

LOS VENDE HUMO DE BCA LTD Y EXPRESIDENTS

Este es un documento que evidencia como Expressidents es una operación creada en 2024 por parte de BCA LTD [Birmingham Cyber Arms LTD] para infiltrarse en foros hackers donde subían data leaks falsos para que BCA LTD notifique el “problema” y las explicaciones de que sucedió. Creando el problema y la solución hasta principios de 2025

En mayo de 2026 esta empresa “hizo una investigación” con muchas mentiras y manipulando contextos para afirmar que encontraron al “Lider de PampaLeaks” y que fue todo a raíz de un doxeo realizado por “Expressidents”. BCA LTD se invento una pelea porque pensaban que realmente tenían los datos de “El Lider de pampaleaks” y que no se iba a defender

La realidad es que tenían los datos de un ex colaborador que solo era un revendedor autorizado de PampaBot [Como lo podía ser casi cualquier persona que tuviera tokens suficientes para usar un comando de transferir tokens a otro usuario de telegram]

- **Contribuciones:** BogotaLeaks, LaPampaLeaks y otros 2 miembros de PampaLeaks
- **Redactores:** BogotaLeaks y 2 miembros mas
- **Investigador:** LaPampaLeaks

Hilo conductor de las paginas del documento:

2-15: Demostrando como Expressidents no es un hacker legitimo en foros y como operaban los de BCA LTD para crear un problema falso en foros, engañar a los usuarios con leaks falsos y publicitar en X para luego enviarlo a El observador y hacer algo falso, real en la narrativa..

16-24: Mostrando como BCA LTD fue quien dio a conocer en 2024 a Expressidents, incluso con 1 hora de diferencia. Como BCA LTD usando un proyecto alternativo de los mismos dueños de BCA LTD, le hizo una “entrevista” a expressidents y como el observador contribuyo a inflar la imagen y hacer realista una narrativa falsa hasta el día de hoy con las “exclusivas” de el

25-29: Desmontando el falso hackeo a HG [Subsidiaria de ANTEL] y Tickantel

30-31: Desmontando la pelea inventada entre LaPampaLeaks y Expressidents, ademas de demostrar como todo era para darle “reputación” a su personaje falso de BCA LTD en los mercados negros y en los medios de comunicación... Derribar PampaLeaks y que solo quede el


32-34: Mostrando como desde hace mas de 1 año hasta ahora, Mauro Francisco Caseres [Mauro “Eldrich”] siendo dueño y fundador de BCA LTD esta obsesionado con utilizar la imagen de el observador usando a Juan Pablo De Marco para lanzar desinformación sobre nosotros

En diferencia de la investigación “El Lider de PampaLeaks de BCA LTD y El observador.. Esta tiene muchas fuentes, capturas de pantalla y todo es verificable por quien sea que lo lea.

HACKEOS CON DATA LEAKS DE “BASES DE DATOS” SOSPECHOSAS

La primera aparición de ExPresidents fue en Breachforums el 13 de febrero de 2024 con un hackeo a la intendencia de flores con un leak de la base de datos.. El afirma que hay contraseñas y datos de usuarios, agregando un sample con 2 usuarios

Intendencia de Flores (Uruguay, Local Government)
by ExPresidents - Tuesday February 13, 2024 at 07:41 PM



Feb 13, 2024, 07:41 PM
Hello dears,
This is a database dump from Uruguay local government of Flores. It contains some users and plaintext passwords along with more info.
Enjoy.

Sample

Quote:

```
user_id,id_perfil,pass,email,login,nombre,apellido  
1,1,Sebastian,sebastiansuarez@adinet.com.uy,Sebastian,Sebasti,Su?rez  
2,1,planparcial,rubengarciamiranda@yahoo.com.ar,rubengarciamiranda@yahoo.com.ar,Ruben,Garc?a Miranda
```

