El pot de mel

Una història real de hackers a l'Escola

Amb la col·laboració de:
Jordi Enric Martínez Osorio

Dr. Daniel Guasch Murillo

26 de setembre de 2024

Departament d'Enginyeria Telemàtica
UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú

Una història real de hackers a l'Escola

És un dijous tranquil abans de la classe de Seguretat i Administració de Xarxes (SEAX)...

Els TIC es reuneixen per iniciar la primera reunió del dia: esmorzar al bar de l'EPSEVG...

...i descobreixen un fet inquietant: una publicació a la xarxa X esmenta que un servidor de la UPC ha estat víctima d'un ciberatac...

Departament d'Enginyeria Telemàtica

Links

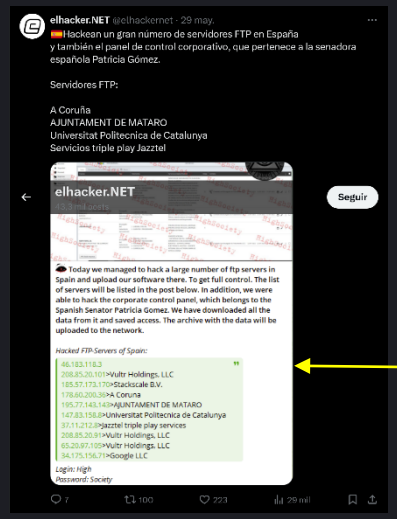
El cas del pot de mel

V

La víctima...

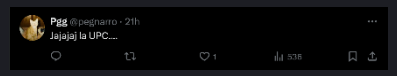
La víctima...

El 2024-05-29 s'han publicat uns missatges pertorbadors a X ...

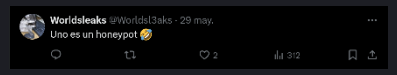


@elhackernet: l'origen...

El servidor d'FTP 147.83.158.8 de la UPC ha estat hackejat...



@pegnarro: l'oportunista...

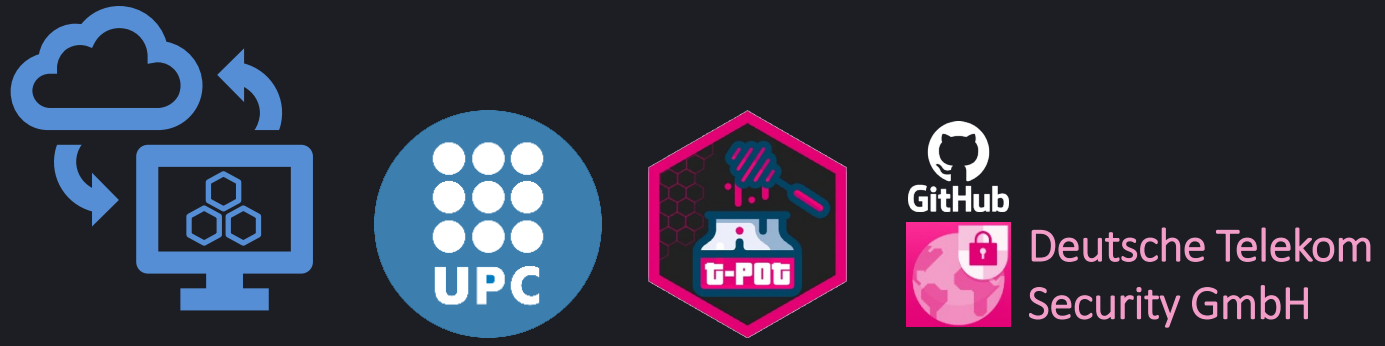


@Worldsl3aks: el curiós... "un és un honeypot!"

https://x.com/elhackernet/status/1795765134465405168?s=46&t=Lu9tDQ9xF8B32ayGabhS1g

La víctima...

El servidor 147.83.158.8 és un honeypot d'ENTEL a l'EPSEVG de la UPC...

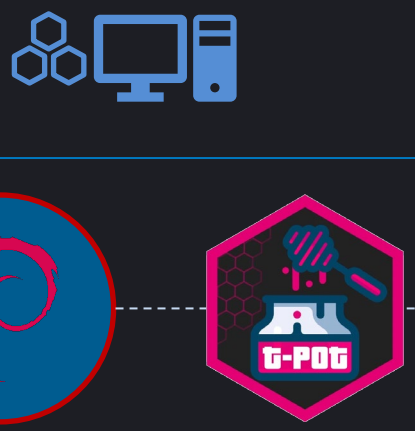


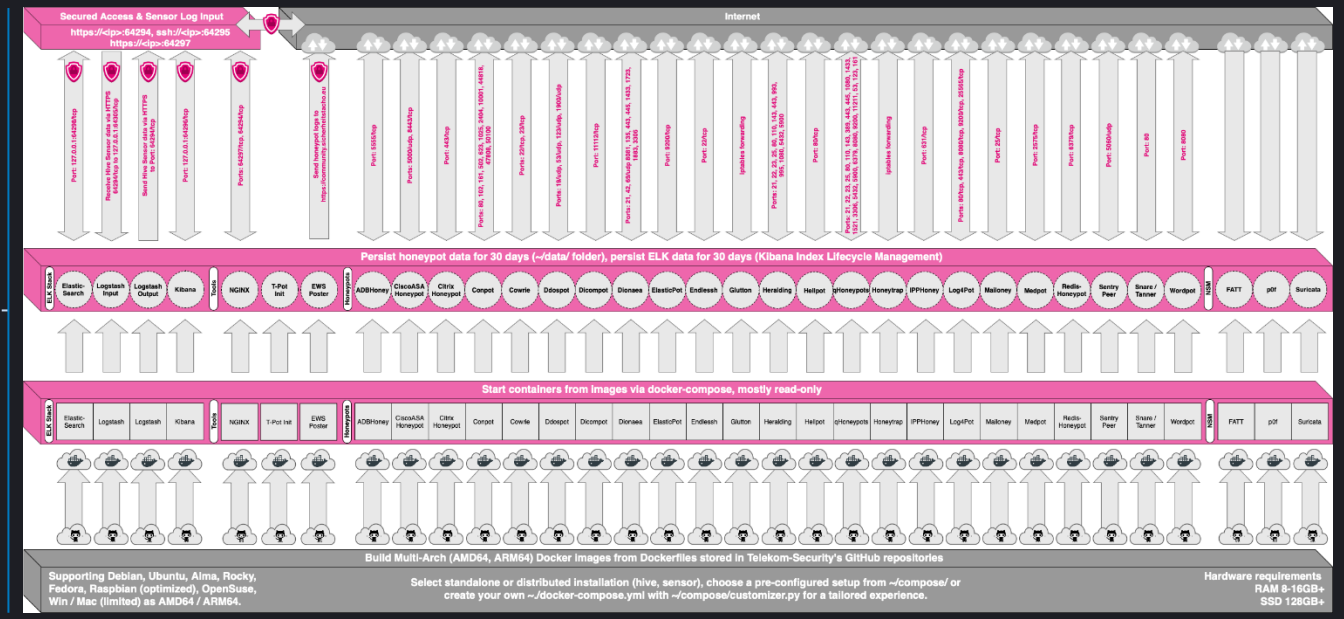
...en missió permanent d'explorar nous atacs, de cercar nous hackers i conèixer nous serveis, arribant allà on no ha estat mai ningú.

Vaja, com la nau estel·lar Enterprise d'Star Trek , però en versió honeypot!

La víctima...

El servidor està basat en una distribució Linux Debian i el honeypot T-Pot...





Alhora, T-Pot és un conjunt de 24 honeypots especialitzats, amb les utilitats d'administració i gestió de la informació corresponents.

https://github.com/telekom-security/tpotce

La víctima...

El sistema analitza i emmagatzema contínuament el tràfic de xarxa adreçat a ell, amb un històric de fins a 3 mesos.


```
[root@dullpie:/data]# du -sh /data
40G     /data
[root@dullpie:/data]# du -s /data
41766236        /data
```

En el moment de l'anàlisi emmagatzema 40 Gbytes de dades d'atacs.

https://www.debian.org COCKPIT https://cockpit-project.org/running

La víctima...

El honeypot es capaç de respondre correctament a peticions d'FTP i permetre un accés fictici...


```
root@toc:~# ftp root@147.83.158.8
Connected to 147.83.158.8.
220 FTP server ready.
331 Password required for root.
Password:
230 User logged in, proceed
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated.  Commands are:

!               edit            lpage           nlist           rcvbuf          struct
$               epsv            lpwd            nmap            recv            sunique
account         epsv4           ls              ntrans          reget           system
append          epsv6           macdef          open            remopts         tenex
ascii           exit            mdelete         page            rename          throttle
bell            features        mdir            passive         reset           trace
binary          fget            mget            pdir            restart         type
bye             form            mkdir           pls             rhelp           umask
case            ftp             mls             pmlsd           rmdir           unset
cd              gate            mlsd            preserve        rstatus         usage
cdup            get             mlst            progress        runique         user
chmod           glob            mode            prompt          send            verbose
close           hash            modtime         proxy           sendport        xferbuf
cr              help            more            put             set             ?
debug           idle            mput            pwd             site
delete          image           mreget          quit            size
dir             lcd             msend           quote           sndbuf
disconnect      less            newer           rate            status
ftp> status
Connected and logged into 147.83.158.8.
No proxy connection.
Gate ftp: off, server (none), port ftpgate.
Passive mode: on; fallback to active mode: on.
Mode: stream; Type: binary; Form: non-print; Structure: file.
Verbose: on; Bell: off; Prompting: on; Globbing: on.
Store unique: off; Receive unique: off.
Preserve modification times: on.
Case: off; CR stripping: on.
Ntrans: off.
Nmap: off.
Hash mark printing: off; Mark count: 1024; Progress bar: on.
Get transfer rate throttle: off; maximum: 0; increment 1024.
Put transfer rate throttle: off; maximum: 0; increment 1024.
Socket buffer sizes: send 16384, receive 131072.
Use of PORT cmds: on.
Use of EPSV/EPRT cmds for IPv4: on.
Use of EPSV/EPRT cmds for IPv6: on.
Command line editing: on.
Version: tnftp 20210827
ftp> exit
221 Goodbye.
root@toc:~#
```

```
root@toc:~# tcpdump host 147.83.158.8
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens18, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:39:27.036222 IP toc.catac.upc.edu.58098 > 147.83.158.8.ftp: Flags [S], seq 2551888237, win 65535, options [mss 1460,sackOK,TS val 3206810901 ecr 0,nop,wscale 2], length 0
10:39:27.041364 IP 147.83.158.8.ftp > toc.catac.upc.edu.58098: Flags [S.], seq 3700492641, ack 2551888238, win 65160, options [mss 1460,sackOK,TS val 2207156703 ecr 3206810901,nop,wscale 7], length 0
10:39:27.041379 IP toc.catac.upc.edu.58098 > 147.83.158.8.ftp: Flags [.], ack 1, win 16384, options [nop,nop,TS val 3206810906 ecr 2207156703], length 0
10:39:27.042935 IP 147.83.158.8.ftp > toc.catac.upc.edu.58098: Flags [P.], seq 1:24, ack 1, win 510, options [nop,nop,TS val 2207156709 ecr 3206810906], length 23: FTP: 220 FTP server ready.
10:39:27.042960 IP toc.catac.upc.edu.58098 > 147.83.158.8.ftp: Flags [.], ack 24, win 16384, options [nop,nop,TS val 3206810907 ecr 2207156709], length 0
10:39:27.043148 IP toc.catac.upc.edu.58098 > 147.83.158.8.ftp: Flags [P.], seq 1:12, ack 24, win 16384, options [nop,nop,TS val 3206810908 ecr 2207156709], length 11: FTP: USER root
10:39:27.043405 IP 147.83.158.8.ftp > toc.catac.upc.edu.58098: Flags [.], ack 12, win 510, options [nop,nop,TS val 2207156710 ecr 3206810908], length 0
10:39:27.077652 IP 147.83.158.8.ftp > toc.catac.upc.edu.58098: Flags [P.], seq 24:57, ack 12, win 510, options [nop,nop,TS val 2207156744 ecr 3206810908], length 33: FTP: 331 Password required for root.
10:39:27.120132 IP toc.catac.upc.edu.58098 > 147.83.158.8.ftp: Flags [.], ack 57, win 16384, options [nop,nop,TS val 3206810985 ecr 2207156744], length 0
10:39:30.232276 IP toc.catac.upc.edu.58098 > 147.83.158.8.ftp: Flags [P.], seq 12:23, ack 57, win 16384, options [nop,nop,TS val 3206814097 ecr 2207156744], length 11: FTP: PASS root
10:39:30.276079 IP 147.83.158.8.ftp > toc.catac.upc.edu.58098: Flags [.], ack 23, win 510, options [nop,nop,TS val 2207159943 ecr 3206814097], length 0
10:39:30.317607 IP 147.83.158.8.ftp > toc.catac.upc.edu.58098: Flags [P.], seq 57:86, ack 23, win 510, options [nop,nop,TS val 2207159984 ecr 3206814097], length 29: FTP: 230 User logged in, proceed
10:39:30.317656 IP toc.catac.upc.edu.58098 > 147.83.158.8.ftp: Flags [.], ack 86, win 16384, options [nop,nop,TS val 3206814182 ecr 2207159984], length 0
10:39:30.317875 IP toc.catac.upc.edu.58098 > 147.83.158.8.ftp: Flags [P.], seq 23:29, ack 86, win 16384, options [nop,nop,TS val 3206814182 ecr 2207159984], length 6: FTP: SYST
10:39:30.318055 IP 147.83.158.8.ftp > toc.catac.upc.edu.58098: Flags [.], ack 29, win 510, options [nop,nop,TS val 2207159985 ecr 3206814182], length 0
10:39:30.318644 IP 147.83.158.8.ftp > toc.catac.upc.edu.58098: Flags [P.], seq 86:105, ack 29, win 510, options [nop,nop,TS val 2207159985 ecr 3206814182], length 19: FTP: 215 UNIX Type: L8
10:39:30.318807 IP toc.catac.upc.edu.58098 > 147.83.158.8.ftp: Flags [P.], seq 29:35, ack 105, win 16384, options [nop,nop,TS val 3206814183 ecr 2207159985], length 6: FTP: FEAT
10:39:30.319498 IP 147.83.158.8.ftp > toc.catac.upc.edu.58098: Flags [P.], seq 105:143, ack 35, win 510, options [nop,nop,TS val 2207159986 ecr 3206814183], length 38: FTP: 211-Features:
10:39:30.360105 IP toc.catac.upc.edu.58098 > 147.83.158.8.ftp: Flags [.], ack 143, win 16384, options [nop,nop,TS val 3206814225 ecr 2207159986], length 0
10:40:27.313345 IP toc.catac.upc.edu.58098 > 147.83.158.8.ftp: Flags [P.], seq 35:41, ack 143, win 16384, options [nop,nop,TS val 3206871178 ecr 2207159986], length 6: FTP: QUIT
10:40:27.314378 IP 147.83.158.8.ftp > toc.catac.upc.edu.58098: Flags [P.], seq 143:157, ack 41, win 510, options [nop,nop,TS val 2207216981 ecr 3206871178], length 14: FTP: 221 Goodbye.
10:40:27.314379 IP 147.83.158.8.ftp > toc.catac.upc.edu.58098: Flags [F.], seq 157, ack 41, win 510, options [nop,nop,TS val 2207216981 ecr 3206871178], length 0
10:40:27.314409 IP toc.catac.upc.edu.58098 > 147.83.158.8.ftp: Flags [.], ack 157, win 16384, options [nop,nop,TS val 3206871179 ecr 2207216981], length 0
10:40:27.314567 IP toc.catac.upc.edu.58098 > 147.83.158.8.ftp: Flags [F.], seq 41, ack 158, win 16384, options [nop,nop,TS val 3206871179 ecr 2207216981], length 0
10:40:27.314762 IP 147.83.158.8.ftp > toc.catac.upc.edu.58098: Flags [.], ack 42, win 510, options [nop,nop,TS val 2207216981 ecr 3206871179], length 0
^C
25 packets captured
25 packets received by filter
0 packets dropped by kernel
root@toc:~#
```

