

 **BlackBerry**® Intelligent Security. Everywhere.

RATS AND INFOSTEALERS: MISSION SPAIN AND CATALONIA

2023/04/20

DRCN 2023

Joseliyo Sánchez – Senior Threat Researcher



Joseliyo Sánchez Martínez

- ▶ Senior Threat Researcher at BlackBerry Cylance
- ▶ Ad-hoc Working Group on Cyber Threat Landscapes at ENISA



@Joseliyo_Jstnk



[linkedin.com/in/joseluissm/](https://www.linkedin.com/in/joseluissm/)

AGENDA

▮ Context

▮ Darkweb

▮ Campaigns

CONTEXT

WHAT'S HAPPENING HERE?

- Last months we have heard of attacks carried out against public organizations in Spain.
 - Most of the attacks had ransomware activity related
- Not in the news, multiple private companies are being targeted by different cybercriminals
- As we could see, there is a special interest in companies based in Catalonia (although there are also companies from different places in Spain)

UPDATE: Hackers threaten to publish data on infectious diseases patients from Barcelona's Hospital Clinic unless they pay €4.2 million

By Chris King · 07 April 2023 · 2:33

```
#include <bits/stdc++.h>
using namespace std;
int main()
{
    InitializeComponent();
    InitializeHackingMainLibrary();
    InitializeVirusLibraries();
    InitializeTrojanLibraries();
    InitializeMemoryHacks();
    InitializeComputerHacks();
    InitializeMobileDevicesHacks();
    loadPossibleVulnerabilities();
    showHackerWindow();
    bool targetSystem(string id, p
    if (isTargetSystemActive(id
        for (int i = 0; i < possib
            if (runProbeVulnera
                setVulnerabili
            if (activate
                for (int
```

El Ayuntamiento de Alcalá de Henar de ciberataque a sus infraestructu



Actualidad, CyberAttacks

Hyundai víctima expuesto datos d

MLuz Dominguez 12/04/2023 Sin comentarios



La Agencia Tributaria sufre un ataque informático en busca de información

- La rápida actuación de los expertos habrían frustrado las intenciones de los cib
- [Estos son los riesgos de conectarse a un wifi público y cómo evitarlos](#)



Agencia Tributaria

WHAT'S COMING TO SPAIN?

- Spain general elections (December approx)
- Regional elections (12 including Community of Madrid, May 28th)
- UE Council Chairmanships until 2024 (from Jun to Dec)
- Income tax return
- UE-CELAC
- Among others

Geopolitical analysis could be important in these scenarios

DARKWEB

DIFFERENT ENTITIES



MARKET



VENDOR



BUYER

MARKET PLATFORMS



- Platforms where you can buy or sell accounts/information leaked
- There also forums giving this information
- Sometimes you need to be referred to access to these forums and markets
- The payment is made with cryptocurrencies

PLATFORMS

genesis.market

usms.me

OPERATION COOKIE MONSTER

THIS WEBSITE HAS BEEN SEIZED

OPERATION COOKIE MONSTER

Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private coordination involving the partners listed below.

To determine if you have been victimized, visit:
havebeenpwned.com or politie.nl/checkyourhack

Been active on Genesis Market? In contact with Genesis Market administrator? Email us, we're interested: FBIMW-Genesis@fbi.gov

FBI



ESTE DOMINIO HA SIDO INTERVENIDO
y se encuentra a disposición de la Autoridad Judicial.



THIS DOMAIN NAME HAS BEEN SEIZED

as part of a Spanish National Police operation pursuant to a judicial warrant.

MARKET VENDORS

- Cybercriminals infecting machines usually with RATs and InfoStealers
- Cybercriminals deploying phishing websites
- Insiders
- Other threat actors



ALCASEC



PAPEL

Detenido Alcasec, el 'robin hood' de los 'hackers' españoles, por crear un Google de datos para mafias criminales

Source: El Mundo



Source: sky.com

MARKET BUYERS



- Cybercriminals
- Government-Sponsored APT Actors
- Hacktivists
- Script kiddies

CAMPAIGNS

FROM PHISHING TO...

Phishing websites are neither new nor fancy. This old technique still working but the difference nowadays is that there are more darkweb markets to sell the information and use it to compromise organizations.

Why is it still working?