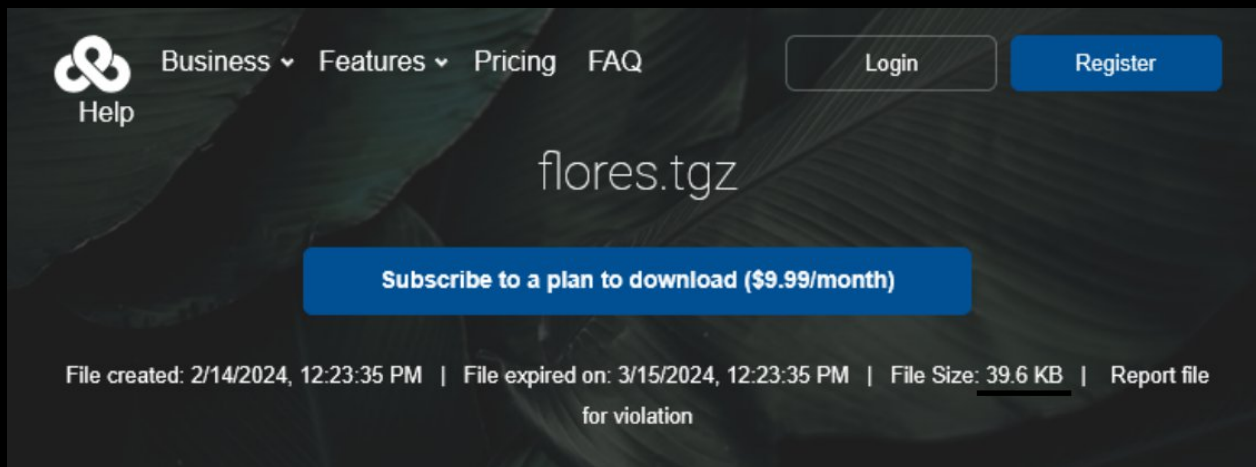
Download

Hidden Content

<https://file.io/oYLridkrmL4X>
<https://ufile.io/iwt6kcca>

ExPresidents
Breached
MEMBER
Posts: 28
Threads: 20
Joined: Feb 2024
Reputation: 21

La “DB” pesa 39.6KB [Ni un solo 1MB] y como el enlace fallecio / hay que pagar no se sabe lo que hay ahí adentro pero no hay que ser muy genio para saber que una base de datos decente no pesa menos de 1MB. Ninguno de los samples de LaPampaLeaks peso eso jamás.



Business ▾ Features ▾ Pricing FAQ Login Register

Help

flores.tgz

Subscribe to a plan to download (\$9.99/month)

File created: 2/14/2024, 12:23:35 PM | File expired on: 3/15/2024, 12:23:35 PM | File Size: 39.6 KB | Report file for violation

Fuentes:

- <https://archive.ph/9TDEK> [Post en el foro]
- <https://archive.ph/rJWIV> [DB en file.io]
- <https://ufile.io/iwt6kcca>
- <https://breachforums.rs/Thread-Intendencia-de-Flores-Uruguay-Local-Government>
- <https://pwnforums.st/Thread-Intendencia-de-Flores-Uruguay-Local-Government>

Se pone mas sospechoso aun cuando los primeros comentarios son de usuarios de bf quejándose de que el link estaba expirado y el en respuesta lo que hizo fue enviar los mismos 2 enlaces que ya había puesto antes [afirma que no podia editar el post]

★ randv
Feb 14, 2024, 01:06 AM
Hello, the link expired

VIP User
VIP
Posts: 4
Threads: 2
Joined: Dec 2023
Reputation: 25

PM Find

ExPresidents
Feb 14, 2024, 12:25 PM
randv Wrote:
Hello, the link expired

Sorry, you are right. New links below (i can't edit the post)

