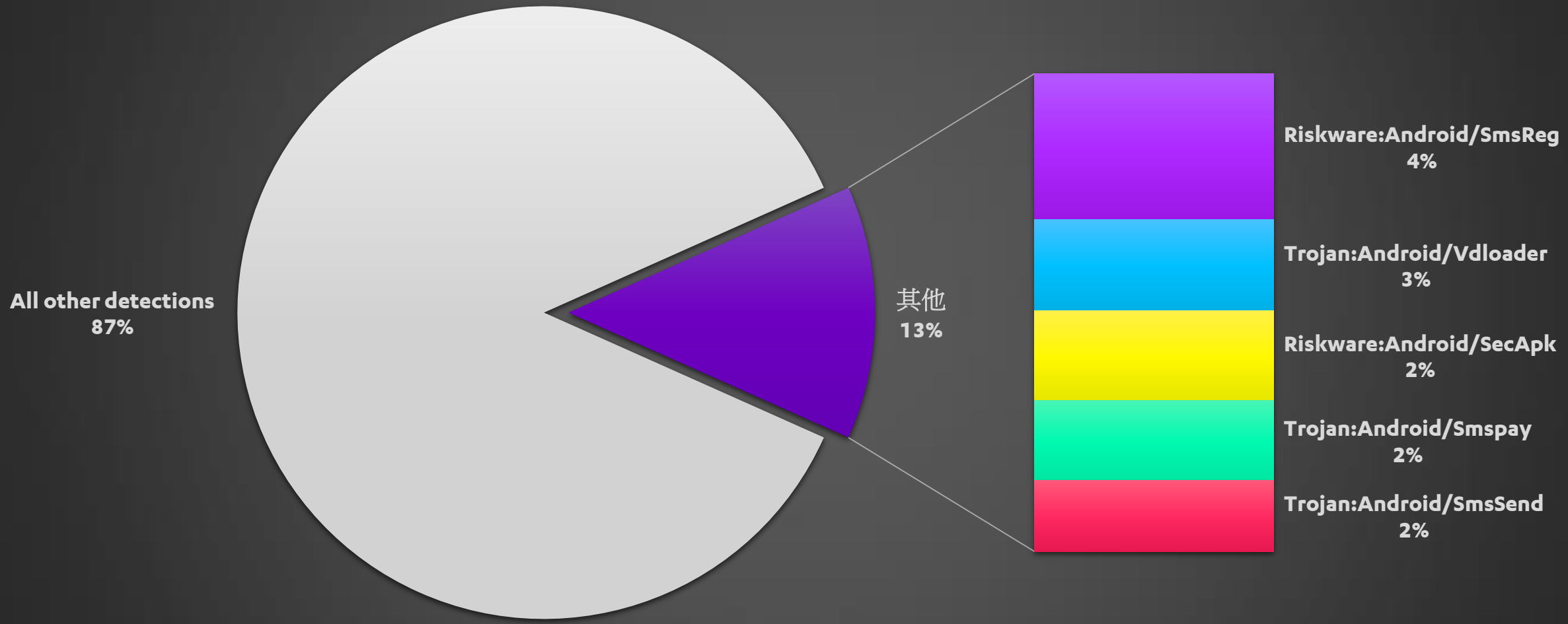
Web-based attack through Router Hijacking

DNS Hijack to redirect to malware websites

F-Secure.

99% of the mobile malware we see are targeted at Android

Top 5 Android detections in Hong Kong 2014 (by % of total Android detections)



Android/SMSreg

The application also collects the following information:

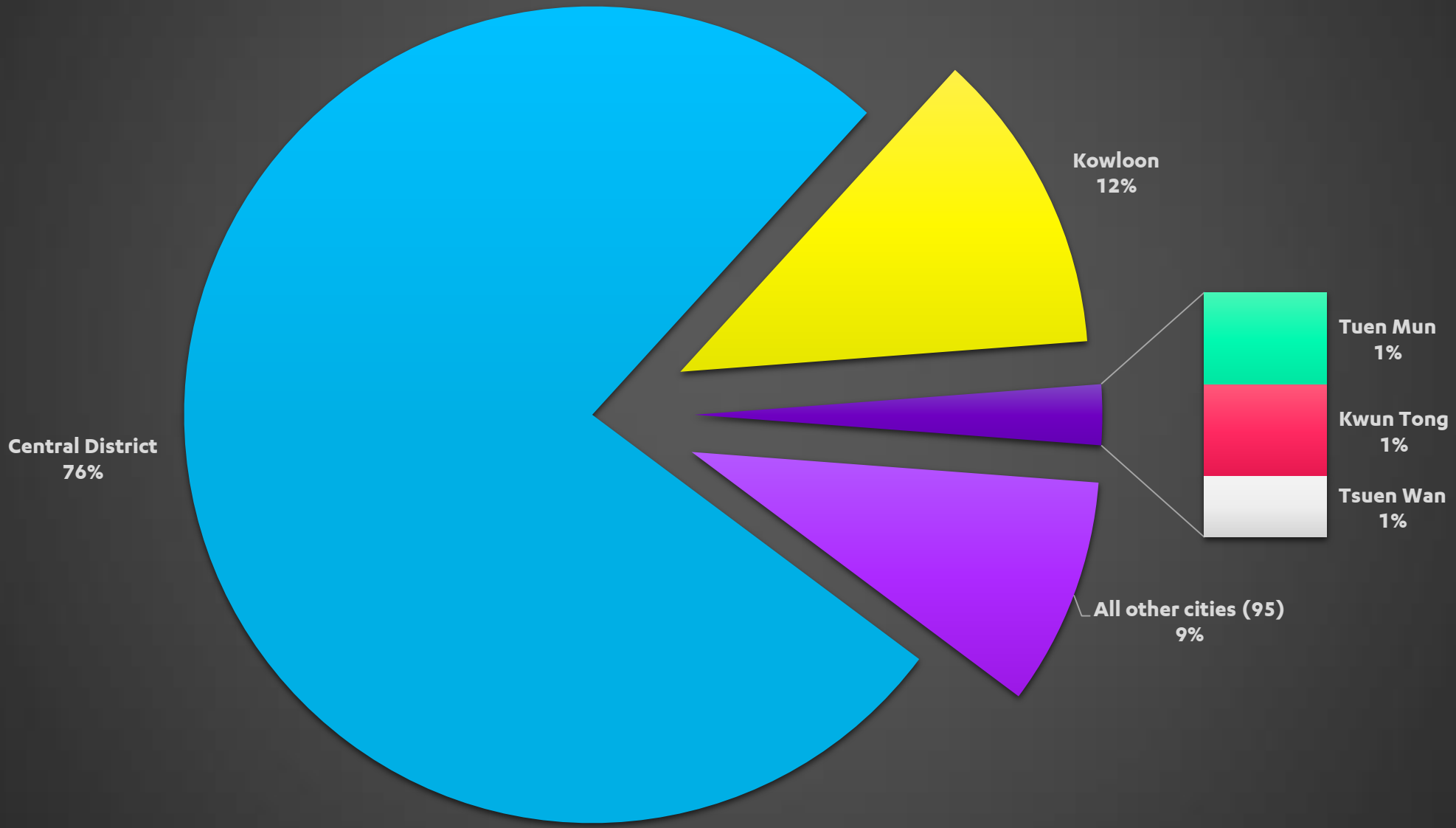
- API key
- Application ID
- Carrier
- Device manufacturer
- Device model
- GPS location
- International Mobile Equipment Identity(IMEI) number
- Network operator
- Package name
- SDK version

F-Secure.


27%
下午8:23
CODE4HK
+852 96 9
在線上
封鎖
新增
2014年9月16日
Check out this Android app designed by CODE4HK for the coordination of OCCUPYCENTRAL!
http://is.gd/bh4adz
下午8:16

F-Secure

Top 5 Cities (by % of all malware detections)



How do you protect 1 Billion devices?

F-Secure.

http://poliisi.fi.id734206428-5829564915.s6818.com/?fl

TEIDÄN SELAIMEN···

POLIISI

Kaikki tietokoneenne tiedostot ovat salattu. Älkää yrittäkö murtaa salakirjoitusta tietokoneellanne!

HUOMIO!

Te olette rikkoneet Tekijänoikeuslakia (Video, Musiikki, Ohjelmat) käyttämällä tai jakamalla laittomasti tekijänoikeus-suojattua materiaalia, täten rikkoen Luku 1, Osa 8, Pykälä 8, joka on osa Suomen Tekijänoikeuslakia.

Luku 1, Osa 8, Pykälä 8 (Suomen rikoslaki) rikkominen johtaa minimipalkkasidonnaiseen sakkorangaistukseen kertoimeltaan kahdestasadasta viitteensataan tai tuomioon kahdesta kahdeksaan vuoteen.