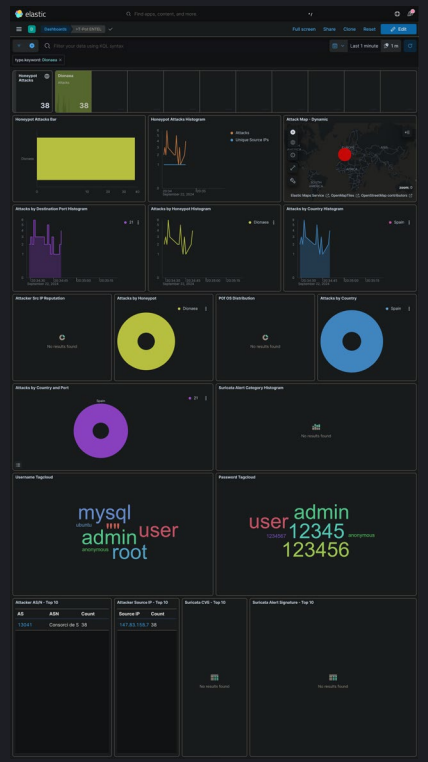
S'hi pot accedir com a root...

...sense estar convidat...

...o introduint qualsevol contrasenya aleatòria...

La víctima...

...així com registrar l'activitat de cada atac...



Dionaea

Detecta 38 atacs

Els usuaris i les contrasenyes utilitzades

La IP atacant i el propietari de la xarxa


```
┌──(dani㉿kali)-[~]
└─$ cat users.txt
root
mysql
ubuntu
admin
user
anonymous
```

```
┌──(dani㉿kali)-[~]
└─$ cat pass.txt
admin
user
12345
123456
1234567
anonymous
```

Hydra

Cracker d'inici de sessions de xarxa

Atac de diccionari:

7 usuaris

6 contrasenyes

38 usuari/contrasenya vàlids!!

```
┌──(dani㉿kali)-[~]
└─$ hydra -L users.txt -P pass.txt ftp://147.83.158.8
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use
in military or secret service organizations, or for illegal purposes (this
is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-22
20:34:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 42 login tries
(1:7/p:6), ~3 tries per task
[DATA] attacking ftp://147.83.158.8:21/
[21][ftp] host: 147.83.158.8   login: ubuntu   password: 12345
[21][ftp] host: 147.83.158.8   login: ubuntu   password: admin
[21][ftp] host: 147.83.158.8   login: root   password: 12345
[21][ftp] host: 147.83.158.8   login: root   password: anonymous
[21][ftp] host: 147.83.158.8   login: mysql   password: admin
[21][ftp] host: 147.83.158.8   login: mysql   password: 123456
[21][ftp] host: 147.83.158.8   login: root   password: admin
[21][ftp] host: 147.83.158.8   login: root   password: 1234567
[21][ftp] host: 147.83.158.8   login: root   password: user
[21][ftp] host: 147.83.158.8   login: ubuntu   password: user
[21][ftp] host: 147.83.158.8   login: root   password: 123456
[21][ftp] host: 147.83.158.8   login: mysql   password: 1234567
[21][ftp] host: 147.83.158.8   login: mysql   password: 12345
[21][ftp] host: 147.83.158.8   login: mysql   password: anonymous
[21][ftp] host: 147.83.158.8   login: mysql   password: user
[21][ftp] host: 147.83.158.8   login: ubuntu   password: 123456
[21][ftp] host: 147.83.158.8   login: anonymous   password: 12345
[21][ftp] host: 147.83.158.8   login: anonymous   password: 123456
[21][ftp] host: 147.83.158.8   login: admin   password: admin
[21][ftp] host: 147.83.158.8   login: admin   password: user
[21][ftp] host: 147.83.158.8   login: admin   password: 12345
[21][ftp] host: 147.83.158.8   login: admin   password: 123456
[21][ftp] host: 147.83.158.8   login: admin   password: 1234567
[21][ftp] host: 147.83.158.8   login: admin   password: anonymous
[21][ftp] host: 147.83.158.8   login: user   password: admin
[21][ftp] host: 147.83.158.8   login: user   password: user
[21][ftp] host: 147.83.158.8   login: user   password: 123456
[21][ftp] host: 147.83.158.8   login: user   password: 12345
[21][ftp] host: 147.83.158.8   login: user   password: 1234567
[21][ftp] host: 147.83.158.8   login: user   password: anonymous
[21][ftp] host: 147.83.158.8   login: anonymous   password: admin
[21][ftp] host: 147.83.158.8   login: anonymous   password: user
[21][ftp] host: 147.83.158.8   password: 1234567
[21][ftp] host: 147.83.158.8   password: anonymous
[21][ftp] host: 147.83.158.8   password: admin
[21][ftp] host: 147.83.158.8   password: user
[21][ftp] host: 147.83.158.8   password: 12345
[21][ftp] host: 147.83.158.8   password: 123456
1 of 1 target successfully completed, 38 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-22
20:34:52
```

C

Context...

Context...

Sobre FTP (protocol de transmissió de fitxers)...

FTP és un estàndard de transmissió de fitxers per Internet...

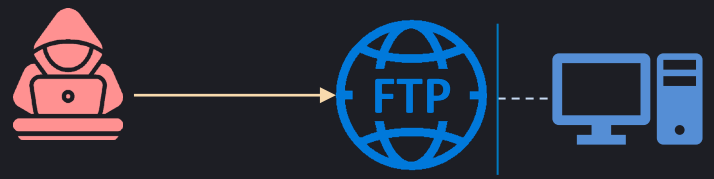
Utilitza els ports TCP/20 i TCP/21...

Aquest protocol es considera no segur per que tota la informació que s'envia no està xifrada.

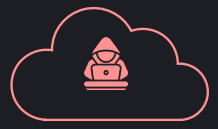
S'utilitza en entorns amb dispositius amb poca capacitat de còmput, com en el camp IoT...

Context...

Quin podria ser l'objectiu del ciberatac...?



Un opció podria ser accedir a les dades dels usuaris del servei...



...un altre podria ser convertir el servidor en el seu núvol personal...

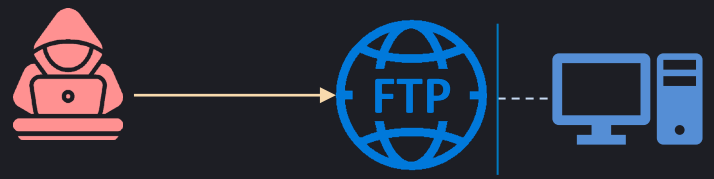
...o bé utilitzar el servidor per atacar altres equips, un zombi...

...simplement impedir la prestació del servei...

...o una combinació de tots plegats...

Context...

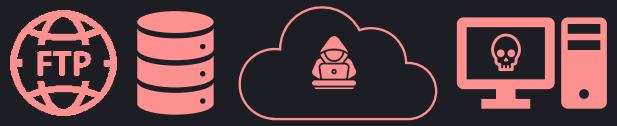
...i quines estratègies han pogut seguir per realitzar l'atac...



Saturar el maquinari
Xarxa, CPU, RAM, disc, etc...

Prendre el control
del servei...

Prendre el control
de tot el sistema...



Context...

Segons el comunicat dels hackers...
...han obtingut el control total del servidor...

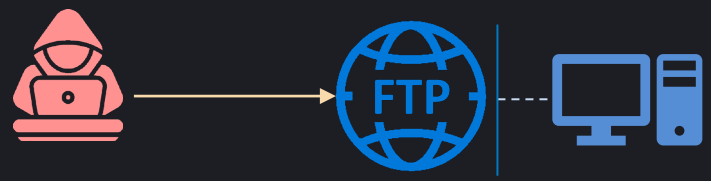
Honeypot creat amb contenidors...

El sistema de contenidors (Docker) és un programari que permet empaquetar i aïllar tot l'entorn d'execució de les aplicacions (executables, dades, controladors, etc...).

cada mitja nit es reinicien amb els fitxers originals...

Context...

S’analitzaran mesures dels darrers dos mesos i mig amb la dashboard T-Pot (del 2024-03-15 al 2024-05-31)...



En total s’han rebut 6.885.756 atacs!

