¿Dónde está *Carmen Sandiego*?

Exponiendo a los Enemigos Ocultos en Iberoamérica

GOBIERNO DE ESPAÑA · MINISTERIO DE DEFENSA

20 cni ANIVERSARIO

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

ESPDEF-CERT Mando Conjunto del Ciberespacio (MCCE)

UN CIBERESCUDO ÚNICO PARA ESPAÑA

Quiénes Somos

Ismael Valenzuela

VP Threat Research & Intelligence
BlackBerry Cylance, USA

@aboutsecurity

linkedin.com/in/ivalenzuela/

Joseliyo Sánchez

Senior Threat Researcher
BlackBerry Cylance, España

@Joseliyo_Jstnk

linkedin.com/in/joseluissm/

Dmitry Bestuzhev

Most Distinguished
Threat Researcher
BlackBerry Cylance, USA

@dimitribest

linkedin.com/in/bestuzhev/

BlackBerry
CYLANCE

Un flashback a los 80

CHILE

SITUACIÓN GEOPOLÍTICA

Chile ha gozado de estabilidad económica gracias a un modelo político que ha permitido que el país incrementara sus riquezas y destinara fondos a iniciativas que no eran prioritarias para otros países de la región. Este mismo modelo ha causado división en la sociedad, resultando en protestas organizadas con colaboración extranjera.

Una economía fuerte con un sistema bancario sólido convirtió a Chile en uno de los objetivos tempranos del crimen cibernético proveniente de Brasil. Dado sus lazos con EEUU, Chile suele verse afectada por ataques dirigidos comúnmente vistos en Norteamérica y otros países del mundo occidental.

Chile – Ataques más notables

Junio 2018

Ataque al Banco de Chile y su red SWIFT.

(APT38 - Lazarus)

Enero 2019

Ataque al Redbanc, la compañía que conecta la infrastructura de ATMs de todos los bancos chilenos.

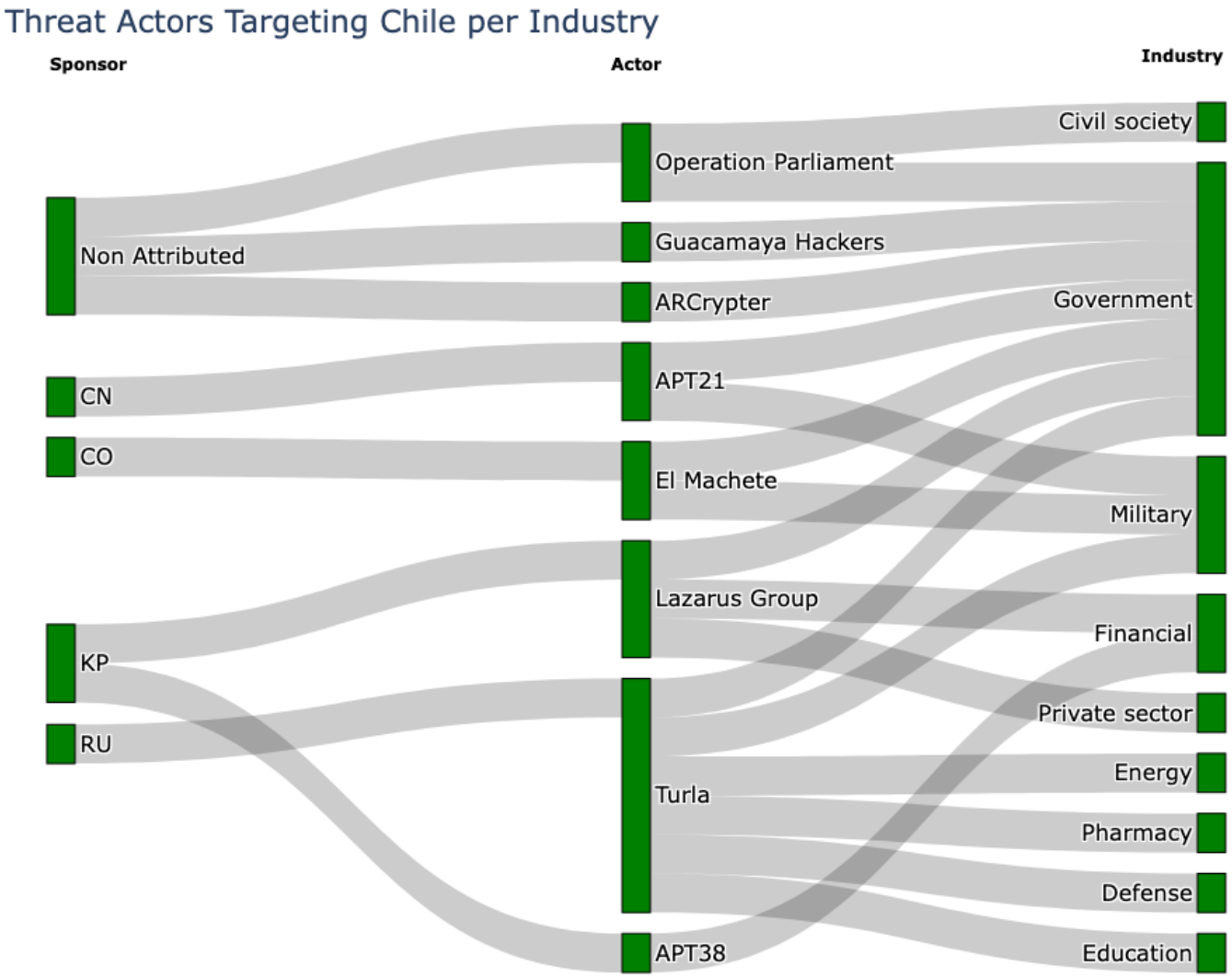
(APT38 - Lazarus)

Agosto 2022

Ataque al Gobierno de Chile con una nueva variante de ransomware, ARCrypter.

(ARCrypter Threat Actor)

Chile – Modelo de amenazas



https://github.com/blackberry/threat-research-and-intelligence/tree/main/Talks

INITIAL VECTOR

- Spearphishing
- Fake interview using LinkedIn and Skype
- Compromise a website

WEAPONS

- KillDisk
- Mimikatz
- Rundll32.exe
- AutoIt
- VBS
- Msiexec.exe

MALWARE

- FASTCASH
- HOPLIGHT
- ARCrypter
- Melcoz
- AgentTesla
- Grandoreiro
- Machete

TECHNIQUES

- T1561.002 - Disk Wipe: Disk Structure Wipe
- T1486 – Data Encrypted for Impact
- T1566.001 - Phishing: Spearphishing Attachment
- T1189 – Drive-by Compromise
- T1059.001 - Command and Scripting Interpreter: PowerShell
- T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
- T1055 – Process Injection
- T1003 – OS Credential Dumping
- T1047 - Windows Management Instrumentation

ECUADOR

SITUACIÓN GEOPOLÍTICA

Después de vivir al margen de la existencia del crimen cibernético durante años, Ecuador se enfrenta a la creciente amenaza de ataques dirigidos por mercenarios a favor de políticos destituidos, y criminales cibernéticos que atacan por igual a la Banca del Ecuador, cajeros automáticos y equipos personales.

Los organismos del orden público han sufrido múltiples ataques por el grupo **Machete**, mientras que para las fábricas de troles de Argentina, Ecuador sigue siendo uno de los mejores clientes. Es usual encontrar ataques con RAT lanzados desde Colombia.

Ecuador – Ataques más notables

Mayo 2016

Ataque a la red SWIFT del Banco del Austro.

(Lazarus Group)

Julio 2021

La empresa de telecomunicaciones CNT, propiedad del gobierno, víctima de RansomEXX.

Septiembre 2021

Banco Pichincha & Ministerio de finanzas atacado por Hotarus Group.

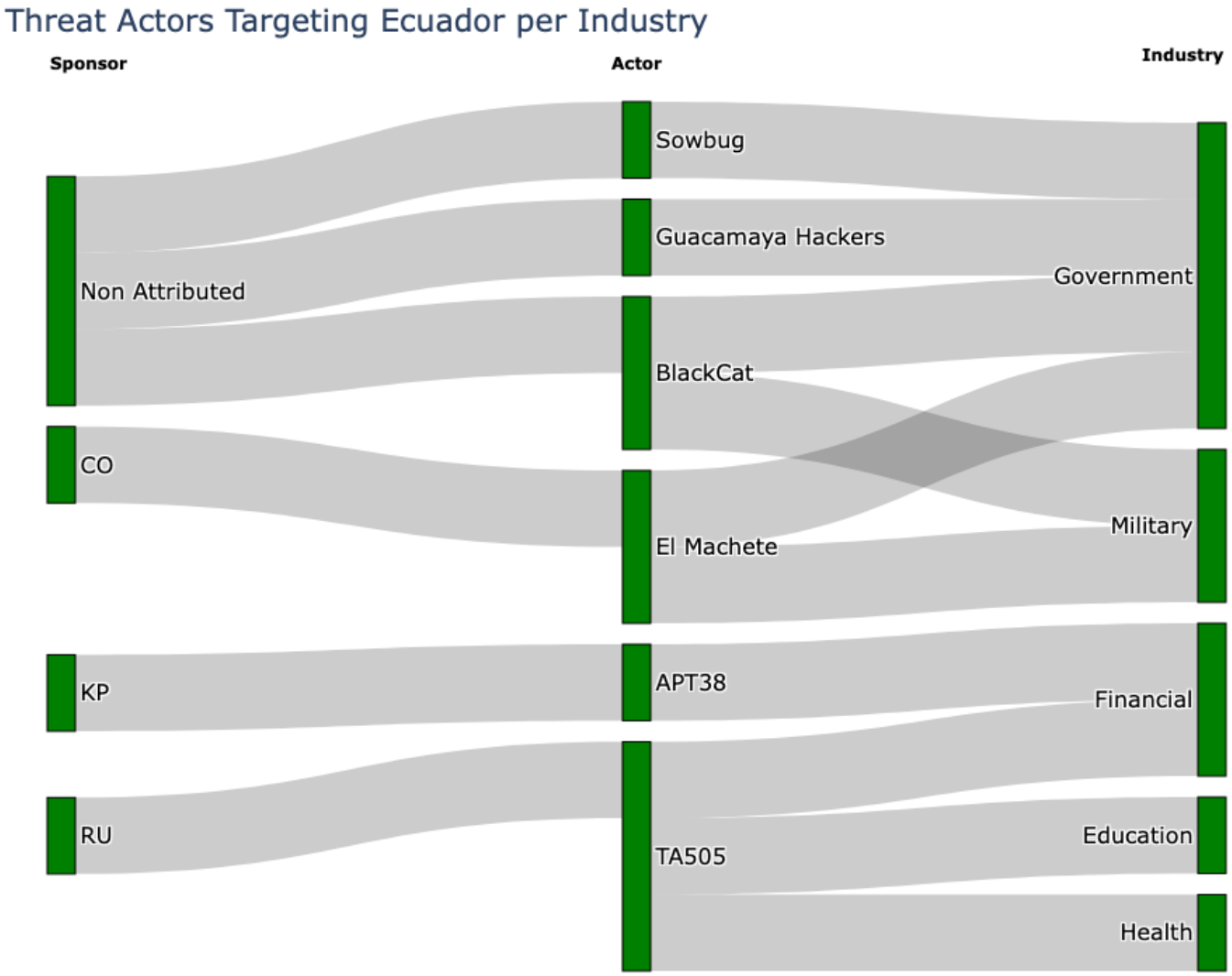
(actualmente desarticulado)

Octubre 2022

BlackCat ataca Fuerzas Armadas de Ecuador.

