Who targets the journalists? and how?

A review of the attack surface in our digital society

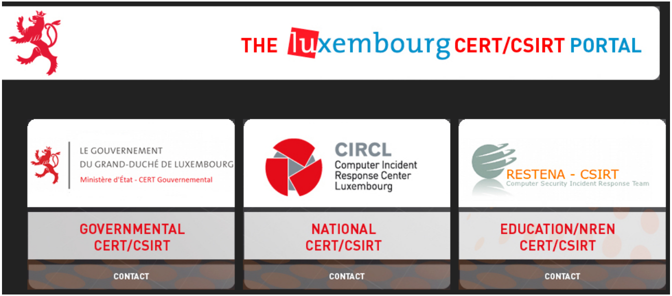
CIRCL
Computer Incident
Response Center
Luxembourg

TLP:WHITE

info@circl.lu

8th February 2014

CIRCL



THE luxembourg CERT/CSIRT PORTAL

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État - CERT Gouvernemental

GOVERNMENTAL CERT/CSIRT

CONTACT

CIRCL
Computer Incident
Response Center
Luxembourg

NATIONAL CERT/CSIRT

CONTACT

RESTENA - CSIRT
Computer Security Incident Response Team

EDUCATION/NREN CERT/CSIRT

CONTACT

- CIRCL is the national Computer Security Incident Response Team (CSIRT) for the Grand-Duchy of Luxembourg
- CIRCL is operated by SMILE, a State funded ”groupement d’intérêt économique” (GIE), designed to improve information security and create new opportunities for Luxembourg

CIRCL Statistics

- CIRCL started as a fully operational national CSIRT team in October 2010
  - In **2011**, we processed more than **4500** events for the past 12 months
  - More than 220 technical investigations and analysis were conducted in 2011
  - In **2013**, we processed **35958** events and conducted more than **1006** technical investigations
- The increase of attacks can be explained by the improved reporting process but also the growing attack surface

Statistics

- The attacks can be separated in 3 main categories (time allocated in 2013):
  - Cybercriminals (financial objective) - (50%)
  - Government-supported attackers[1] (information objective) - (40%)
  - Cyberactivists (political or "fun" objective) - (10%)
- There are more than 230 "official" operational intelligence agencies[2] worldwide and the Snowden leaks are just a small part of a single intelligence agency in US
- But what these organizations are really doing against companies, citizens and journalists? How do they proceed?

[1] Between 2011 and 2013, the increase is significant

[2] http://en.wikipedia.org/wiki/List_of_intelligence_agencies

A small advertising...

`http://www.youtube.com/watch?v=R63CRBNLE2o`

Governmental grade malware

- **HackingTeam**[3]
  - Based in Milan (Italy)
  - 40+ employees, on 6 continents, used by several dozen countries [4]
  - Malwares names: Crisis, DaVinci, Morcut, Remote Control System
  - Operating Systems: Windows, Mac, Linux
  - Mobile Devices: iOS, Android, Windows Mobile, Blackberry, Symbian
- **Gamma International GmbH**[5]
  - Based in Munich (Germany)
  - Bypass 40 Antivirus [6]
  - Malware name: Finfisher, Finspy
  - Operating Systems: Windows, Mac, Linux
  - Mobile Devices: iOS, Android, Windows Mobile, Blackberry, Symbian

[3] http://www.symantec.com/connect/blogs/crisis-advanced-malware

[4] http://www.wired.com/threatlevel/2013/06/spy-tool-sold-to-governments/

[5] https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf

[6] http://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf

Use Cases

- 2011 - Egypt, human rights activists - Gamma [7]
- 2011 - UAE, Ahmed Mansoor, human rights activist - HackingTeam, VUPEN [8]
- 2012 - Bahrain, human rights activists - Gamma
- 2012 - Morocco, journalists (Mamfakinch) - HackingTeam
- 2013 - FinFisher Command&Control servers detected in Bahrain, Brunei, the Czech Republic, Ethiopia, Indonesia, Mongolia, Singapore, the Netherlands, Turkmenistan, and the United Arab Emirates (UAE)[9]
- CIRCL analyzed some similar cases targeting journalists but also citizens

