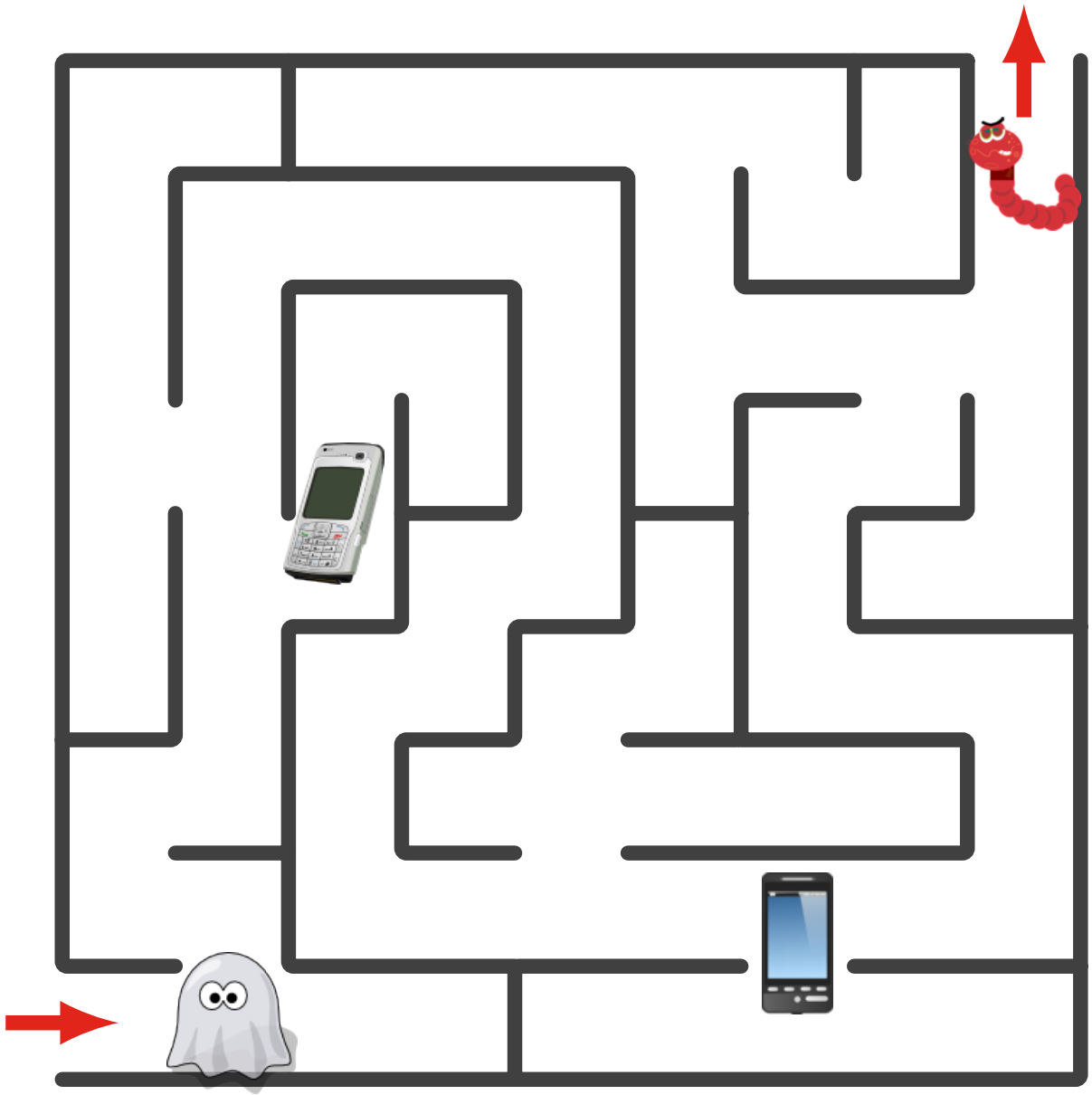
The Mobile Malware Maze

Axelle Apvrille, Fortinet

BruCON, September 2023

The Mobile Malware Maze



Blogs, links, Internet have a short memory

- Pico: "*What a fantastic discovery this palace of Knossos is! It dates -2000 BC. What art, what talent! Admire that!*"
- His son: "*Don't exaggerate. The discovery of mobile phones is far more useful...*"

Who am I?

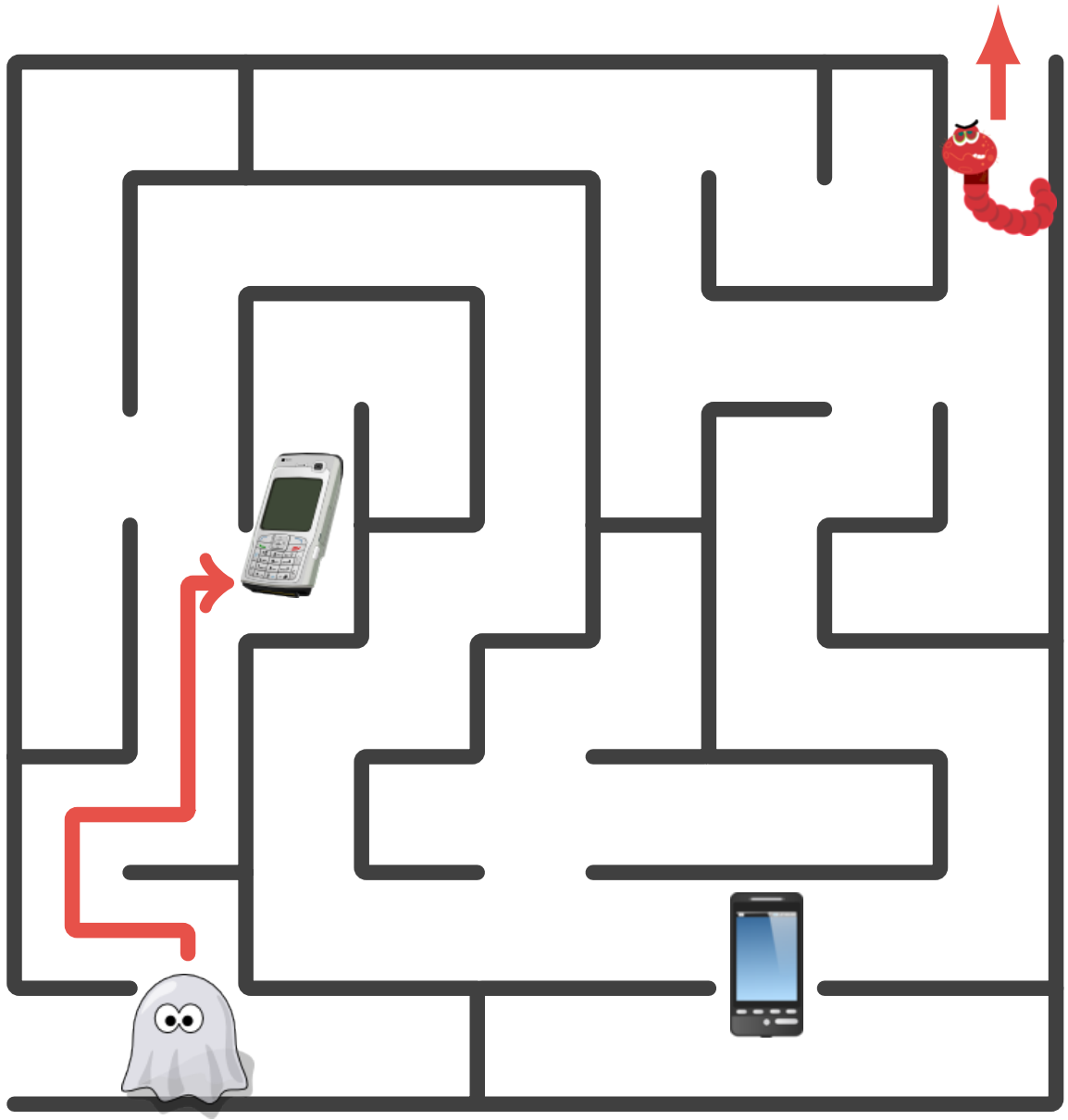
1st mobile virus: **Cabir**

@ Fortinet

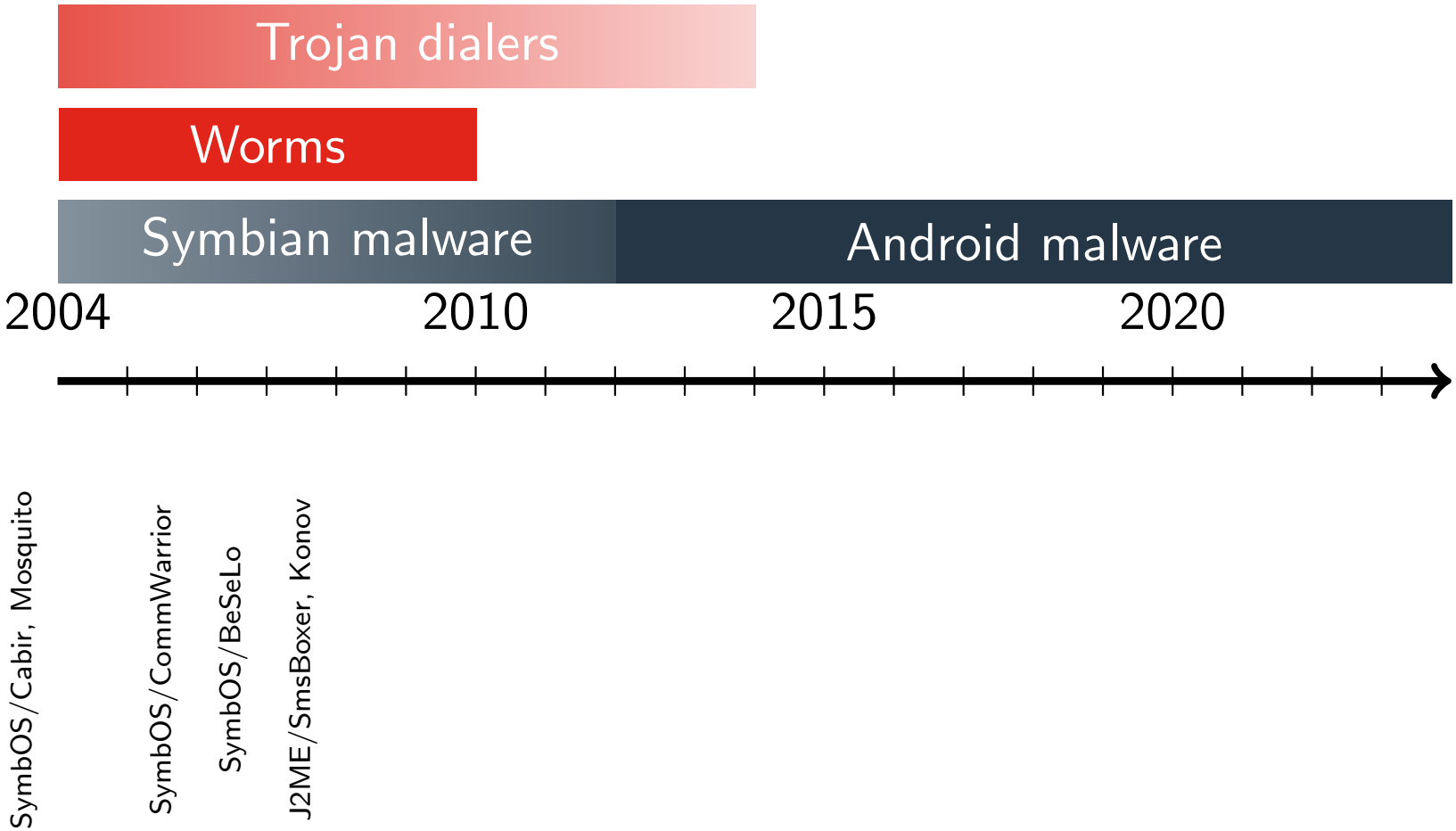
2004 **2008**

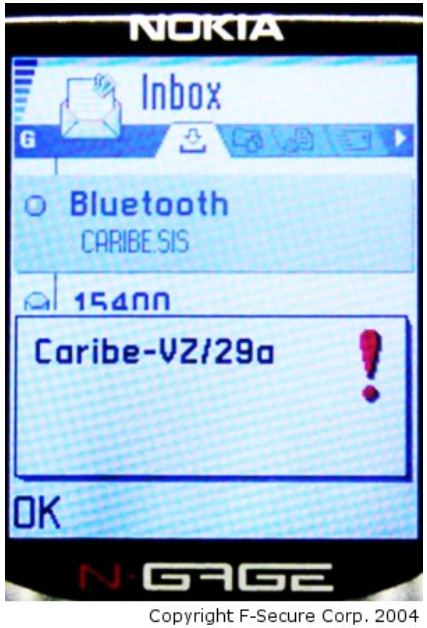
Security developer	Malware researcher
crypto algorithms, PKCS, timestamping, runtime authentication of binaries, TrustZone...	Mobile malware, IoT malware, Ph0wn

The Mobile Malware Maze



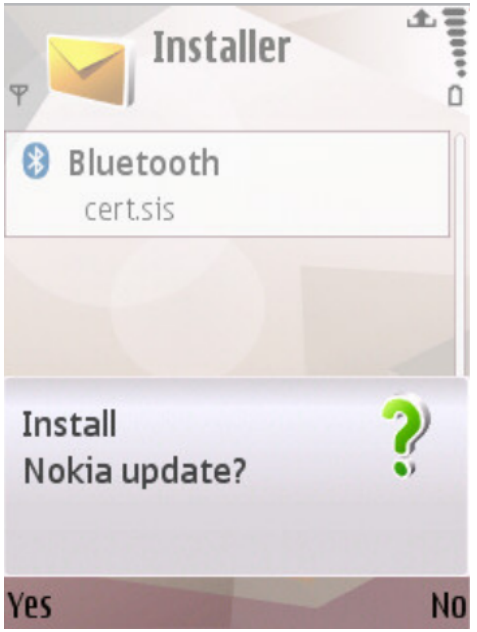
Mobile malware chronology: the Symbian era





Cabir (2004)

BeSeLo (2008)



ZitMo (2010)

Images from https://www.f-secure.com/v-descs/cabir.shtml,

https://github.com/cryptax/talks/tree/master/Insomnihack-2011,

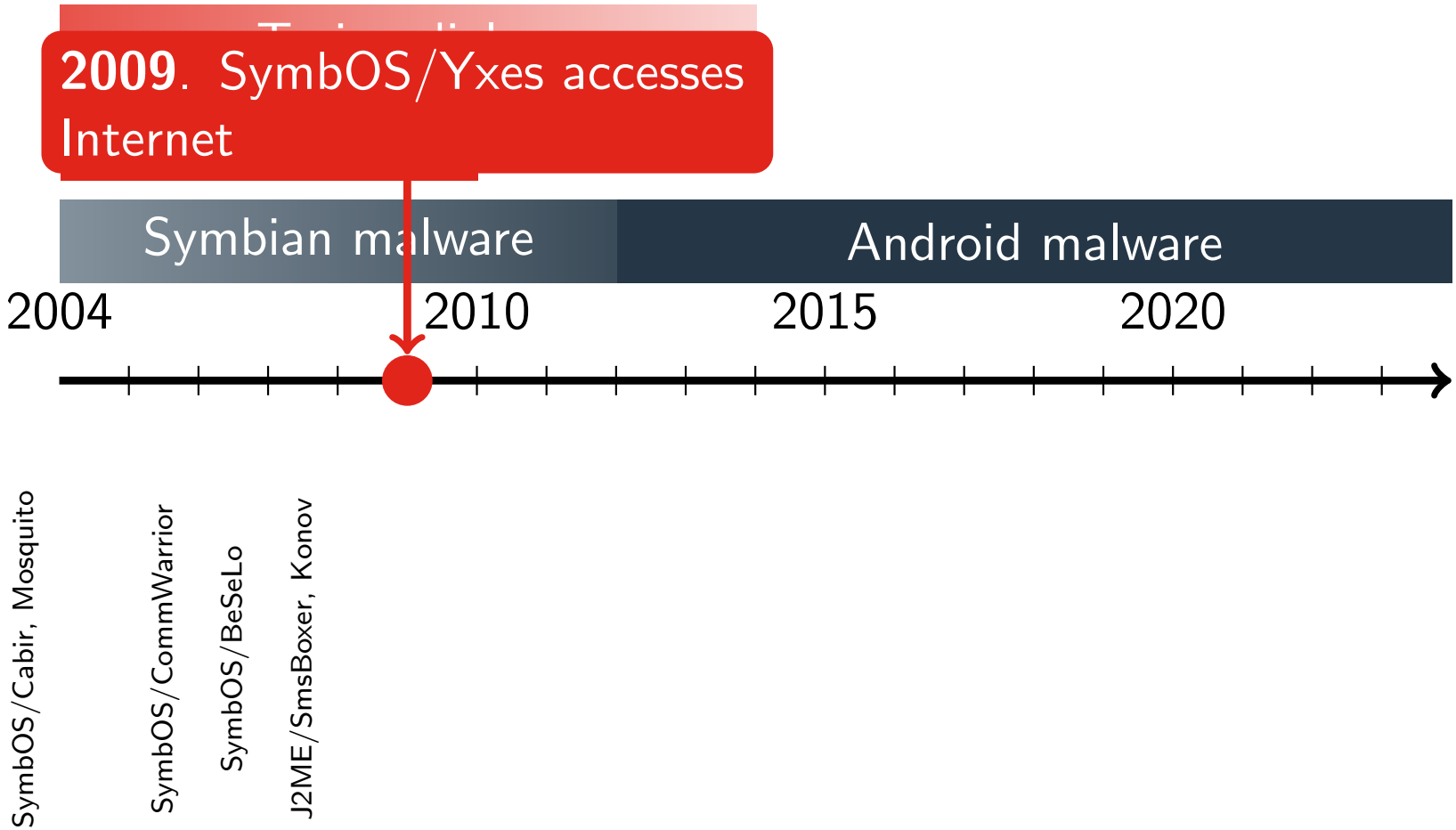
https://www.fortiguard.com/encyclopedia/virus/497339/symbos-beselo-c-worm