Olette laittomasti selanneet tai jakaneet laitonta pornografista materiaalia (tietokoneeltanne on löydetty lapsipornoksi luokiteltavaa kuvamateriaalia yms). Täten olette rikkoneet Suomen rikoslain lukua 202 jonka rangaistuksena on tuomio neljästä kahteentoista kuukauteen.

Tietokoneeltanne on suoritettu laiton murtautuminen ilman teidän henkilökohtaista tietoa tai osallistumista asiaan, tietokoneenne saattaa olla virustartunnan tai haittaohjelman kohteena, olette täten syyllistyneet Henkilökohtaisen tietokoneen vastuuttomaan käyttöön. Suomen Rikoslain 210 luvun mukaan rangaistuksena on sakko 100,000 EUR asti ja/tai tuomio neljästä yhdeksään vuoteen.

Kyseisen rikkeen pykälien mukaan Suomen rikoslaissa Kesäkuusta 28, 2011, tämä rikkomus (mikäli tapahtuu ensimmäisen kerran - eikä ole toistunut) saatetaan käsitellä tapauskohtaisesti mikäli maksatte sakon.

Avataksenne tietokoneenne lukituksen ja välttääksenne lainmukaiset jatkotoimenpiteet olette velvollinen maksamaan lukituksen avausmaksun 100 EUR, maksettava PAYSAFECARD:in välityksellä (teidän on hankittava PAYSAFECARD, talletettava saldolle 100 EUR ja tarjottava koodi). Koodi on ostettavissa suurimmassa osassa kaupoista ja bensa-asemista. PAYSAFECARD on mahdollista ostaa kaupoista maan sisällä.

Miten maksan sakon avatakseni tietokoneeni lukituksen?

1. Etsi lähin PAYSAFECARD jälleenmyyjä:

2. Osta PAYSAFECARD prepaid muodossa ja lataa tilille 100 EUR kassalla.
3. Kirjoittakaa oma PAYSAFECARD koodinne ja lähettäkää "AVAA TIETOKONEENI LUKITUS NYT"

Helsinki,
Southern finland,
Finland

paysafecard
pay cash, pay safe
SUOJATTU MAKSUKAAVAKE

Kirjoittakaa PAYSAFECARD koodin

1 2 3 4 5 6 7 8 9 0 poistaa

AVAA TIETOKONEESI LUKITUS NYT!

Huomatkaa: Sakko on maksettava 12 tunnin kuluessa. 12 tunnin kuluttua sakon maksamismahdollisuus vanhenee. Kaikki tietokoneenne data tullaan takavarikoimaan ja teitä vastaan tullaan toimeksipanemaan lainmukaiset toimenpiteet mikäli sakkoa ei makseta.

Source: The Daily Beast


hello.
New SMS
Tyler
Hey, I'm running late for the meeting. I'll be there in 5 mins!
9
47

F-Secure.


Audi
Audi drive select
Bordbuch
Car Systeme
17:37
Set individual
A7

BMW fixes security flaw in its in-car software

FRANKFURT | Fri Jan 30, 2015 10:15am EST

RELATED NEWS

REFILE-UPDATE 2-Facebook takes blame for service outages, which hit wider Web

Jan 30 (Reuters) - German luxury carmaker BMW has fixed a security flaw that could have allowed hackers to unlock the doors of up to 2.2 million Rolls-Royce, Mini and BMW vehicles, it said on Friday.