Send emails from
compromised
account



Identify platforms
using the same
password



Sell the account
in the darkweb or
forums



Perform espionage
activities in the
account

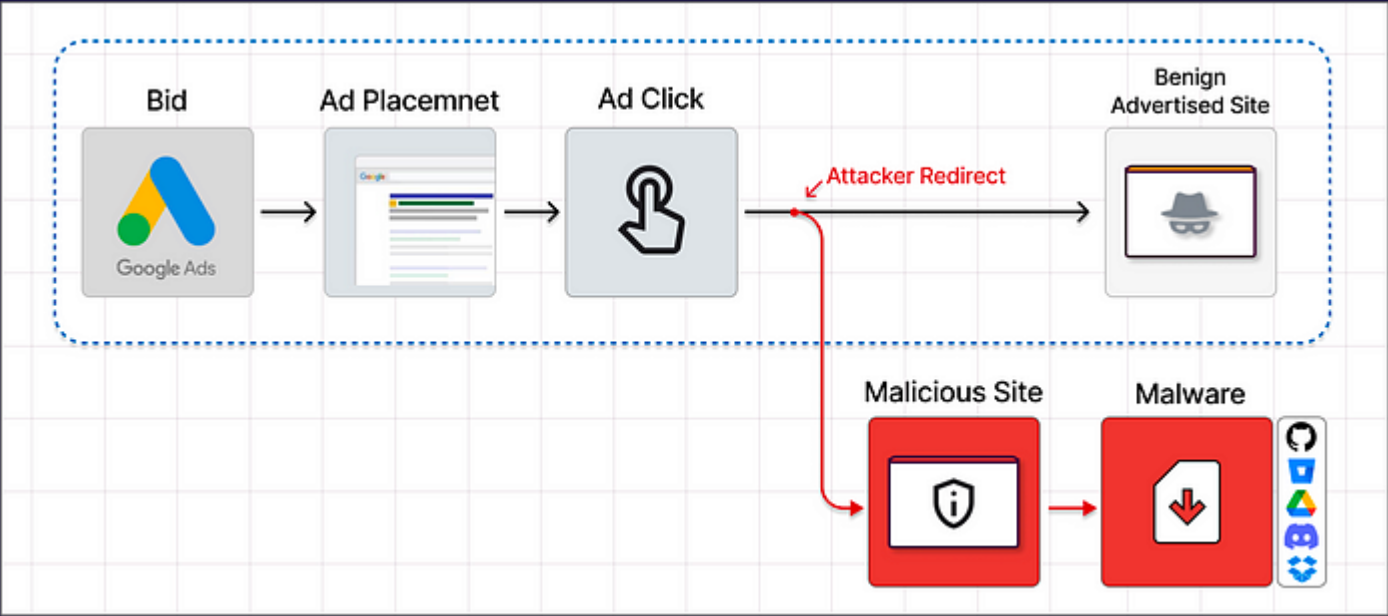
AEAT CAMPAIGN



<https://blogs.blackberry.com/en/2023/04/massive-spear-phishing-campaign-impersonating-spain-tax-agency>