Mobile Phone Lab

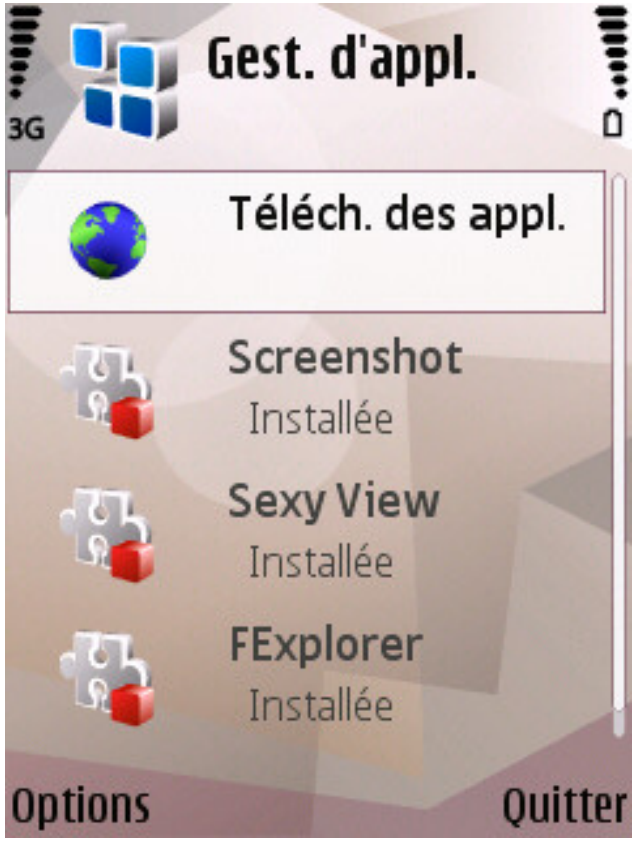
Mobile Phone Lab

Some mobile phones ... expanded

SymbOS/Yxes: an important turn in mobile malware

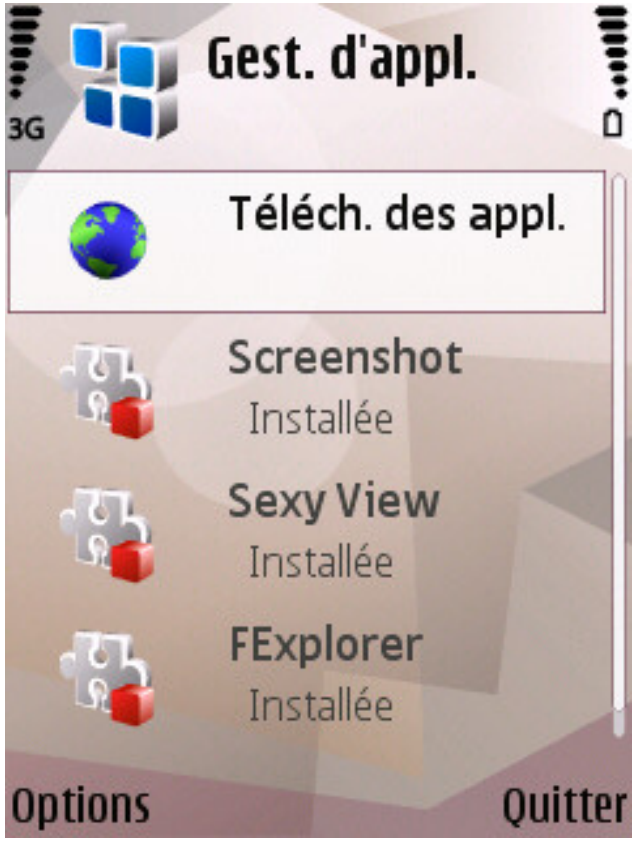


SymbOS/Yxes: old, but not stupid



https://github.com/cryptax/talks/tree/master/EICAR-2010

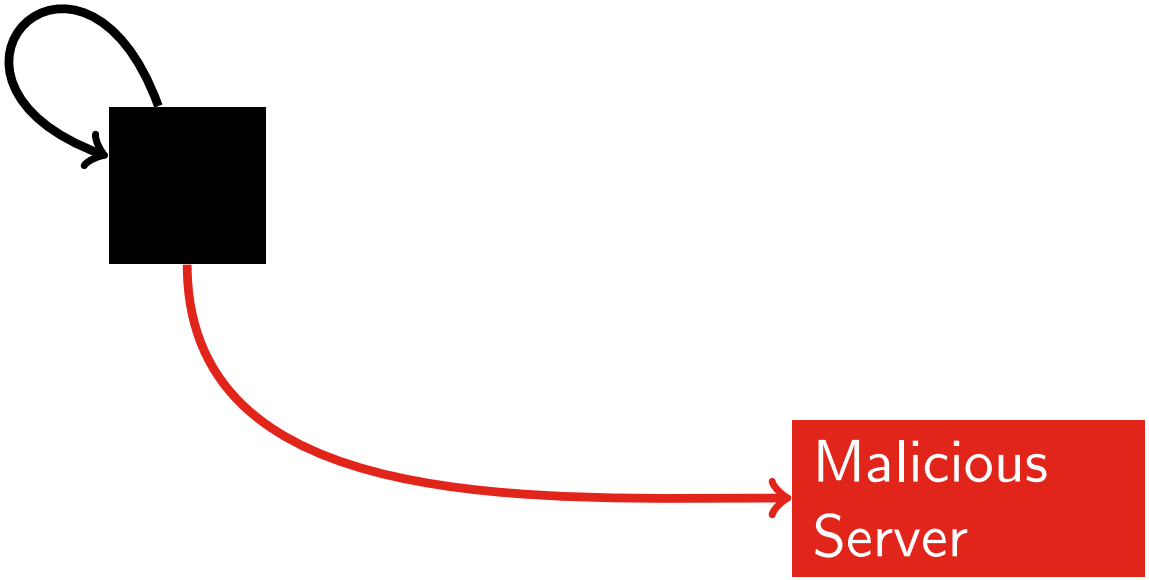
SymbOS/Yxes: old, but not stupid

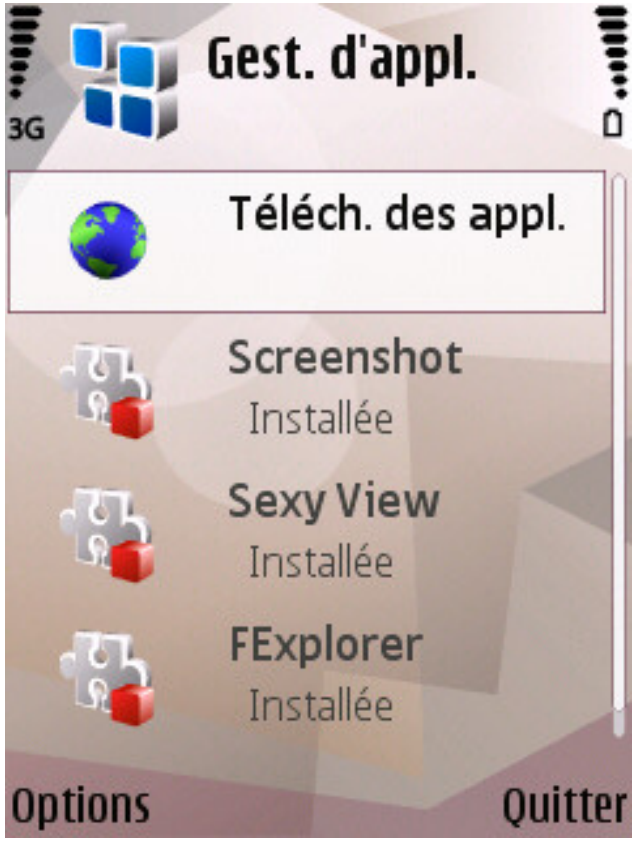


https://github.com/cryptax/talks/tree/master/EICAR-2010

SymbOS/Yxes: old, but not stupid

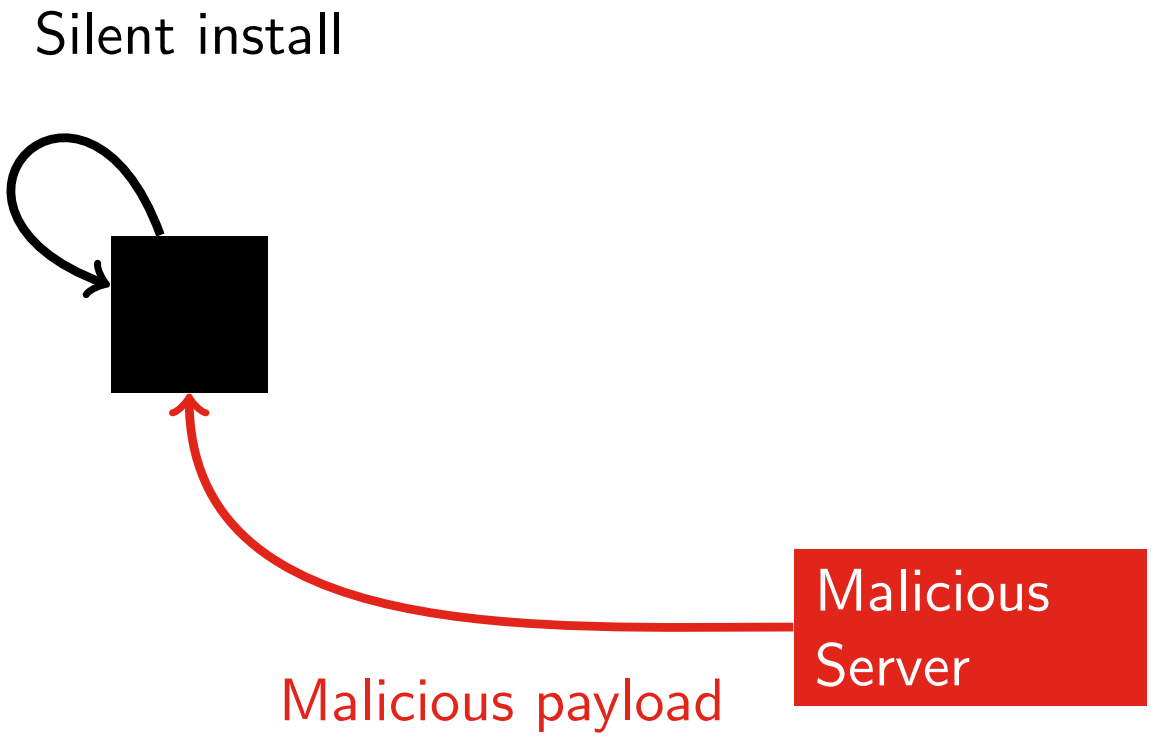
Decrypt URL

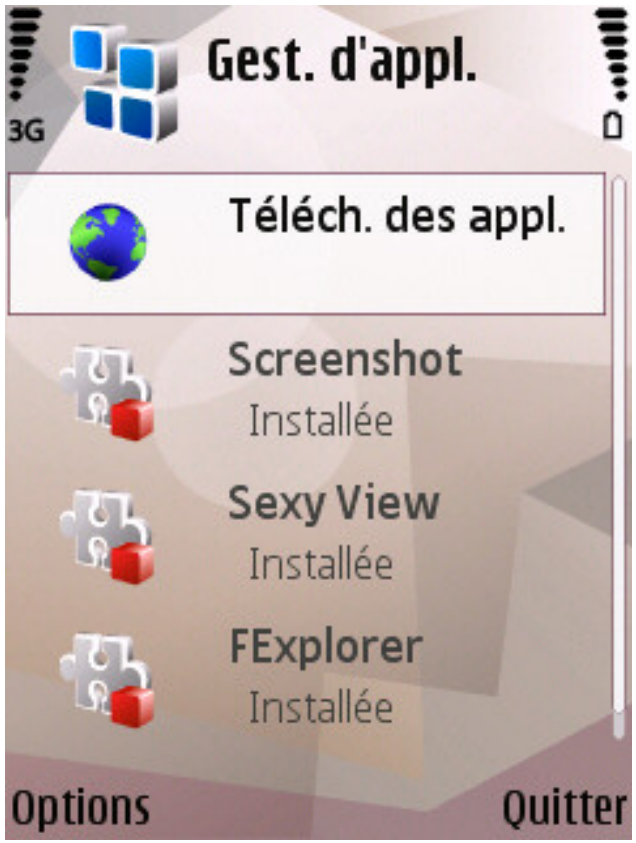




https://github.com/cryptax/talks/tree/master/EICAR-2010

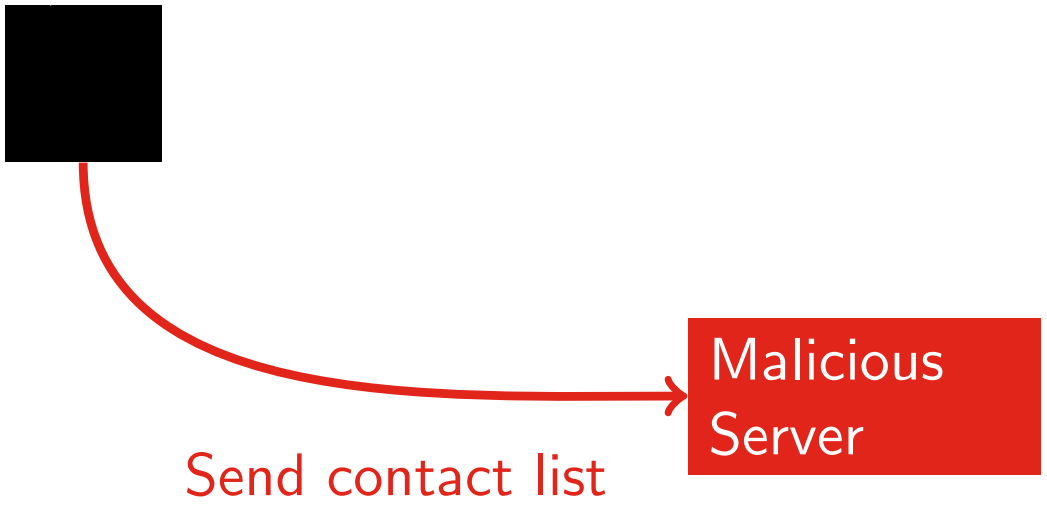
SymbOS/Yxes: old, but not stupid

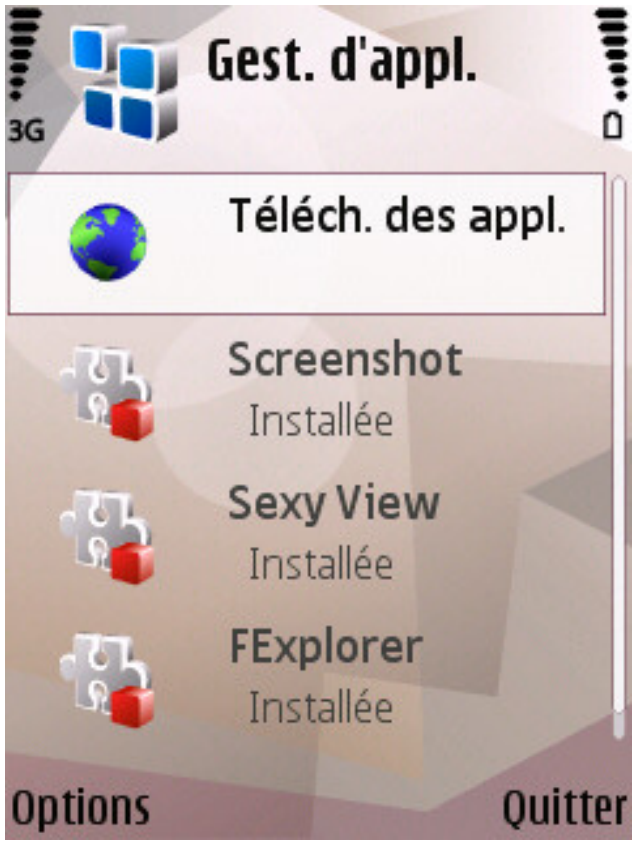




https://github.com/cryptax/talks/tree/master/EICAR-2010

SymbOS/Yxes: old, but not stupid

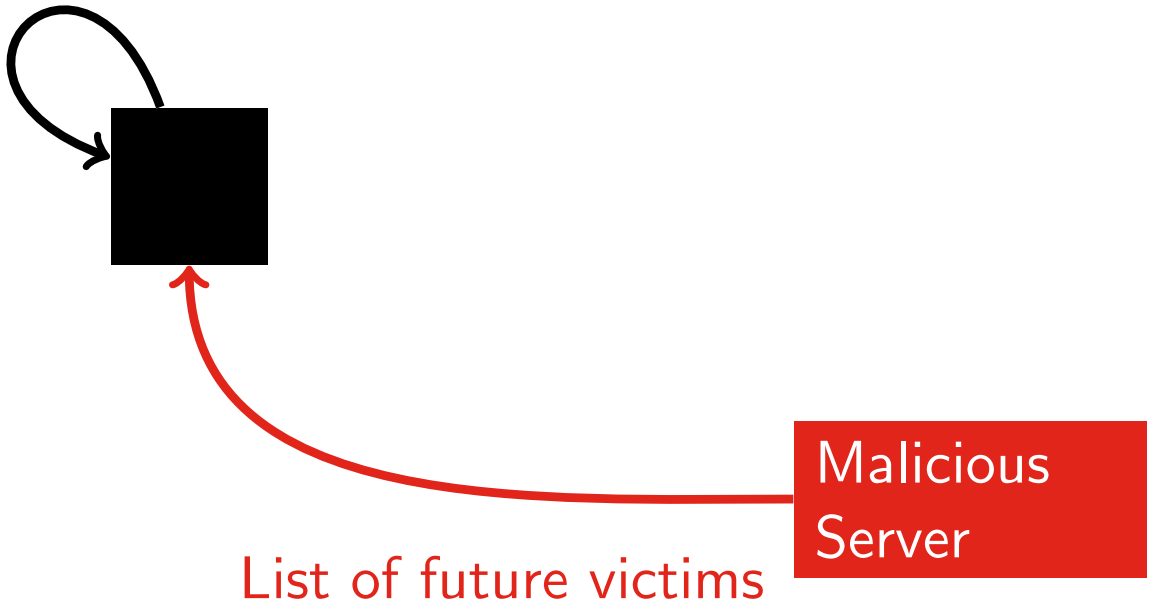


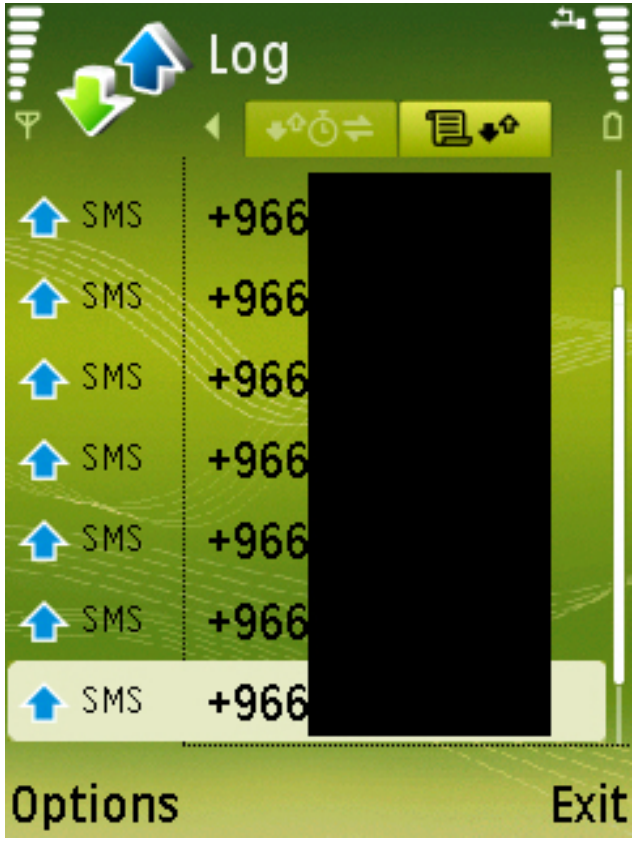


https://github.com/cryptax/talks/tree/master/EICAR-2010

SymbOS/Yxes: old, but not stupid

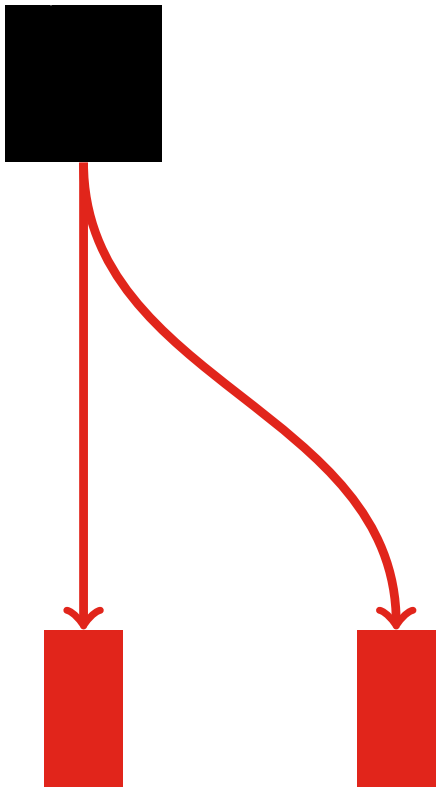
Kill file manager app





https://github.com/cryptax/talks/tree/master/EICAR-2010

SymbOS/Yxes: old, but not stupid



Send SMS with link to malware

https://github.com/cryptax/talks/tree/master/EICAR-2010

It used to be difficult to connect to Internet on a phone

```
.text:7C8C2478  SUB     R0, R11, #0xAC
.text:7C8C247C  BL      _ZN15TCommDbConnPrefC1Ev ; TCommDbConnPref constructor
.text:7C8C2480  SUB     R0, R11, #0xAC
.text:7C8C2484  MOV     R1, #3                   ; ECommDbDialogPrefDoNotPrompt
.text:7C8C2488  BL      _ZN15TCommDbConnPref19SetDialogPreferenceE17TCommDbDialogPref