Hackers turn security camera DVRs into bitcoin miners

Published time: April 03, 2014 01:57
Edited time: April 04, 2014 11:58

Get short URL

Reuters / Eddie Keogh

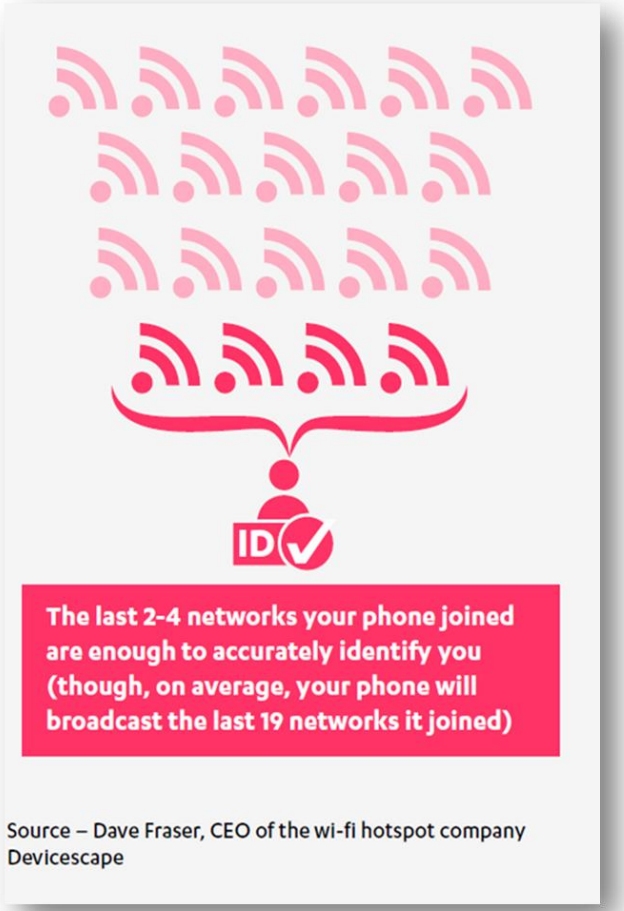
TAINTED LOVE: HOW WI-FI BETRAYS US

We are in a WiFi connected World

F-Secure.

The big question is..

- How do you differentiate a real or fake WiFi Access Point that you are connecting?
- How do you know if there is some one snooping the WiFi traffic for passwords and usernames that are not encrypted?



The wifi Experiment with EuroPol

The Equipment

- Raspberry Pi mini-computer system
- UTMS aerial
- a wi-fi aerial
- A battery pack with a life of around two days
- a USB port
- and a number of elastic bands

F-Secure.

THE EXPERIMENT

THE F-SECURE WI-FI EXPERIMENT

WHAT HAPPENED IN 30 MINUTES?

Our access point saw **250** devices

33 connected to our access

21 were identified

- 16 IPhone
- 1 IPad
- 3 Androids
- 1 PC

32 MB of traffic has been captured

53 internet services were used in this traffic

6 users agreed to the T&Cs before the page was disabled

The facts and figures from thirty minutes of our open access point

F-Secure

I HAVE READ AND AGREE TO THE LICENSE AGREEMENT

Accept terms and continue

FREE WIFI
TERMS OF SERVICE

These Terms of Service & Acceptable Use Policy (the "Terms") govern your use of services provided by F-Secure ("Service"). Your use of the Service represents your agreement to these Terms. If you do not agree with these Terms, do not use the Service.

Description of the Service

The Service is provided by F-Secure. The Service provides you with access to the Internet via certain high-speed Internet access points ("Locations"). Primarily, this access is provided via a Wi-Fi network using an 802.11 standard (the "Wi-Fi Service"). To access the Wi-Fi service, you must have a device that is compatible with the specific Wi-Fi equipment deployed
at the Location. In some instances, the Service will provide you with access to the Internet via a wired connection as part of a managed network (the "Wired Internet Service").
The Service is intended for the limited purposes of allowing access to the public Internet for e-mail, web browsing,
download files via the 'ftp' protocol typically im
such web browser programs and for purposes
consistent with the terms of service. The Servic
intended for high-bandwidth applications such
of video.

SECURITY WARNING

The unsecured nature and ease of connection t
hotspots increases the risk that unauthorized p
access
your phone, laptop or other device or your communications over the Wi-Fi network. Wi-Fi customers should take precautions to lower the security risks. If you have VPN, we recommend that you connect through it for optimum security. We also encourage our users to observe standard security practices. You should ensure that computer hard drives are not shared; that laptops have firewall protection; and that security software is installed, functional and updated on your device. We recommend that you avoid transmitting or accessing sensitive personal information over the Wi-Fi network, and that you only connect to
known Wi-Fi hotspots.

Charges/Billing/Payment

Where applicable, you agree to pay all charges and fees related to your use of the Service, including taxes, fees, surcharges or other assessments applicable to the Service.

Modifications to the Service / Updates to the Terms
We reserve the right to modify or discontinue, temporarily or permanently, at any time and from time to time, the Service (or any function or feature of the Service or any part thereof, including but not limited to rates and charges) with or
without notice. You agree that we will not be liable to you or

Operational Limits of the Service

associated facilities. There is no guarantee of bandwidth. Your connection speed may not be suitable for some applications,
and particularly those involving real-time or near real time, high-bandwidth uses such as video streaming or video conferencing. You understand and agree that temporary interruptions of the Service may occur as normal events in the
provision of the Service and that we will not be liable for such interruptions. You further understand and agree that we have no control over third party networks you may access in the course of your use of the Service, and therefore, delays and disruptions of other network transmissions are beyond our control.