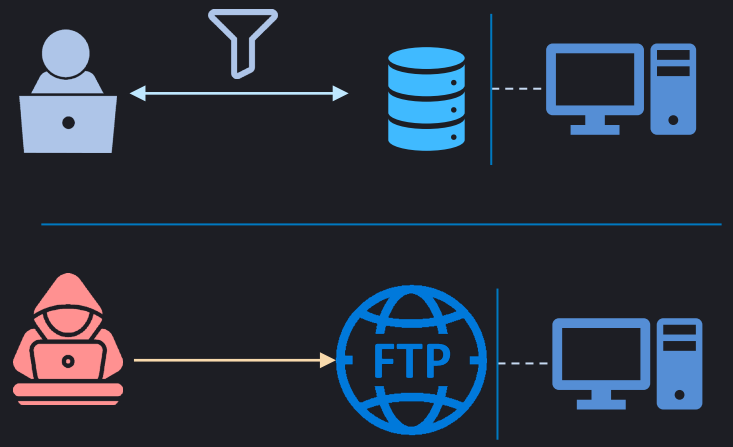
El servei FTP ha rebut 9.887 atacs, amb 838 adreces IP involucrades

E

L'evolució de la investigació...

L'evolució de la investigació...

Per arribar a esbrinar què ha passat cal anar obtenint i analitzant el seguit de pistes ocultes entre les dades...



Caldrà anar aplicant els filtres corresponents a les dades emmagatzemades...

...per construir una imatge del què ha passat

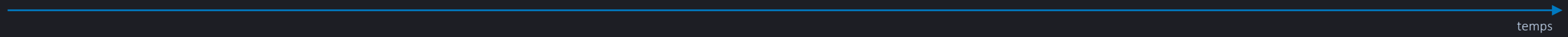
L'evolució de la investigació...

Es verifica que el honeypot ha estat sempre operatiu...

El monitor de recursos del sistema mostra que el honeypot ha estat operatiu en tot moment...

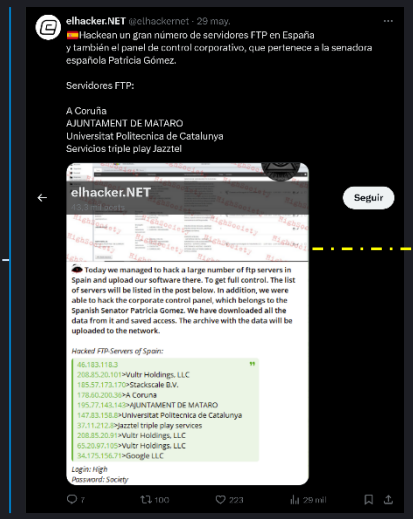
L’evolució de la investigació...

...cronograma dels fets (1)...



L’evolució de la investigació...

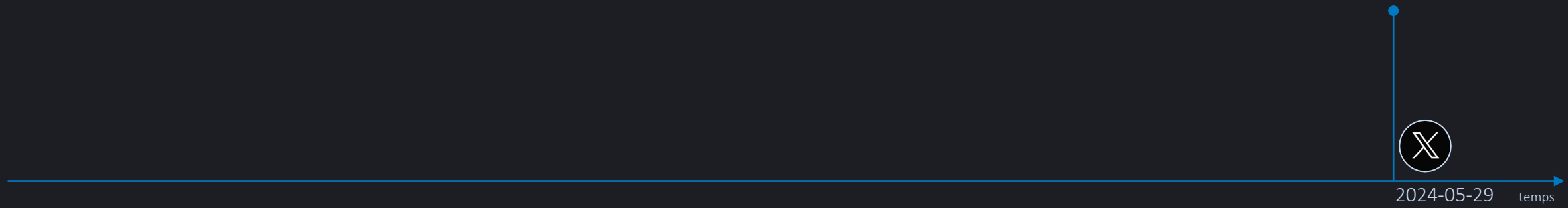
Tot comença amb la lectura del missatge a X...



El missatge es publica el 29 de maig de 2024...

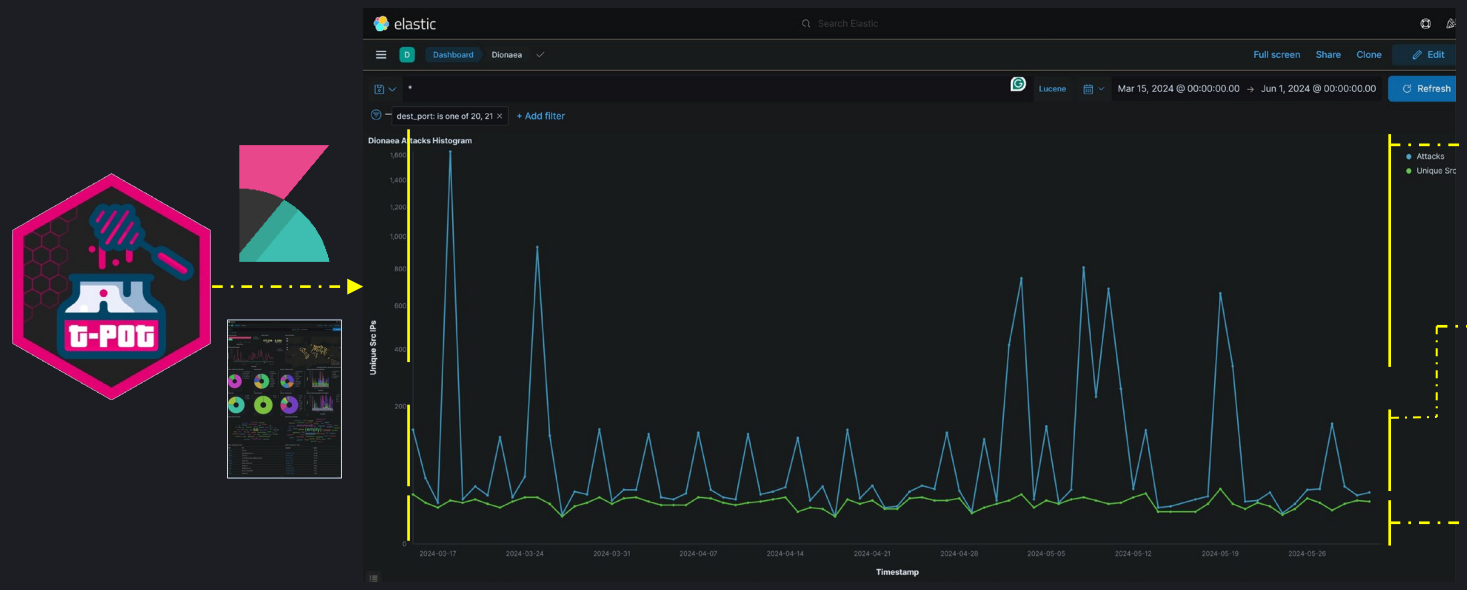
L’evolució de la investigació...

...cronograma dels fets (2)...



L'evolució de la investigació...

...s'identifiquen 3 patrons d'atac al protocol FTP...



Els puntuals, de curta durada i alta intensitat...

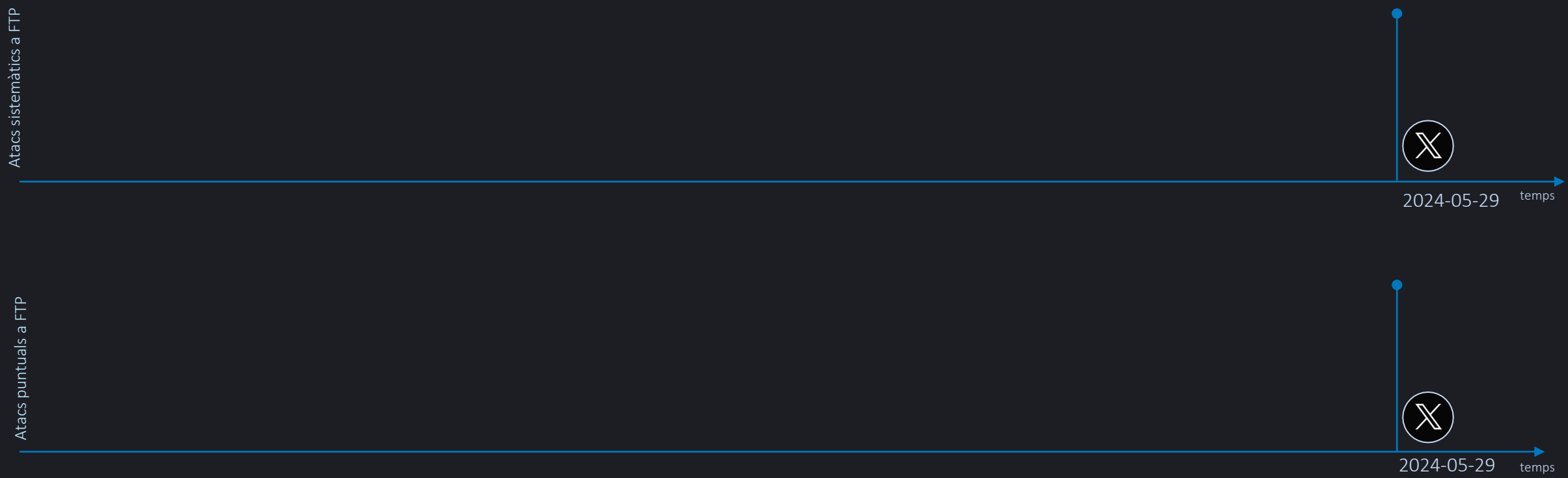
El sistemàtic, de llarga durada i poca intensitat...

El quotidià, que s'ignora (~43 atacs diaris, IP≈atac)...

6.885.756 atacs Honeypot → 158.462 atacs Dionaea → 9.887 atacs FTP → 6.513 atacs FTP analitzats

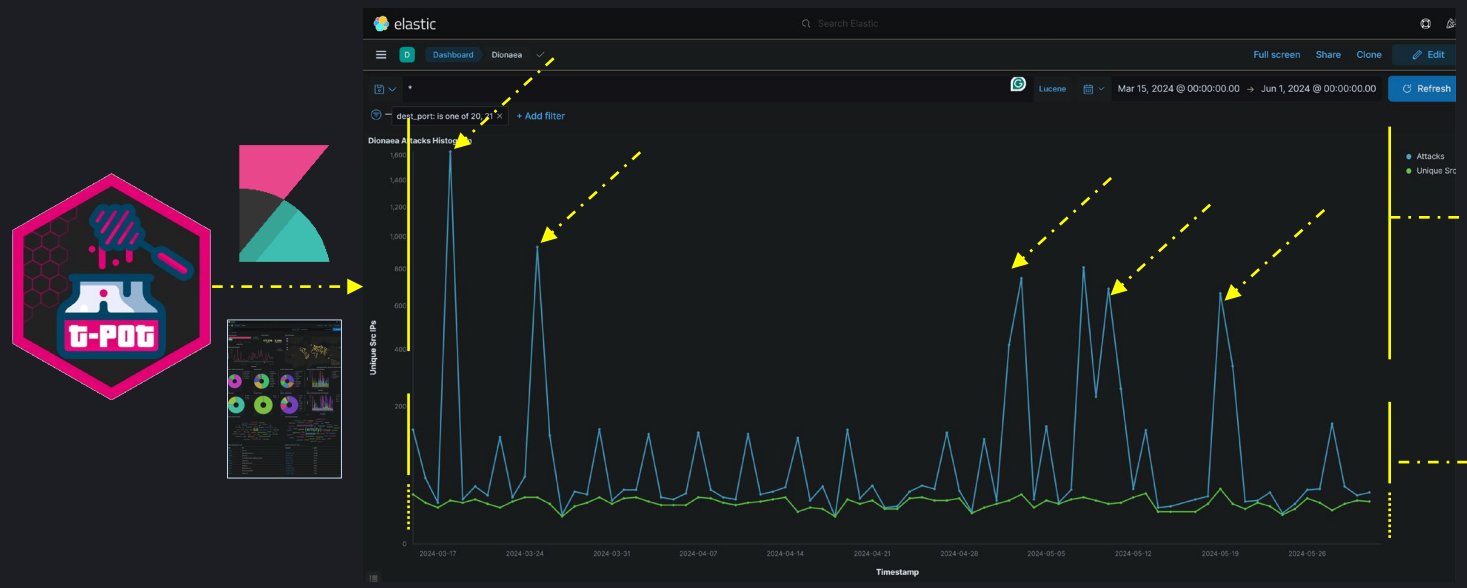
L’evolució de la investigació...

...cronograma dels fets (3)...