BlackBerry CYLANCE

Ecuador – Modelo de amenazas



https://github.com/blackberry/threat-research-and-intelligence/tree/main/Talks

BlackBerry CYLANCE

INITIAL VECTOR

- Valid accounts
- Spearphishing
- Exploit Public-Facing Apps

WEAPONS

- Msiexec.exe
- Cscript.exe
- PowerShell.exe
- Mimikatz

MALWARE

- ransomEXX
- Grandoreiro
- Guildma
- Machete
- PHP Ransomware

TECHNIQUES

- T1486 - Data Encrypted for Impact
- T1105 – Ingress Tool Transfer
- T1133 – External Remote Services
- T1566.002 - Phishing: Spearphishing Link
- T1003 – OS Credential Dumping
- T1490 - Inhibit System Recovery
- T1140 - Deobfuscate/Decode Files or Information
- T1071.001 - Application Layer Protocol: Web Protocols

COLOMBIA

SITUACIÓN GEOPOLÍTICA

Pese a apoyarse fuertemente en EEUU, Colombia vive tiempos de incertidumbre. Los efectivos que recibieron entrenamiento ciber-ofensivo especializado, han terminado usando este conocimiento para fines varios, y algunas de sus operaciones han acabado fuera de control.

El crimen cibernético se ha apoyado principalmente en diferentes familias RAT tanto para Windows, como para Android. Estas han llegado a ser una especialidad del país.
Con el reciente cambio de la fuerza política, existe más incertidumbre sobre lo que podrá pasar en el entorno de amenazas de Colombia.

Colombia – Ataques más notables

Durante 2020

Operación Spalax

(posiblemente APT-C-36)

Mayo 2020

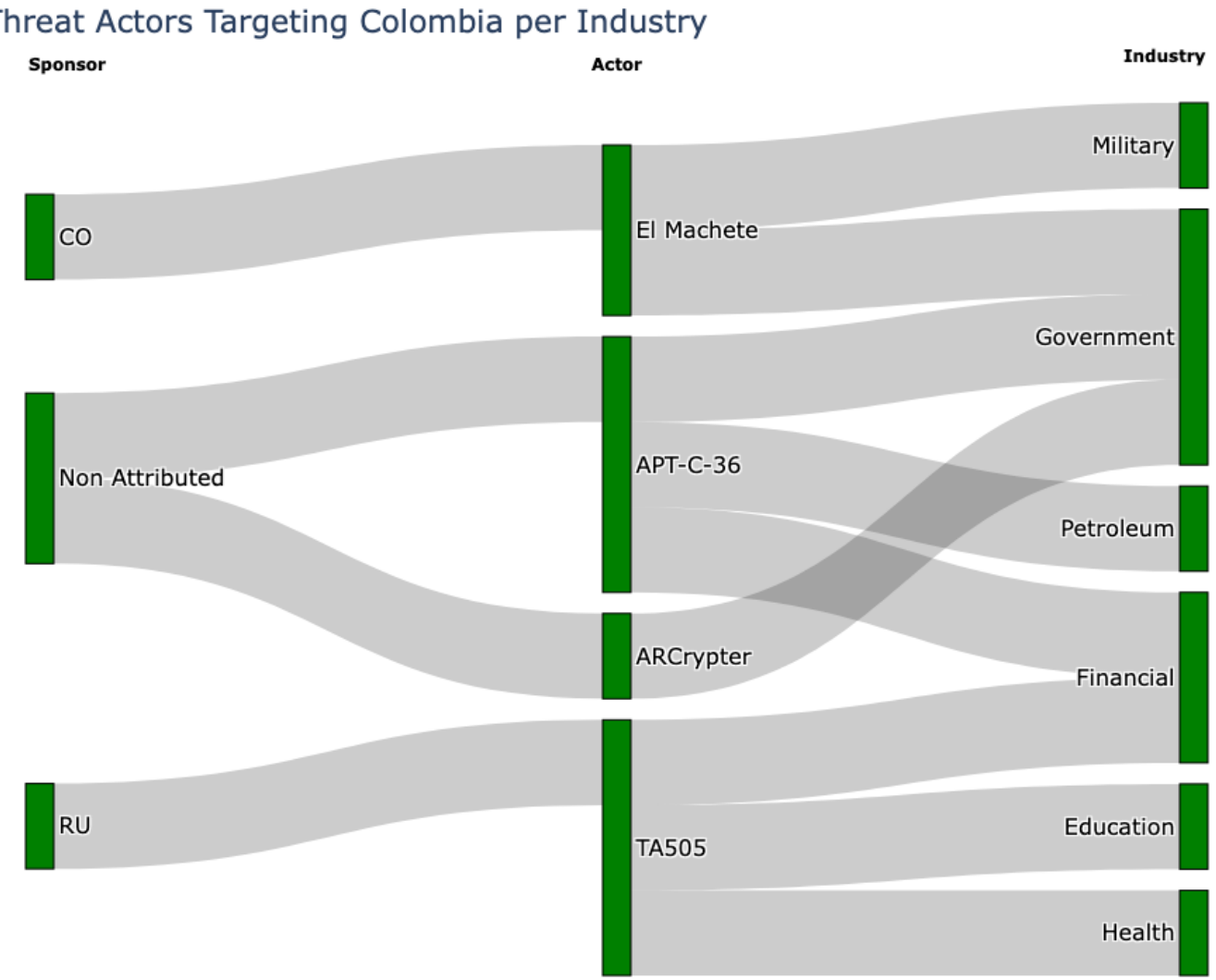
Ataques continuos a las insitituciones gubernamentales y corporativas en Colombia.

(APT-C-36)

Octubre 2022

Ataque contra el Instituto Nacional de Vigilancia de Medicamentos y Alimentos, utilizando un nuevo ransomware, ARCrypter.