Hidden Content
<https://file.io/oYLridkrmL4X>
<https://ufile.io/iwt6kcca>

Breached
MEMBER
Posts: 28
Threads: 20
Joined: Feb 2024
Reputation: 21

Find

Richard2250
Feb 14, 2024, 09:00 PM
Hi, links expired

ExPresidents
Feb 15, 2024, 03:28 PM
Richard2250 Wrote:
Hi, links expired

Hey man ufile is working check the post above yours

Breached
MEMBER
Posts: 28
Threads: 20
Joined: Feb 2024
Reputation: 21

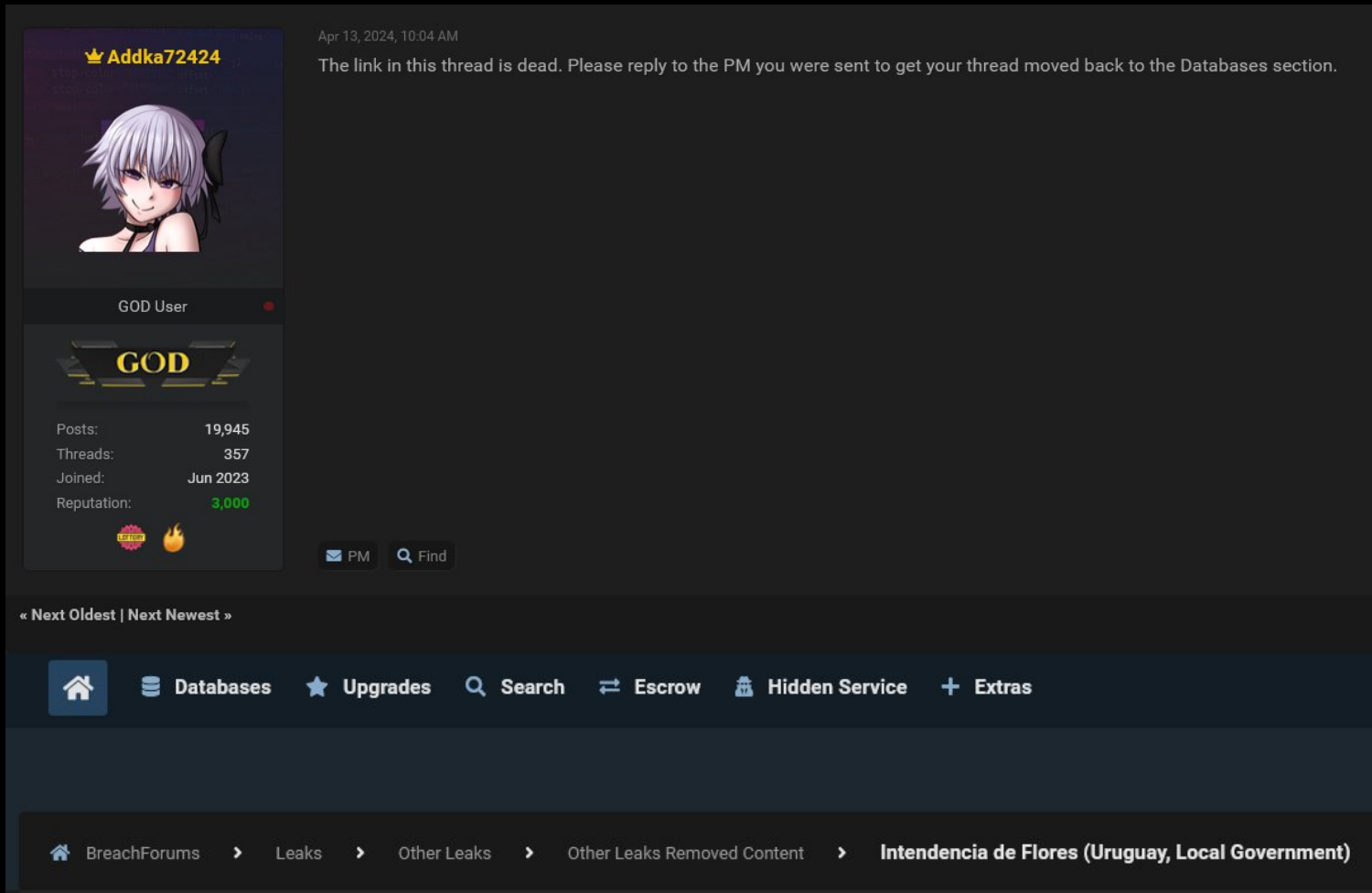
Find

Luego el usuario Richard2250 le comenta que el enlace esta expirado y le contesta que funciona y que el enlace estaba arriba de el