RECENT GOOGLE ADS CAMPAIGN

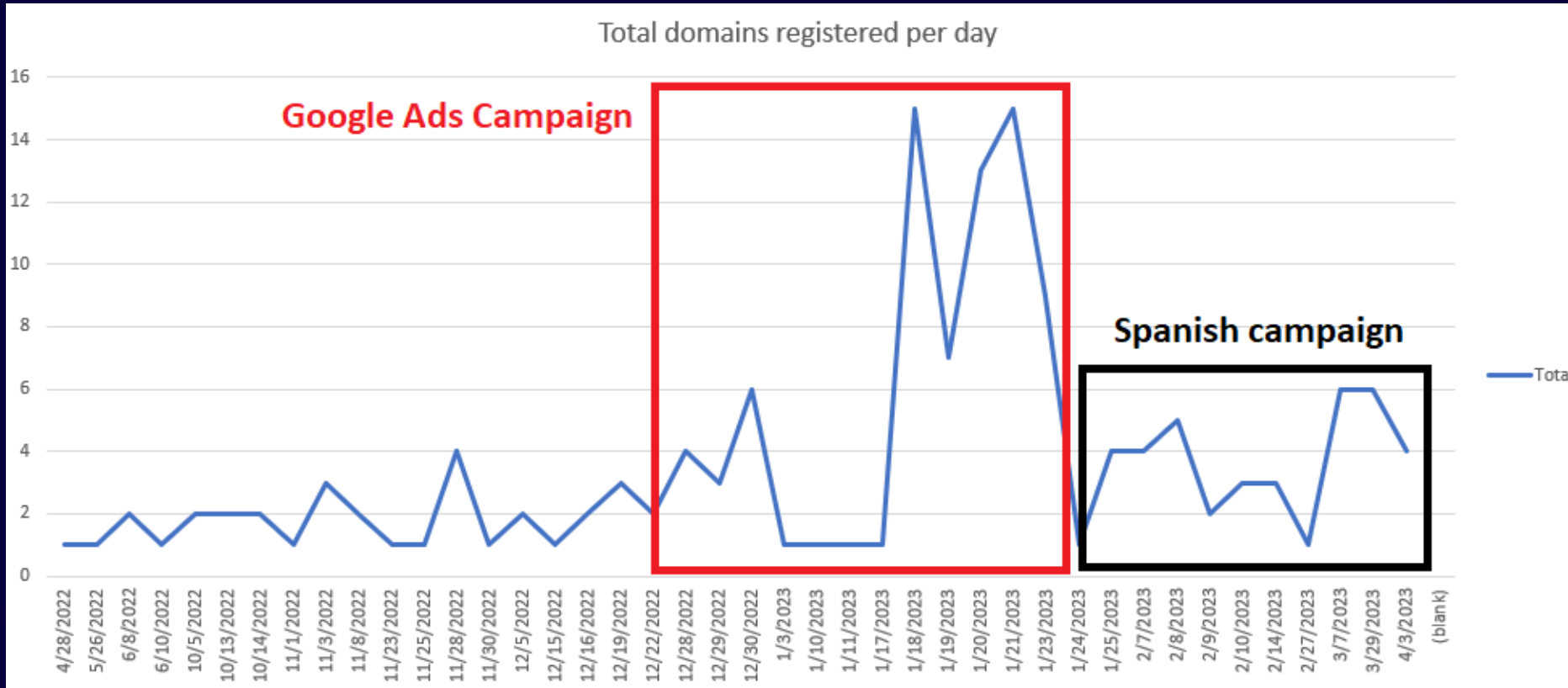
Few months ago, there was a campaign using Google Ads Platform, which helps to promote the pages indicated by the client and to offer it among the first search results users come across.



Source: Guardio Labs

RECENT GOOGLE ADS CAMPAIGN