Colombia – Modelo de amenazas



https://github.com/blackberry/threat-research-and-intelligence/tree/main/Talks

INITIAL VECTOR

- Spearphishing
- Google Drive and Dropbox

WEAPONS

- AutoIt
- AutoHotkey
- Msiexec.exe
- VBS
- Mshta.exe
- duckdns

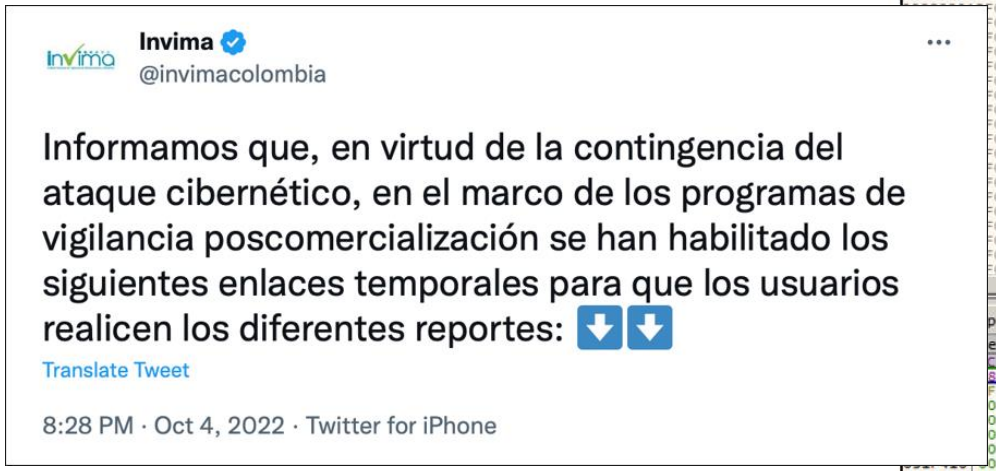
TECHNIQUES

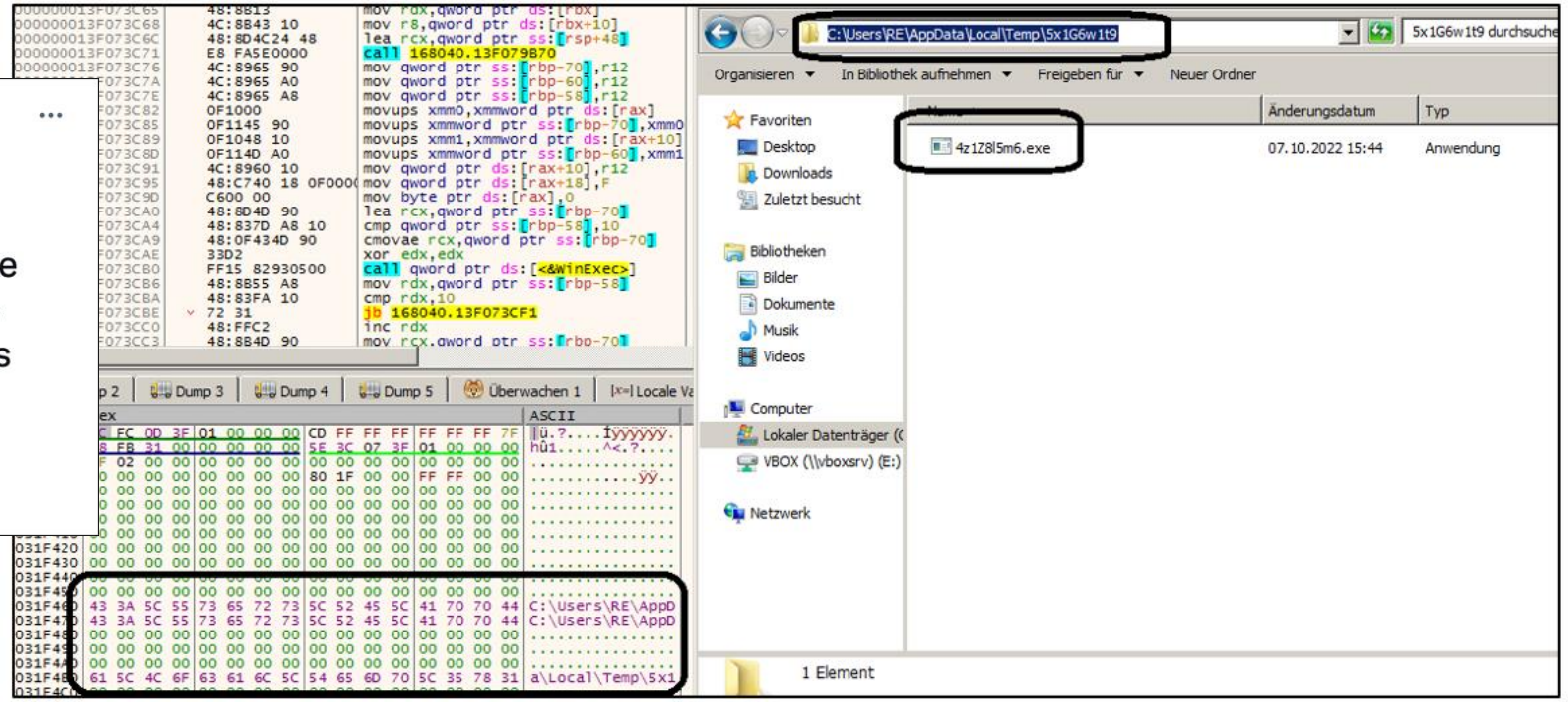
- T1486 – Data Encrypted for Impact
- T1571 – Non-Standard Ports
- T1568 – Dynamic Resolution
- T1102 – Web Service
- T1204.002 - User Execution: Malicious File
- T1036.005 - Masquerading: Match Legitimate Name or Location
- T1176 – Browser Extensions
- T1417.002 - Input Capture: GUI Input Capture (Mobile)

MALWARE

- PYSA (Mespinoza)
- ARCrypter
- Avemaria RAT
- njRAT
- AsyncRAT
- RemcosRAT
- Brazilian trojans
- BianLian
- AgentTesla

Colombia – ARCrypter





Address	Length	Type	String
.rdata:0000...	00000034	C	Z:_ARC_WorkSolution\\cryptopp860\\rijndael_simd.cpp
.rdata:0000...	0000002F	C	Z:_ARC_WorkSolution\\cryptopp860\\sha_simd.cpp
.rdata:0000...	0000002F	C	Z:_ARC_WorkSolution\\cryptopp860\\sse_simd.cpp
.rdata:0000...	00000030	C	Z:_ARC_WorkSolution\\cryptopp860\\gf2n_simd.cpp
.rdata:0000...	0000001A	C	Z:_ARC\\Encrypter 2.0.pdb

https://blogs.blackberry.com/en/2022/11/arcrypter-ransomware-expands-its-operations-from-latin-america-to-the-world

BlackBerry CYLANCE

MEXICO

SITUACIÓN GEOPOLÍTICA

México sufre una situación grave de desconfianza interna, lo que ha llevado que existan varios programas de espionaje dentro de la administración, sin el conocimiento de todos los organismos gubernamentales. Esto a dado lugar a programas de espionaje clandestinos, ilegales y descontrolados.

El crimen cibernético se lucra a través de robos en ATMs, ataques dirigidos a los bancos y ataques masivos a usuarios con el objetivo de encontrar roles privilegiados que den acceso a compañías. Brasil suele realizar ensayos con sus troyanos bancarios en México.

México – Ataques más notables

Enero 2018

El Lazarus Group ataca Bancomext.

Desde Abril a Diciembre 2019

TA505 ataca a instituciones financieras en México.

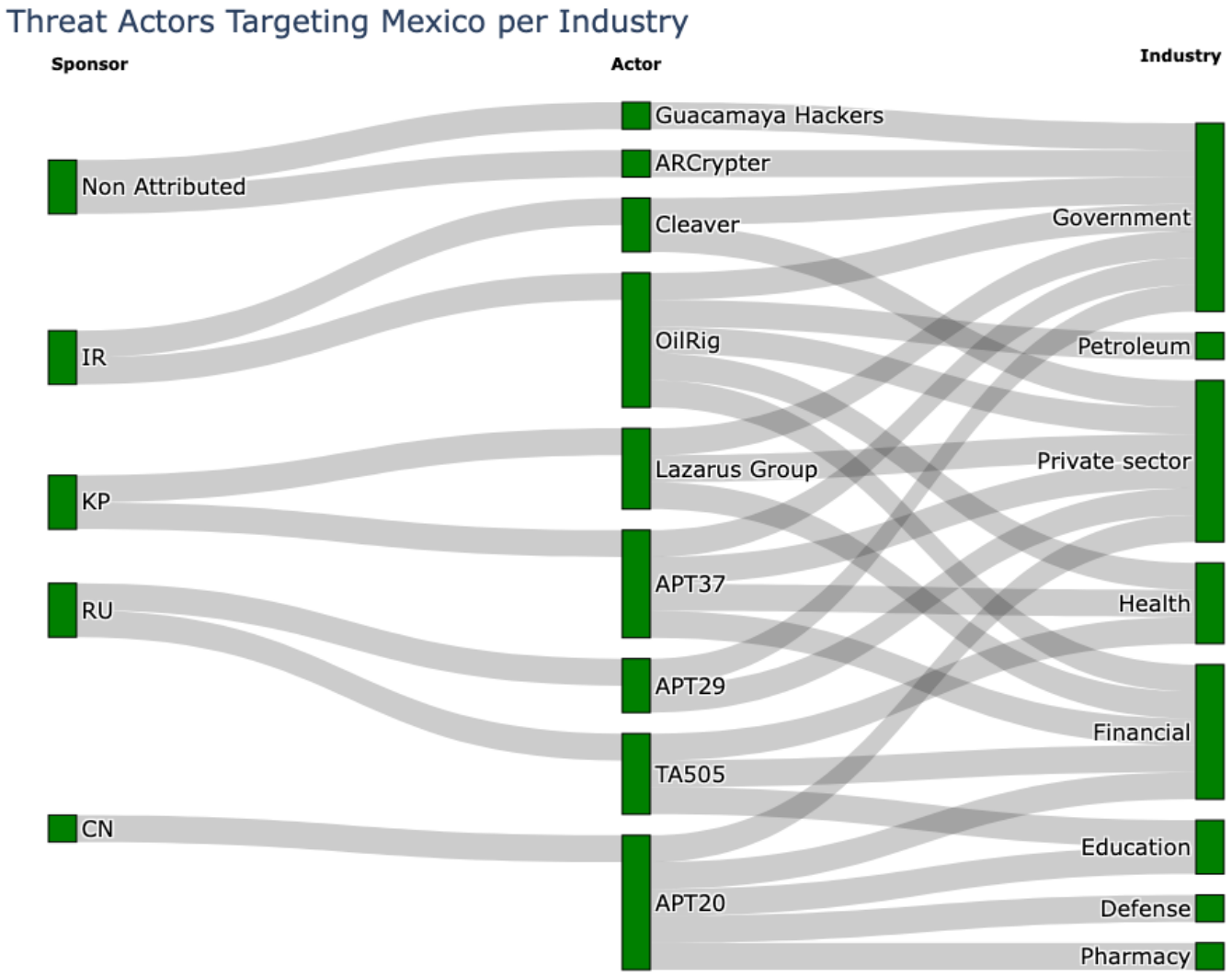
Operación Wocao en Diciembre

Durante 2022

Más de 2 TB de emails filtrados procedentes de varias empresas a modo de protesta.