L'evolució de la investigació...

...es localitzen les dates dels atacs...

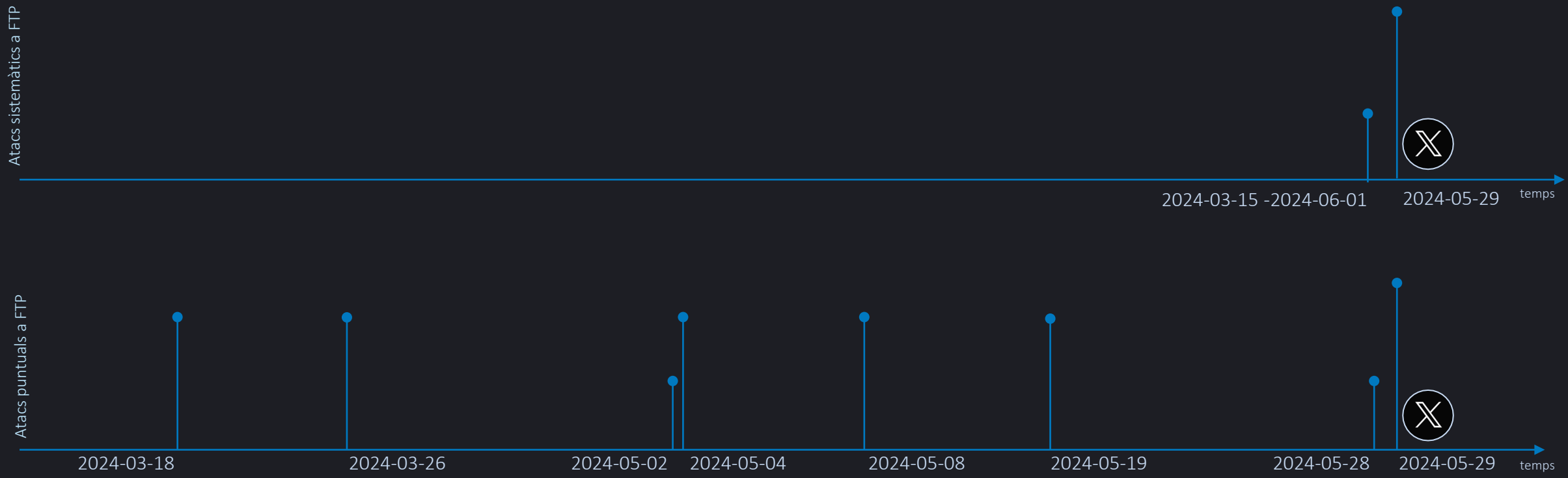


6 atacs en el període analitzat...

18 atacs en el període analitzat...

L'evolució de la investigació...

...cronograma dels fets (4)...



L'evolució de la investigació...

...es determina el volum d'atacs en cada cas...

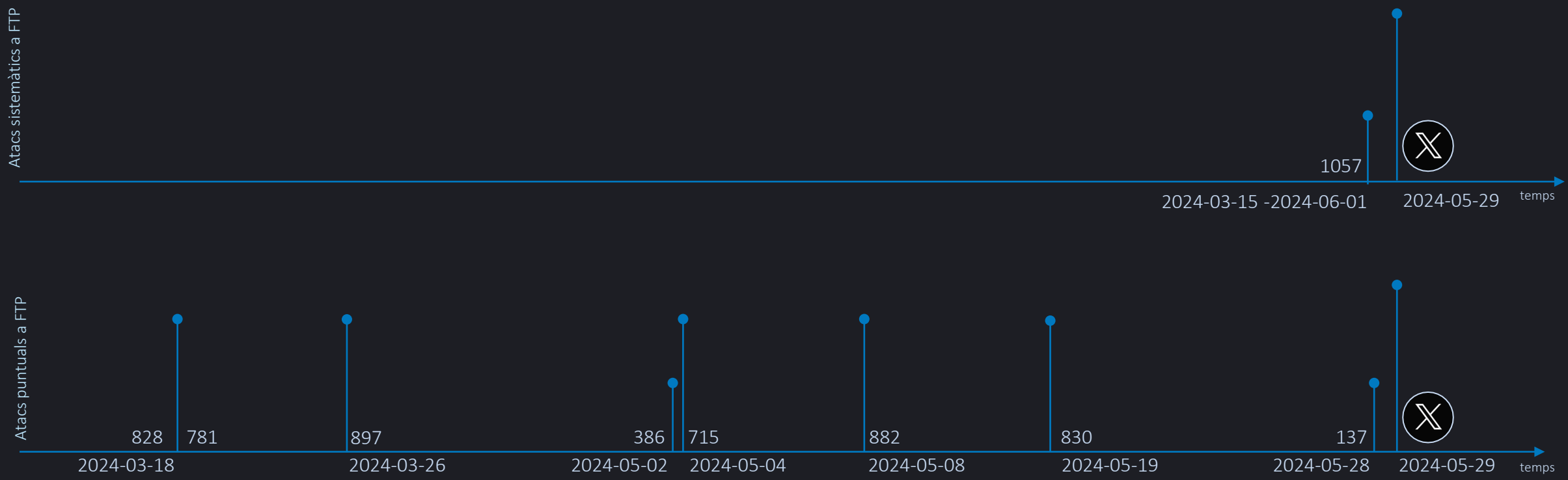
Dionaea - Attacker Src IP - Top 10

Source IP	Count
185.193.206.21	830
172.233.39.227	103
34.140.108.54	6
147.45.44.52	4
34.140.130.61	4
35.216.153.140	4
164.92.169.200	3
165.154.134.156	3
104.199.68.30	2
128.1.210.10	2

Els atacs poden pertànyer a 1 o diversos equips...

L'evolució de la investigació...

...cronograma dels fets (5)...



L'evolució de la investigació...

...s'esbrinen les adreces IP dels atacants...

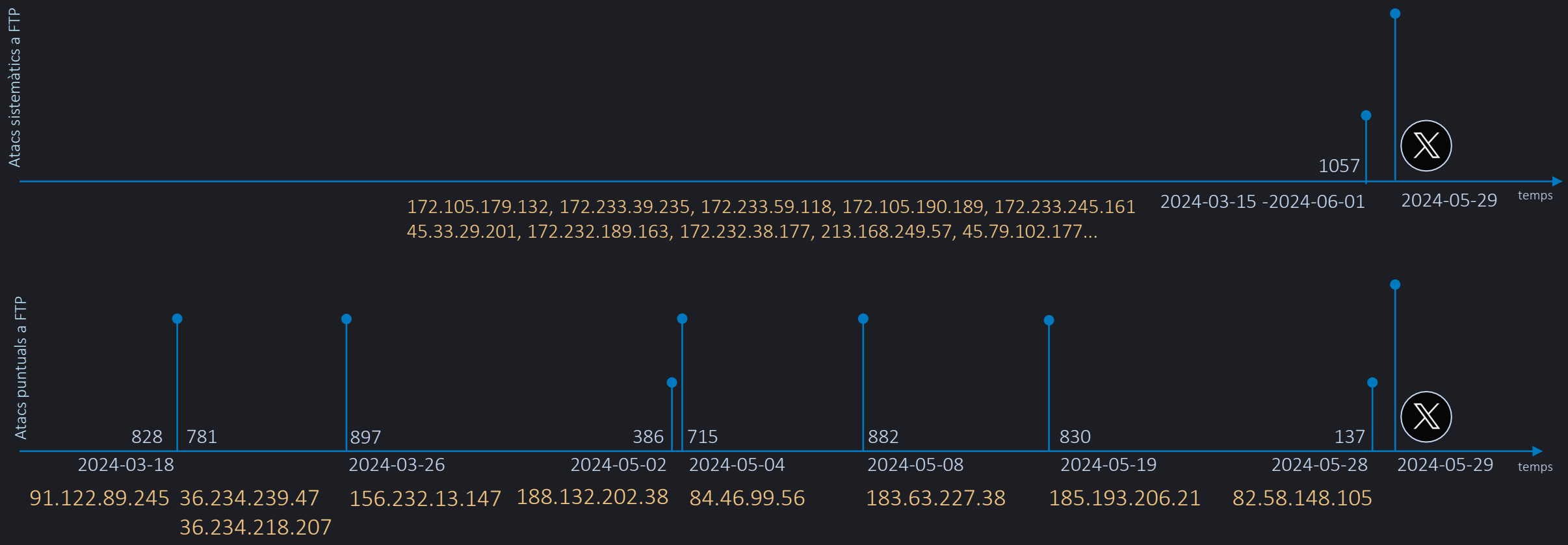
Dionaea - Attacker Src IP - Top 10

Source IP	Count
185.193.206.21	830
172.233.39.227	103
34.140.108.54	6
147.45.44.52	4
34.140.130.61	4
35.216.153.140	4
164.92.169.200	3
165.154.134.156	3
104.199.68.30	2
128.1.210.10	2

Les adreces IP identifiquen cada equip a Internet

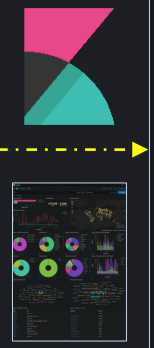
L'evolució de la investigació...

...cronograma dels fets (6)...



L'evolució de la investigació...

...s'esbrina el proveïdor d'accés a Internet (ISP) de cada IP...



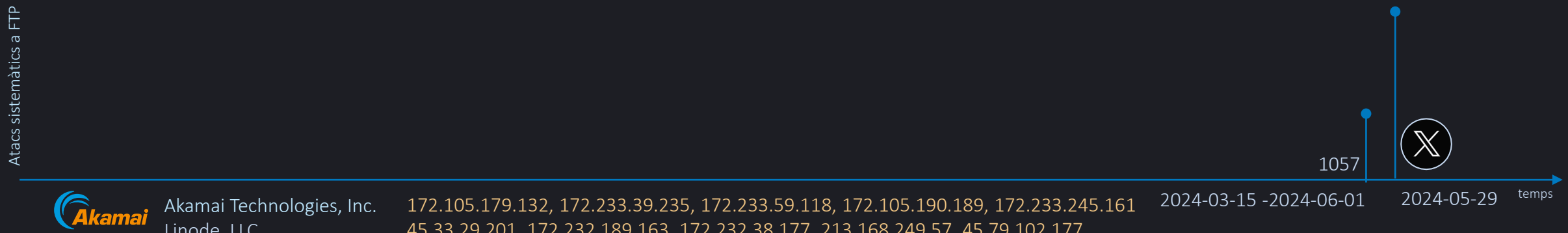
Dionaea - Attacker AS/N - Top 10

ASN	AS
58305	SYN LTD
57355	networkers.pl Sp. z o.o.
199539	Vertex Ltd.
4750	CS LOXINFO PUBLIC COMPANY LIMITED
35598	Inetcom LLC
132530	Bestec Telecom Ltd.
15169	Google LLC
14061	DigitalOcean, LLC
4134	No.31,Jin-rong Street
63949	Linode, LLC

Cada adreça IP pertany a un proveïdor d'accés a Internet (ISP) registrat...

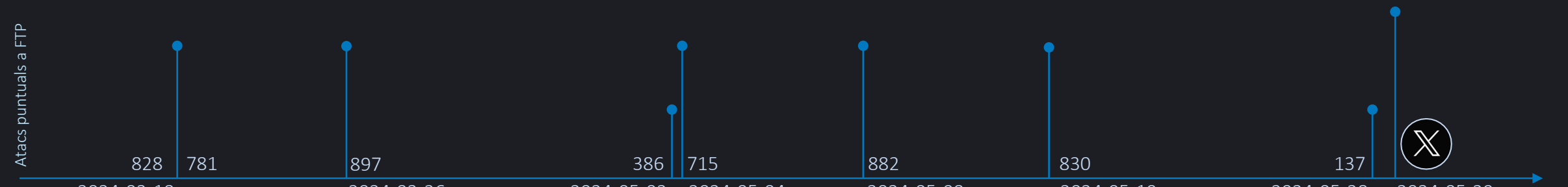
L'evolució de la investigació...

...cronograma dels fets (7)...