                                                 ; SetDialogPreference of connection
```

1. Parse each Internet Access Point (IAP): retrieve Access Point Name (APN), proxy server and port
2. Select desired IAP
3. Do not display confirmation dialog: `DoNotPrompt`, requests `NetworkServices` capability
4. Build and send HTTP request

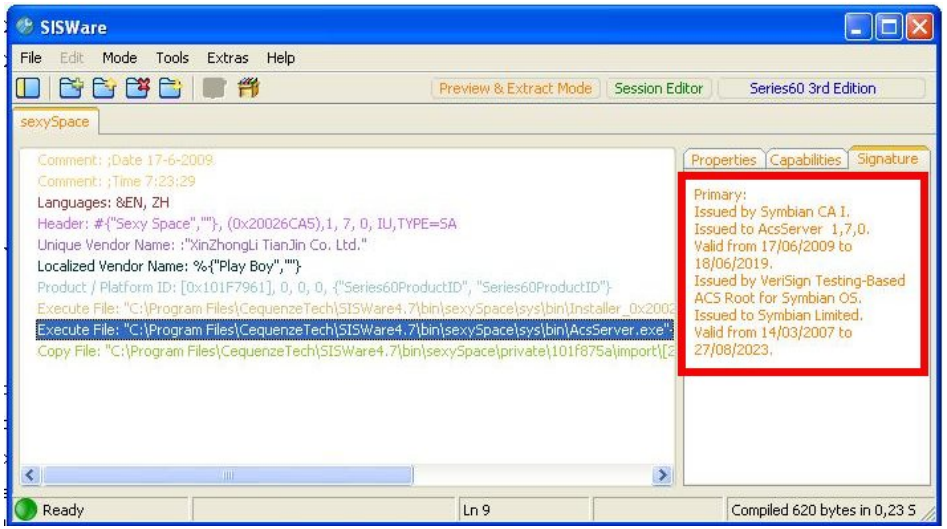
Symbian capabilities

Restricted capabilities used by SymbOS/Yxes

	Symbian	Android
Access Internet	NetworkServices	INTERNET
Retrieve IMEI	ReadDeviceData	READ_PRIVILEGED_PHONE_STATE
Kill other apps	PowerMgmt	KILL_BACKGROUND_PROCESSES*
Location	Location	ACCESS_FINE_LOCATION

* no longer available - can only kill your own process

Old, but not stupid: Application Signature

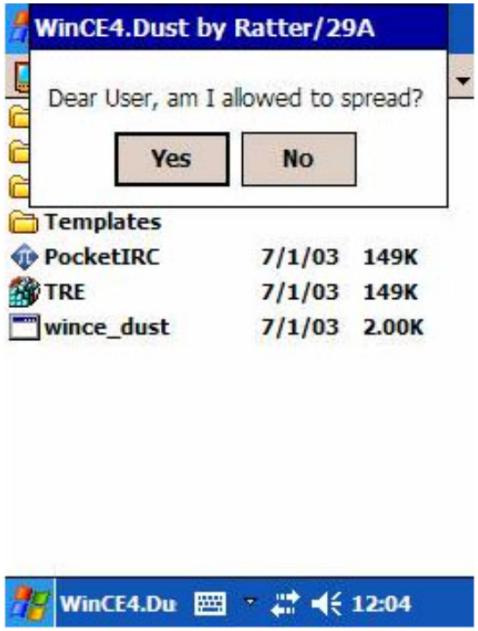


Fee	USD per year
Symbian Express	20
Android	25*
Apple	99

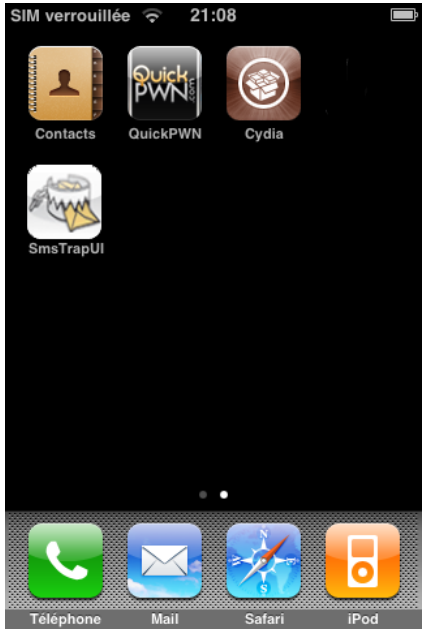
* lifetime

- Symbian applications were **signed**
- Signed applications had access to extra **capabilities**
- Malware author presumably paid the **Symbian Express Signed** fee: 20 USD / year
- The certificate was later revoked

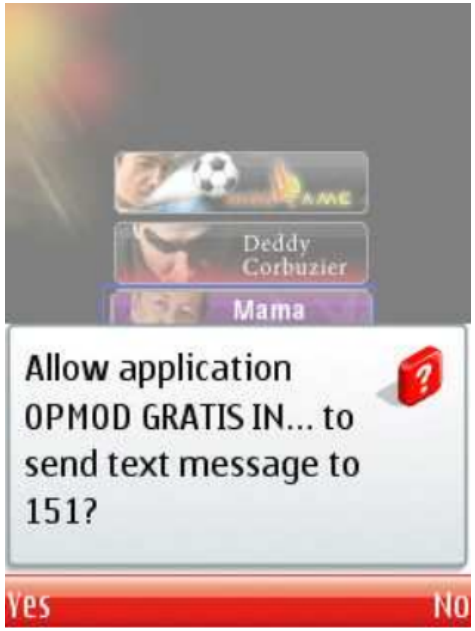
Other early mobile malware



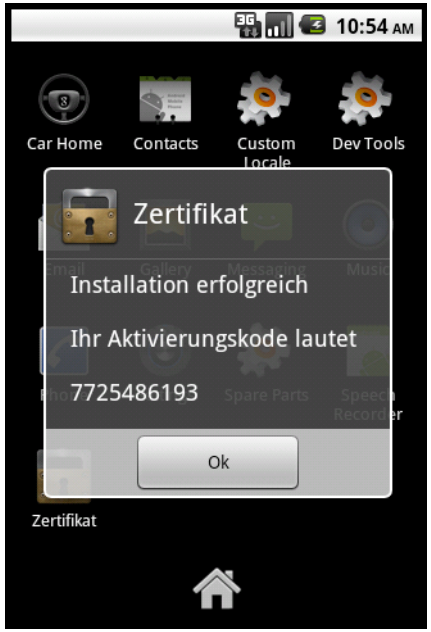
WinCE/Dust (2004)



iOS/Trapsms (2009)



J2ME/GameSat (2010)

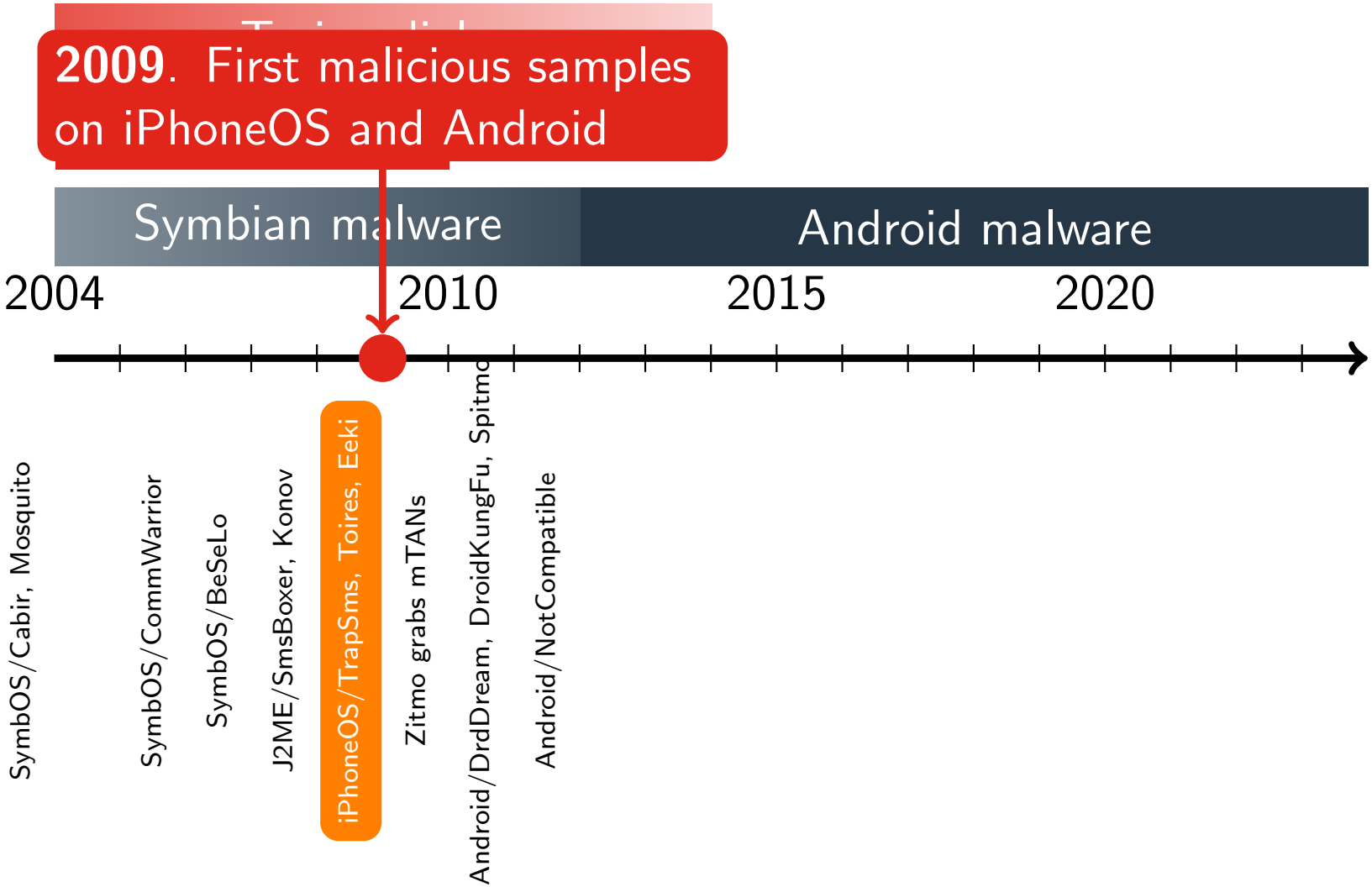


ZitMo for BlackBerry (2012)

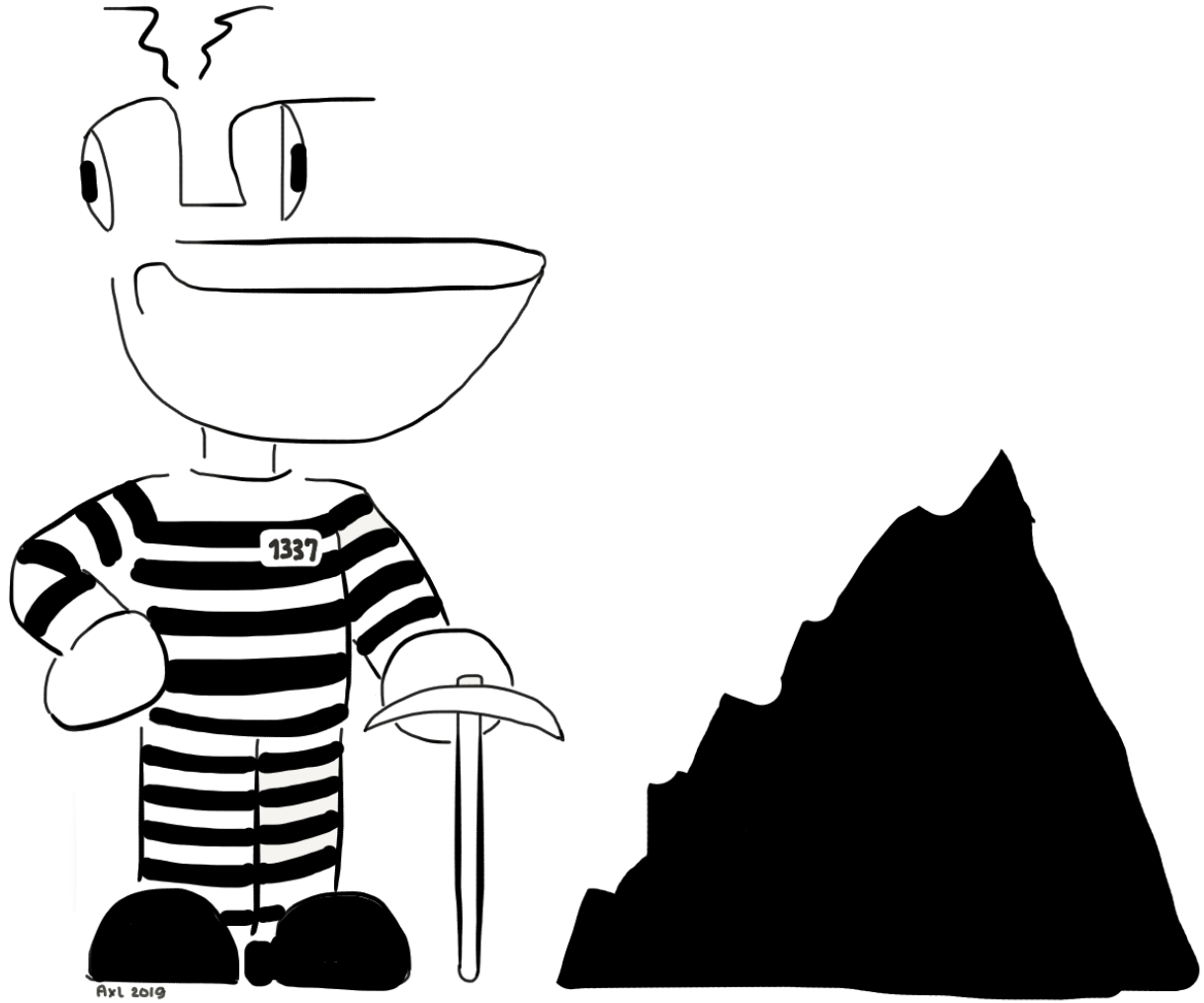
References:

- https://www.geekzone.co.nz/content.asp?contentid=3379
- https://www.fortiguard.com/encyclopedia/virus/906713
- https://github.com/cryptax/talks/tree/master/Confidence-2010
- https://web.archive.org/web/20120715000000*/https://www.securelist.com/en/blog/208193760/New_ZitMo_for_Android_and_Blackberry