Guacamaya Hackers - Leaks

México – Modelo de amenazas



https://github.com/blackberry/threat-research-and-intelligence/tree/main/Talks

INITIAL VECTOR

- Valid accounts
- Spearphishing
- Exploit Public-Facing Apps

WEAPONS

- Schtasks.exe
- PowerShell.exe
- Cscript.exe
- Msiexec.exe
- VBS
- Vssadmin.exe

TECHNIQUES

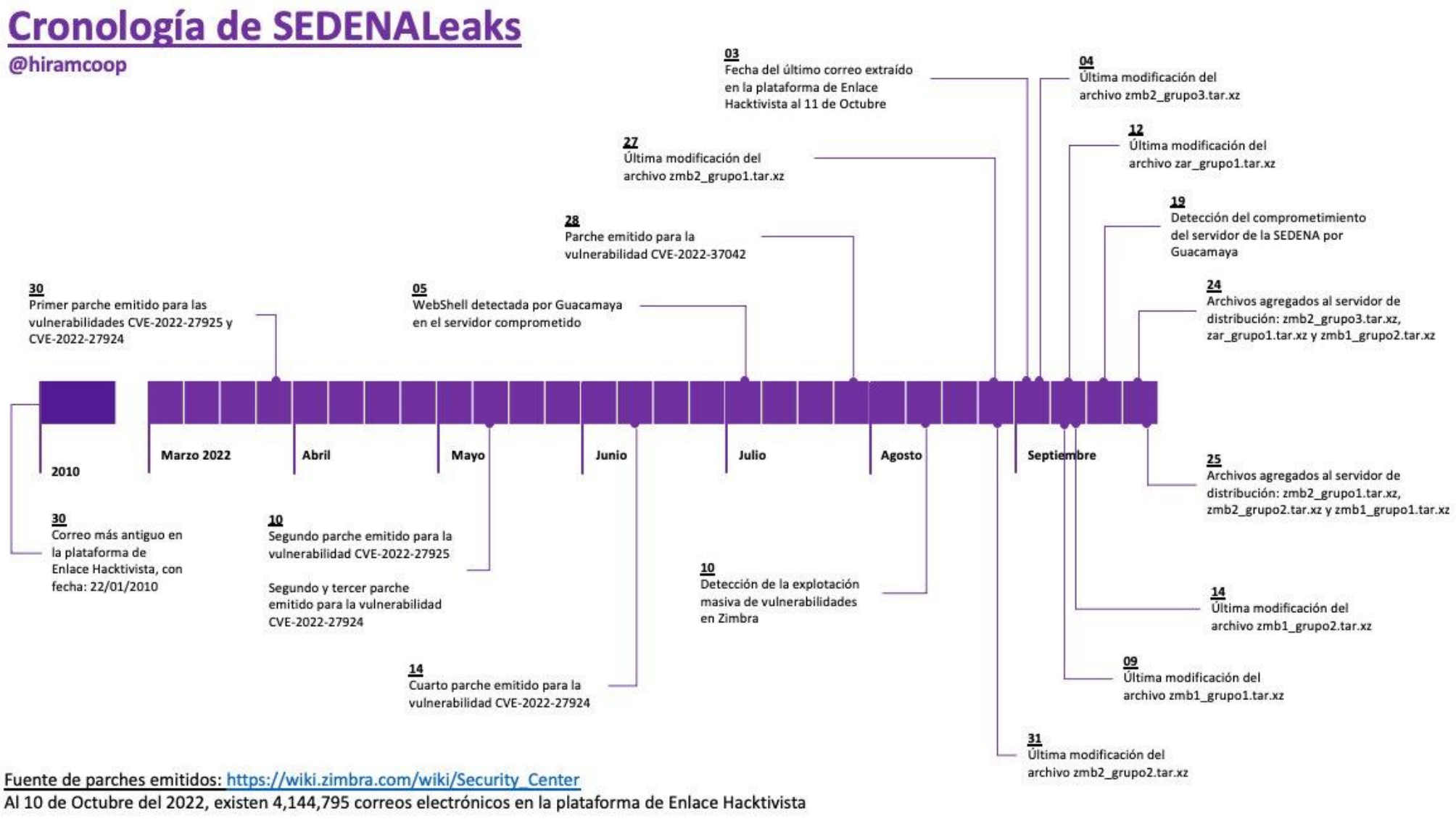
- T1548.002 - Abuse Elevation Control Mechanism: Bypass User Account Control
- T1059.001 - Command and Scripting Interpreter: PowerShell
- T1041 - Exfiltration Over C2 Channel
- T1105 - Ingress Tool Transfer
- T1133 – External Remote Services
- T1047 - Windows Management Instrumentation
- T1486 – Data Encrypted for Impact
- T1204.002 - User Execution: Malicious File
- T1053.005 – Scheduled Task/Job: Scheduled Task

MALWARE

- KONNI
- Melcoz
- Redline
- BlackCat
- Emotet
- Grandoreiro
- FlawedAmmyy RAT

Sedena Leaks by Guacamaya Hackers

CVE-2022-27925
CVE-2022-27924
CVE-2022-37042
CVE-2022-41352



https://twitter.com/hiramcoop/status/1579526972333383680/photo/1

Guacamaya Hackers Leaks

INITIAL VECTOR

- Vulnerabilidades en Zimbra, ProxyShell, ProxyLogon

RECONOCIMIENTO Y MOVIMIENTO LATERAL

- NMAP
- Mimikatz con la extensión Kiwi
- Metasploit

EXFILTRACIÓN

- Powershell, Metasploit

PERSISTENCIA

- Webshells
- Misc Backdoors

Más de 2 TB de correos electrónicos filtrados procedentes de varias empresas a modo de protesta.

- Quiborax (Chile) – Minería
- ENAMI EP (Ecuador) – Minería
- Agencia Nacional de Hidrocarburos ANH (Colombia) – Petróleo
- New Granada Energy Corporation (Colombia) – Petróleo
- Oryx Resources (Venezuela) – Petróleo
- Tejucana (Brasil) – Minería
- Ministerio de Ambiente y Recursos Naturales (Guatemala) – Gobierno

BlackBerry CYLANCE

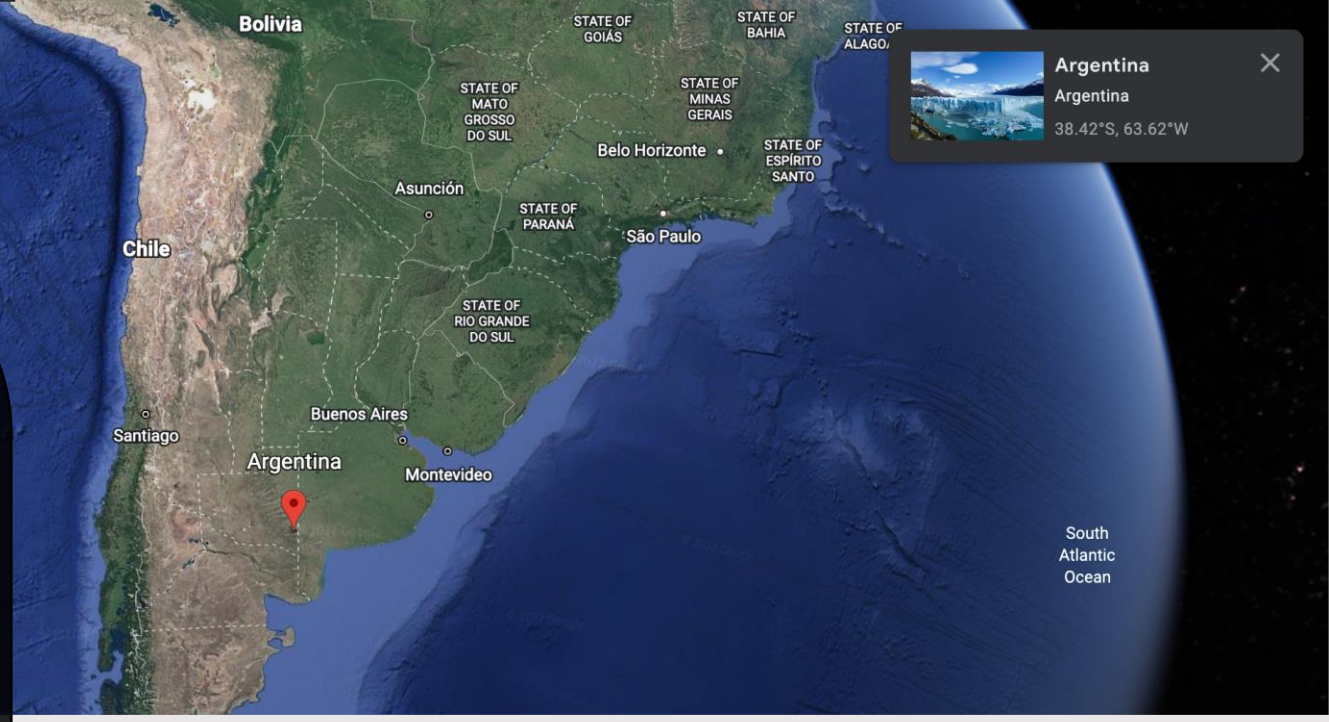
ARGENTINA

SITUACIÓN GEOPOLÍTICA

La compleja situación política y económica que el país arrastra desde hace años, junto con el legado científico, han dado forma al entorno de amenazas actual en el país.

Por un lado, se han formado grupos especializados en fábricas de troles que se especializan en manipular la opinión pública a través de las redes sociales.

Además, hay indicios de la existencia de actores de amenazas dirigidos que están atacando a otros países a nivel mundial. Presumimos, con confianza media, que estos pertenecen a grupos mercenarios que trabajan para el mejor postor.



Argentina – Ataques más notables

Septiembre 2020

Netwalker ransomware lleva a cabo una intrusión contra el gobierno Argentino.