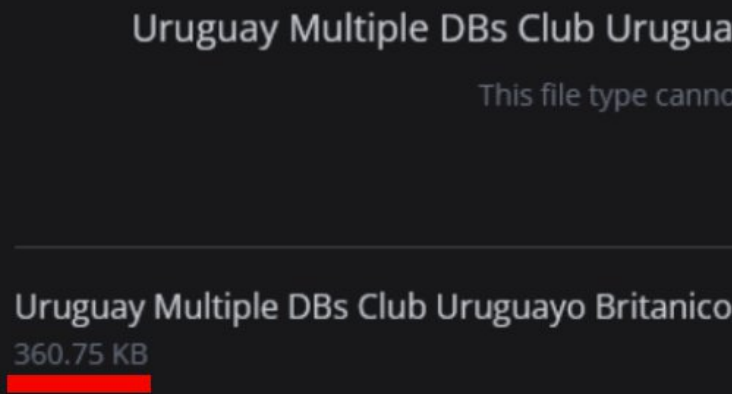
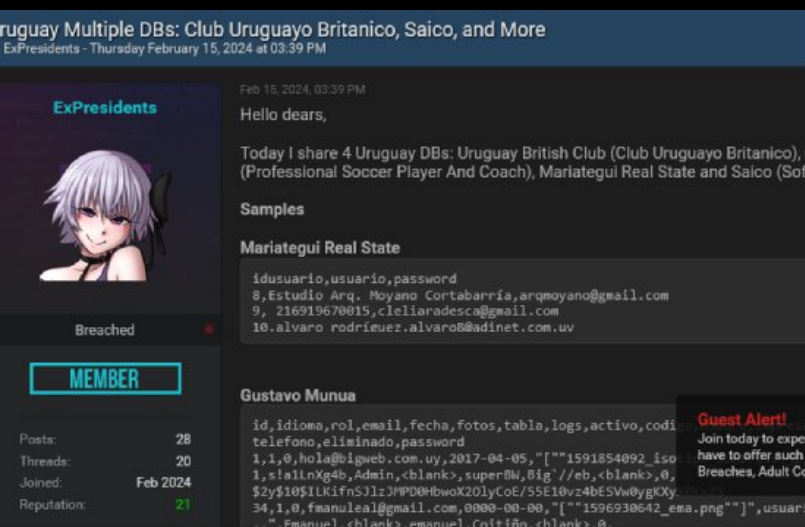
Recordemos que son los mismos enlaces que el publico en el post inicial, asi que si estaban caidos antes.. Estan caidos tambien los que el comento porque son los mismos...

Por lo que ademas de no parecer estar interesado en que los users descargen su base de datos.. La misma base de datos pesa muy poco para ser una DB gubernamental

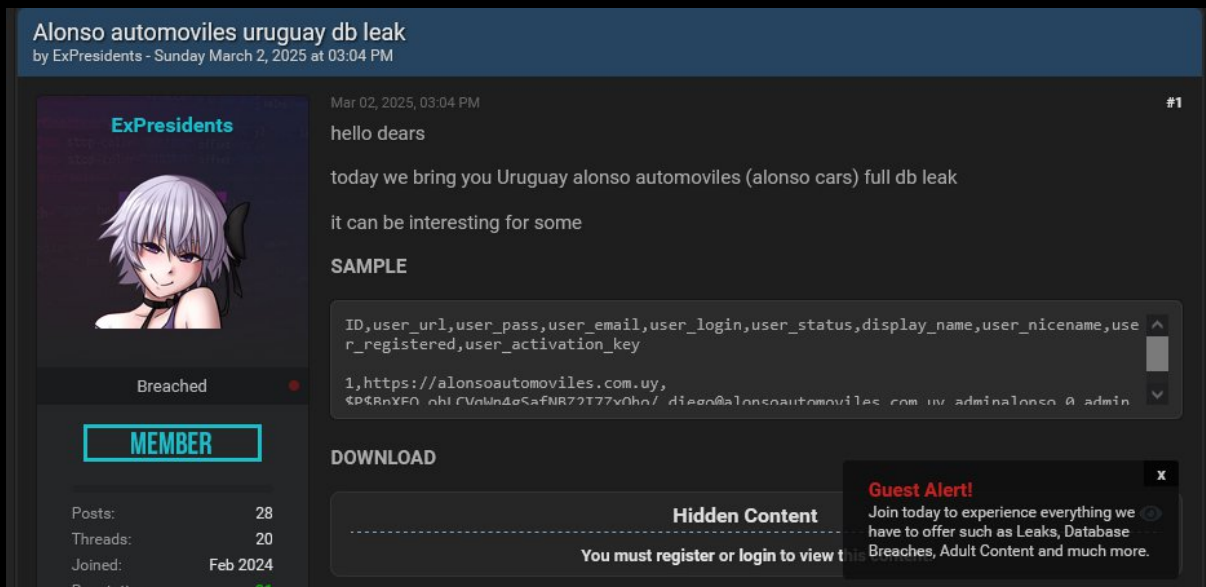
Luego algunos decian que funcionaban, otros no.. Y al final el thread del post de Expresidents fue bloqueado por un admin para comentar y llevado a Other Leaks Removed Content por tener los enlaces caidos. El admin le dijo que lo contacte para mover de nuevo el thread [es para actualizar el enlace caido]. Mayo de 2026 y el post sigue en el mismo estado...