We at BlackBerry have observed that, the **same infrastructure** used for this Google Ads campaign was used to register multiple domains using the same technique of **web proxy**



46.173.218.229

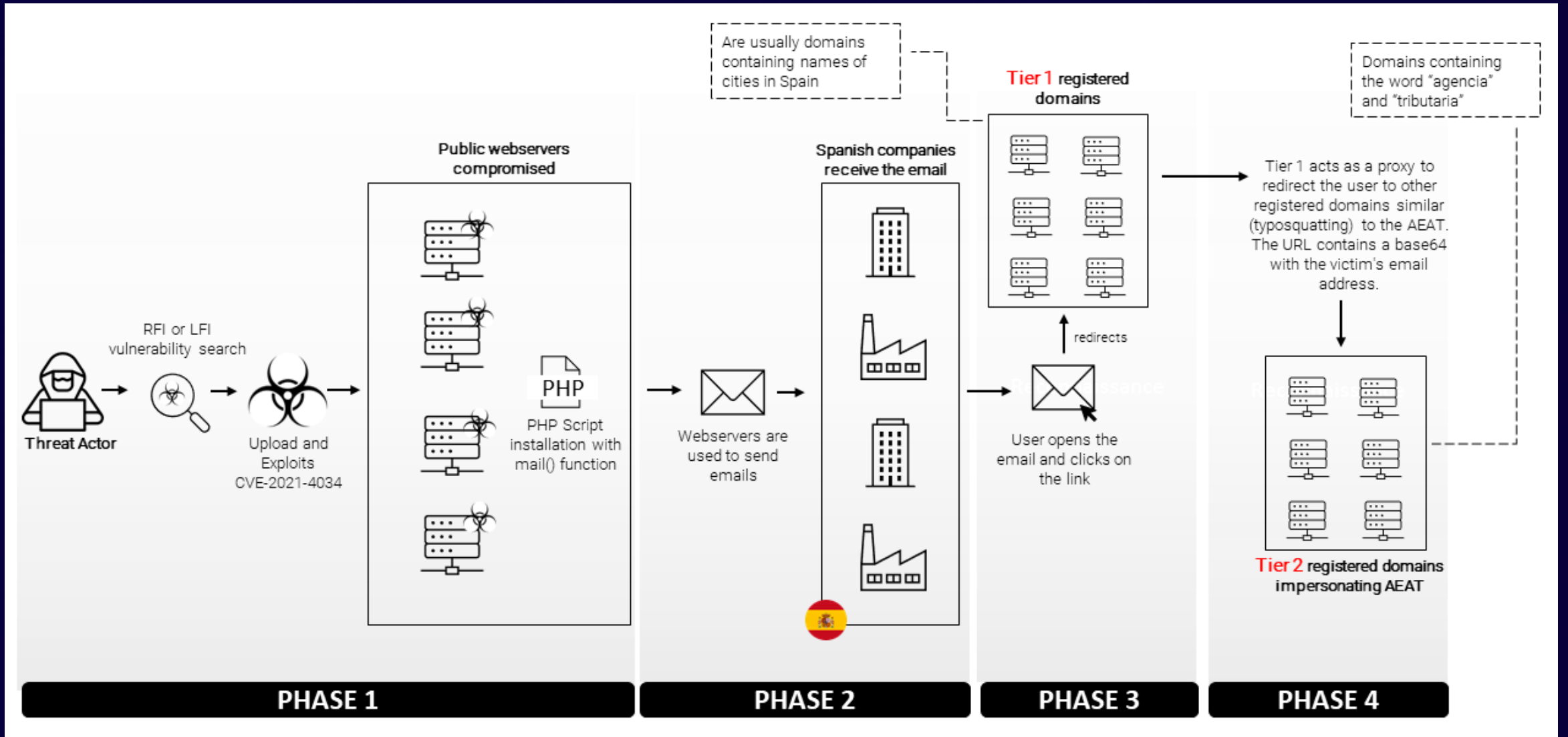
Tier 1 domains
References to Spanish cities in the domain name
Tier 2 domains
References to AEAT in the domain name