Akamai Technologies, Inc.
Linode, LLC

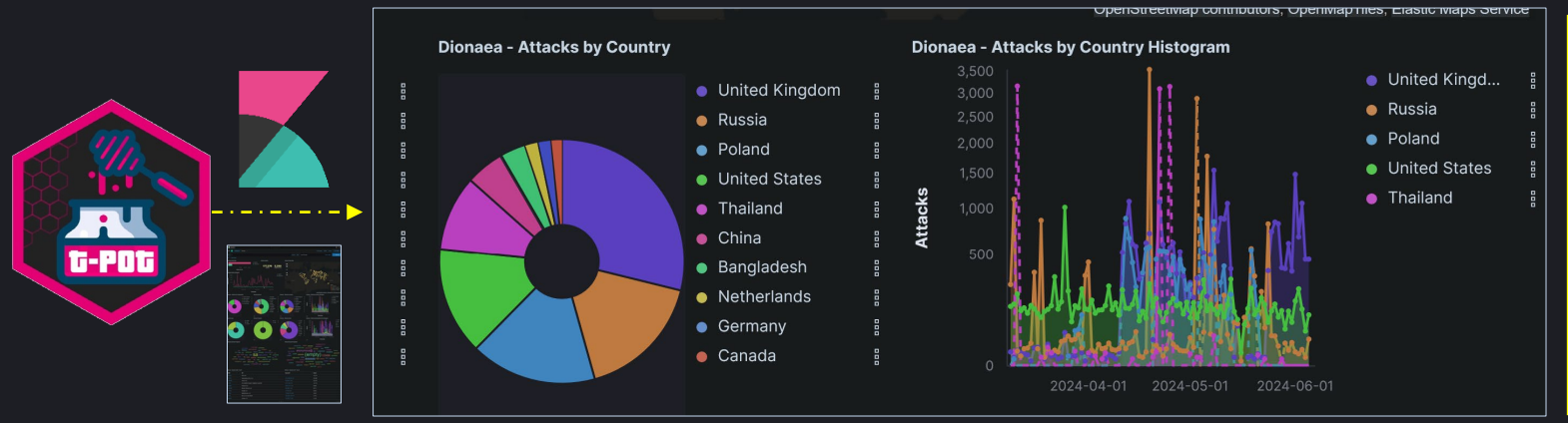
172.105.179.132, 172.233.39.235, 172.233.59.118, 172.105.190.189, 172.233.245.161
45.33.29.201, 172.232.189.163, 172.232.38.177, 213.168.249.57, 45.79.102.177...



91.122.89.245	36.234.239.47 36.234.218.207	156.232.13.147	188.132.202.38	84.46.99.56	183.63.227.38	185.193.206.21	82.58.148.105
PJSC Rostelecom	Asia Pacific Network Information Centre	Yisu Cloud Ltd	Pembe Gul Isguzar Karagoz	wilhelm.tel GmbH	Asia Pacific Network Information Centre	LTD SibMediaFon	Telecom Italia S.p.A.

L’evolució de la investigació...

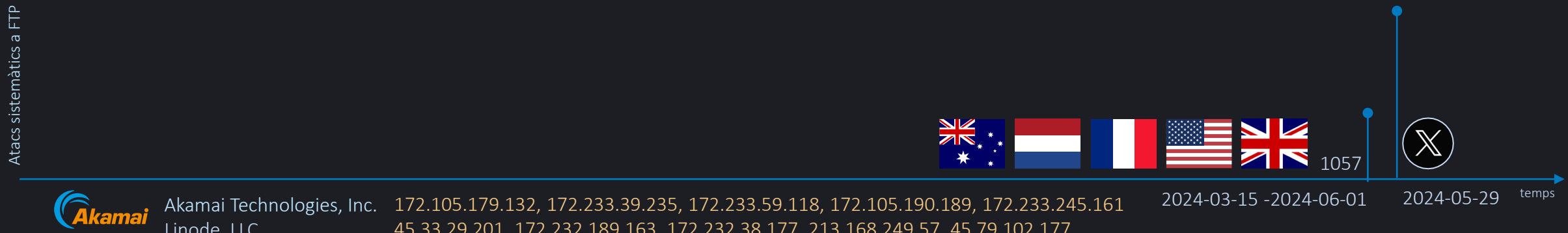
...es troba el país on s’ha utilitzat cada adreça IP



Cada adreça IP està ubicada en un país...

L'evolució de la investigació...

...cronograma dels fets (8)...



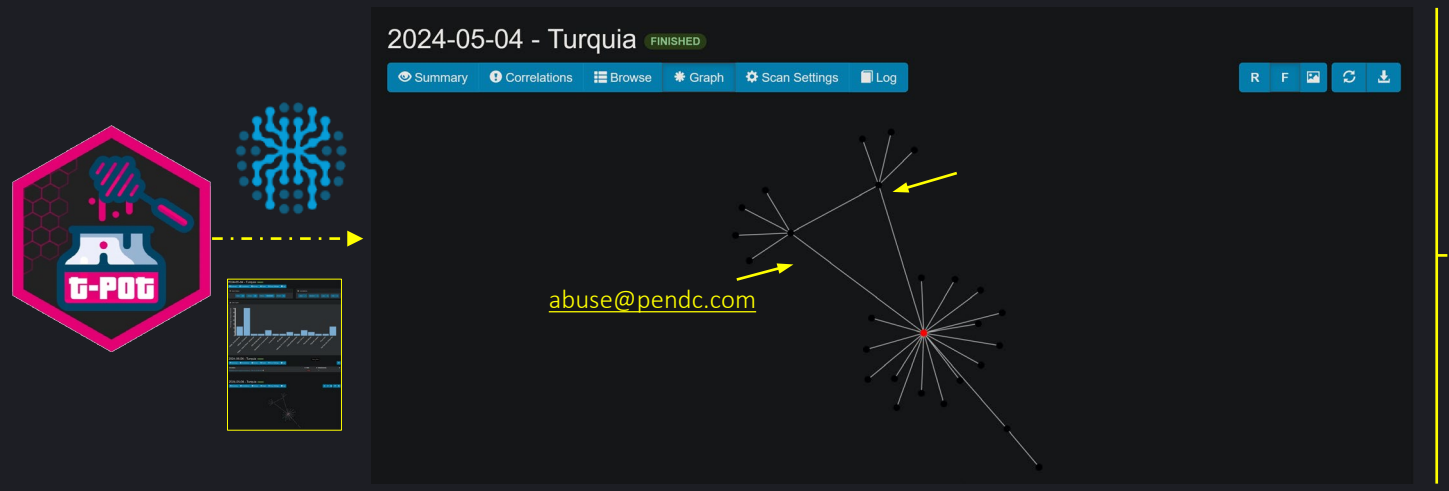
Akamai Technologies, Inc. 172.105.179.132, 172.233.39.235, 172.233.59.118, 172.105.190.189, 172.233.245.161
Linode, LLC 45.33.29.201, 172.232.189.163, 172.232.38.177, 213.168.249.57, 45.79.102.177...

2024-03-15 -2024-06-01 2024-05-29

2024-03-18		2024-03-26	2024-05-02	2024-05-04	2024-05-08	2024-05-19	2024-05-28	2024-05-29
91.122.89.245	36.234.239.47 36.234.218.207	156.232.13.147	188.132.202.38	84.46.99.56	183.63.227.38	185.193.206.21	82.58.148.105	
PJSC Rostelecom	Asia Pacific Network Information Centre	Yisu Cloud Ltd	Pembe Gul Isguzar Karagoz	wilhelm.tel GmbH	Asia Pacific Network Information Centre	LTD SibMediaFon	Telecom Italia S.p.A.	

L'evolució de la investigació...

...Es cerca l'empresa usuària de cada IP en bases de dades públiques d'intel·ligència (OSINT) amb Spiderfoot...



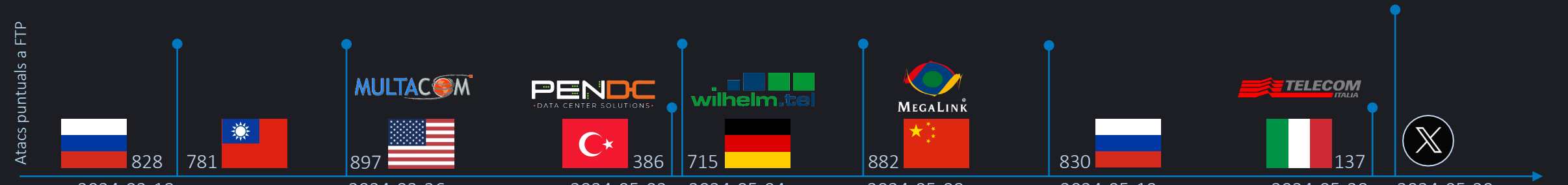
Les petjades (footprint) de cada IP emmagatzemades en bases de dades OSINT es poden relacionar, creant gràfics que permeten descobrir informacions clau...

L'evolució de la investigació...

...cronograma dels fets (9)...

Akamai Technologies, Inc.
Linode, LLC

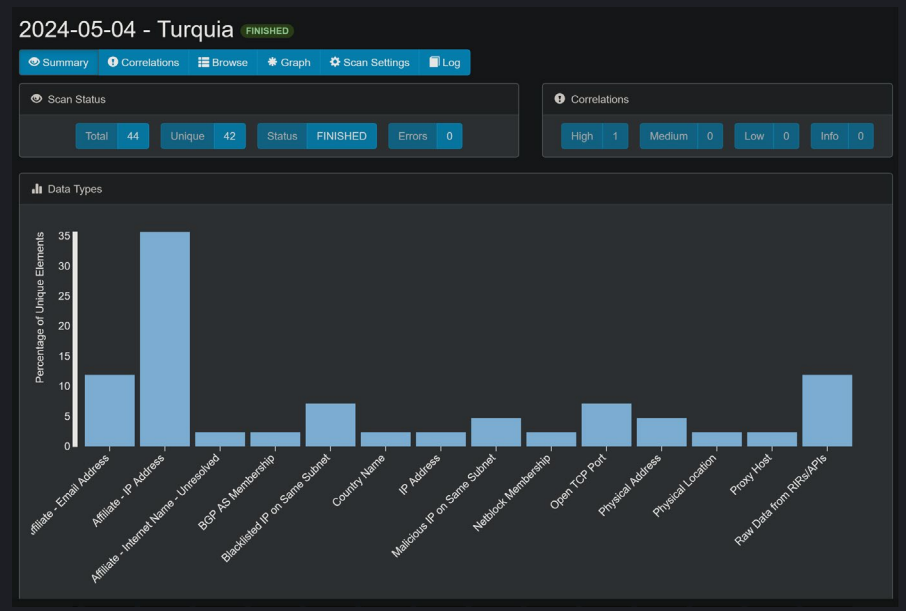
172.105.179.132, 172.233.39.235, 172.233.59.118, 172.105.190.189, 172.233.245.161
45.33.29.201, 172.232.189.163, 172.232.38.177, 213.168.249.57, 45.79.102.177...



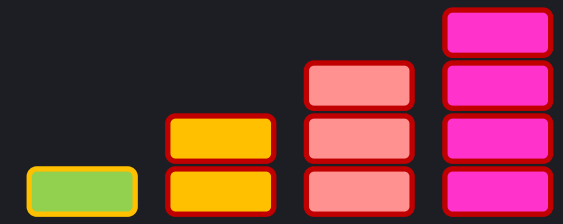
91.122.89.245	36.234.239.47 36.234.218.207	156.232.13.147	188.132.202.38	84.46.99.56	183.63.227.38	185.193.206.21	82.58.148.105
PJSC Rostelecom	Asia Pacific Network Information Centre	Yisu Cloud Ltd	Pembe Gul Isguzar Karagoz	wilhelm.tel GmbH	Asia Pacific Network Information Centre	LTD SibMediaFon	Telecom Italia S.p.A.

L'evolució de la investigació...

...s'obté una valoració de la perillositat coneguda de cada IP...