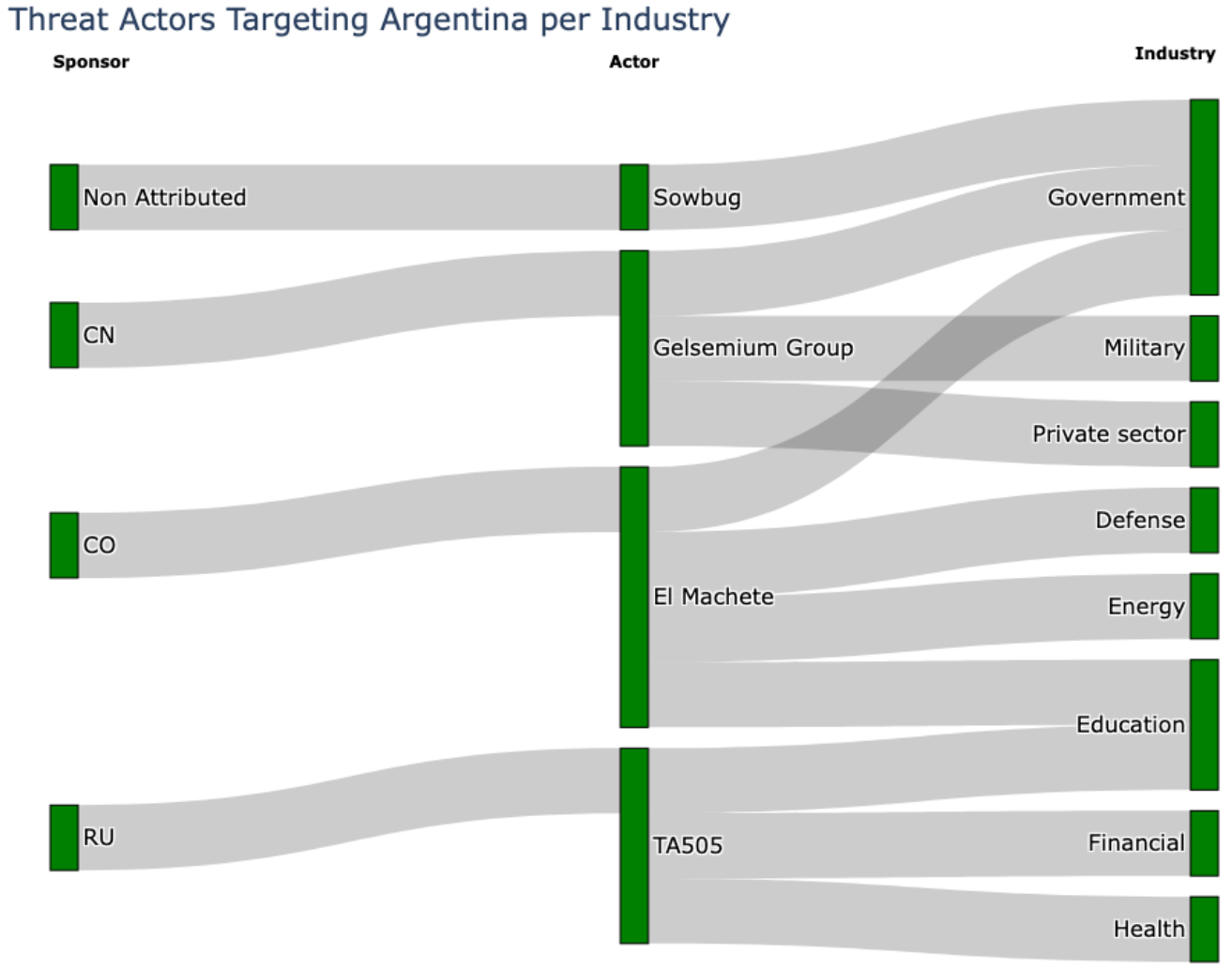
Agosto 2022

Ataque contra el poder judicial en Córdoba, Argentina, con ransomware PLAY.

Septiembre 2022

El grupo Everest Ransomware ataca al gobierno Argentino cifrando la información.

Argentina – Modelo de amenazas



https://github.com/blackberry/threat-research-and-intelligence/tree/main/Talks

INITIAL VECTOR

- Email addresses leaked
- Valid accounts
- Exploit applications

WEAPONS

- Msiexec.exe
- Vssadmin.exe
- WMI
- Powershell.exe

MALWARE

- PLAY
- Guildma
- Gelsemium IIS Backdoor
- Everest ransomware
- Netwalker
- Machete

TECHNIQUES

- T1190 - Exploit Public-Facing Application
- T1505.003 - Server Software Component: Web Shell
- T1047 - Windows Management Instrumentation
- T1490 - Inhibit System Recovery
- T1204.002 - User Execution: Malicious File
- T1218.007 - System Binary Proxy Execution: Msiexec
- T1132.001 - Data Encoding: Standard Encoding
- T1041 - Exfiltration Over C2 Channel
- T1133 - External Remote Services

BRASIL

SITUACIÓN GEOPOLÍTICA

El sistema legal actual, complejo y contradictorio, impide que se luche de forma efectiva contra el crimen cibernético, que siempre ha destacado como una especialidad del país.

Varios grupos han lanzado ataques contra el Boleto, ATMs, POS y sistemas Windows. Existe un cluster de grupos criminales que se ha establecido como líderes en la región, expandiendo sus operaciones hacia Europa (España, Portugal), Latinoamérica y EEUU.

Aprovechando el conocimiento previo de la infraestructura de sus víctimas, los actores de amenazas han lanzado ataques sofisticados contra sistemas Linux. El caso del Symbiote (2022) es un ejemplo de dicha tendencia.

Brasil – Ataques más notables

Diciembre 2019

Operación Wocao.

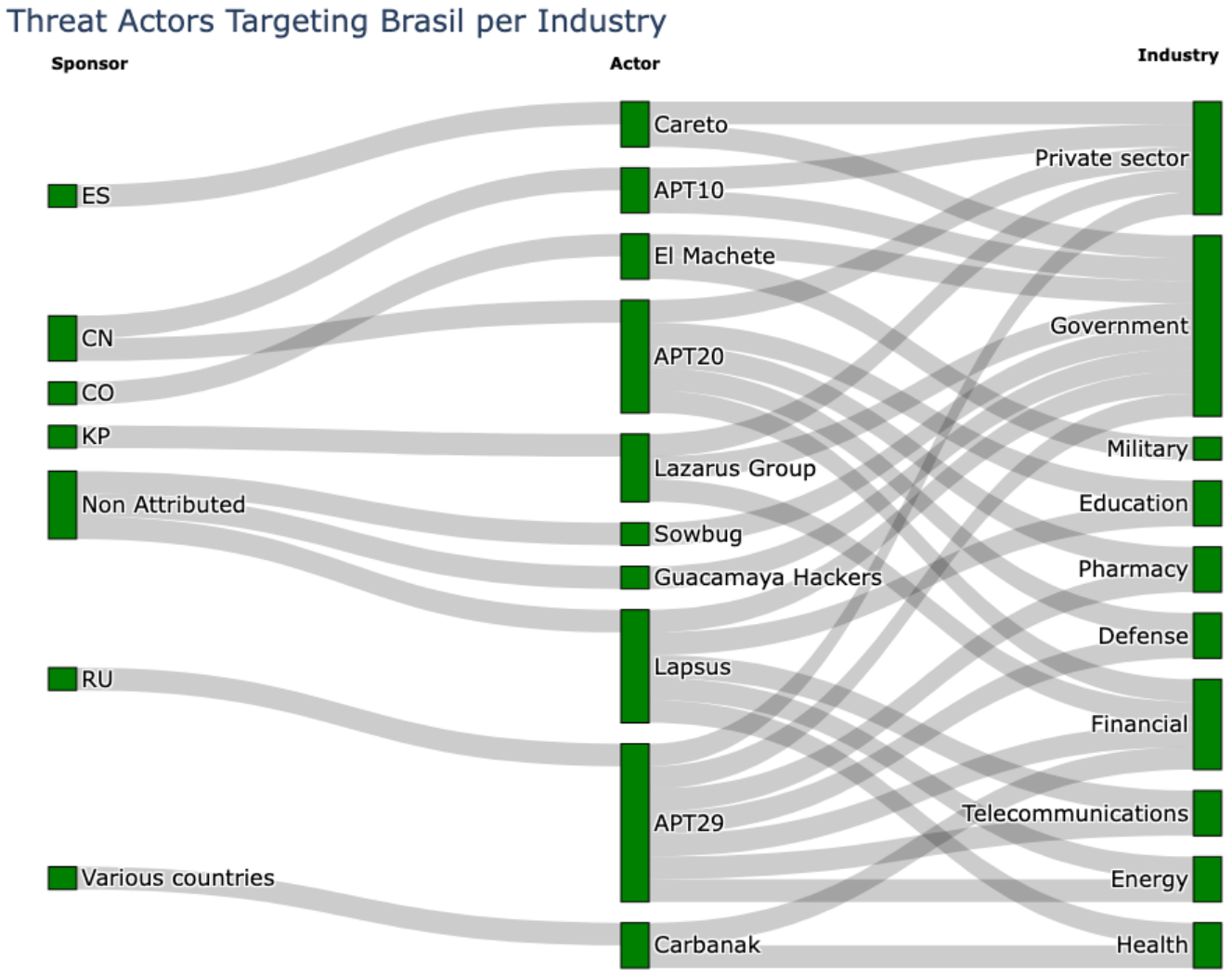
Diciembre 2021

Ataque contra el Ministerio de Salud de Brasil elimina datos de vacunación COVID-19.

Noviembre 2022

Nueva actividad relacionada con el backdoor DTrack usada por Lazarus Group contra diferentes sectores.

Brasil – Modelo de amenazas



https://github.com/blackberry/threat-research-and-intelligence/tree/main/Talks

INITIAL VECTOR

- Spearphishing
- Exploit Public-Facing Apps

WEAPONS

- PowerShell.exe
- Msiexec.exe
- Cobalt Strike
- Mimikatz
- AutoIt
- AutoHotkey

TECHNIQUES

- T1071.001 - Application Layer Protocol: Web Protocols
- T1027.004 – Obfuscated Files or Information: Compile After Delivery
- T1133 – External Remote Services
- T1568 – Dynamic Resolution
- T1190 - Exploit Public-Facing Application
- T1105 – Ingress Tool Transfer
- T1505.003 - Server Software Component: Web Shell
- T1059 - Command and Scripting Interpreter
- T1555.003 - Credentials from Password Stores: Credentials from Web Browsers

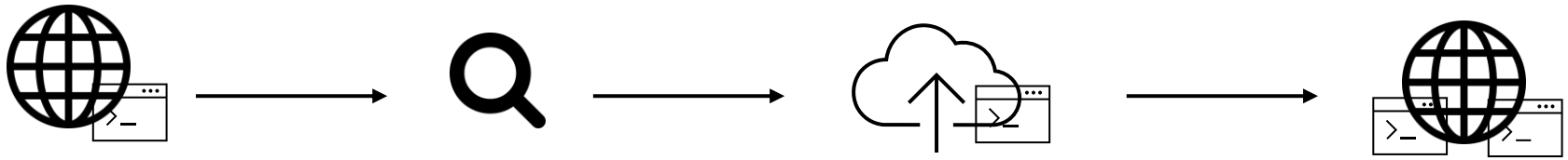
MALWARE

- Amadey
- Emotet
- Melcoz
- Grandoreiro
- RedLine
- DTrack
- Prilex
- Bizarro
- Machete
- Symbiote

Brasil – Operación Wocao

Los adversarios de Operation Wocao utilizaron esas webshells (que no eran suyas) para reconocimiento y movimientos laterales

Ambas webshells continuaron en uso durante casi toda la operación



Se identificaron algunos servidores infectados con webshells explotando versiones de JBOSS

Después de la fase de reconocimiento, los adversarios subieron sus propias webshells