THE EMAIL

Email spoofing technique to send the emails.

The image shows a screenshot of an email interface with several annotations. On the left, the email header shows a sender 'AgenciaTributaria <noreply@correo.aeat.com.es>' with a red box and a red arrow pointing to it, labeled 'Fake sender'. Below the header, there is a list of notification details. A yellow box highlights the URL 'https://agenciatributaria.gob.es' in the text 'Puede acceder a esta notificación en la Dirección Electrónica Habilitada Única (DEHÚ) del Punto de Acceso General, disponible en: https://agenciatributaria.gob.es', with a yellow arrow pointing to it and the text 'Redirects to a registered pre'. On the right, there are two callouts. The top one shows a link 'https://sebarcelona.com/anuncio/update.php?' with a red box around it and a red arrow pointing to the text 'notificación.' in the email body, labeled 'Hyperlink'. The bottom callout shows a link 'https://medicalmadrid.com/anuncio/update.php?' with a red box around it and a red arrow pointing to the text 'https://agenciatributaria.gob.es' in the email body, also labeled 'Hyperlink'. The email content includes: 'Aviso de notificación de la Agencia Tributaria @', 'AgenciaTributaria <noreply@correo.aeat.com.es>', 'ESTE EMAIL SE CORRESPONDE CON UN AVISO DE UNA NOTIFICACIÓN POSTAL.', 'Le informamos que está disponible una nueva notificación para Titular con los siguientes datos:', 'Titular @', 'Organismo emisor: Agencia Estatal de Administración Tributaria, con DIR3: EA0028512', 'Identificador: 2299031217395', 'Concepto: Notificación administrativa', 'Vínculo: Titular', 'Puede acceder a esta notificación en la Dirección Electrónica Habilitada Única (DEHÚ) del Punto de Acceso General, disponible en: https://agenciatributaria.gob.es', 'Le facilitamos un enlace directo a la notificación.', 'Esta notificación se facilita por vía electrónica de acuerdo con lo previsto en el artículo 42.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que se emitan en papel.', 'La notificación se recibirá en todo caso en papel, aplicándose los plazos que en la misma se indiquen. Adicionalmente podrá recibir esta notificación por distintas vías electrónicas. Si accediera a su contenido la fecha en que se produzca su primer acceso.', 'Gobierno de España', 'n administrativa (Serie SE0249)', 'https://sebarcelona.com/anuncio/update.php?', 'Click or tap to follow link.', 'notificación.', 'Hyperlink', 'los artículos 41 y 43 de la Ley 39/2015, de 1 de octubre, del Procedim', 'https://medicalmadrid.com/anuncio/update.php?', 'Click or tap to follow link.', 'https://agenciatributaria.gob.es', 'Hyperlink', 'Común de las Administraciones Públicas, la aceptación de la notificación, el rechazo exp'

THE INFRASTRUCTURE



THE PHISHING

Acceso con datos de su DNI/NIE x +

agenciatributaria.live/hrhhgxfqy/main.php? [redacted] A==

GOBIERNO DE ESPAÑA MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

Agencia Tributaria Sede electrónica

ÁREA PERSONAL ES v

Dirección de correo electrónico
[redacted]

Contraseña
Escriba su contraseña de correo electrónico.