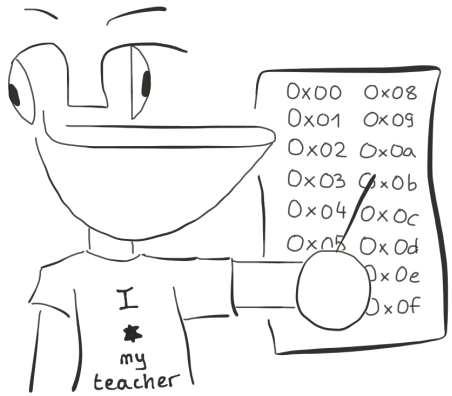
Mobile malware chronology

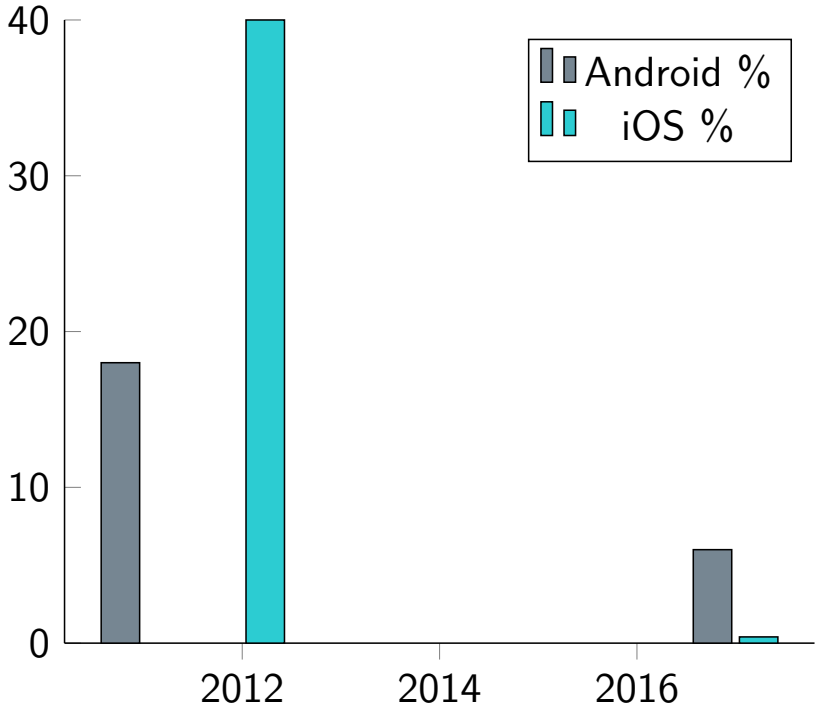


Rooting / Jailbreak phones used to be more common



Rooting iOS and Android

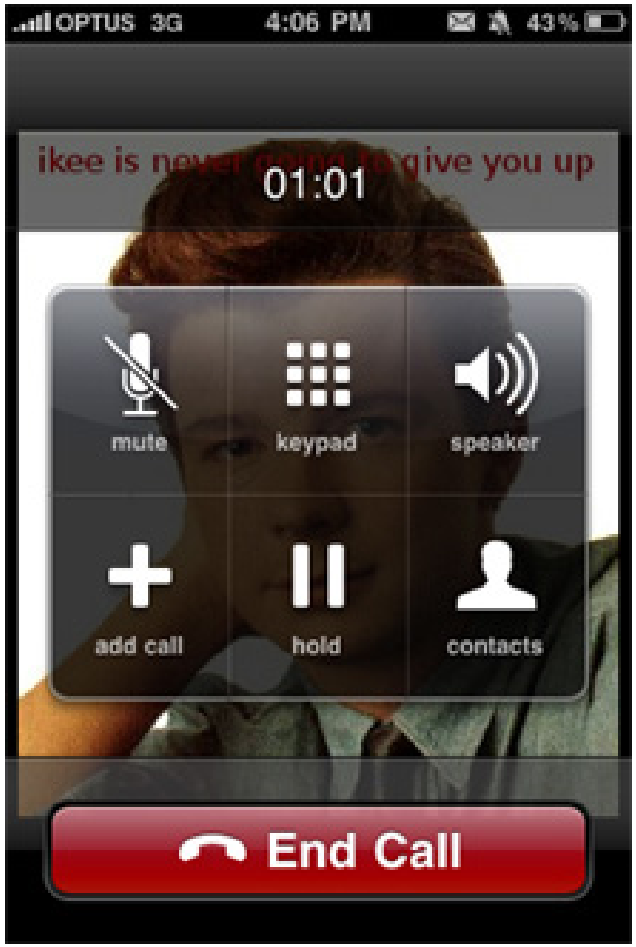




Motivations in 2012	**Motivations in 2023**
Access a large community of app	Install custom OS
Use important missing features e.g. share connection	Security research
Theme customization etc	

Quizz: Earn a collector sticker!

What was the modified root password?



iPhoneOS/Eeki.A (2009)

Picture from https://www.zdnet.com/article/rickroll-virus-attacks-iphones-3039867163/

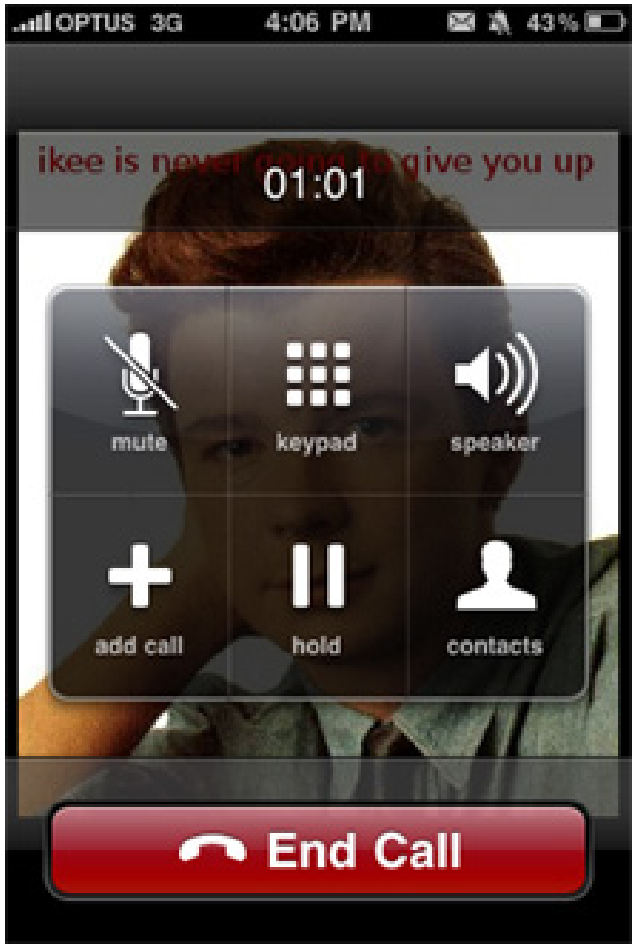
Collector sticker of Ph0wn CTF!

Quizz: Earn a collector sticker!

What was the modified root password?

`ohshit`

Eeki.B did something more dangerous, do you remember?



iPhoneOS/Eeki.A (2009)

Picture from https://www.zdnet.com/article/rickroll-virus-attacks-iphones-3039867163/

Collector sticker of Ph0wn CTF!

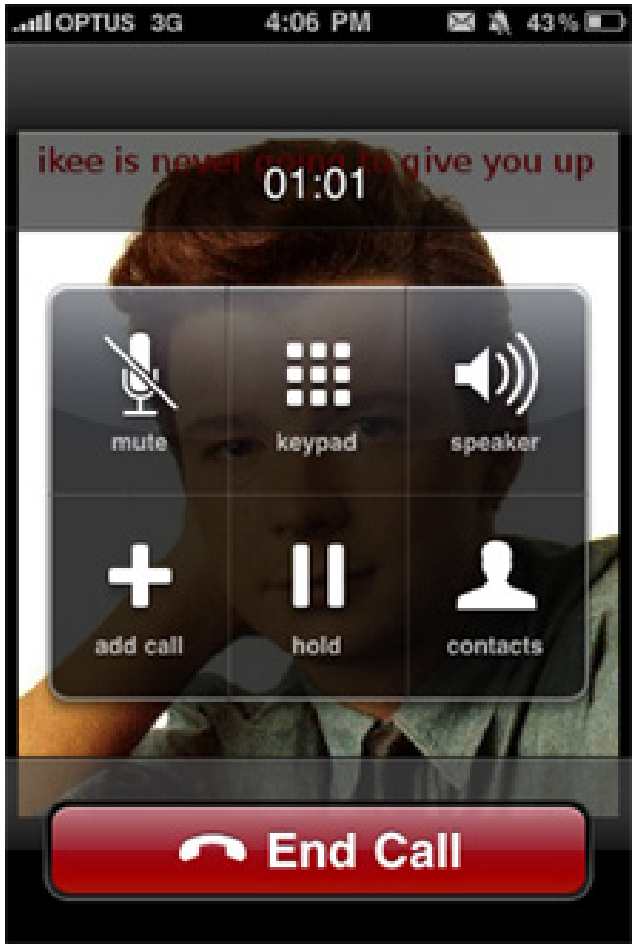
Quizz: Earn a collector sticker!

What was the modified root password?

`ohshit`

Eeki.B did something more dangerous, do you remember?

Redirected requests of mobile bank to a phishing website



iPhoneOS/Eeki.A (2009)

Picture from https://www.zdnet.com/article/rickroll-virus-attacks-iphones-3039867163/

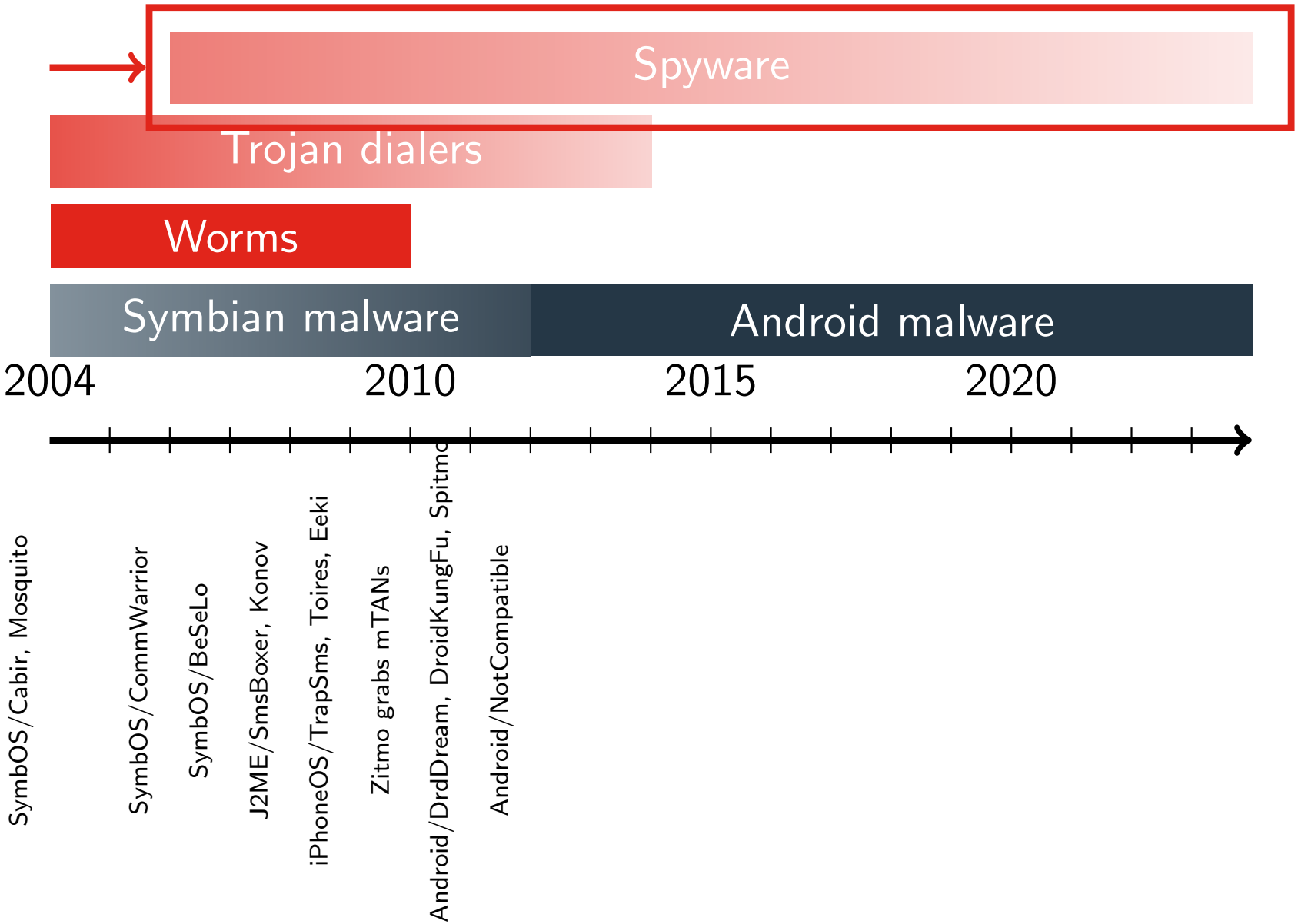
Collector sticker of Ph0wn CTF!

Many early Android malware use root exploits

Exploit	Malware
Exploid	DrdDream, Zhash
RATC	DrdDream, DroidKungFu (2011)
Gingerbreak	GingerMaster (2012)

- https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-SzalayChandraiah.pdf
- https://www.cs.ucr.edu/~zhiyunq/pub/ccs15_root_providers.pdf
- https://thehackernews.com/2012/02/androidbmaster-exploits-root-access-to.html
- https://www.trendmicro.com/fr_fr/research/17/i/zniu-first-android-malware-exploit-dirty-cow-vulnerability.html

Mobile spyware



Spyware appeared early, and are still around

SymbOS/Flexispy (2006)

SymbOS/CallMagic (2009)

References:

- https://www.f-secure.com/sw-desc/spyware-symbos-flexispy-f.shtml,
- https://www.fortiguard.com/encyclopedia/virus/1065586

2023: Spying is omnipresent

1. Adware, mobile analytics
2. Spouse, kid spyware
3. State-sponsored surveillance

References:

- https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/
- https://blog.talosintelligence.com/mercenary-intellexa-predator/
- https://www.virusbulletin.com/uploads/pdf/conference_slides/2013/dePontevesApvrille-VB2013.pdf

2023: Spying is omnipresent

Back to News

BLASTPASS

NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild

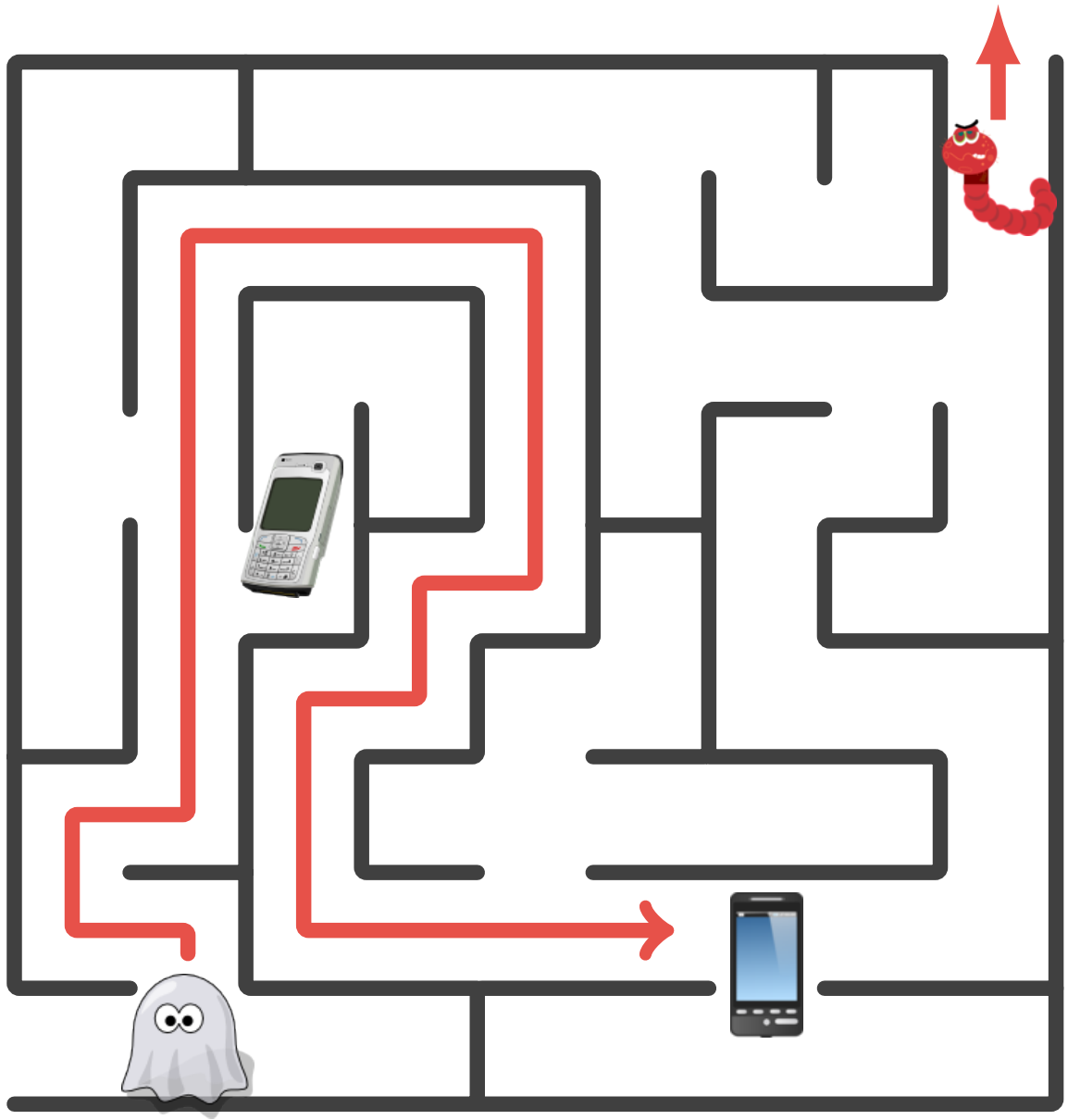
September 7, 2023

1. Adware, mobile analytics
2. Spouse, kid spyware
3. State-sponsored surveillance

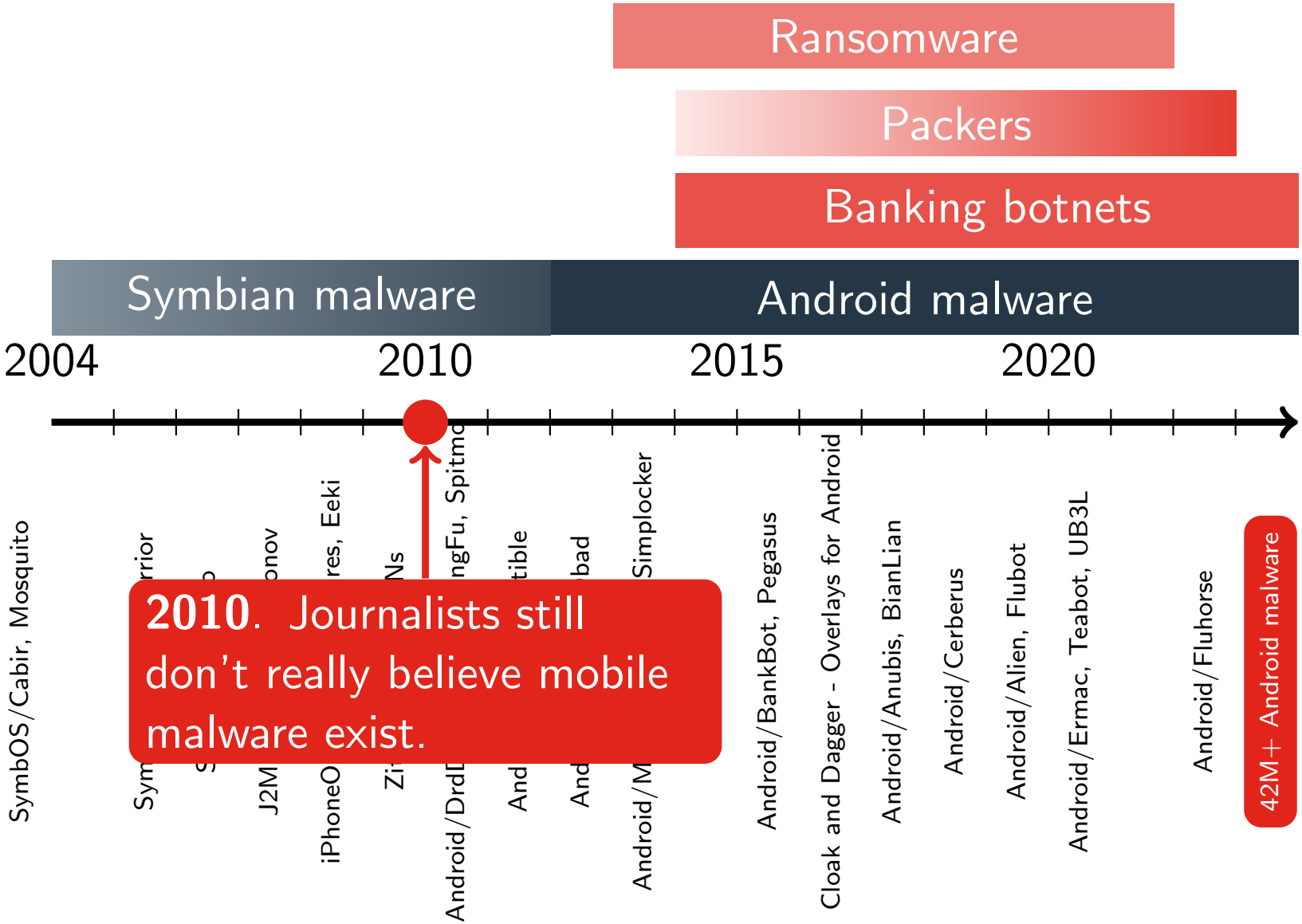
References:

- https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/
- https://blog.talosintelligence.com/mercenary-intellexa-predator/
- https://www.virusbulletin.com/uploads/pdf/conference_slides/2013/dePontevesApvrille-VB2013.pdf

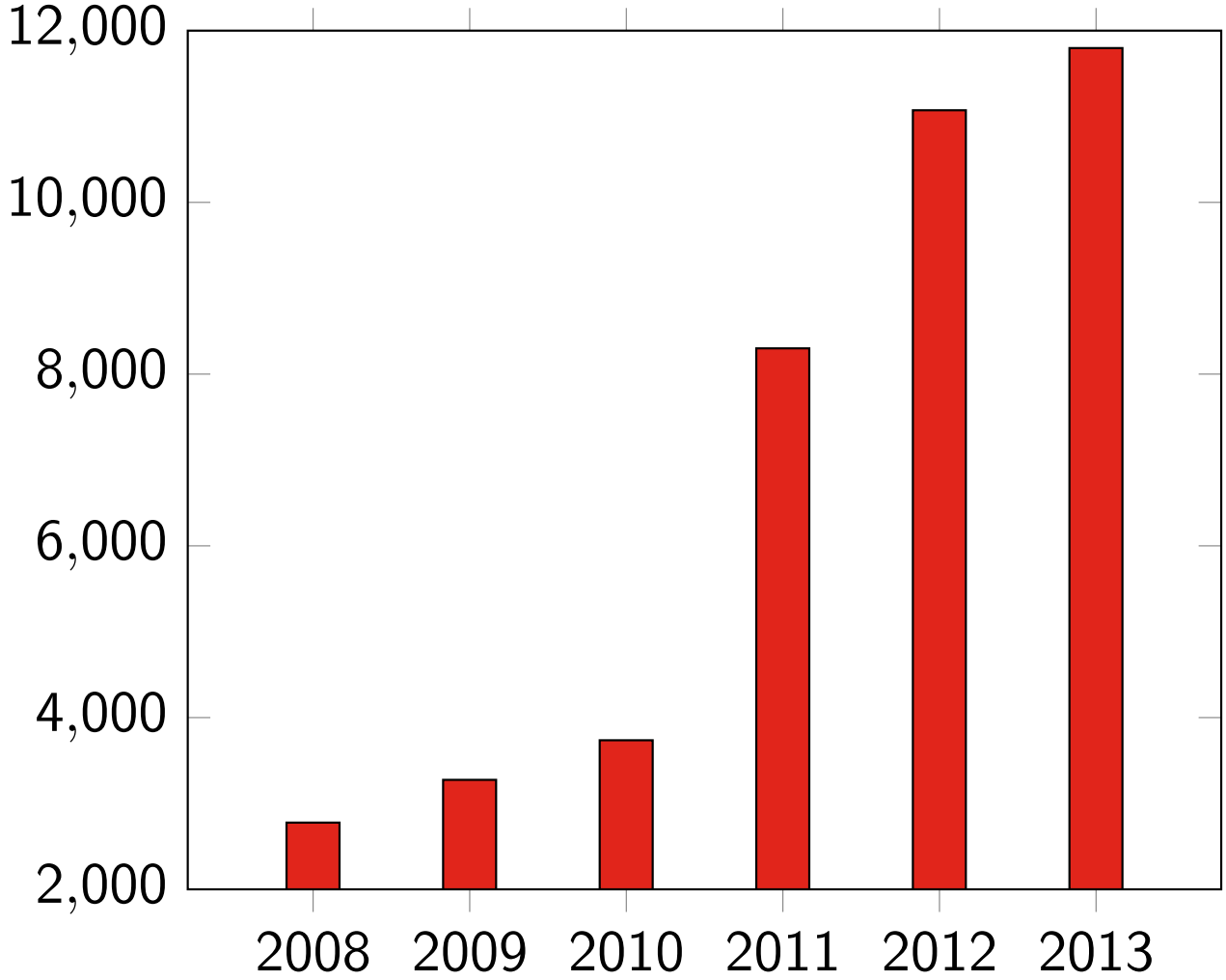
The Mobile Malware Maze



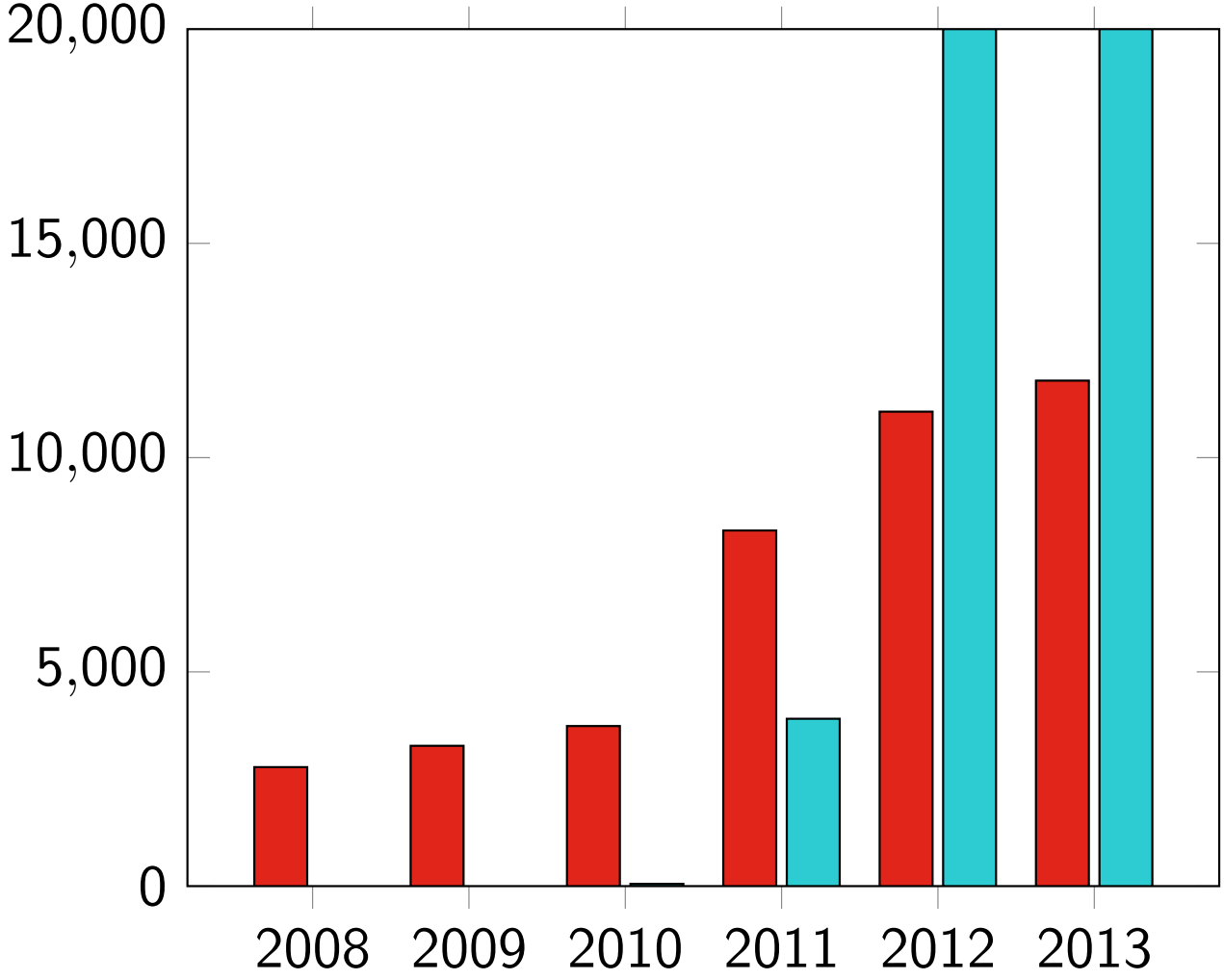
Explosion of Android malware



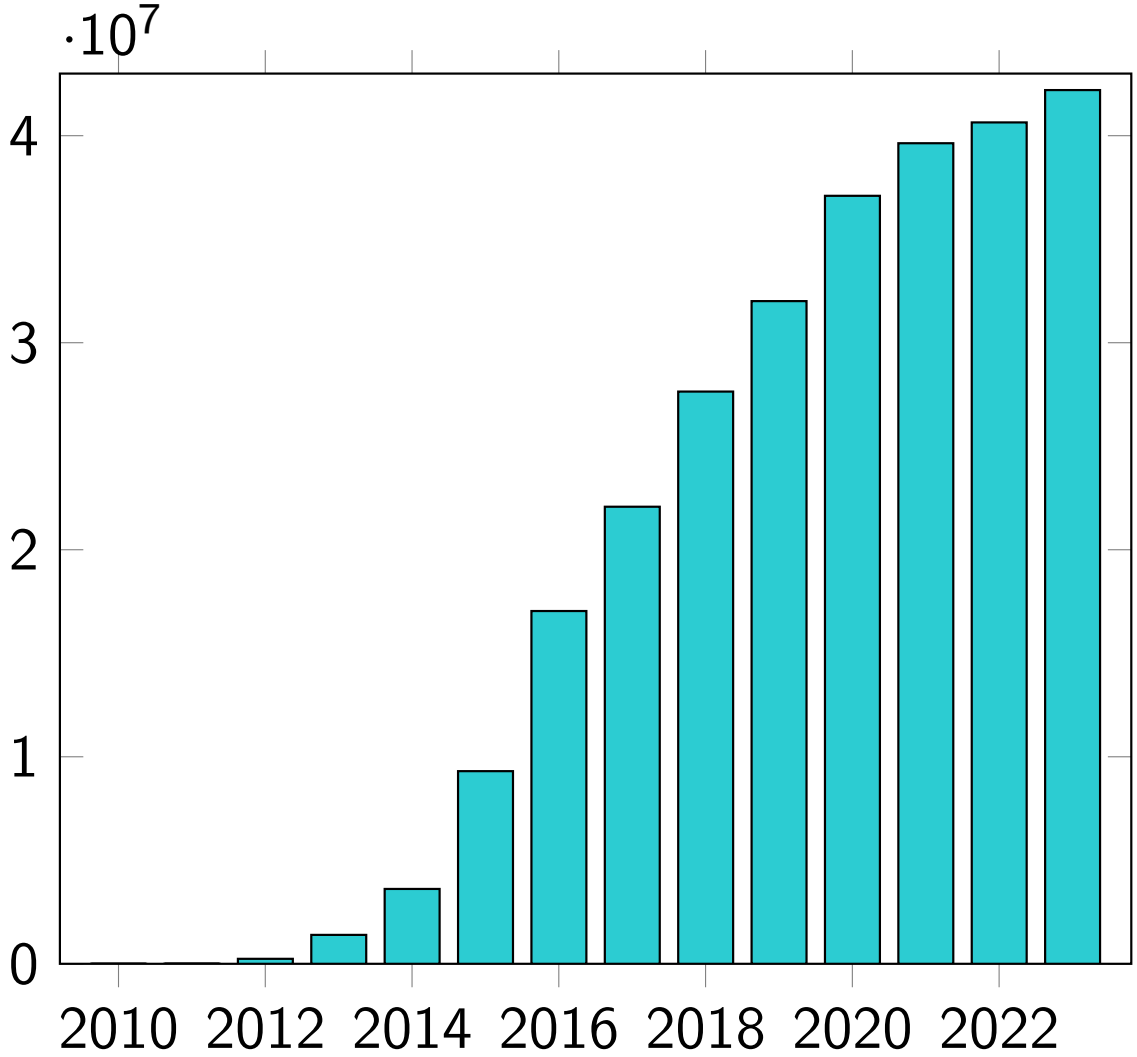
Malicious Symbian samples



Comparing Symbian malware and Android malware



Android malware dominate by 2012.
In 2013, only 3% of malware are on Symbian.



42 million malicious Android samples

but you need to understand what a sample is

Symbian: 12,000, iOS: 8,000

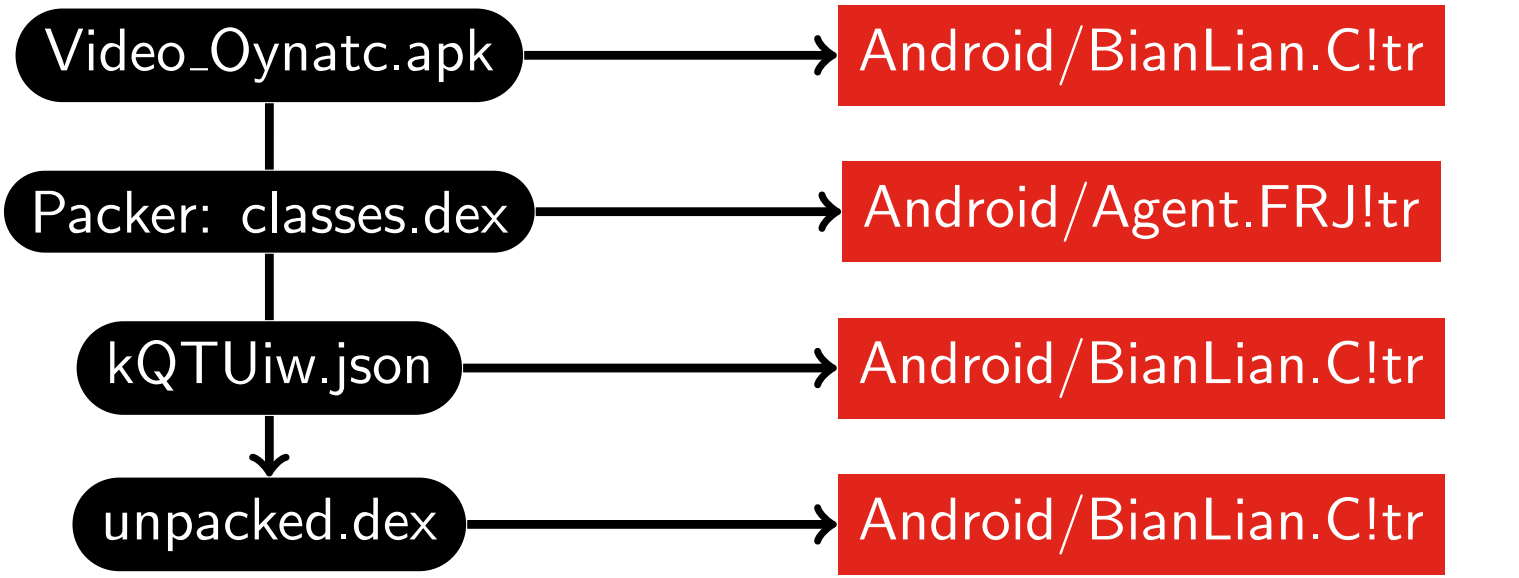
It's difficult to count malware

Possible approximations:

- Samples
- Families

The figures are approximate. The important point is that there is a **huge** amount of Android malware

Sample: a good approximation, but over-estimated



Count: **4** samples

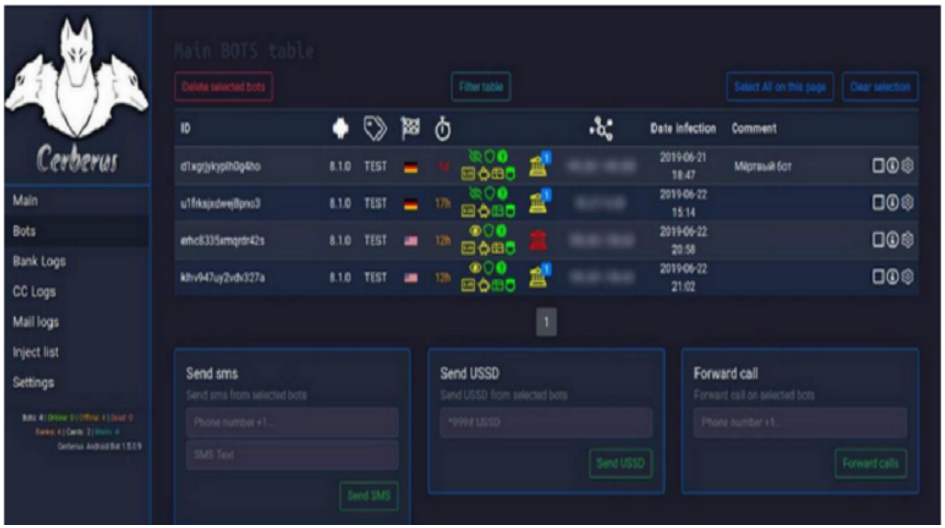
Families: would be nice... but nobody knows how to do it!