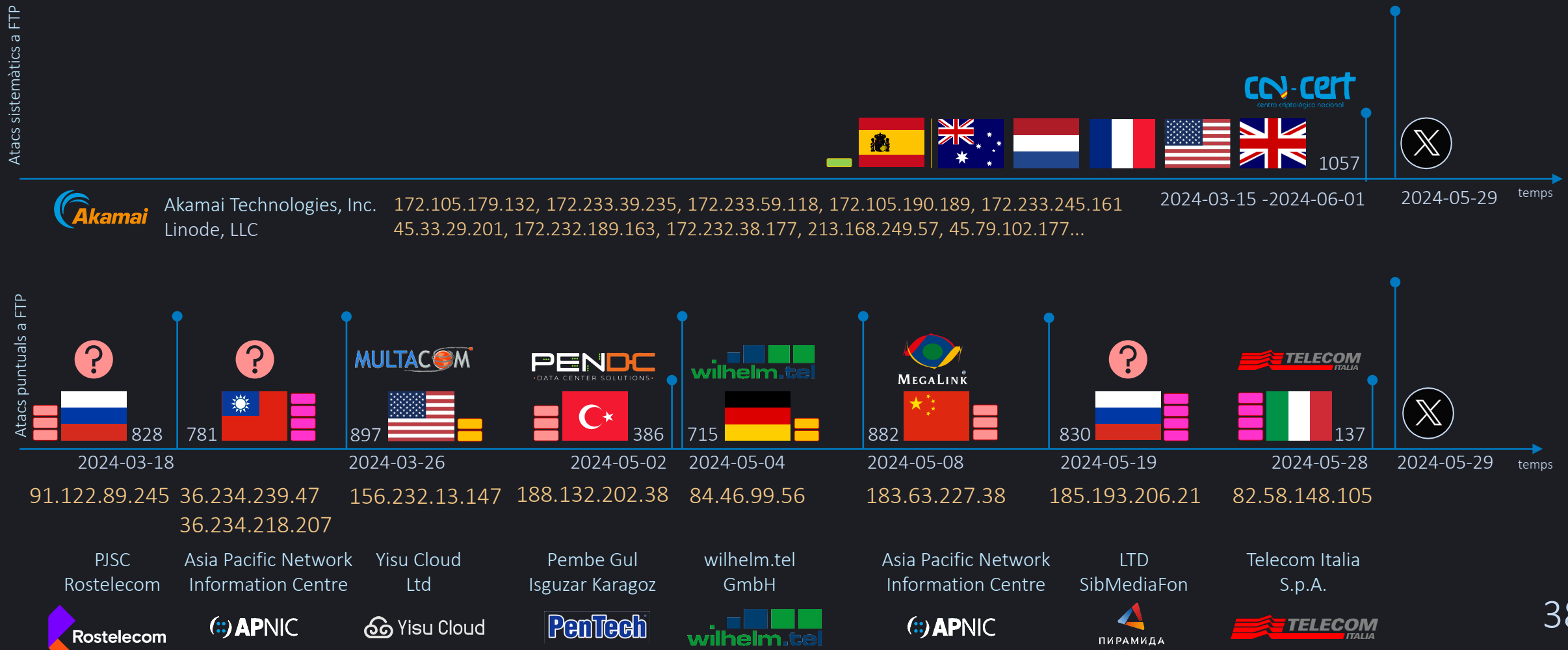


La perillositat que suposa cada IP es calcula segons mètriques de les bases de dades OSINT...



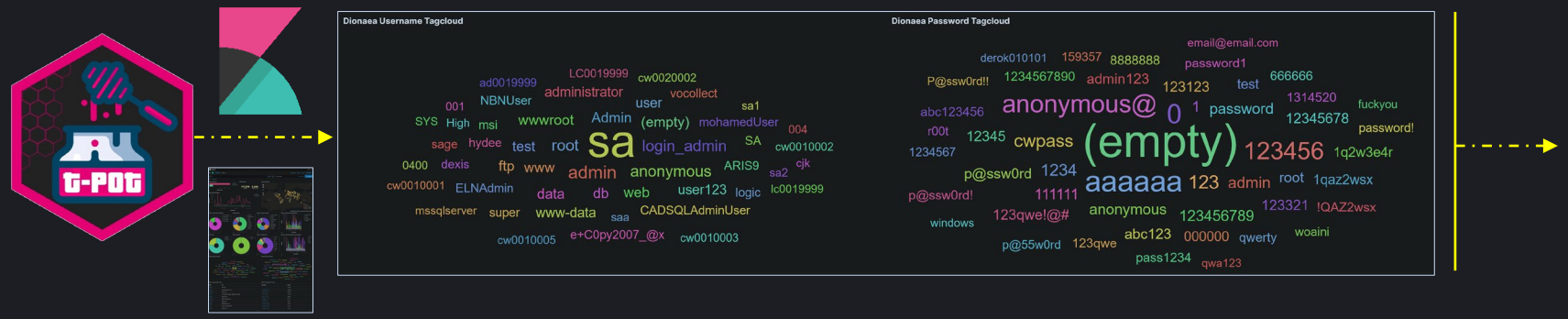
L'evolució de la investigació...

...cronograma dels fets (10)...



L'evolució de la investigació...

...s'identifiquen els valors d'autenticació en els accessos FTP...



Per accedir al servidor cal autenticar-se amb usuari i contrasenya...

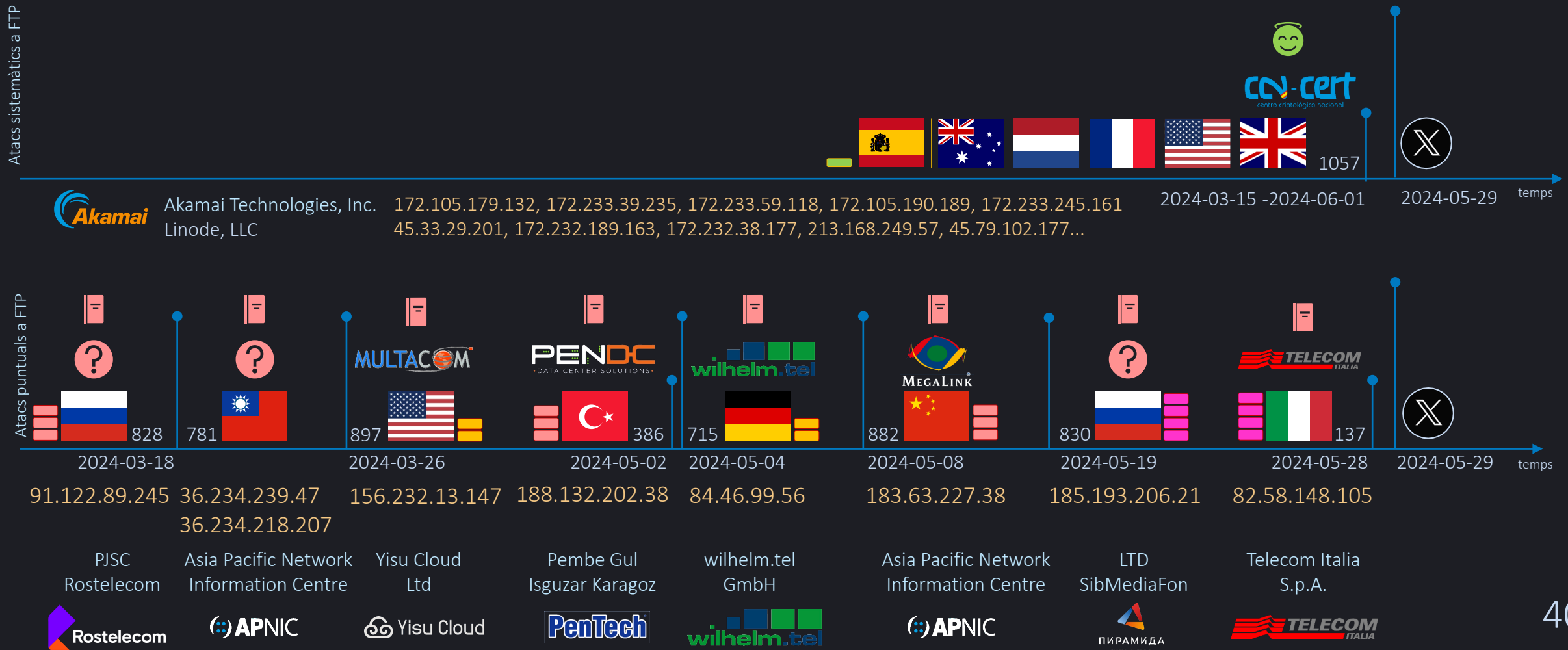
...una cosa és mirar i l'altre forçar l'entrada...

Accés anònim

Diccionaris d'usuaris i contrasenyes

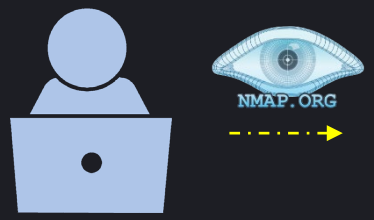
L'evolució de la investigació...

...cronograma dels fets (11)...



L’evolució de la investigació...

...s’intenta detectar si les IP involucrades encara són actives...




```
------------------------------------------------------------
            Cerca i anàlisi d'una adreça IP.
------------------------------------------------------------
Equip:                  t-pot.epseveg.upc.edu [127.0.1.1]
Usuari:                 uid=0(root) gid=0(root) grups=0(root)
Sistema operatiu:       Debian 12.5 GNU/Linux (bookworm)
Versió:                 info_ip.sh v.0.120 (07/02/2023)
                        info_funcions.sh v.0.125 (20/03/2024)
Data d'inici:           2024-06-09 a les 21:53:05
Data de finalització:   2024-06-09 a les 21:53:10
Durada de les tasques:  5s
------------------------------------------------------------
```

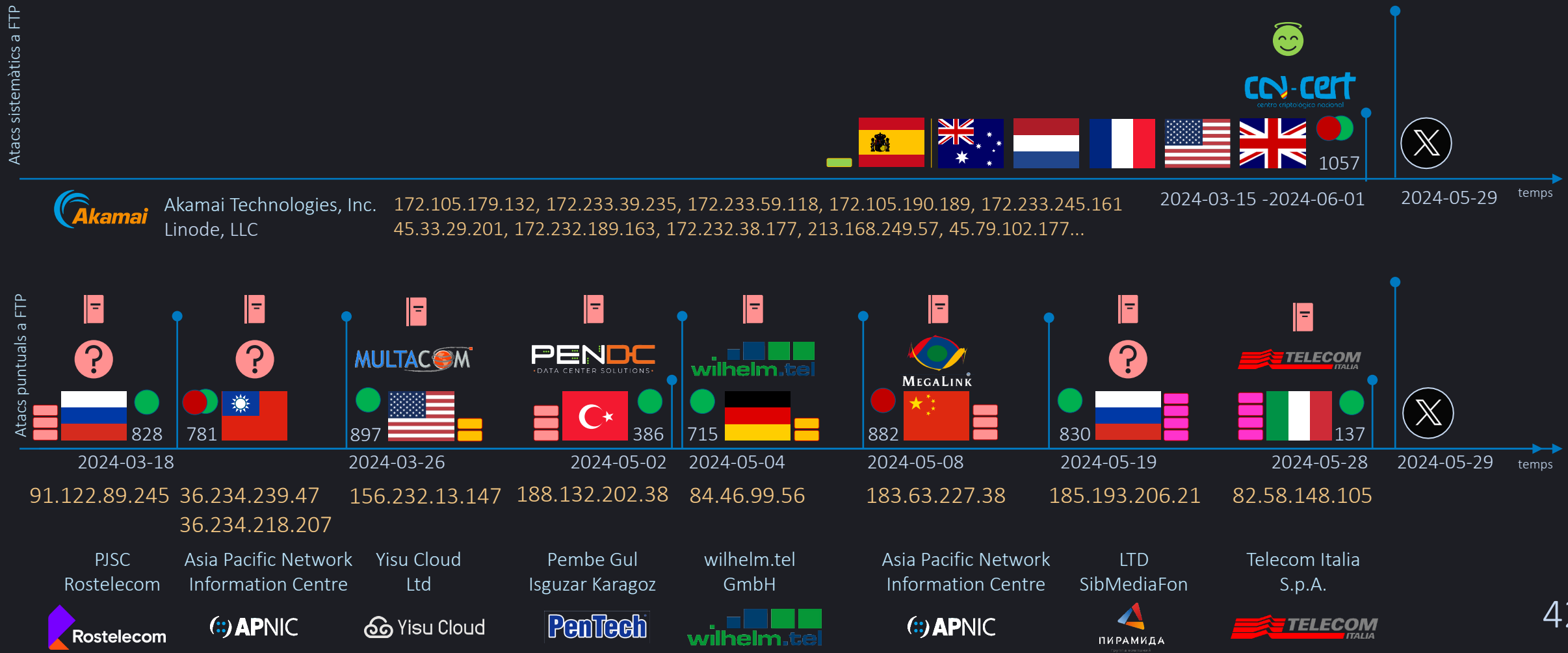
```
------------------------------------------------------------------------------------
            Resultat de la geolocalització de l'adreça IP 172.105.179.132.
------------------------------------------------------------------------------------
Equip identificat:  172.105.179.132 (-)
Xarxa propietaria:   [] ()
Entitat titular:     ()
Gestor ASN:         AS63949 Akamai Connected Cloud
Localització:       Sydney (CP 1001), New South Wales, Austràlia ()
Coordenades:        Latitud -33.8678 i longitud 151.2073, amb zona horària Australia/Sydney

------------------------------------------------------------------------------------
                Resultat de l'escaneig de l'adreça IP 172.105.179.132.
------------------------------------------------------------------------------------
L'equip 172.105.179.132 no respon.
```

L’equip respon...