Resultado clave

Credenciales de VPN

PsExec

SmbExec

Checkadmin

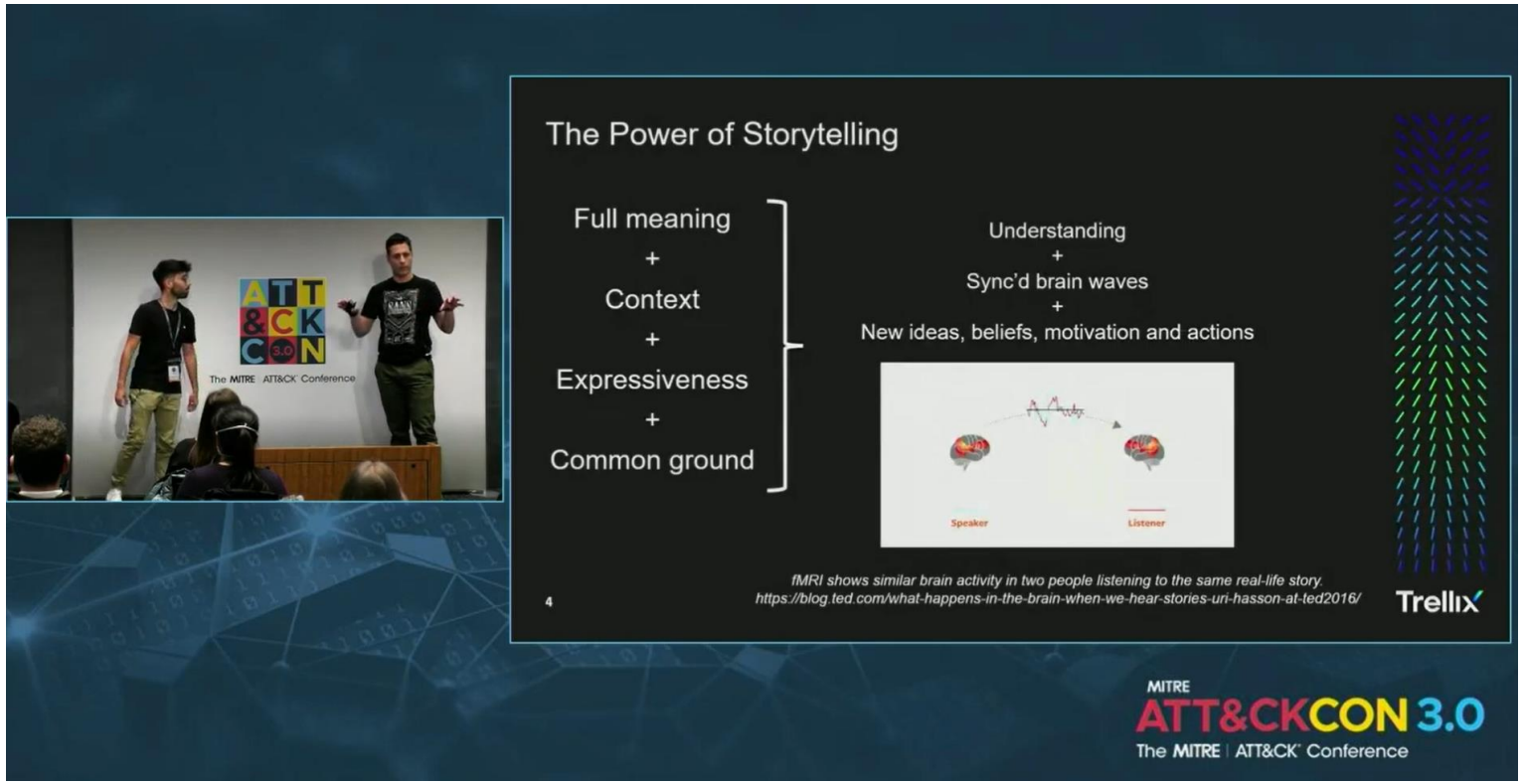
BloodHound

Mimikatz

https://www.fox-it.com/media/kadlze5c/201912_report_operation_wocao.pdf

BlackBerry CYLANCE

Threat Sightings



https://www.youtube.com/watch?v=eRHw-An9NuI


```
{
    "summary": {
        "sightings": 5,
        "behaviors": 76,
        "weapons": {…
        },
        "types": {
            "File Created": 18,
            "Network Accessed": 3,
            "Process Created": 48,
            "ApiInvoked": 2,
            "Scheduled Task Creation": 1,
            "Scheduled Task Changed": 1,
            "Service Creation": 1,
            "RegValue Modified": 1,
            "RegValue Read": 1
        },
        "lolbas": 13,
        "tools": 21,
        "malware": 5,
        "adversaries": 1,
        "tactics": {
            "initialAccess": 1,
            "persistence": 5,
            "commandAndControl": 5,
            "execution": 13,
            "defenseEvasion": 8,
            "discovery": 30,
            "credentialAccess": 6,
            "collection": 4
        },
        "techniques": {
            "T1190": 1,
            "T1505.003": 3,
            "T1071.001": 1,
            "T1095": 2,
            "T1090": 1,
            "T1059.001": 3,
            "T1140": 1,
            "T1059.003": 3,
            "T1106": 2,
            "T1090.003": 1,
            "T1083": 6,
            "T1055": 1,
            "T1069.001": 3,
            "T1082": 1,
            "T1018": 4,
```

```
    "weapons": {
        "JexBoss": 2,
        "Unknown webshell": 4,
        "XServer": 5,
        "powershell.exe": 3,
        "dir.exe": 1,
        "Process Launcher": 2,
        "CheckAdmin.exe": 3,
        "getos.py": 3,
        "keylogger": 1,
        "cmd.exe": 2,
        "schtasks.exe": 4,
        "cscript.exe": 1,
        "OAKMZ.vbs": 1,
        "sc.exe": 2,
        "wmic.exe": 1,
        "doscmd/copy": 1,
        "Mimikatz": 3,
        "procdump.exe": 1,
        "PowerSploit": 1,
        "net.exe": 2,
        "wevtutil.exe": 2,
        "doscmd/time": 1,
        "doscmd/type": 2,
        "doscmd/dir": 4,
        "makecab.exe": 1,
        "WinRAR.exe": 1,
        "doscmd/del": 1,
        "netstat.exe": 3,
        "taskkill.exe": 1,
        "reg.exe": 3,
        "SharpHound": 1,
        "zos.exe": 2,
        "ntbscan": 2,
        "iie.exe": 2,
        "dnsquery": 1,
        "tasklist.exe": 2,
        "ping.exe": 2,
        "ipconfig.exe": 1,
        "dnscmd.exe": 1
    },
```


BlackBerry CYLANCE

Threat Sightings

```
threatSightings:
  - sighting: Initial Access - Threat actors used webshells already on the servers and also used their own to gain initial access.
    - behavior: Cmd.exe is executed to load a command received from the webshell to spawn schtasks.exe
      type: Process Created
      id: 1c8d5839-fcde-4197-ab89-ead9189b7fdb
      weapon: cmd.exe
      processes:
        - process: C:\\Windows\\System32\\cmd.exe
          cmdLine:
          - 'cmd.exe /c cd /d c:\\temp & schtasks /create /u <DOMAIN>\<USERNAME> /p "<PASSWORD>" /ru system /sc daily /tr "cmd /c powershell.exe -ep bypass -file c:\\s.ps1" /tn win32times /f'
      att&ck:
        execution:
        - "T1059.003 - Command and Scripting Interpreter: Windows Command Shell"
    - behavior: There are two ways used by XServer to execute commands on the victim system. This is the second one, using API Calls···
    - behavior: Two versions of Agent were found on the systems. One was written in C# and the other one in Python and compiled with py2exe.···
  - sighting: Collection and Execution - Mutiple tools are deployed in the system to get information and execute processes
    id: ea8c3361-18fb-485f-8156-fc9283ab2492
    behaviors:
    - behavior: A basic custom tool is deployed in the victim system
    - behavior: The custom tool dir.exe is executed to get informatic
    - behavior: A custom process launcher tool was used to execute pr
    - behavior: Process Launcher use the Windows API to launch and ir
    - behavior: Threat actors deploy an old version checkadmin.exe t
    - behavior: CheckAdmin is launched to get information about privi
    - behavior: Besides the old version of checkadmin.exe, threat act
    - behavior: Threat actors deploy a custom tool to get informatio
    - behavior: The tool to get information about the OS was executed
    - behavior: getos.py uses SMB to get information from remote syst
    - behavior: A custom keylogger was used to obtain password for th
    - behavior: Cmd.exe is executed to load a command received from t
    - behavior: Scheduled tasks is used to execute malicious code···
    - behavior: The task is created in the system···
    - behavior: The scheduled task is executed using PowerShell···
    - behavior: After executing the PowerShell code, the scheduled ta
    - behavior: The task is removed from the s ystem···
    - behavior: The VBS Script which was created in the initial stage
    - behavior: A text file is created to store the information from
    - behavior: Cmd.exe is executed to load a command received from t
```

```
- behavior: The task is created in the system
  type: Scheduled Task Creation
  id: 26168045-0c39-4b5d-8ccb-8013a180216b
  weapon: schtasks.exe
  scheduledTasks:
    - commands: "cmd /c powershell.exe -ep bypass -file c:\\s.ps1"
      name: win32times
  notes:
  - The actor attempts to mislead the victim with the name of the task
  - You can get more in event ID 4698
  att&ck:
    execution:
    - "T1053.005 - Scheduled Task/Job: Scheduled Task"
```