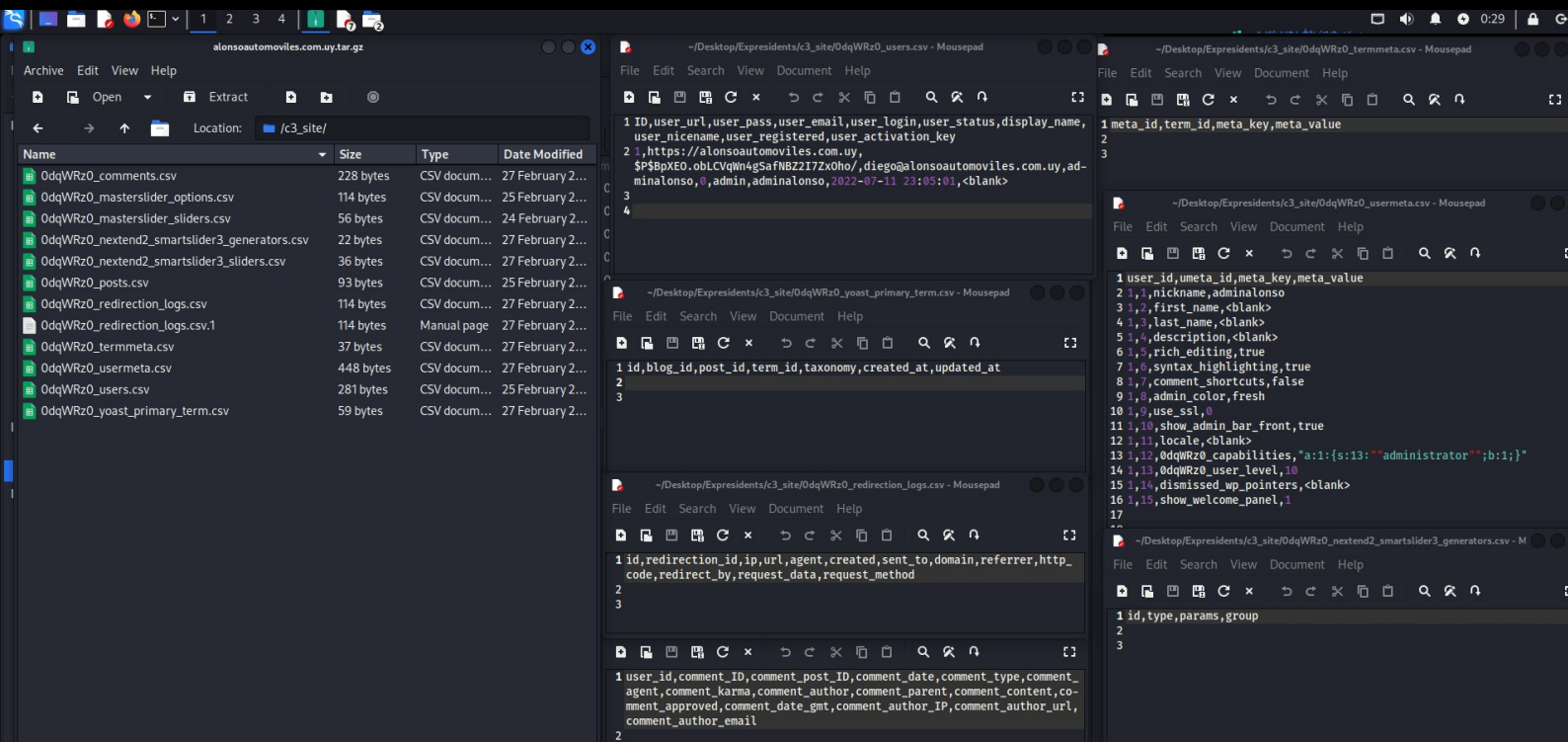
La siguiente publicación el supuestamente filtra muchas bases de datos juntas de uruguay.. Estas bases de datos todas juntas en un archivo 7z pesan tan solo 360KB. Si alguien entra a un sistema privado con muchas bases de datos [en este caso de futbol uruguayo] pesaria todo mucho mas que tan solo 360KB... Tampoco ninguna de las "victimas" confirma nada...