L’equip no respon...

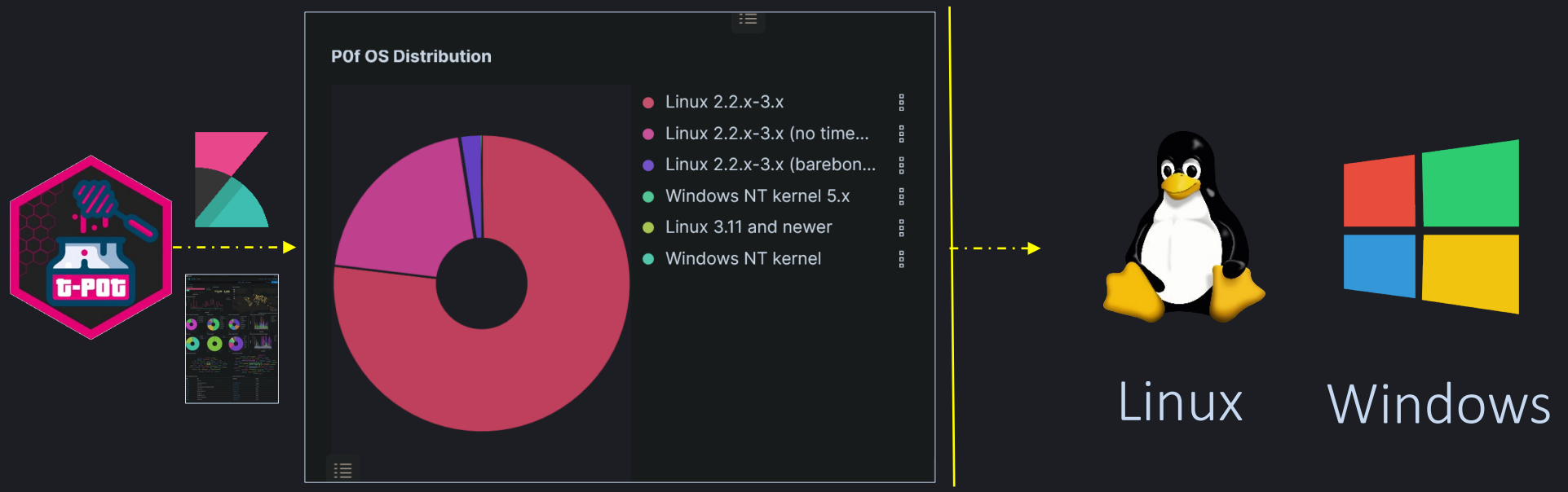
L'evolució de la investigació...

...cronograma dels fets (12)...



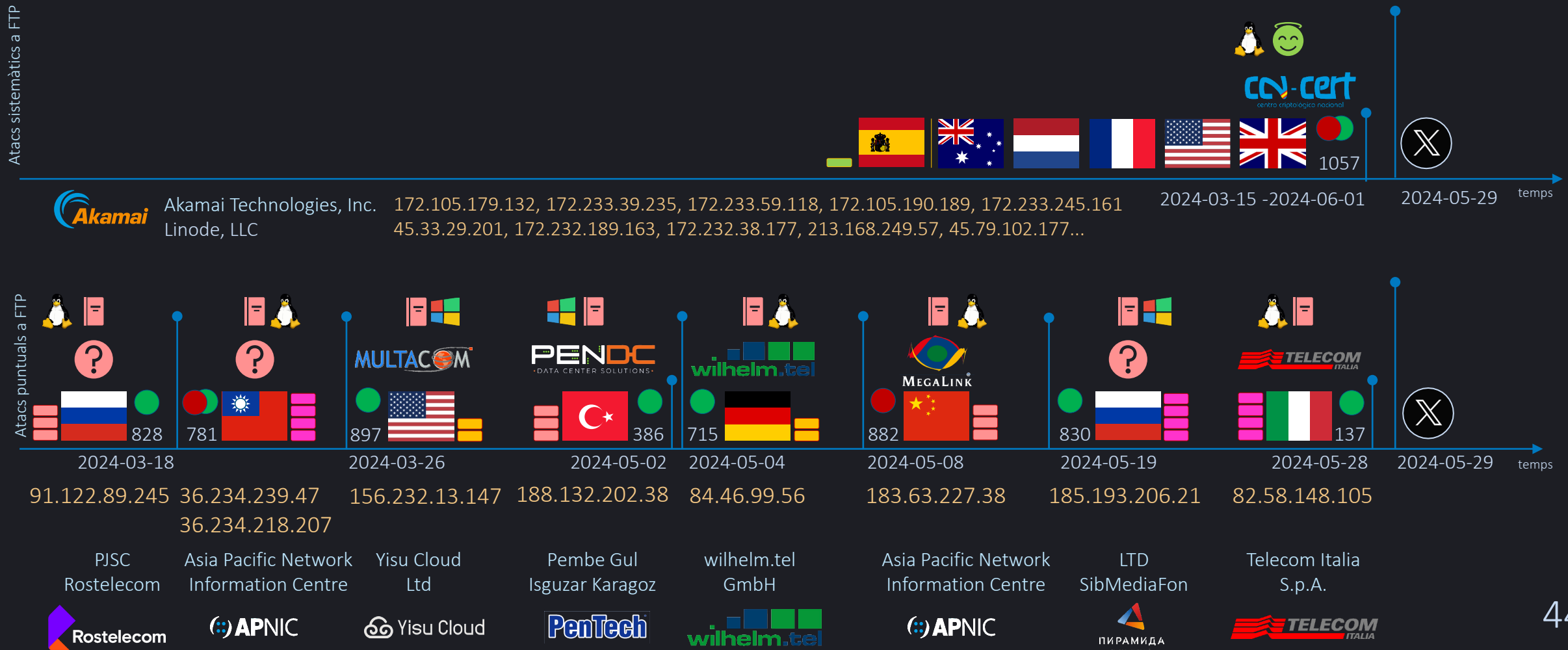
L'evolució de la investigació...

...així com quin sistema operatiu utilitzen...



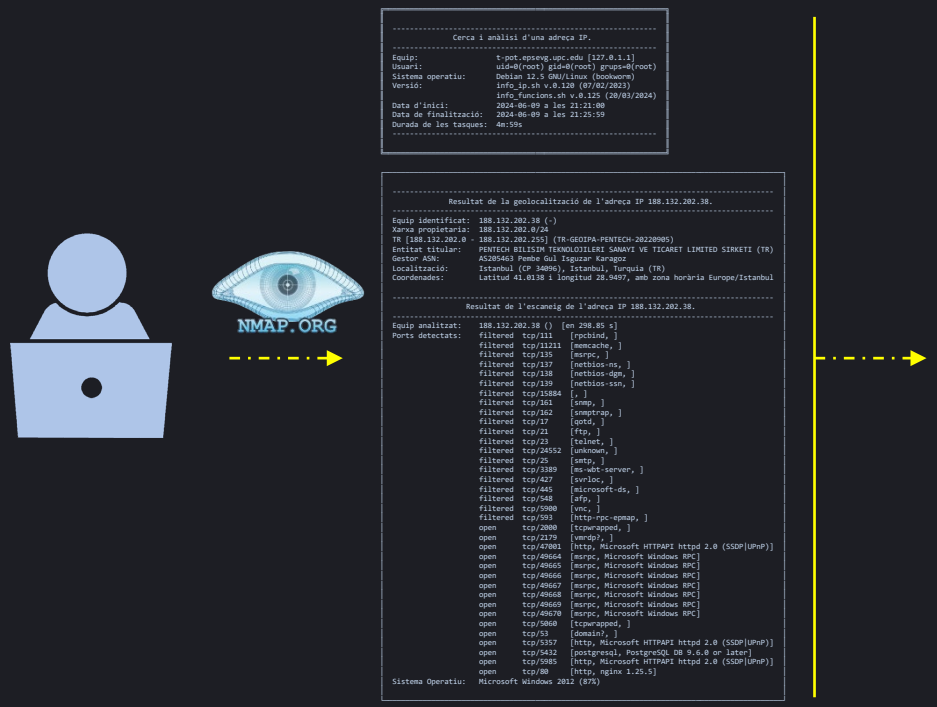
L'evolució de la investigació...

...cronograma dels fets (13)...



L'evolució de la investigació...

...s'inicia un anàlisi actiu per establir quin serveis té actius cada IP...

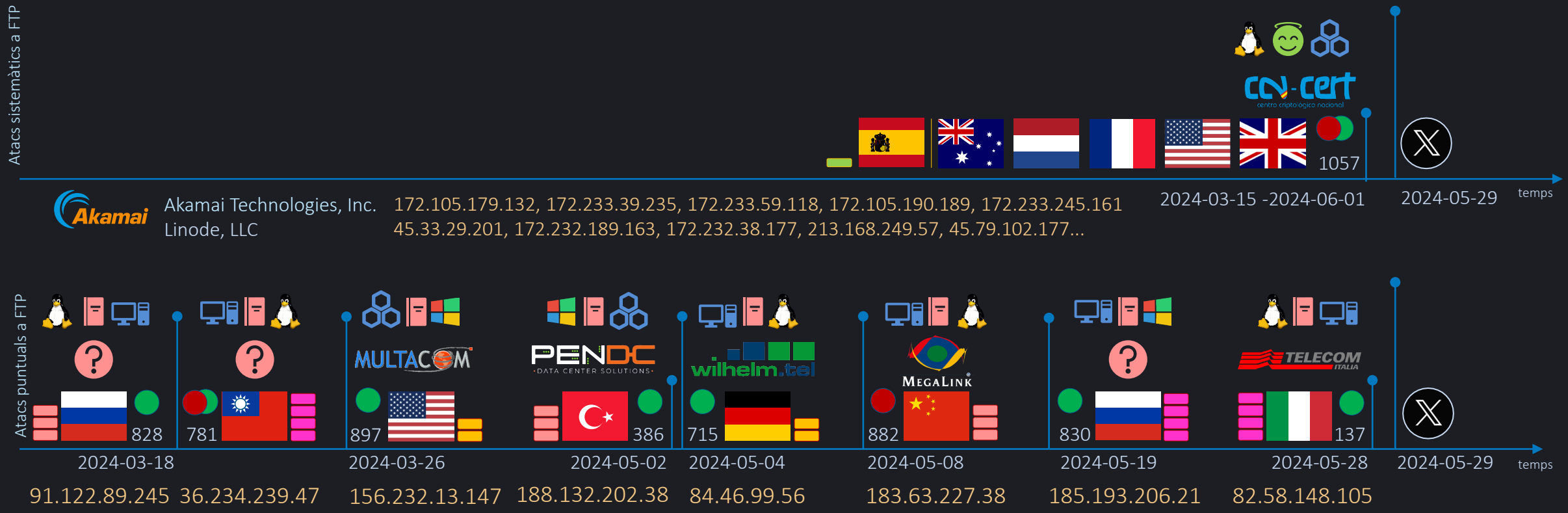


Es un equip d'anàlisi de xarxa...

NO està clar el seu propòsit...

L'evolució de la investigació...

...cronograma dels fets (14).

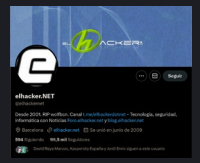


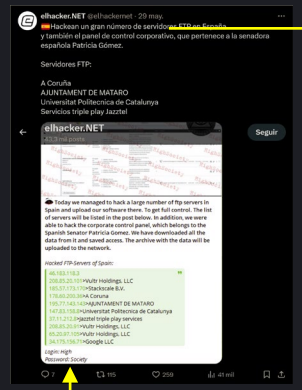
C

Conclusions

Conclusions

De l'anàlisi del missatge es dedueix que...