BlackBerry CYLANCE

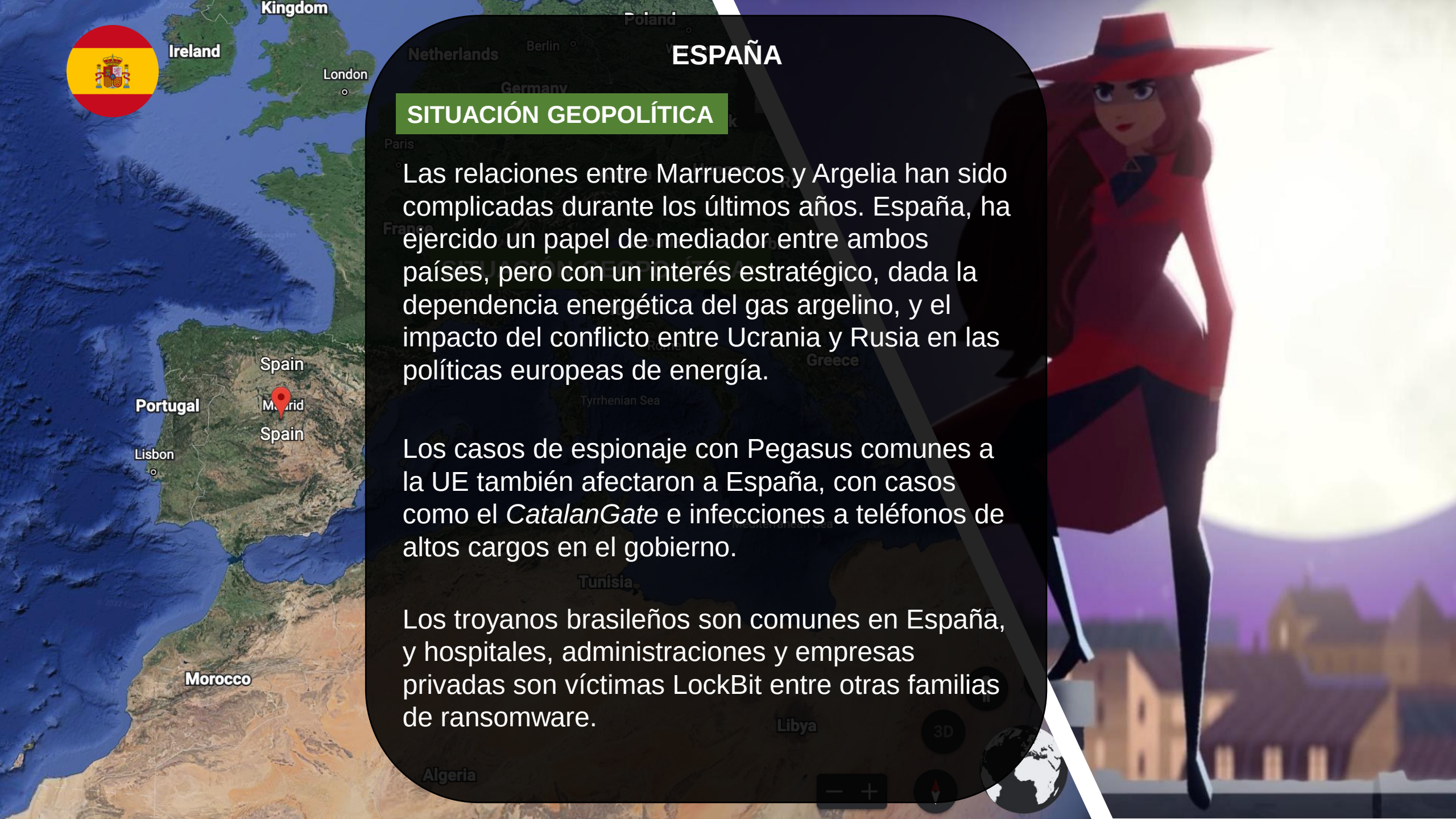
ESPAÑA

SITUACIÓN GEOPOLÍTICA

Las relaciones entre Marruecos y Argelia han sido complicadas durante los últimos años. España, ha ejercido un papel de mediador entre ambos países, pero con un interés estratégico, dada la dependencia energética del gas argelino, y el impacto del conflicto entre Ucrania y Rusia en las políticas europeas de energía.

Los casos de espionaje con Pegasus comunes a la UE también afectaron a España, con casos como el *CatalanGate* e infecciones a teléfonos de altos cargos en el gobierno.

Los troyanos brasileños son comunes en España, y hospitales, administraciones y empresas privadas son víctimas LockBit entre otras familias de ransomware.



España – Ataques más notables

Marzo 2018

El líder del grupo Carbanak, responsable del robo de más de 1 billón de euros a más de 100 entidades financieras, arrestado en Alicante.

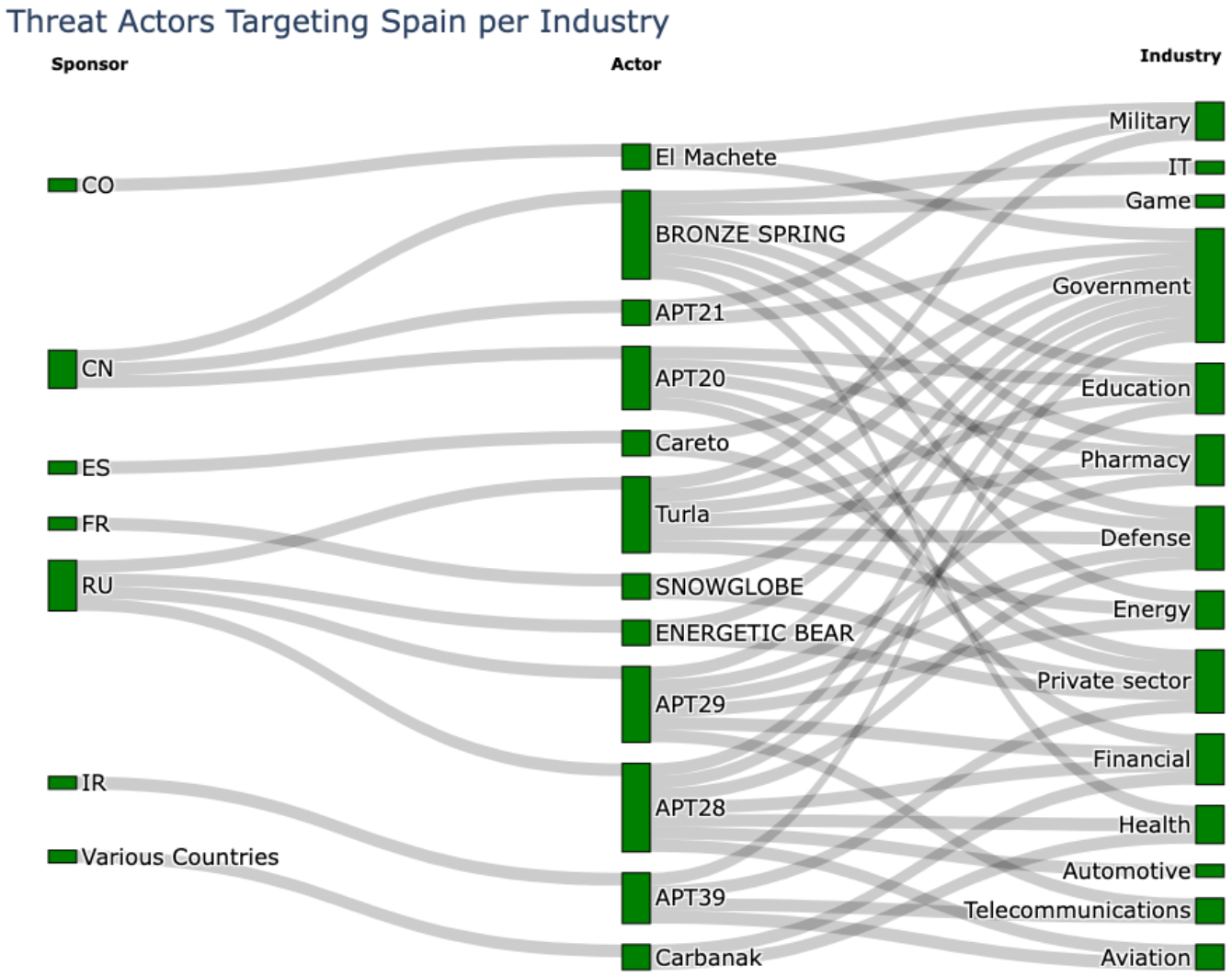
Julio 2020

Ciber-ataque de REvil contra infrastructura crítica incluyendo la red ferroviaria de España, resultando en el robo de más de 800GB de datos.

Mayo 2022

Software de espionaje Pegasus instalado en dispositivos móviles de altos cargos y personas de interés con fines politicos.