[7] https://www.f-secure.com/weblog/archives/00002114.html

[8] https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/

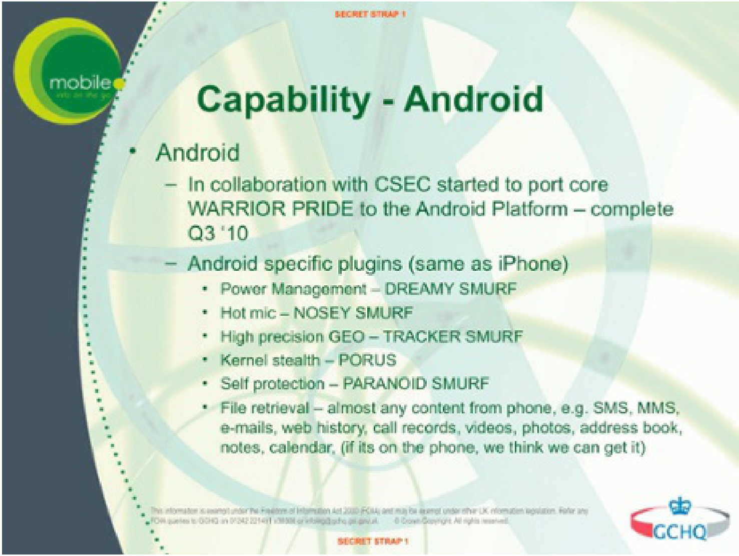
[9] https://citizenlab.org/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/

What should I do to limit the risks of such attack?

- Dedicate a browser for your sensitive activities (e.g. web banking or alike)
- Disable unused plugins and use NoScript or similar trusted add-ons in your browser
- Use a bootable CD/USB like tails[10] to access suspicious sources
- Keep an eye on your laptop (e.g. use unique stickers to cover screws) and don't leave it unattended
- Think twice before doing an action on Internet (e.g. open suspicious URLs, inserting USB keys, open document from unknown sources)

[10] `https://tails.boum.org/`

What about your other laptop?



SECRET STRAP 1

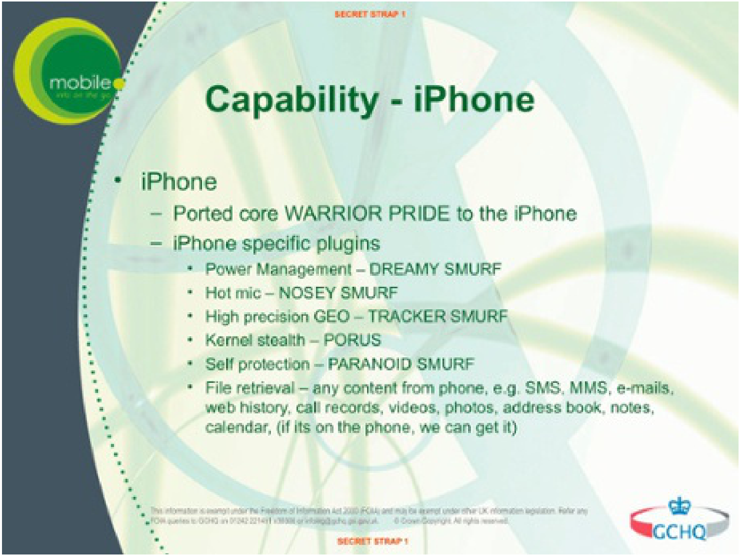
Capability - Android

- Android
  - In collaboration with CSEC started to port core WARRIOR PRIDE to the Android Platform – complete Q3 '10
  - Android specific plugins (same as iPhone)
    - Power Management – DREAMY SMURF
    - Hot mic – NOSEY SMURF
    - High precision GEO – TRACKER SMURF
    - Kernel stealth – PORUS
    - Self protection – PARANOID SMURF
    - File retrieval – almost any content from phone, e.g. SMS, MMS, e-mails, web history, call records, videos, photos, address book, notes, calendar, (if its on the phone, we think we can get it)

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on 01242 221491 x30306 or infoleg@gchq.gsi.gov.uk. © Crown Copyright. All rights reserved.

SECRET STRAP 1

What about your other branded laptop?