Entrar

Agencia Tributaria

Accesibilidad

Aviso de seguridad

Aviso legal

Validación del certificado de sede

Protección de datos

Política lingüística

Estructura y navegación en la sede electrónica

Contacta con nosotros

Teléfonos de interés

Buscador de oficinas

Cita previa

Buzones de sugerencias

Denuncias

Suscripción newsletter

Suscripción RSS

Ayuda

Buscar

Consultas informáticas

Diseños de registro

Horario de interrupciones de sede

Manuales, vídeos y folletos

Simuladores

Todas las ayudas

Enlaces de interés

Ministerio de Hacienda y Función Pública ↗

Fiscalidad autonómica y local ↗

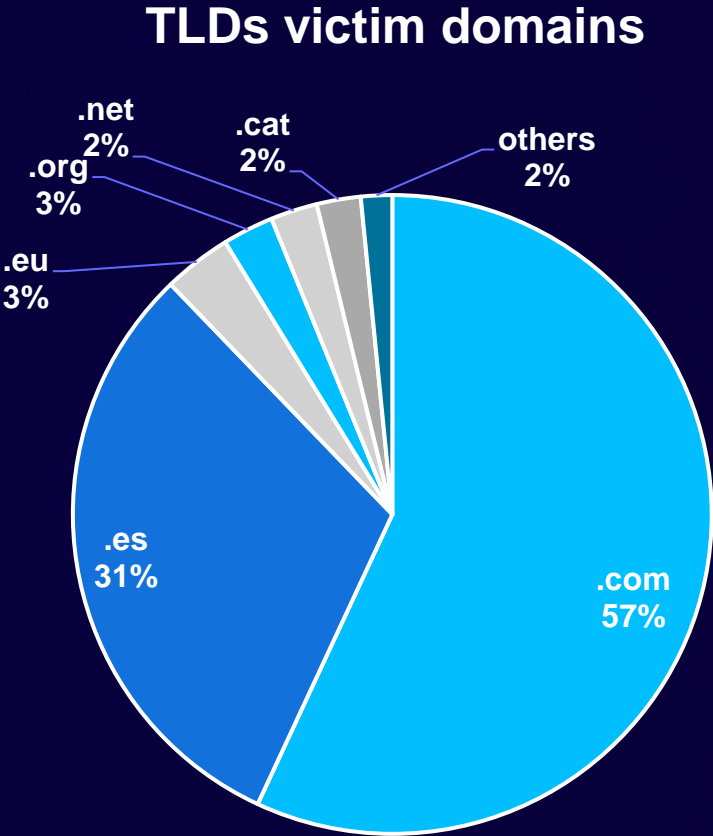
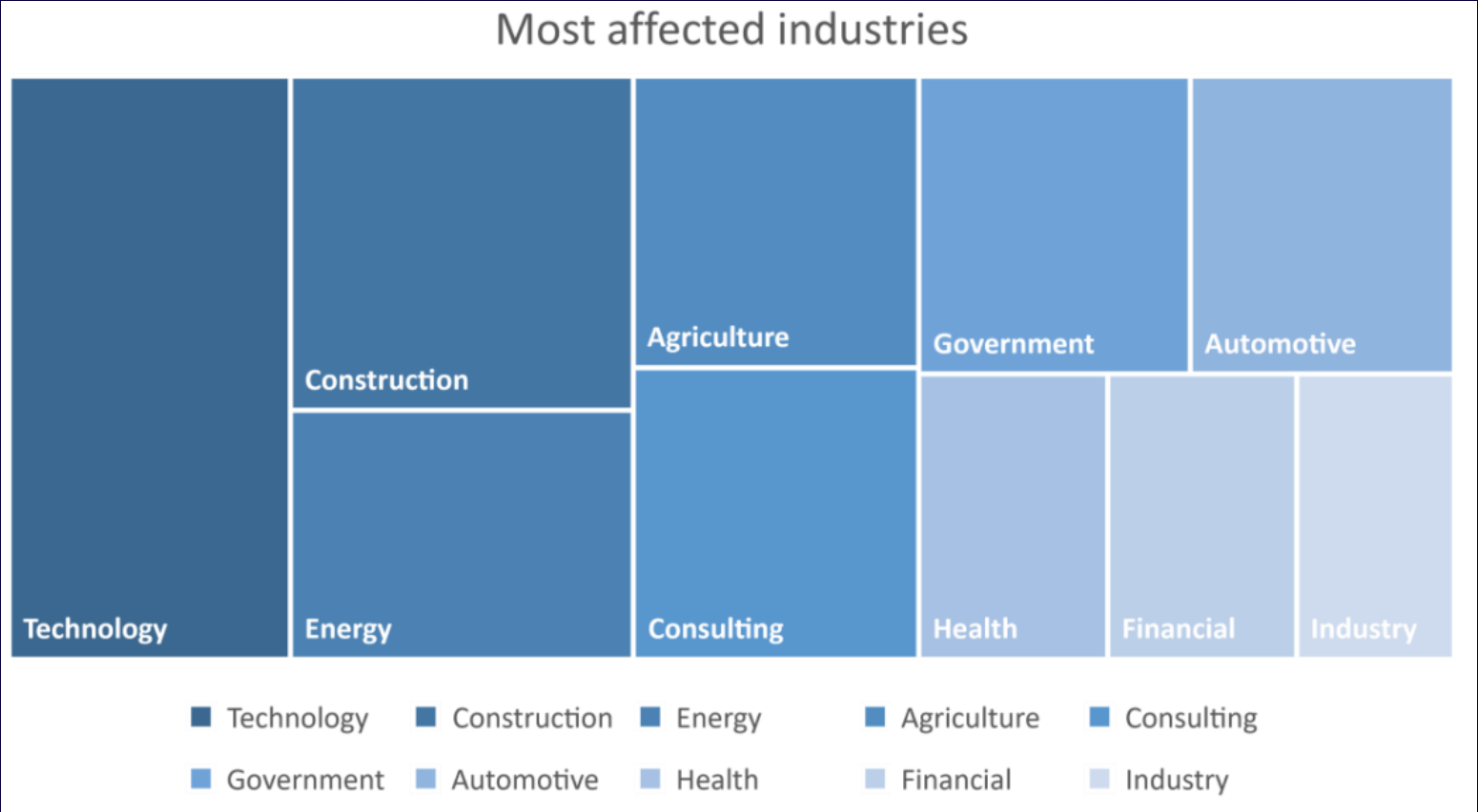
Consejo para la Defensa del Contribuyente