España – Modelo de amenazas



https://github.com/blackberry/threat-research-and-intelligence/tree/main/Talks

BlackBerry CYLANCE

INITIAL VECTOR

- Spearphishing
- Valid accounts

WEAPONS

- PsExec
- BloodHound
- Mimikatz
- PowerShell.exe
- Wscript.exe
- Cobalt Strike

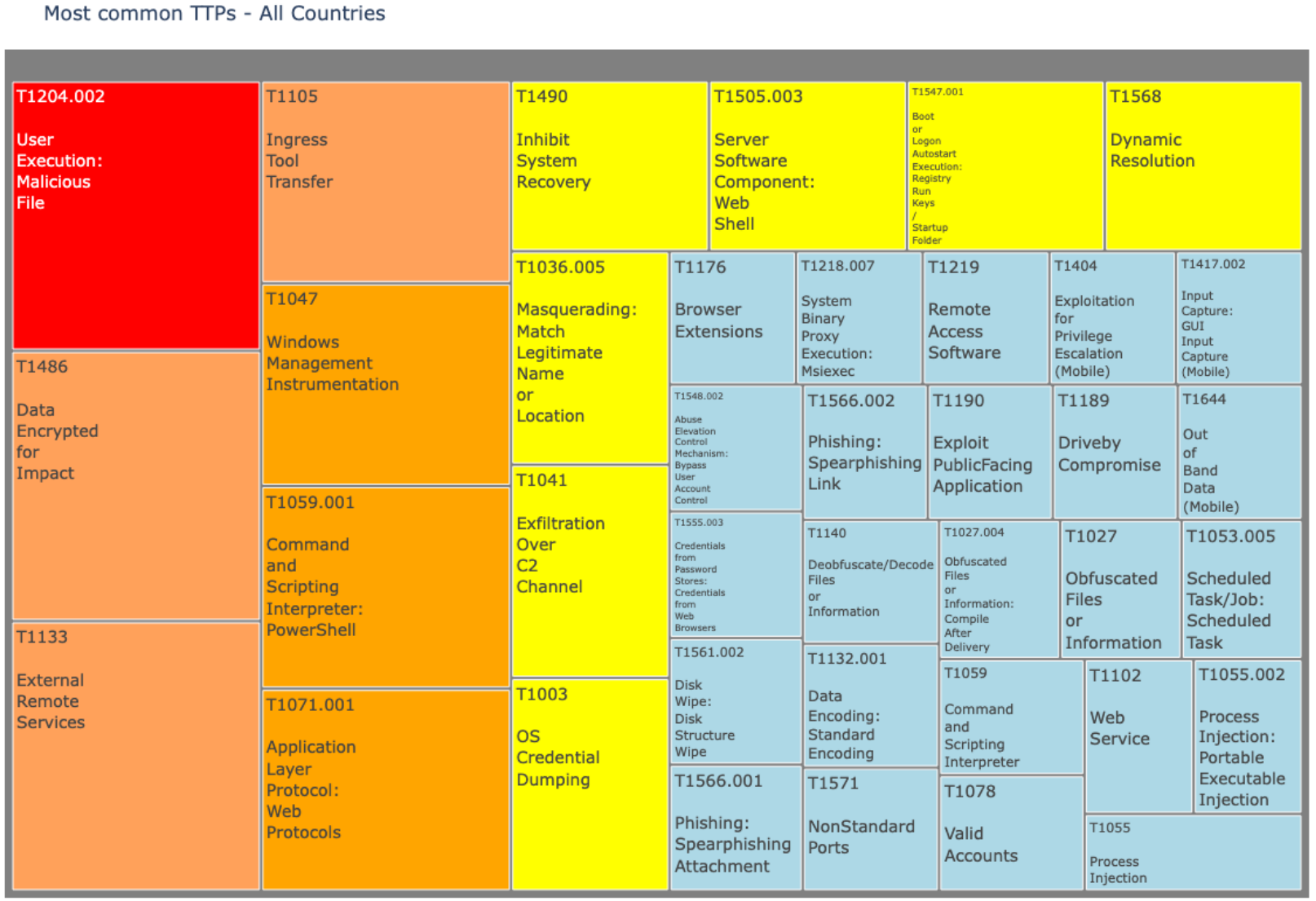
TECHNIQUES

- T1219 – Remote Access Software
- T1055.002 - Process Injection: Portable Executable Injection
- T1071.001 - Application Layer Protocol: Web Protocols
- T1047 - Windows Management Instrumentation
- T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
- T1078 – Valid Accounts
- T1036.005 - Masquerading: Match Legitimate Name or Location
- T1404 - Exploitation for Privilege Escalation (Mobile)
- T1644 - Out of Band Data (Mobile)

MALWARE

- Carbanak
- Revil
- WannaCry
- Pegasus
- Netwalker
- Grandoreiro
- Mekotio
- Machete

Agregación TTPs – modelo de amenazas



Fuentes:

- Telemetría interna BlackBerry Cylance
- Virustotal Intelligence
- Reportes CTI

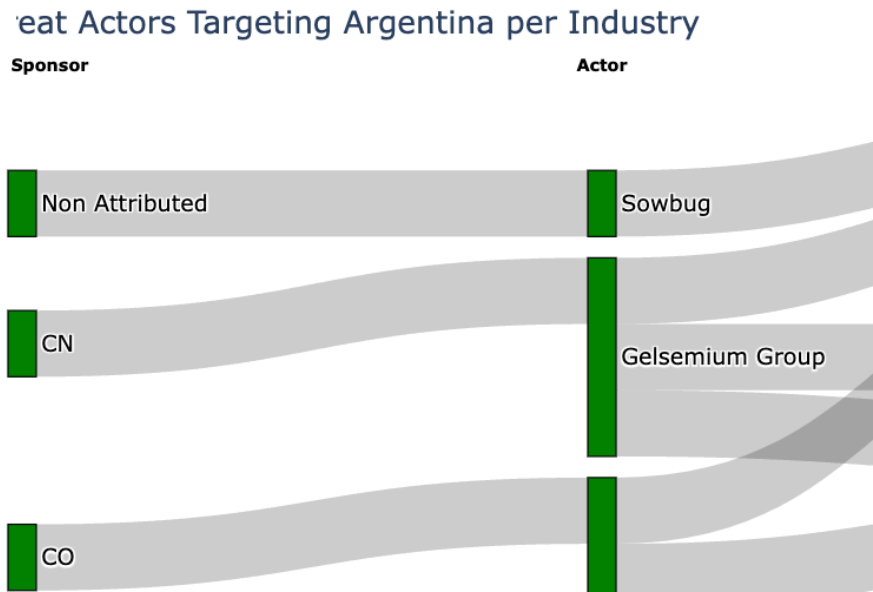
BlackBerry CYLANCE

MITRE ATT&CK VS D3FEND

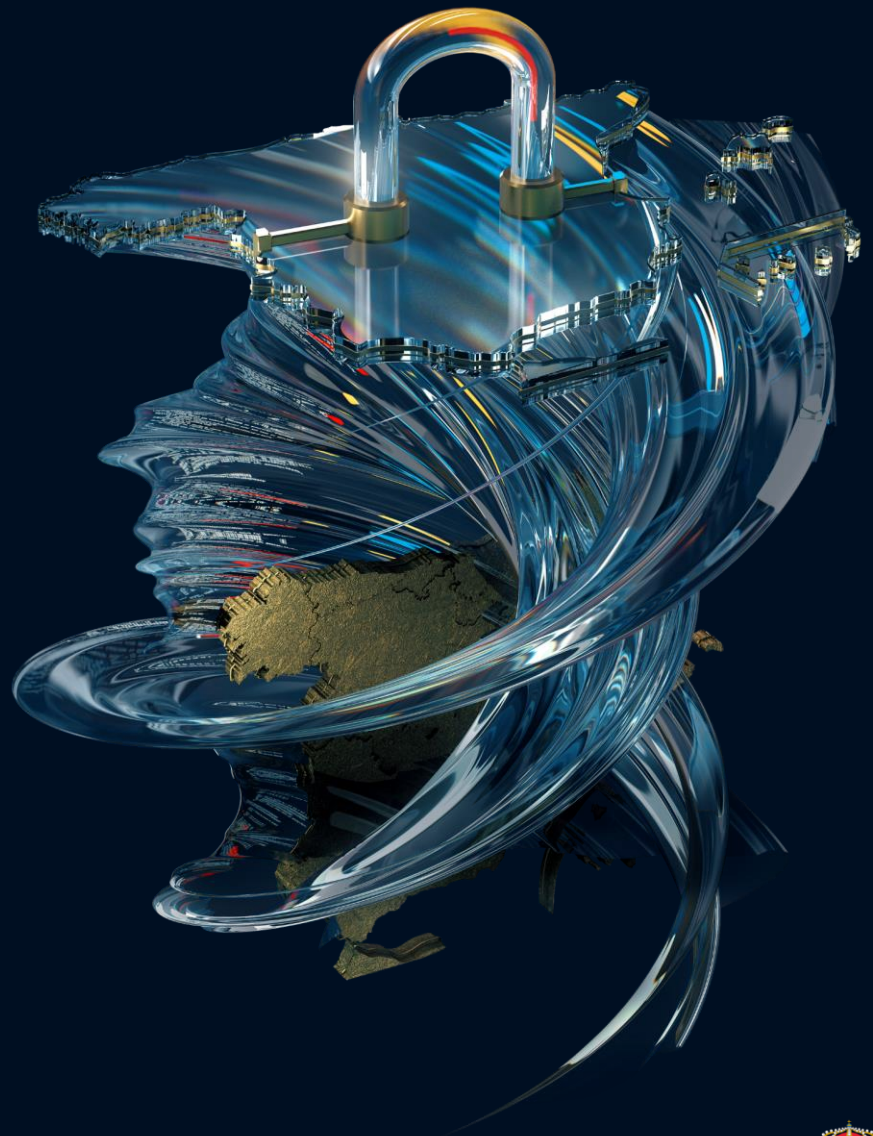
Entregables

- CSVs de modelos de amenazas
- CSV de TTPs por actor y region
- Jupyter Notebooks con gráficas Sankey y Treemap
- Threat Sighting de operación Wocao
  - Otras exportaciones para TIPs
- PDF de esta presentación

```
import plotly.graph_objects as go

fig = go.Figure(data=[go.Sankey(
    node = dict(
        pad = 15,
        thickness=20,
        line=dict(color='black', width=1),
        label = unique_source_target,
        color='green'
    ),
    link = dict(
        source = links_dict['source'],
        target = links_dict['target'],
        value = links_dict['value']

    xtfont=dict(color="black", size=16)


    ate_layout(title='Threat Actors Targeting Argentina per Industry',
                font_size=16,
                autosize=True,
                width=1000,
                height=800)

    nnotation(dict(font=dict(color="black",size=12), x=0, y=1.06, showarrow=False, text
    nnotation(dict(font=dict(color="black",size=12), x=0.5, y=1.06, showarrow=False, te
    nnotation(dict(font=dict(color="black",size=12), x=1, y=1.07, showarrow=False, text

)
```



https://github.com/blackberry/threat-research-and-intelligence/tree/main/Talks/



MUCHAS GRACIAS

GOBIERNO DE ESPAÑA · MINISTERIO DE DEFENSA

20 cni ANIVERSARIO

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

ESPDEF-CERT Mando Conjunto del Ciberespacio (MCCE)

UN **CIBERESCUDO ÚNICO** PARA **ESPAÑA**

BlackBerry CYLANCE

XVI JORNADAS STIC CCN-CERT

IV JORNADAS DE CIBER_DEFENSA: ESPDEF-CERT

Ismael Valenzuela

Joseliyo Sánchez

¿DÓNDE ESTÁ CARMEN SANDIEGO? EXPONIENDO A LOS ENEMIGOS OCULTOS EN IBEROAMÉRICA

Se analizarán amenazas que se ocultan en los países iberoamericanos, incluyendo los actores locales y provenientes de otras regiones más activos en España, Chile, México, Argentina, Brasil, Colombia y Ecuador, sus motivaciones, y sus TTPs.

JUEVES 1 DE DICIEMBRE – SALA 25 – 10:10 AM

GOBIERNO DE ESPAÑA · MINISTERIO DE DEFENSA

20 cni ANIVERSARIO

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

ESPDEF-CERT Mando Conjunto del Ciberespacio (MCCE)

UN CIBERESCUDO ÚNICO PARA ESPAÑA