Third Party Content Disclaimer/ Links to Third Party Sites
Content provided by Third Party Providers ("Third Party Content") has not been independently authenticated in whole or in part by us. This Service may be linked to other websites which are not under our control. We are providing these links to you only as a convenience, and the inclusion of any link to such sites does not imply endorsement by us.

Privacy Policy

Registration data has not been taken from you to ensure your

General Use Restrictions

Subject to your acceptance of and compliance with these Terms, you are hereby granted the right to use the Service through a
non-exclusive, non-transferable and non-assignable limited license. The Service is provided for your use only (unless otherwise specifically stated) and you agree not to reproduce, duplicate, copy, sell, transfer, resell or exploit for any
commercial purposes your subscription to or membership in the Service, any portion of the Service, use of the Service, or access to the Service. You have no right to resell, sublicense, assign or transfer your right to access the Service.

Software Use Restrictions

Any software that is made available to download with the Service (the "Software") is the copyrighted work of us and/or Third
Party Providers. Use of the Software is governed by the terms of the end user license agreement, if any, which accompanies or is included with the Software (the "License Agreement").

Submissions

their legality, reliability, appropriateness, originality and copyright.

Disclaimer of Warranties

UNLESS OTHERWISE EXPLICITLY STATED, THE MATERIALS AND THE SERVICE ARE PROVIDED "AS IS", AND ARE FOR PERSONAL USE ONLY. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. AT&T MAKES NO REPRESENTATIONS, WARRANTIES, GUARANTIES AS TO THE QUALITY, SUITABILITY, TRUTH, ACCURACY OR COMPLETENESS OF THE SERVICE OR ANY OF THE MATERIALS PROVIDED WITH THE SERVICE. ANY QUESTIONS REGARDING THE MATERIALS SHOULD BE DIRECTED TO THE PROVIDERS OF SUCH MATERIALS. HOWEVER, WE DO NOT AUTHORIZE ANYONE TO MAKE A WARRANTY ON OUR BEHALF AND YOU MAY NOT RELY ON ANY STATEMENT OF WARRANTY BY A THIRD PARTY AS A

Indemnity

your use
of the Service; (c) your violation of these TOS; (d) your violation of any rights of another; and (e) use of your account and any Sub-Account whether or not such usage is expressly authorised by you.

Liability of Customer

YOU HAVE SOLE RESPONSIBILITY FOR ADEQUATE PROTECTION AND BACKUP OF DATA AND/OR EQUIPMENT USED IN CONNECTION WITH THE SERVICE AND WILL NOT MAKE A CLAIM AGAINST US FOR LOST DATA, RE-RUN TIME, INACCURATE OUTPUT, WORK DELAYS OR LOST PROFITS RESULTING FROM THE USE OF THE SERVICE AND MATERIALS.
YOU AGREE TO DEFEND, INDEMNIFY AND HOLD US HARMLESS (INCLUDING OUR PARENT AND AFFILIATE COMPANIES, EMPLOYEES, OFFICERS, DIRECTORS AND AGENTS) FROM, AND YOU COVENANT NOT TO SUE US FOR, ANY CLAIMS BASED ON, OR STEMMING FROM, YOUR USE OF THE SERVICE AND MATERIALS.

Your first born child

In using this service, you agree to relinquish your first born child to F-Secure, as and when the company requires it. In the event that no children are produced, your most beloved pet will be taken instead. The terms of this agreement stand for eternity.

Accept terms and continue

LESSONS LEARNED FROM THE EXPERIMENT:

- Industry should be more transparent
  - Terms of service
  - Personal Data belongs to the consumer, not provider
- Regulators should act
  - Controls imposed
  - WiFi AP to be certified as safe, like https
- Consumers should protect themselves
  - Encryption, VPN services
  - Turn off WiFi when not in use

How should I protect myself?

5 Tips to safe smartphone usage

- Downloading new APPS
  - Do get it from a trusted store (eg google play)
  - Be wary of FREE apps from 3rd party app stores
  - Review and scrutinize permissions when installing and APP
- URL links in IM
  - Do not click any links sent via Whatsapp, Line, WeChat or other IM without verifying
- Social Media
  - Do NOT trust everything you see on your FB, confirm a news before sharing it
- Use Encryption or VPN services over public wifi networks
- Use a security software solution

2015 Outlook

- Mobile malware continues to rise as adoption of smart mobile devices are getting more common
- Internet of Things infection will move from concept to mainstream
- Privacy will be more important than security

SWITCH ON FREEDOM