Punto de Acceso General ↗

Portal de la transparencia ↗

Otros enlaces de interés

MOST AFFECTED VICTIMS



FINAL GOALS

RATs



InfoStealers





Spyware



USE OF REAL EMAILS TO DISTRIBUTE RATS AND INFOSTEALERS

[REDACTED] Y PROYECTOS, SL OFERTA 2602200

 Irene Martinez <[REDACTED].com>
To [REDACTED]

 [REDACTED] Y PROYECTOS, SL OFERTA 2602200.rar
337 KB

[CORREO DE ORIGEN EXTERNO] NO haga clic en los enlaces de este mensaje a menos que conozca al remitente y sepa que el contenido es seguro.

buenas tardes,

por favor, le rogamos que nos envíe su mejor precio, disponibilidad y plazos de entrega en consulta adjunta. ([REDACTED] Y PROYECTOS, SL OFERTA 2602200)

Tenga en cuenta lo siguiente:

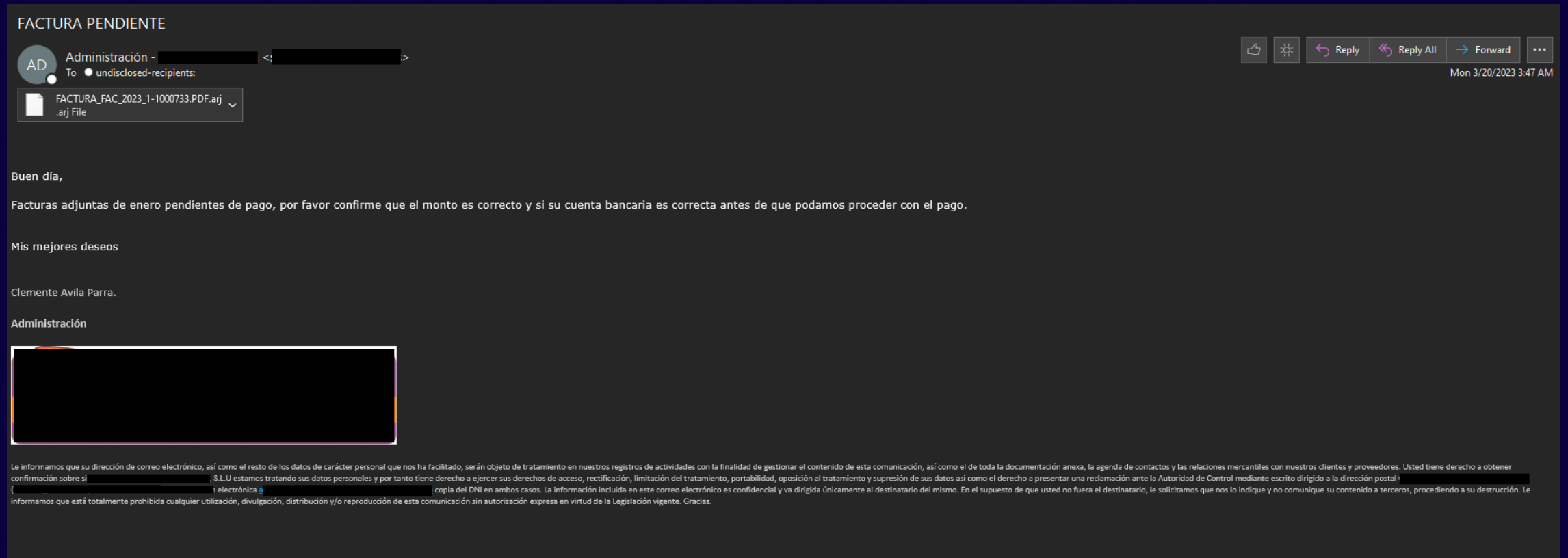
1. Mencione nuestro número de referencia en su cotización

Gracias.

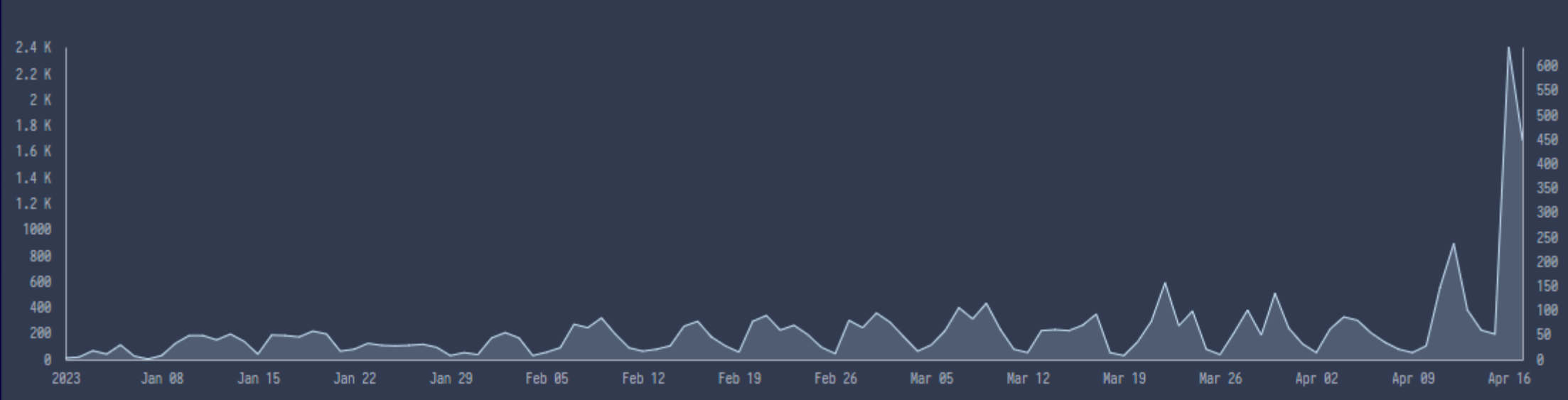
Irene Martinez
Technical Dept.
[REDACTED] PROJECTS GROUP, SL
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
Email: IreneMartinez@[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