- There is **no document formally describing a given family**
- It would take **too many human resources** to do so!
- How do we name malware which re-use code from **2 different families**?
- There are **human errors** in naming: e.g BankBot vs BianLian
- Which name do we give to a **dropper** of various malware? BankBot!tr.dldr?
- Family names are **not universal** e.g BianLian, Hydra, Bian, Hqwar...

It's even worse than samples
Family count is different from one vendor to another

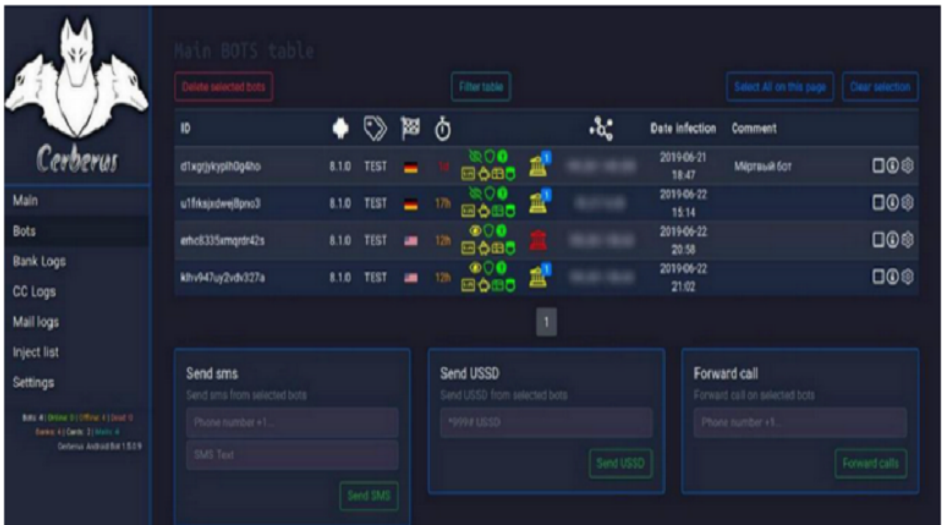
The Mobile Malware Maze

Current Trends: All in One Mobile Botnets



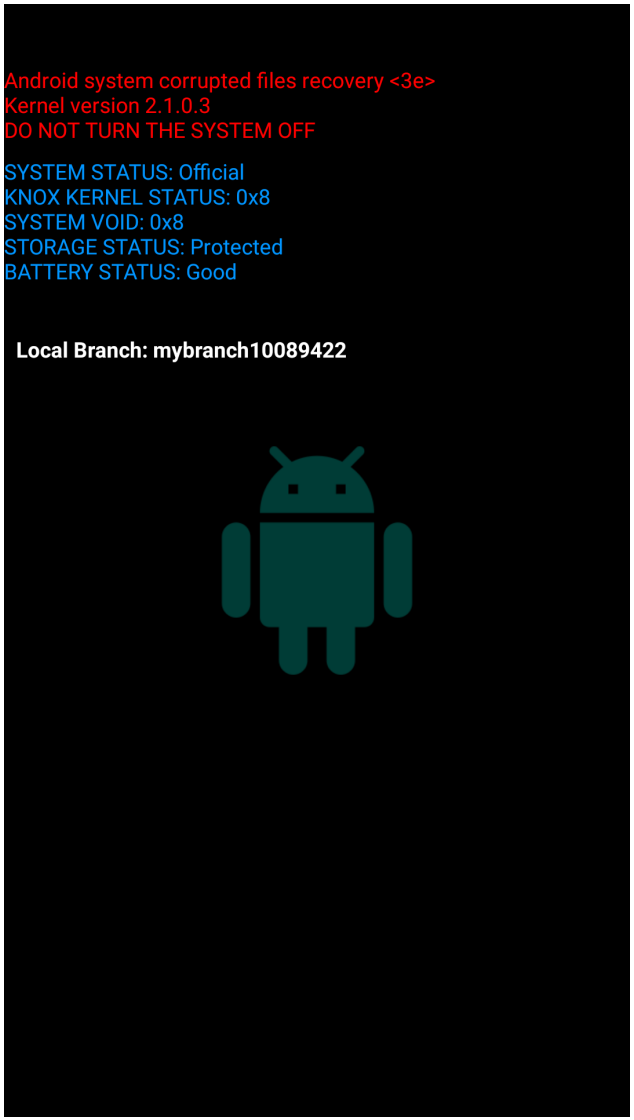
- Stealing credentials (banking trojan)

Current Trends: All in One Mobile Botnets



- Stealing credentials (banking trojan)
- Remote control (RAT)

Current Trends: All in One Mobile Botnets



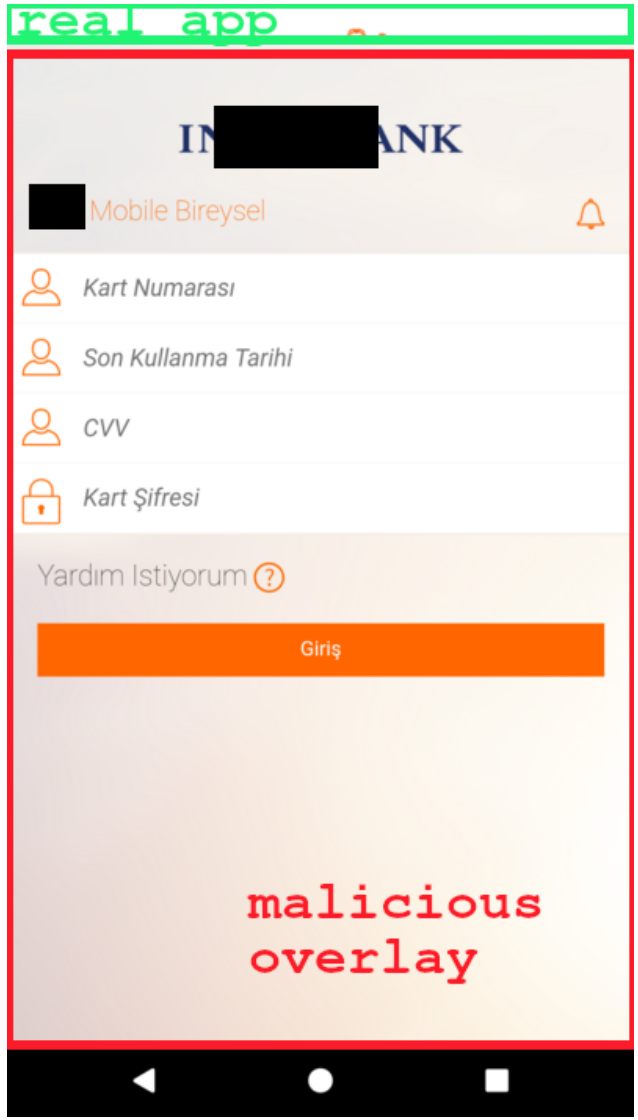
- Stealing credentials (banking trojan)
- Remote control (RAT)
- Screen lock, ransom (ransomware)

The typical Android malware in 2023

- Packed, and obfuscated

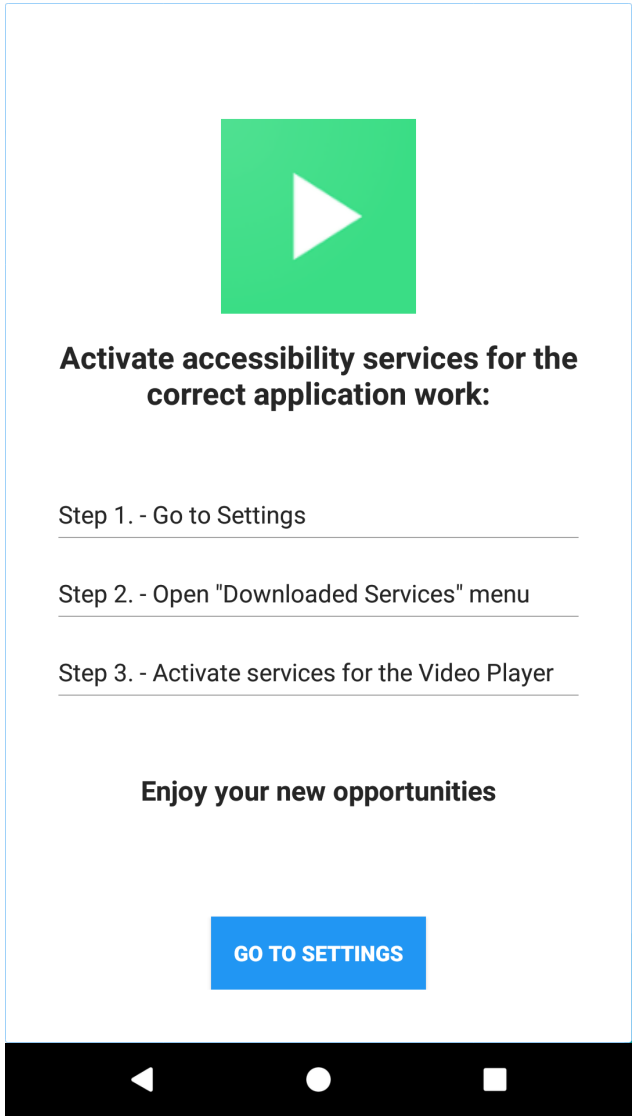
The typical Android malware in 2023

- Packed, and obfuscated
- Abuse the Accessibility API. Disable Play Protect, Display Overlays.

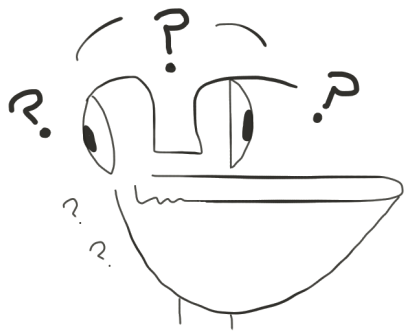


The typical Android malware in 2023

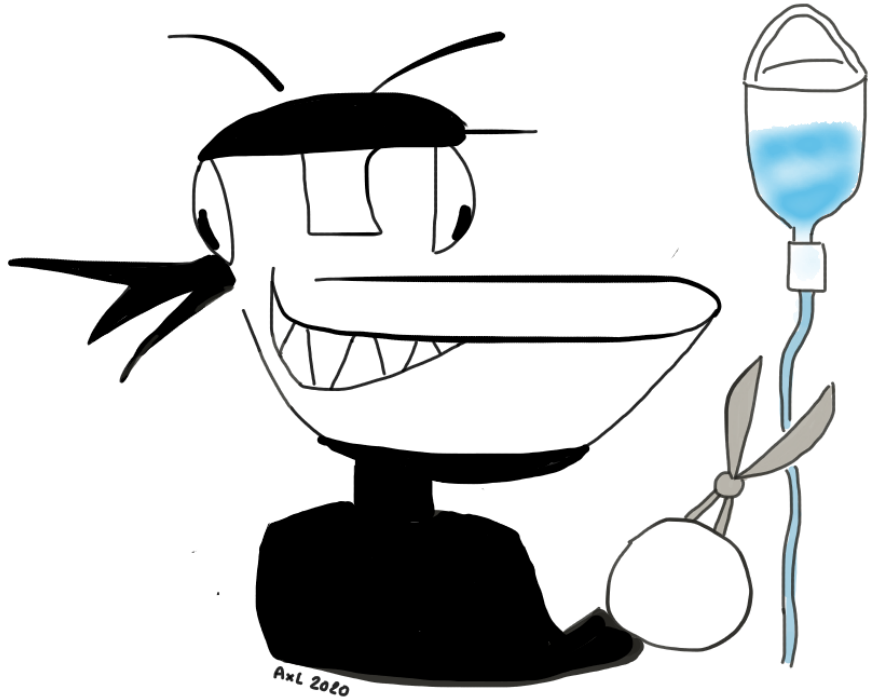
- Packed, and obfuscated
- Abuse the Accessibility API. Disable Play Protect, Display Overlays.
- Difficult to notice for the victim



Flutter: the new trend?



- With **Flutter**, develop with a **single codebase** for mobile platforms (and non-mobile), and compile **natively**
- Far more **difficult to reverse** for malware analysts
- Insufficient / Non adapted tools
- MoneyMonger, Fluhorse
- Read `https://www.fortinet.com/blog/threat-research/fortinet-reverses-flutter-based-android-malwa`



Threat Actors

This is the PAST

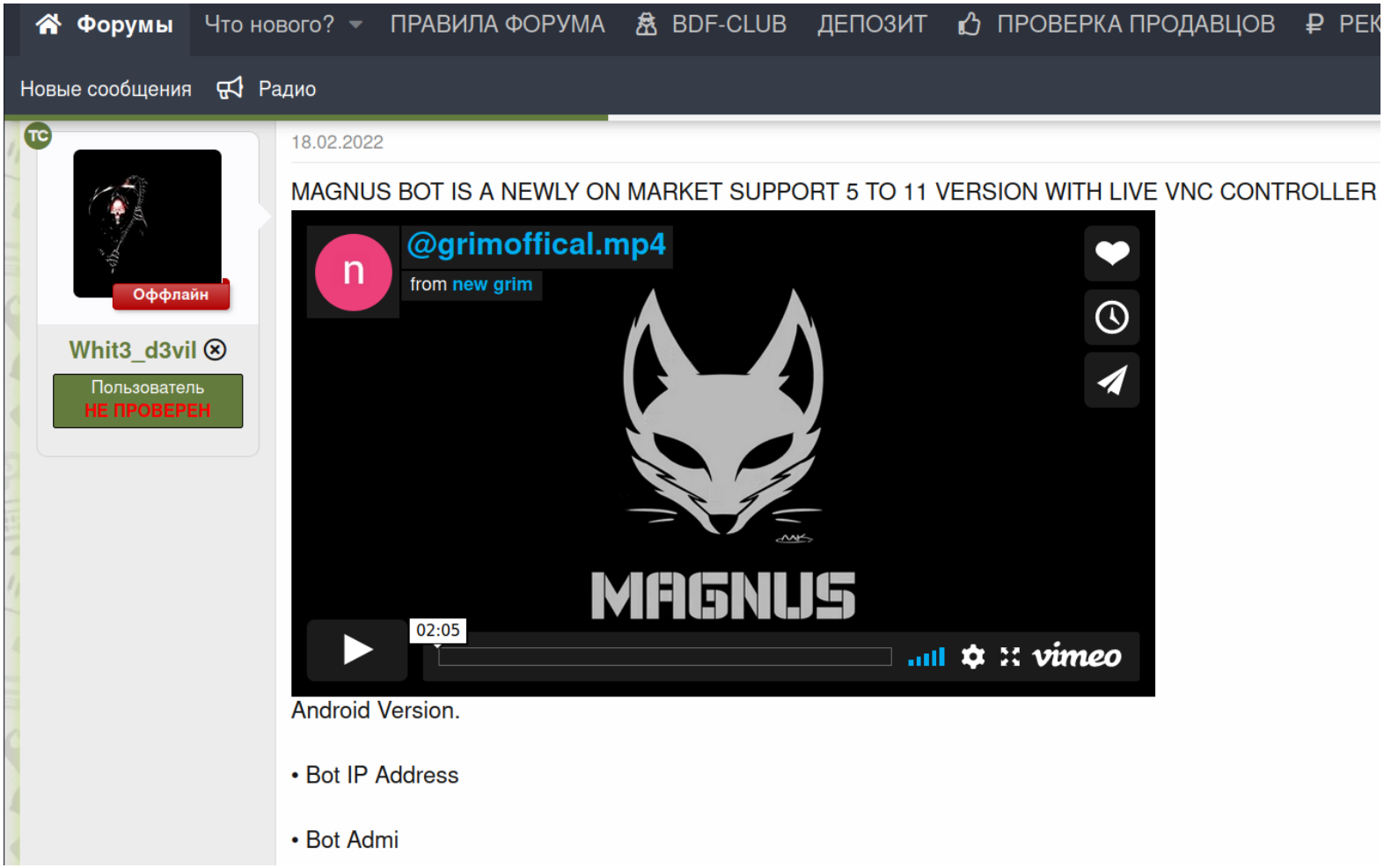
- **1971**. Bob Thomas creates *Creeper* as **Proof of Concept**
- **1975**. John Walker wrote *Animal* specifically to cause **no harm**.
- **1982**. Richard Skrenta wrote *Elk Cloner* at 15, to **play pranks**
- **1986**. Basit (19) and Amjad Farooq Alvi wrote a *boot sector virus* to **protect their own heart monitoring program**.
- **1989**. Dr Joseph Pope wrote *AIDS* ransomware to **donate the funds to AIDS**.

