Mal ware

Un 10mTalk sui malware

FinFisher

germany

https://en.wikipedia.org/wiki/FinFisher

Pegasus

NSO Group



Hacking team

Italy

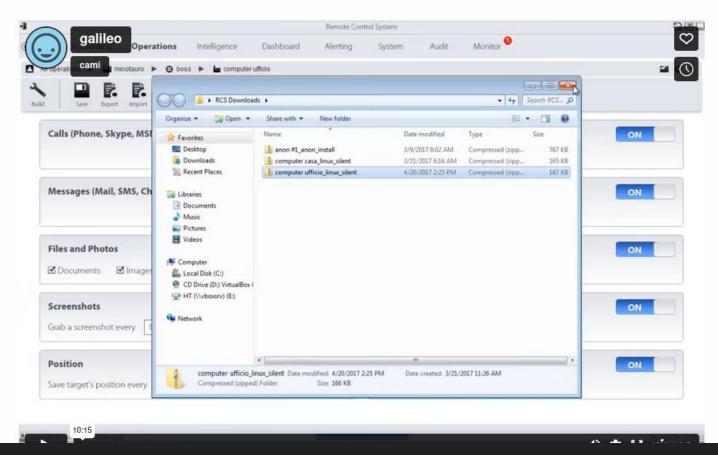
https://wikileaks.org/hackingteam/

hackOrDIYE

malware?

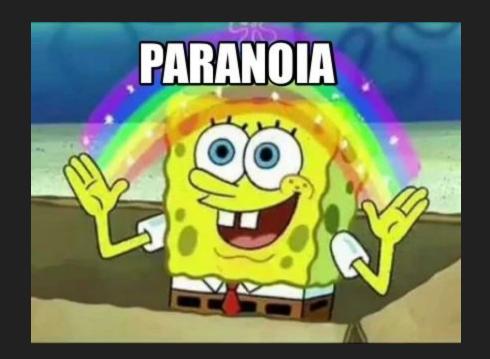
Cosa sono i trojan?

Di trojan di stato - details



https://www.autistici.org/underscore/di-trojan-di-stato-details.html

Si ma quindi, paranoia?



Come facciamo col telefono?

Il telefono



???

Brucia il telefono

E nella lotta contro il tempo che ci impone la macchina, che carte gioca il goderere del tempo, il produttivismo, l'essere sempre localizzabile e il fatto che i nostri affetti passano per tim, wind o laika?

https://bruciailtelefono.noblogs.org/

Brucia il telefono

Il controllo della polizia
Le intercettazioni
La localizzazione
Gli IMSI-catchers
I captatori informatici
La retenzione dei dati
I telefoni intelligenti
Buone pratiche

Il controllo sociale
Più isolatx
Più scemx
Più spettatricx
Lettera di unx tossicx

Responsabili ed implicazioni Finanziare il capitale

Yes, but I need to use that!

- Limit mobile usage
- Disable notifications sounds and vibrations
- Don't use many groups
- Don't click on random links (via chat app but also via SMS!)
- Don't open weird attachments (such as random video)
- Encrypt your phone
- Update your phone anytime you can
- Leave your phone home anytime you can
- Don't power off the phone before a meeting or an action
- Do not rely on phone for important communications

And..

And even that my device is acting suspiciously, WTF!

- Don't panic
- Limit usage to minimal conversation
- Enable device usb debug
- Enable traffic notification systray
- Run a backup via adb

And use some of these tools to analyze malwares

Mobile Verification Toolkit



https://github.com/mvt-project/mvt

Mobile Verification Toolkit

Mobile Verification Toolkit (MVT) is a collection of utilities to simplify and automate the process of gathering forensic traces helpful to identify a potential compromise of Android and iOS devices.

https://docs.mvt.re/en/latest/install/

androidQF

https://github.com/botherder/androidqf

```
C:\androidgf windows amd64.exe
                androidaf - Android Ouick Forensics
Started new acquisition dad557de-c457-45fd-aa23-3f3fedd07e92
Extracting device properties...
Extracting device settings...
Extracting list of running processes...
Extracting device diagnostic information. This might take a while...
Downloading copies of installed apps...
Found a total of 331 installed packages
Would you like to download copies of all apps or only non-system ones?
v Only non-system packages
Found Android package: system.framework
Downloaded /data/app/~~ouN9uPoDFrrXECbW3wT92g==/system.framework-A8rmOWm9ftj09nDxRcdasg==/base.apk to dad557de-c457-45f
 aa23-3f3fedd07e92\apks\system.framework system.framework-A8rmOWm9ftj09nDxRcdasg.apk
Would you like to take a backup of the device?
v Only SMS
Generating a backup with argument com.android.providers.telephony. Please check the device to authorize the backup...
Backup completed and stored at dad557de-c457-45fd-aa23-3f3fedd07e92\backup.ab
Acquisition completed.
Press Enter to finish ...
```

Civilsphere VPN

https://www.civilsphereproject.org/



- Ask for an Emergency VPN
- Receive the VPN files
- Install wireguard on your phone
- Use the VPN for 5 days
- Wait for Civilsphere report
- Remove wireguard
- Receive VPN report
- You may know if you have malware

Yea, but who is fighting against that?

- This malware business is big
- Surveillance Capitalism is increasing
- Activists are in constant threat
- Market not regulated
- Early laws on malware lacks of consistency and reality
- Usage is up to every administration
- We know individuals and corporation can buy this technology
- We need someone able to inform and contrast on that

Citizenlab – http://citizenlab.ca



Amnesty.tech



Hackmeeting.org





*

Samba

;

@

*

Autistici

4

org