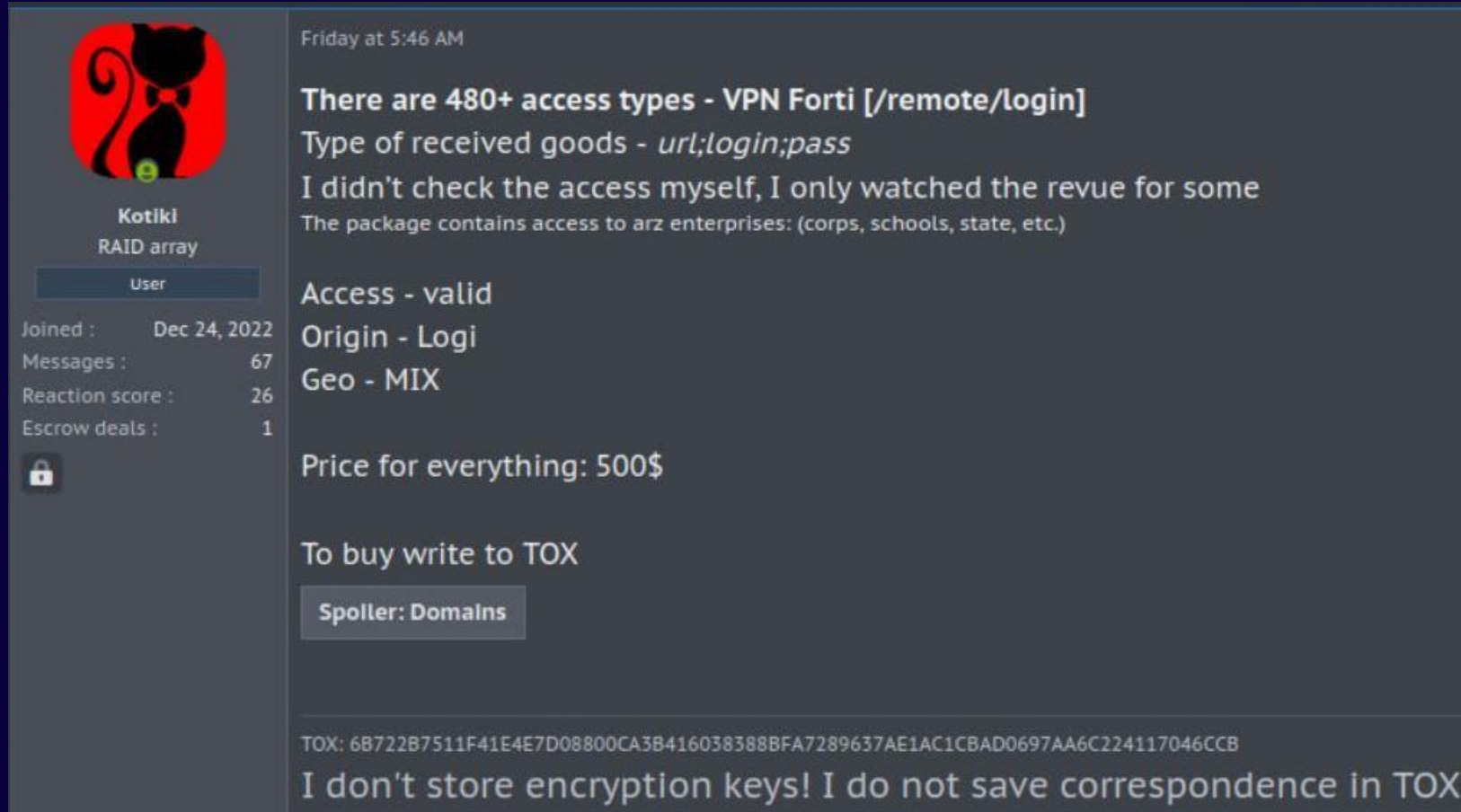
USE OF REAL EMAILS TO DISTRIBUTE RATS AND INFOSTEALERS



PUBLIC DISTRIBUTION OF AGENT TESLA AND GULoader



AND FINALLY... THE INFORMATION IS THERE



Kotiki
RAID array
User

Joined : Dec 24, 2022
Messages : 67
Reaction score : 26
Escrow deals : 1

Friday at 5:46 AM

There are 480+ access types - VPN Forti [/remote/login]
Type of received goods - *url;login;pass*
I didn't check the access myself, I only watched the revue for some
The package contains access to arz enterprises: (corps, schools, state, etc.)

Access - valid
Origin - Logi
Geo - MIX

Price for everything: 500\$

To buy write to TOX

Spoller: Domains

TOX: 6B722B7511F41E4E7D08800CA3B416038388BFA7289637AE1AC1CBAD0697AA6C224117046CCB

I don't store encryption keys! I do not save correspondence in TOX!

The BlackBerry logo, featuring a stylized grid of dots to the left of the word "BlackBerry" in a bold, italicized sans-serif font, followed by a registered trademark symbol (®).

Intelligent Security. Everywhere.



[linkedin.com/in/joseluissm/](https://www.linkedin.com/in/joseluissm/)



[@Joseliyo_Jstnk](https://twitter.com/Joseliyo_Jstnk)