Created for money, political strategy or warfare

Cybercriminals advertize on Telegram

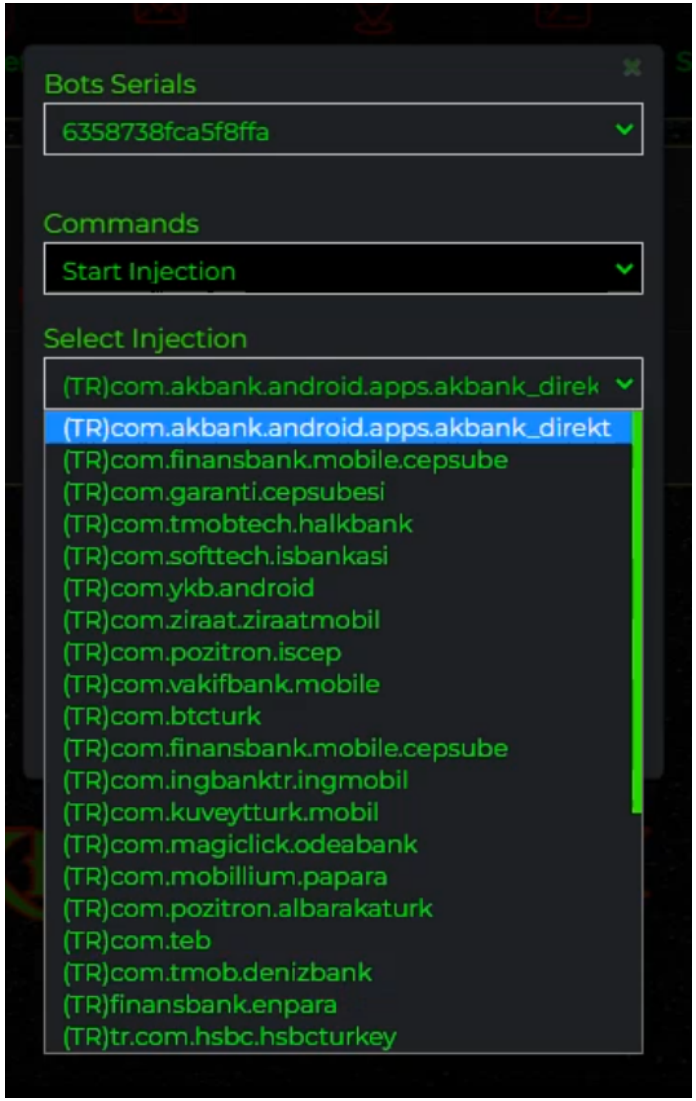
Craxs RAT for Android

They promote their work with videos



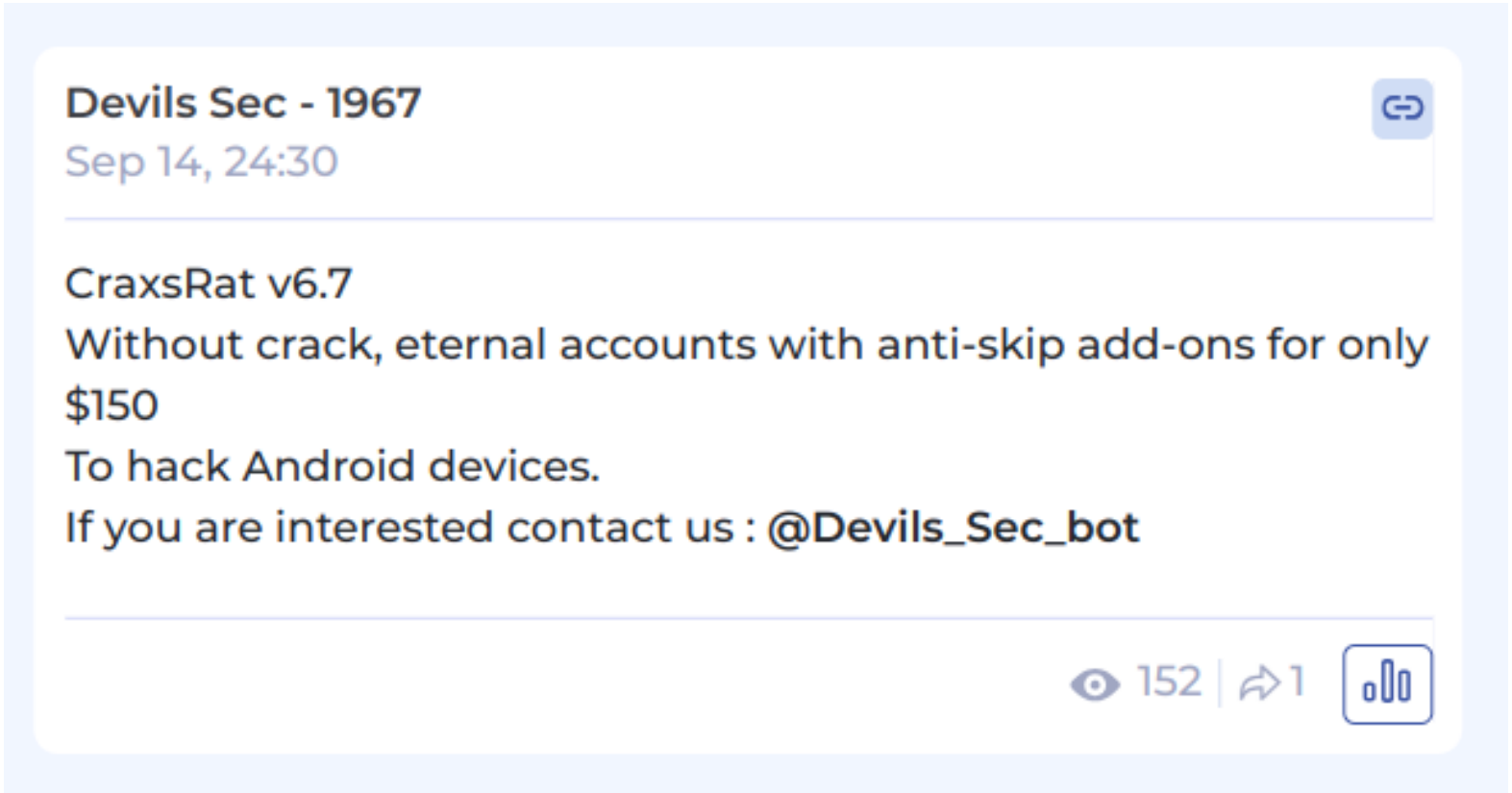
See https://www.fortinet.com/blog/threat-research/grim-magnus-android-botnets

They provide demos

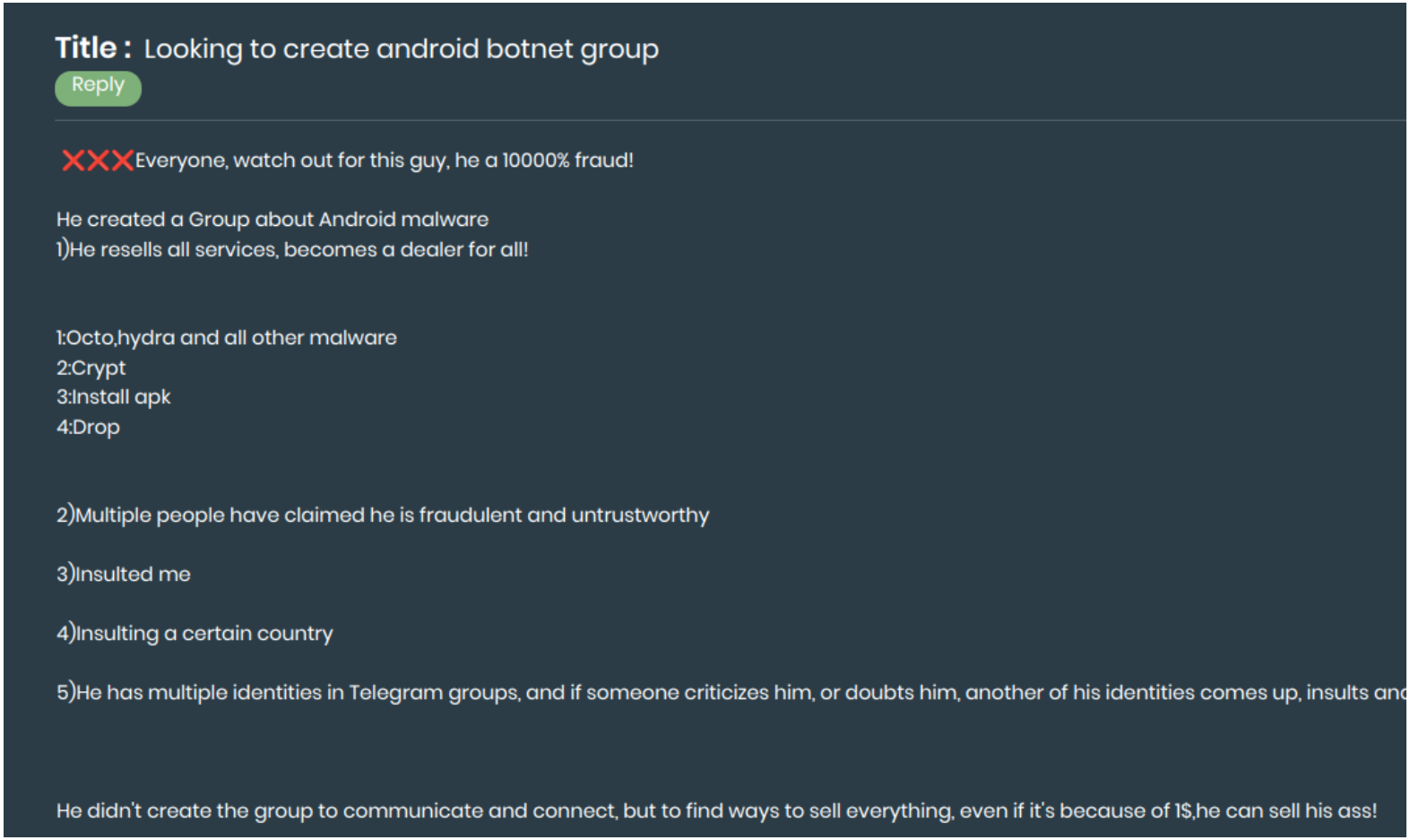


GRIM bot

They sell underground



Sometimes, they steal each other!



Title : Looking to create android botnet group

Reply

❌❌❌Everyone, watch out for this guy, he a 10000% fraud!

He created a Group about Android malware
1)He resells all services, becomes a dealer for all!

1:Octo,hydra and all other malware
2:Crypt
3:Install apk
4:Drop

2)Multiple people have claimed he is fraudulent and untrustworthy

3)Insulted me

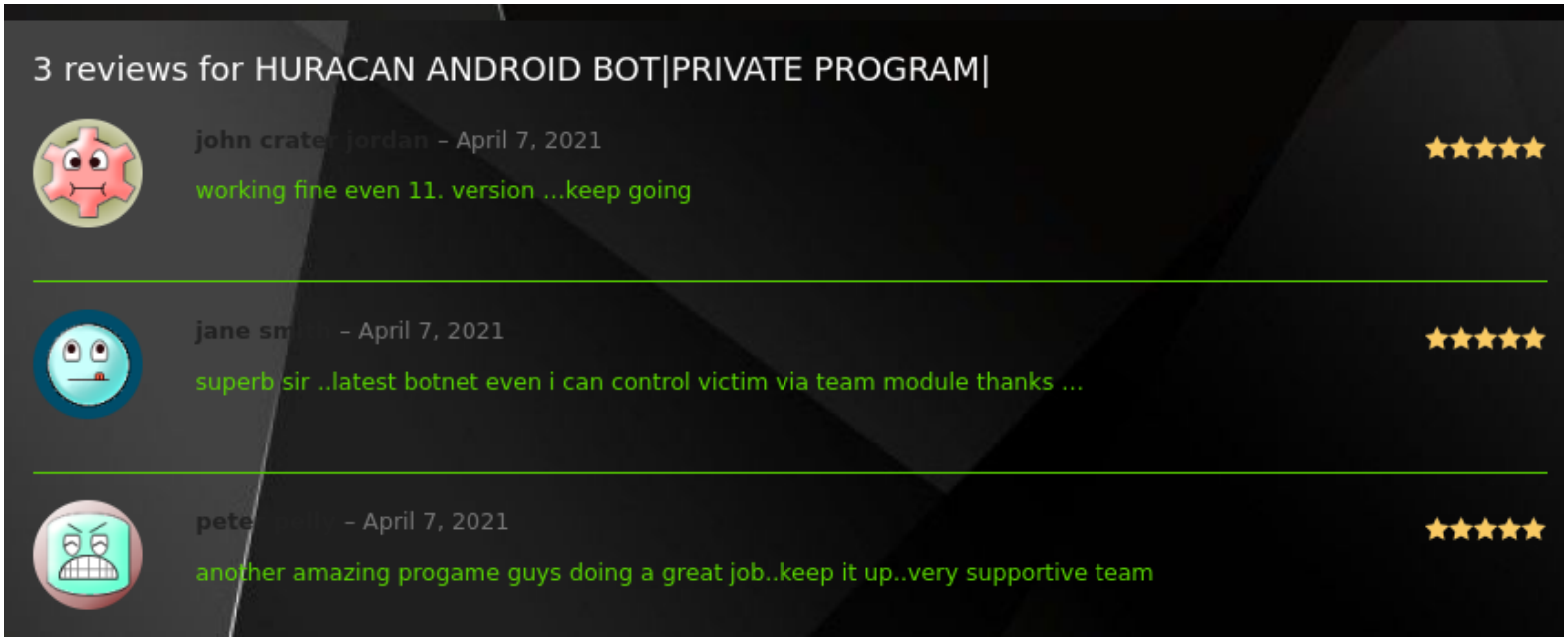
4)Insulting a certain country

5)He has multiple identities in Telegram groups, and if someone criticizes him, or doubts him, another of his identities comes up, insults and

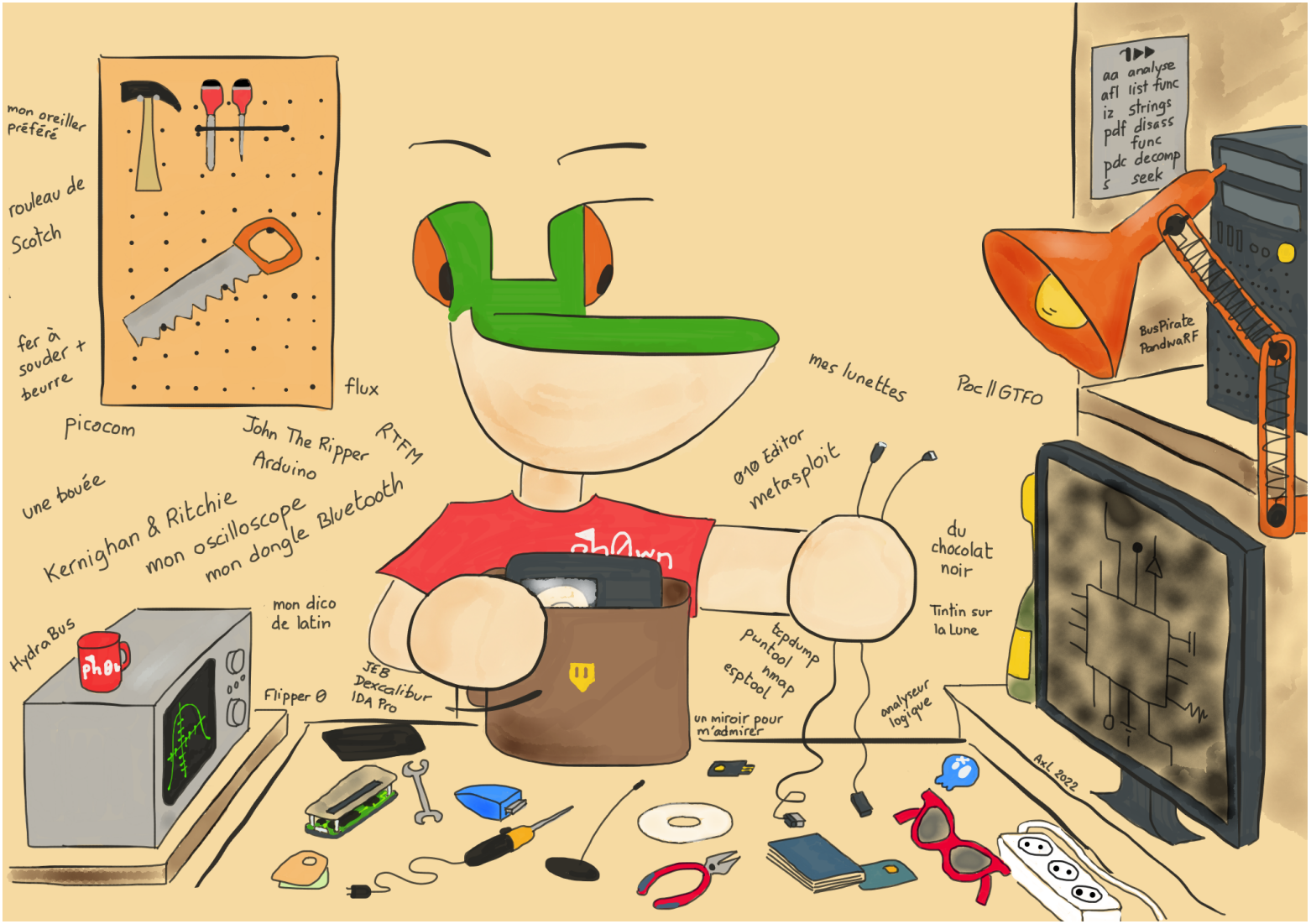
He didn't create the group to communicate and connect, but to find ways to sell everything, even if it's because of 1$,he can sell his ass!