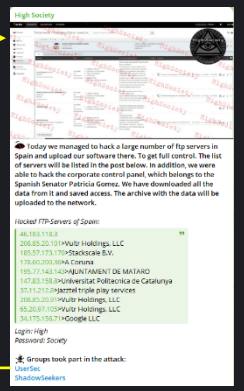




Es va publicat el 29 de maig de 2024.

L'atac és anterior a aquesta data.

Però quants dies abans...?



Els atacants formen part del grup High Society Hacker Alliance.

Qui són i què volen...?

UserSec

ShadowSeekers

Conclusions

...de l'anàlisi dels atacs, s'identifiquen 3 tipus de perfils segons el seu comportament...

- Perfil d'atac: s'han identificat clarament 2 atacs. El "qui", el "com" i el "des d'on" encaixen perfectament.
- Perfil sospitós: en 5 casos, si bé les organitzacions a que pertanyen semblen "de fiar", el fet d'intentar accedir com a superusuari i la reputació de les adreces IP utilitzades fa "mal pensar".
- Perfil de sondeig; hi ha 1 sondeig sistemàtic ben identificat. Només intenten accedir-hi amb l'usuari anònim. Semblen bona gent.

Conclusions

...i de l'anàlisi dels atacs es plantegen diferents hipòtesis...

Qui: Telecom Italia

Quan: 2024-05-28

Com: Atac de diccionari (137 accessos)

Des d'on: 82.58.148.105 (Telecom Italia)
Siano, Campania, 72, Italy, IT

Per què:

Sembla una reacció a la publicació de la notícia a la web de High Society.

Potser és només un sondeig "intrusiu" dels serveis TIC de seguretat de l'entitat.

Encara que mai se sap...

Conclusions

...encara que sembla força probable que aquesta sigui certa...

Qui:	UserSec?
Quan:	2024-05-19
Com:	Atac de diccionari (830 accessos)
Des d'on:	185.193.206.21 (LTD SibMediaFon) Nazarovo, Krasnoyarsk Krai, KYA, Russia, RU
Per què:	Són hackers! Aquest podria ser l'atac real del grup UserSec que s'anuncia a la web de High Society. Tant el volum, com la data, l'origen i la seguretat detectades ho podrien suggerir...

Conclusions

...així com que el honeypot no passa desapercebut...

Qui:	Megalink
Quan:	2024-05-08
Com:	Atac de diccionari (882 accessos)
Des d'on:	183.63.227.38 (China Telecom) Xiaolou, Guangdong, GD, China, CN
Per què:	Potser és només un sondeig "molt intrusiu" dels serveis TIC de seguretat de l'entitat. Encara que mai se sap...

Conclusions

...deu ser cosa de feeling...

Qui: Wilhwlm.tel

Quan: 2024-05-03

Com: Atac de diccionari (715 accessos)

Des d'on: 84.46.99.56 (wilhelm.tel GmbH)
Hamburg, HH, Germany, DE

Per què: Potser és només un sondeig "molt intrusiu" dels serveis TIC de seguretat de l'entitat.

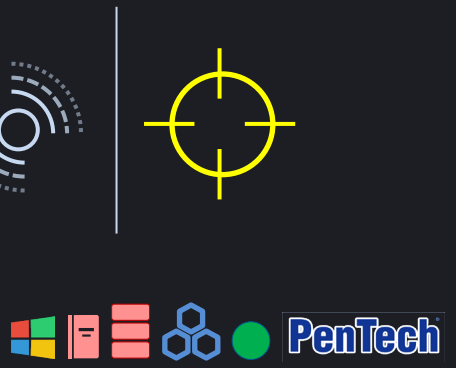
Encara que mai se sap...

Conclusions

...o de que siguin fans de la UPC...

Qui:	PenDC
Quan:	2024-05-02
Com:	Atac de diccionari (386 accessos)
Des d'on:	188.132.202.38 (Pembe Gul Isguzar Karagoz) Osmangazi, Bursa Province, 16, Turkey, TR
Per què:	Potser és només un sondeig "molt intrusiu" dels serveis TIC de seguretat de l'organització.

Encara que mai se sap...



Conclusions

...o simplement s'avorreixen...

Qui: Multacom

Quan: 2024-03-26

Com: Atac de diccionari (897 accessos)

Des d'on: 156.232.13.147 (Guangzhou Yisu Cloud Limited)
Los Angeles, California, CA, United States, US

Per què: Potser és només un sondeig "molt intrusiu" dels serveis TIC de seguretat de l'organització.

Encara que mai se sap...

Conclusions

...res més enllà d'una sospita i molta imaginació...

Qui:	?
Quan:	2024-03-18
Com:	Atac de diccionari (781 accessos)
Des d'on:	36.234.239.47, 36.234.218.207 (Chunghwa Telecom Co.,Ltd.) Miaoli, Miaoli, MIA, Taiwan, TW
Qui:	?
Com:	Atac de diccionari (828 accessos)
Des d'on:	91.122.89.245 (Rostelecom) Sant Petersburg, Rússia, RU
Per què:	Són hackers! Sembla un atac verídic! Al tenir un mateix perfil d'atac es sospita que es tracta d'un grup, liderat per la IP russa.
	Encara que mai se sap...

Conclusions

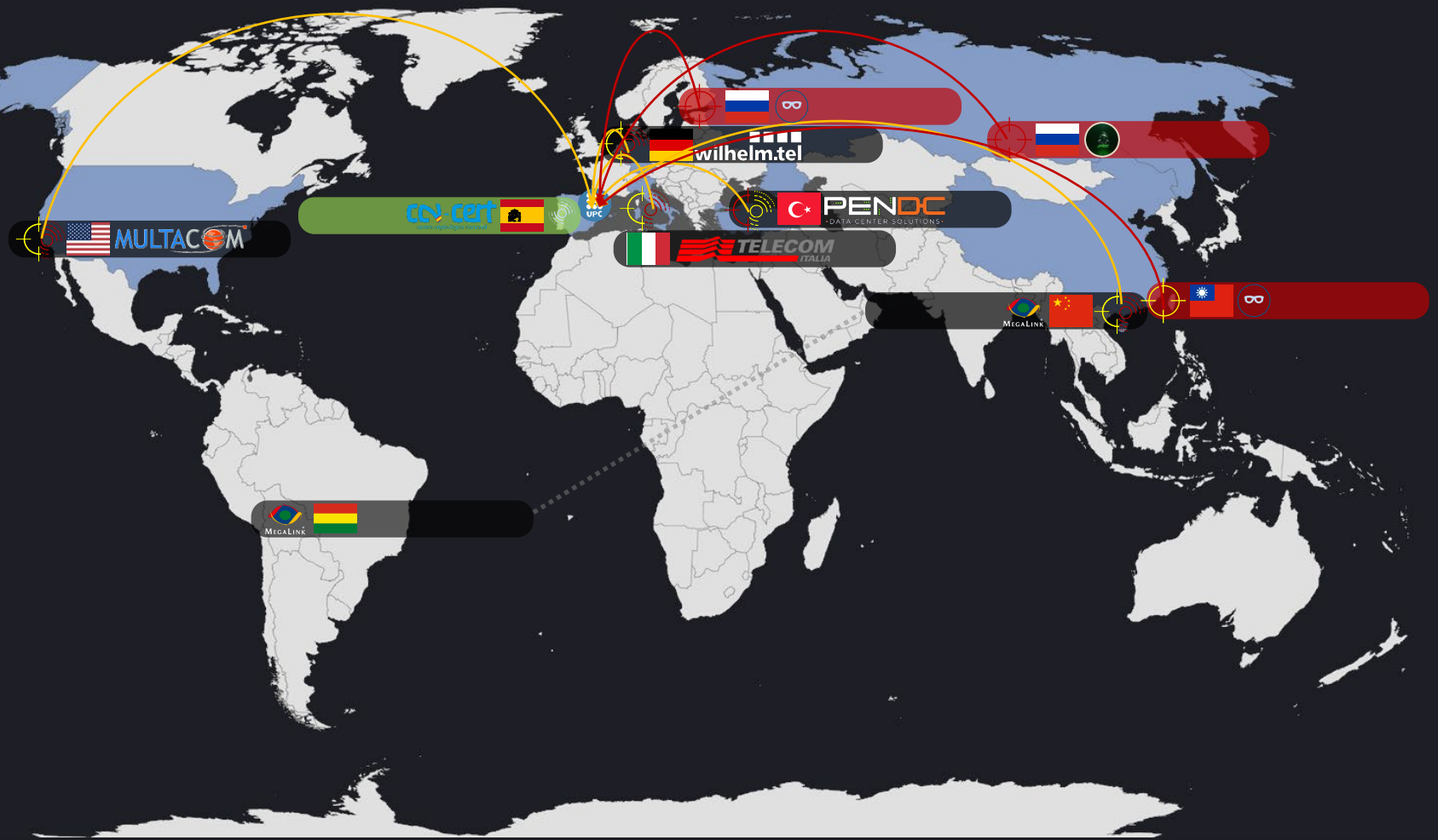
...i que cal tenir els amics a prop.

Qui:	Centro Criptográfico Nacional
Quan:	2024-03-15 – 2024-06-01
Com:	Accés anònim
Des d'on:	múltiples adreces... (Akamai Technologies, Inc.) múltiples contrades...
Per què:	El servidor està sent sistemàticament monitoritzat pel Centro Criptográfico Nacional...

Per tant... no són sospitosos de l'atac al servei FTP... Volem dir que ha estat un plaer coincidir amb vostès!

Conclusions

Resumint...



Conclusions

...i algunes reflexions...

Sobre les adreces IP identificades:

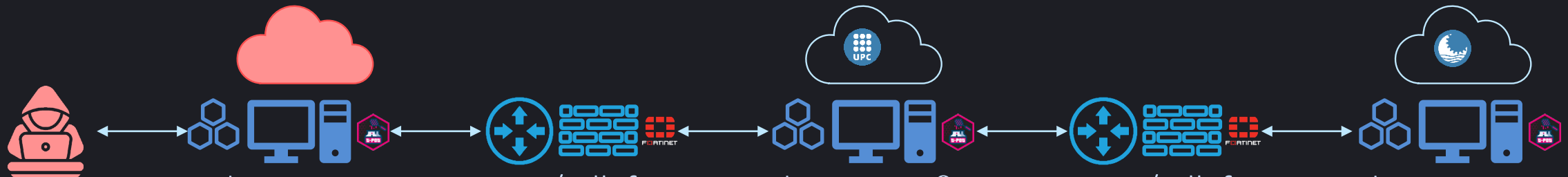
- S'han utilitzat únicament en 1 atac en el temps a 1 servei concret.
- Constaven a les bases de dades d'adreces amb mala reputació.
- No tenen per que coincidir geogràficament amb l'atacant o la víctima.
- La probabilitat de que es mantinguin operatives va decreixent en el temps.

Sobre els atacants:

- No es pot discriminar entre l'organització i l'usuari atacant.
- Pot ser difícil identificar la finalitat de l'accés (sondeig i/o atac).

Conclusions

Un tallafocs ben configurat estalvia molts mal de caps...



Dades d'atacs del 23/09/2024

honeypot α

Attacks	Ddospot	Ciscoasa	Honeytrap	Cowrie	Adbhoney	Dionaea	Tanner	ConPot	ElasticPot	Sentrypeer
109,154	44,649	44,625	14,249	4,098	429	296	157	151	123	116

honeypot β

Honeypot ...	Cowrie	Honeytrap	Tanner	Adbhoney	Dionaea	CitrixHoneypot	ElasticPot	Ciscoasa	Ddospot
2,996	1,852	966	104	34	26	10	2	1	1

honeypot χ

Honeypot ...	Honeytrap	Adbhoney	ElasticPot	Dionaea	Tanner	Redishoneypot	Ciscoasa	CitrixHoneypot	Ddospot	Ipphoney
1,373	1,267	38	23	21	10	6	3	2	1	1

Conclusions

...i queda demostrat que...

Més val un pot de mel...
...que mil barrils de vodka!

L i n k S

El cas del pot de mel