SECRET STRAP 1

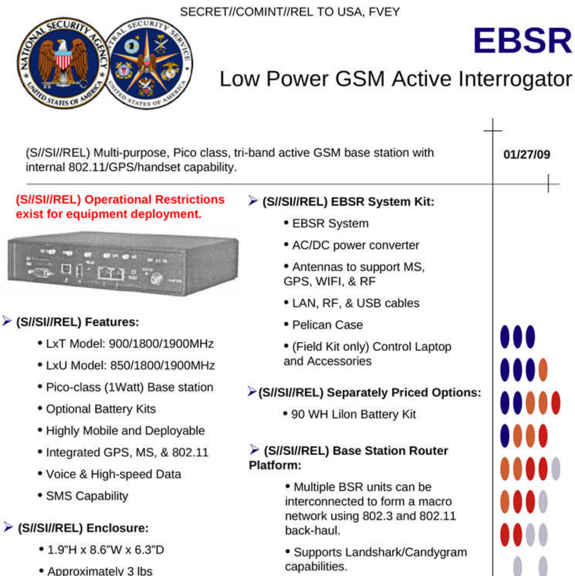
Capability - iPhone

- iPhone
  - Ported core WARRIOR PRIDE to the iPhone
  - iPhone specific plugins
    - Power Management – DREAMY SMURF
    - Hot mic – NOSEY SMURF
    - High precision GEO – TRACKER SMURF
    - Kernel stealth – PORUS
    - Self protection – PARANOID SMURF
    - File retrieval – any content from phone, e.g. SMS, MMS, e-mails, web history, call records, videos, photos, address book, notes, calendar, (if its on the phone, we can get it)

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on 01242 221491 x30306 or infoleg@gchq.gsi.gov.uk. © Crown Copyright. All rights reserved.

SECRET STRAP 1

Can you trust the GSM network?



SECRET//COMINT//REL TO USA, FVEY

EBSR

Low Power GSM Active Interrogator

(S//SI//REL) Multi-purpose, Pico class, tri-band active GSM base station with internal 802.11/GPS/handset capability.

01/27/09

(S//SI//REL) Operational Restrictions exist for equipment deployment.

➤ **(S//SI//REL) Features:**

- LxT Model: 900/1800/1900MHz
- LxU Model: 850/1800/1900MHz
- Pico-class (1Watt) Base station
- Optional Battery Kits
- Highly Mobile and Deployable
- Integrated GPS, MS, & 802.11
- Voice & High-speed Data
- SMS Capability

➤ **(S//SI//REL) Enclosure:**

- 1.9"H x 8.6"W x 6.3"D
- Approximately 3 lbs

➤ **(S//SI//REL) EBSR System Kit:**

- EBSR System
- AC/DC power converter
- Antennas to support MS, GPS, WIFI, & RF
- LAN, RF, & USB cables
- Pelican Case
- (Field Kit only) Control Laptop and Accessories

➤ **(S//SI//REL) Separately Priced Options:**

- 90 WH LiIon Battery Kit

➤ **(S//SI//REL) Base Station Router Platform:**

- Multiple BSR units can be interconnected to form a macro network using 802.3 and 802.11 back-haul.
- Supports Landshark/Candygram capabilities.

A mobile phone is a computer with tracking capabilities but what can I do?

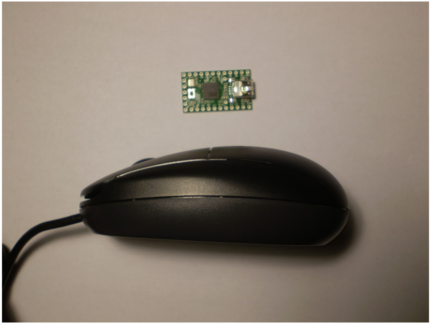
- SMS can be intercepted not only on the mobile network but at various places in the network
- End-to-end encrypted[11] instant messaging can provide better security than mobile communications
- If you really need SMS, TextSecure[12] can provide an additional layer of security including storage
- If you cannot used secure instant messaging, RedPhone or Discretio[13] can be an alternative on mobile phones

[11] https://securityinabox.org/en/pidgin_main

[12] https://whispersystems.org/

[13] https://www.discretio.com/

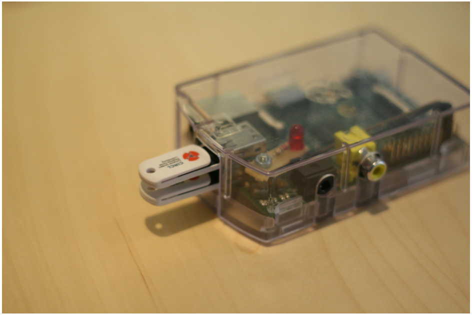
Do you trust "your" USB devices?



- Is this a mouse or a mouse with an additional keyboard?
- Additional keyboard (with pre-encoded actions)[14] in a mouse for 20,- EUR

[14] http://www.irongeek.com/i.php?page=security/programmable-hid-usb-keystroke-dongle

Exchanging documents over USB?



- USB keys are exchanged between people all the time and are a major infection vector
- We developed CIRCLean[15] to provide a concrete solution to this issue

[15] https://www.circl.lu/projects/CIRCLean/

Contact

- info@circl.lu
- https://www.circl.lu/
- OpenPGP fingerprint: CA57 2205 C002 4E06 BA70 BE89 EAAD CFFC 22BD 4CD5
- Found suspicious documents? Do you need a custom training for your journalists in the (battle)field? Don't hesitate to contact CIRCL