Taken from FortiRecon service

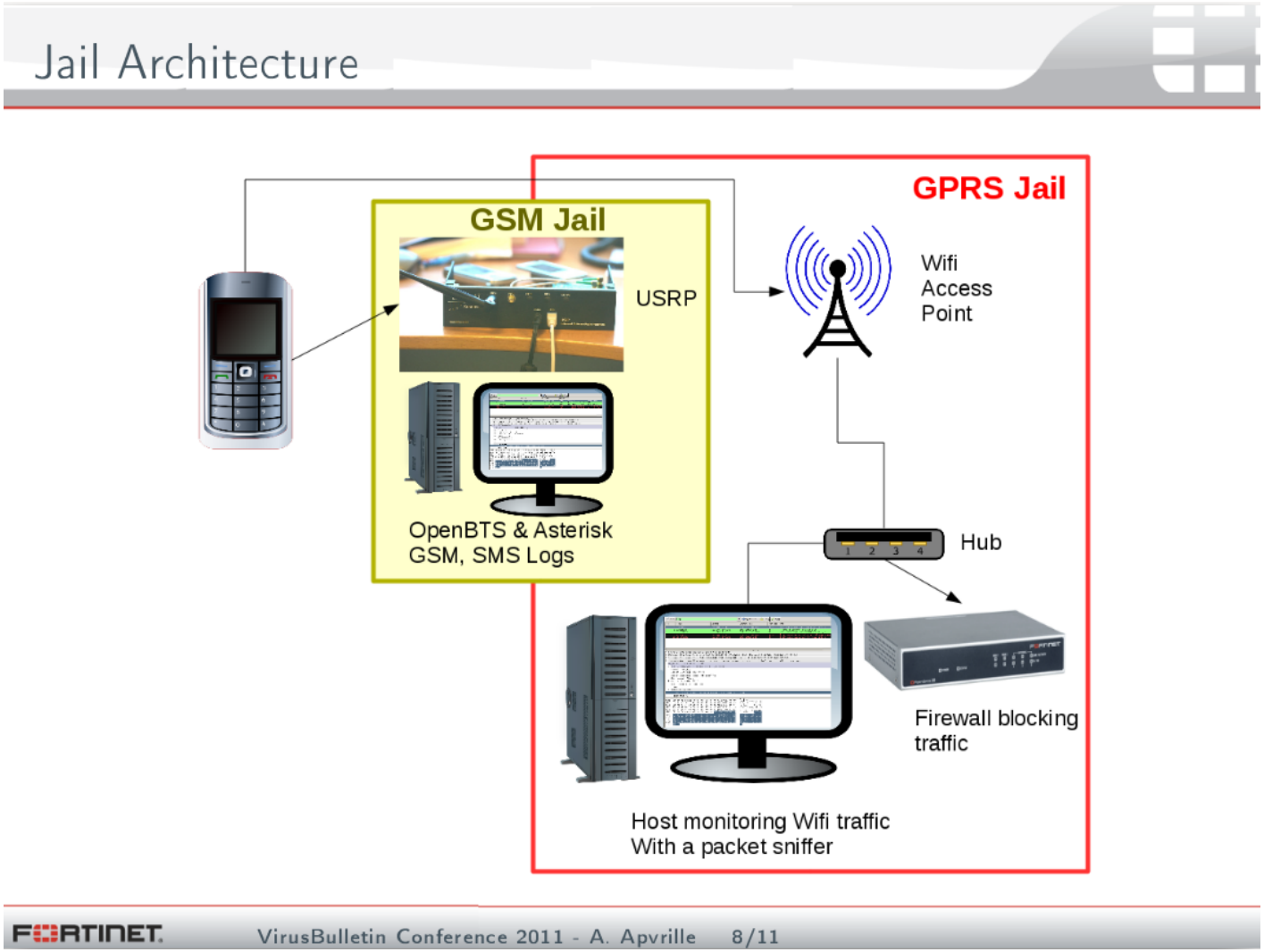
Their bots get reviewed



Tools


mon oreiller préféré
rouleau de Scotch
fer à souder + beurre
flux
Picocom
John The Ripper
RTFM
Arduino
une bouée
Kernighan & Ritchie
mon oscilloscope
mon dongle Bluetooth
mes lunettes
Poc || GTFO
aa analyse
afl llist func
iz strings
pdf disass func
pdc decomp
s seek
BusPirate
PandwaRF
0x0 Editor
metasploit
du chocolat noir
Tintin sur la Lune
tcpdump
Puntool
nmap
esptool
analyseur logique
un miroir pour m'admirer
JEB
Dexcalibur
IDA Pro
Flipper 0
mon dico de latin
HydraBus
AxL 2022

We usually don't need USRP or OpenBTS anylonger



Presented at Virus Bulletin, 2011

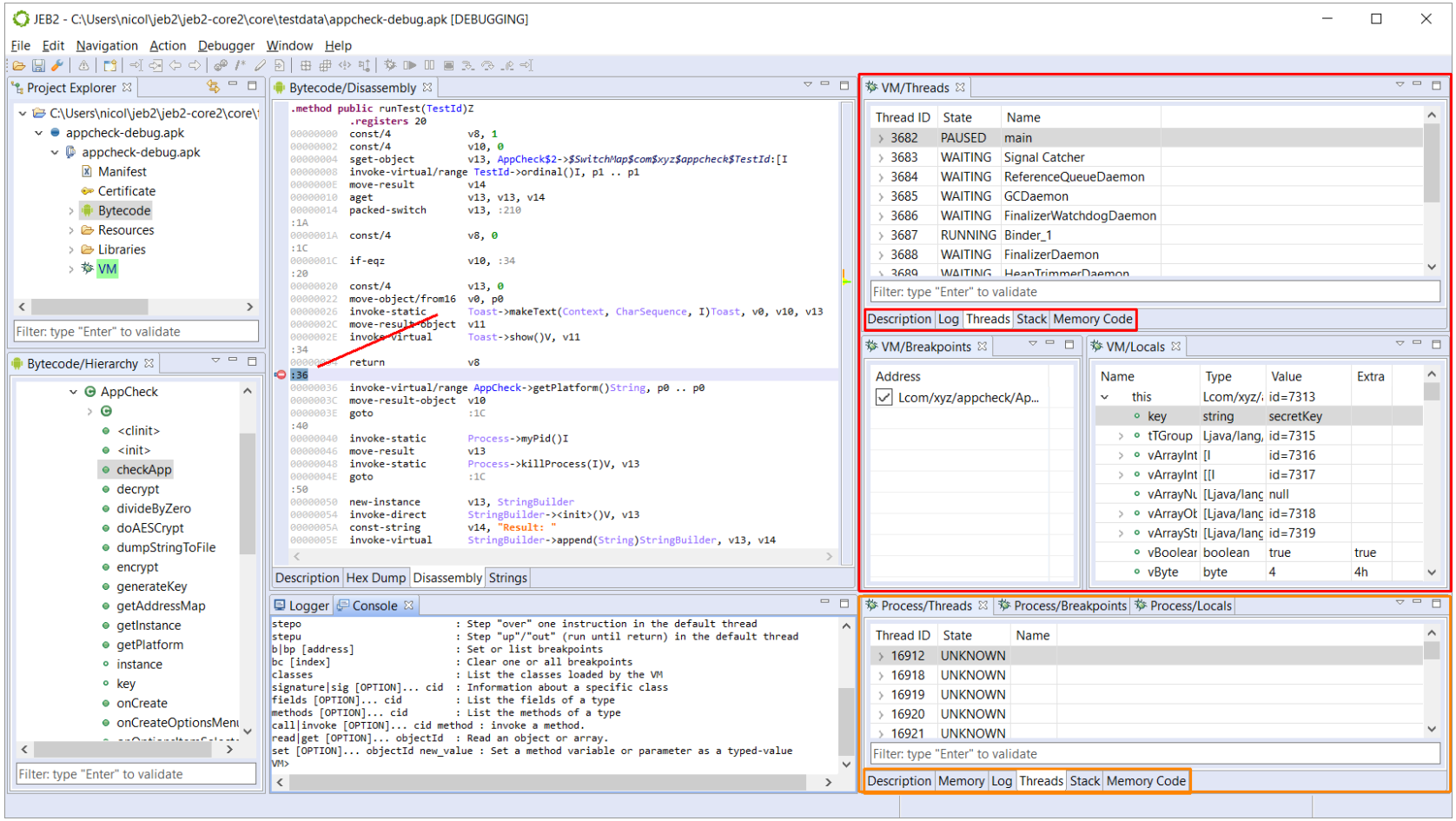
Debugging used to be difficult to setup

- **2009**. AppTrk for Symbian with IDA Pro.
- **2011**. AndBug uses the Java Debug Wire Protocol to interact with Android apps. More like a preliminary Frida.

```
andbug shell –pid 1662
>> methods
com.android.insecurebankv2.DoTransfer
```

2023: Debugging is still difficult

- **Frida** (2015). **Instrumentation, not really a debugger**. But very helpful. Create hooks.
- **JEB Debugger** (2016). Limited inspects of variables.



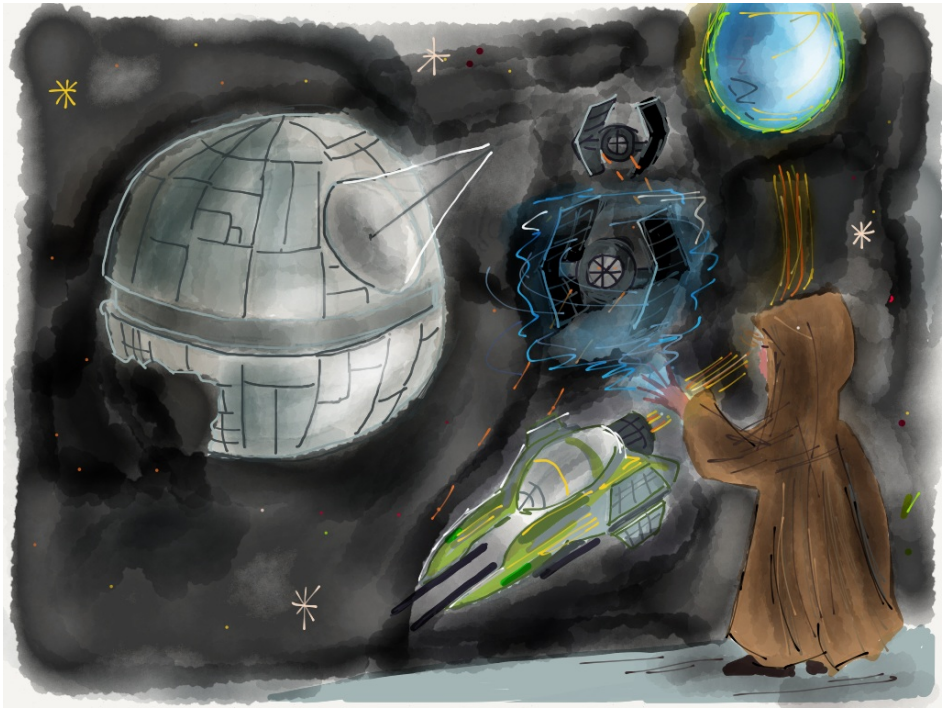
Source: https://www.pnfsoftware.com/jeb/manual/debugging/

Dynamic analysis is **ev1l**

Static analysis **ruleZ**

Why you should limit dynamic analysis

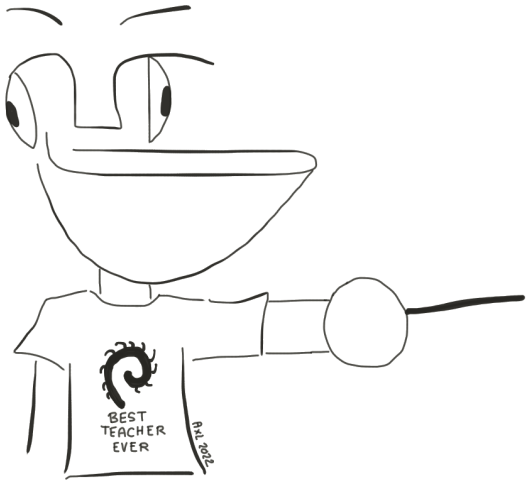
1. You are being lazy. Don't give into the Dark Side.
2. You won't see it all.
3. You risk propagation.
4. You provide information to Threat Actors.



Conclusion

**So, did you enjoy it?*

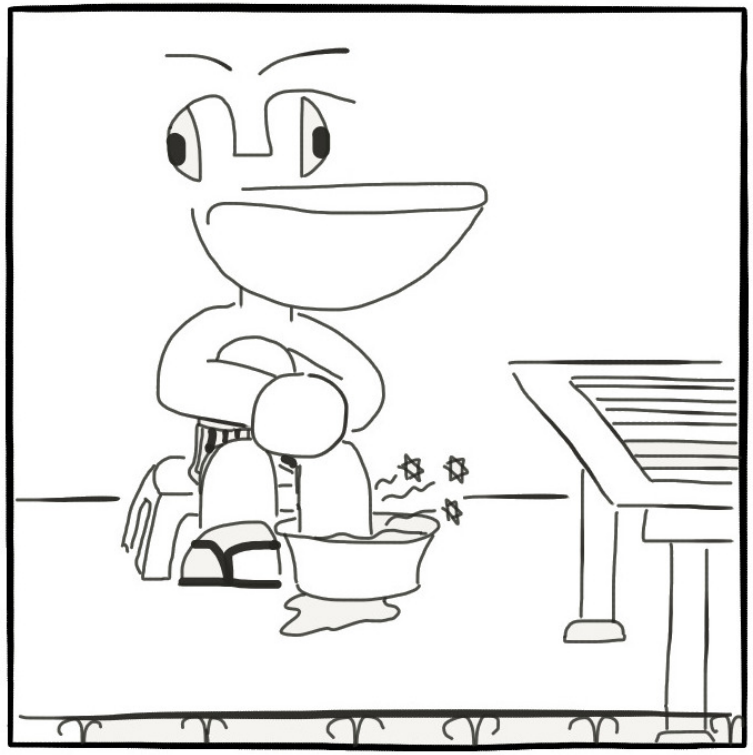
Topics of Interest for Research



- Debuggers
- Symbolic execution
- Detection of AI generated malware
- Dealing with cross-platform malware
- Write **articles** and backup them to you can recover them in 15 years!

Are you working on **Security** or **In-Security**?

Don't shoot in yourself in the foot!



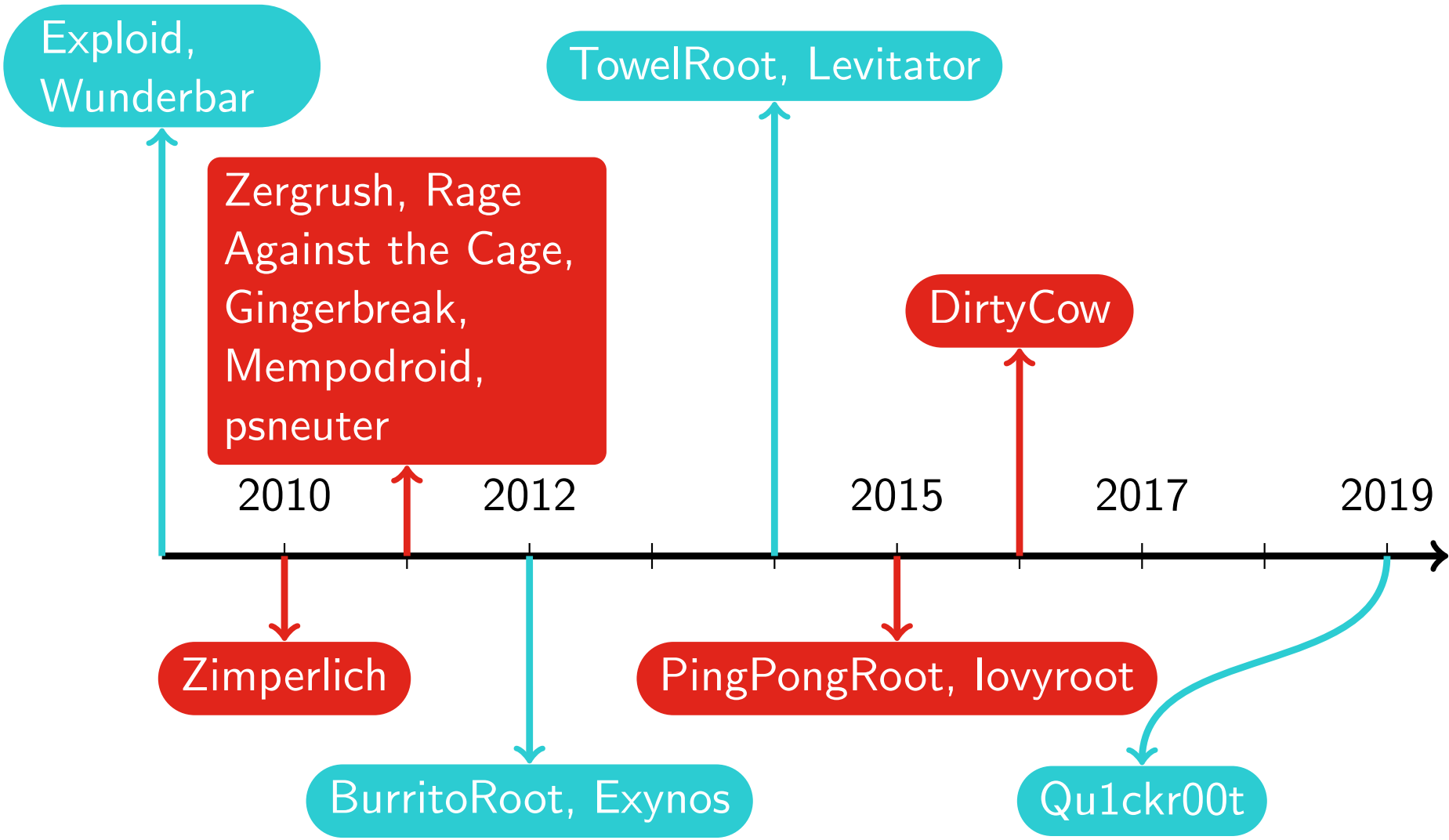
Questions?

Contact:
Mastodon:
@cryptax@mastodon.social
X: @cryptax
E-mail: aapvrille@fortinet.com

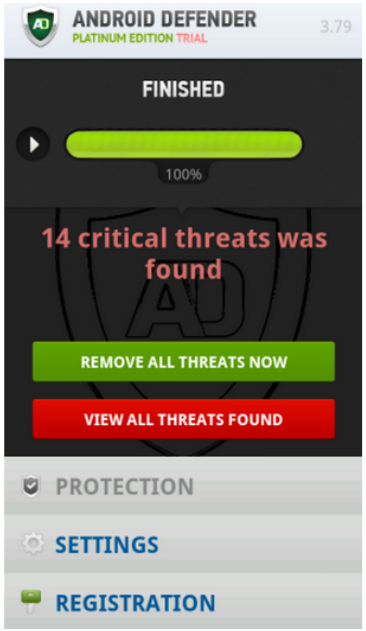
Feel like a CTF on smart devices in a sunny location? Join **Ph0wn CTF** on November 25, 2023!
French Riviera, https://ph0wn.org
Mastodon: @ph0wn@infosec.exchange
X: @ph0wn

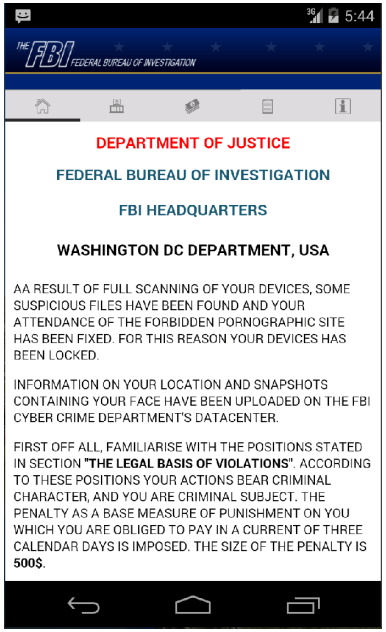
Those slides were created with LaTeX
Pico le Croco is a character I created many years ago - his website https://pico.masdescrocodiles.fr
I am longing for belgian waffles

Android root exploits



Mobile Ransomware





References:

- https://www.virusbulletin.com/virusbulletin/2016/12/vb2015-paper-android-ransomware-turning-cryptolocker-crypto-unlock
- https://www.fortinet.com/blog/threat-research/locker-an-android-ransomware-full-of-surprises
- https://web-assets.esetstatic.com/wls/2016/02/Rise_of_Android_Ransomware.pdf

Still maintained and helpful

- APKTool
- AXMLPrinter
- Smali / Baksmali
- Dex2Jar
- DroidLysis

New

- Frida, and Frida-based tools
- Better decompilers
- Faster emulators

RIP

- Androsim, dedexer...