En el post donde la unica respuesta es de LaPampaLeaks.. El postea un hackeo a un sitio web de automoviles en uruguay junto a un enlace de descarga y un enlace en el que habia que pagar monedas del foro para descargar. El unico que hizo eso fue LaPampaLeaks



Lo que encontro fue solo unos archivos .csv que no tenian nada mas que info del frontend y en la db del sample que solo tenia un usuario [el mismo que se muestra en el sample]. Abajo una captura enviada por LaPampaLeaks de todos los archivos de ese "hackeo" y "leak"



- <https://archive.ph/UUFPq> [Post en clon de BF]
- El zip esta en la misma carpeta que los pdfs de todo esto
- <https://archive.ph/i6Eoy> [Post del hackeo a Club de futbol uruguayo]
- <https://archive.ph/tqyaX> [archivo de descarga del hackeo a Club de futbol uruguayo]

Como opera expresidents es subir bases de datos de muy dudosa legitimidad, incluso poniendo mas dificil la descarga haciendo que los usuarios pagen monedas del grupo [para tener esas monedas hay que pagar al foro o hacer posts] o haciendo enlaces temporales

Luego veremos los intereses que pueden tener para actuar así después.. Ahora veremos como Expresidents falso hackear a la DGI y como supuestamente “vendía acceso” a cuentas de la DGI y la Republica Afap... Y como supuestamente agregaron informacion de “penades”..

Uruguay dgi and republica afap accounts for sale
by ExPresidents - Wednesday December 4, 2024 at 02:17 PM

Dec 04, 2024, 02:17 PM (This post was last modified: Dec 04, 2024, 03:02 PM by ExPresidents.) #1

hello dears

today we have accounts of dgi (direccion general impositiva the country tax office) and rafap (republica afap private retirements office)

we sell access to person and company logins on the two web sites

buyer can have acces to data how email, telephone, savings, and can start tramits in name of the account as open a company

this can help you validate identities for things like proof of funds or identity

we have hundres of logins ask us in dm if you need someone or a company in specifcly

we have a special one too but its sold as separate

Guest Alert!
Join today to experience everything we have to offer such as Leaks, Database Breaches, Adult Content and much more.

MEMBER

Posts: 28
Threads: 20
Joined: Feb 2024
Reputation: 21

Ministerio de Economía y Finanzas | **DGI** DIRECCIÓN GENERAL IMPOSITIVA | **Servicios en línea**

Información al Contribuyente

GUSTAVO CARLOS PENADES ETCHEBARNE

Atención
El acceso a este RUC debe realizarse a través de la Identidad Digital (con cédula y contraseña) de las personas vinculadas que se detallan a continuación.
Mas información: [aquí](#)

Tipo Doc.	Nro.Doc.	Nombre	Rol
CI	18953675	PENADES ETCHEBARNE GUSTAVO CARLOS	Administrador por RUT

1.5.3

SAMPLE

REPUBLICA AFAP Institucional Sistema Previsional Servicios HOLA DIEGO

Nosotros como personas que estamos en el mercado detectamos muy bien las cosas que están mal acá..

Lo primero es que esta en la sección de “other leaks” envés de ventas.. Lo segundo no dicto ningún precio para el vender el acceso a cuentas.. Lo tercero, el no pone método de contacto ni que que le escriban al MD del foro para comprar el acceso a las cuentas

También claramente, se metio via stelear a una cuenta [mas abajo mas info]

REPUBLICA AFAP Institucional Sistema Previsional Servicios

DATOS DE CONTACTO

Teléfono principal (*)
26130469

Teléfono alternativo (*)
091035822

Correo electrónico (*)
seba_cardoso1@hotmail.com

Confirmación correo electrónico (*)
seba_cardoso1@hotmail.com

Lo que hizo "Expresidents" es logearse a una cuenta de un usuario infectado con stelear que se pueden encontrar fácil con Intelx y otras tools.. AGESIC y DGI al analizar el "hackeo" fue decir que lo mas probable es que le robaron las cuentas directamente a los usuarios

www.elobservador.com.uy/ciencia-y-tecnologia/hackers-accedieron-cuentas-usuarios-la-dgi-y-republica-afap-y-aseguran-poder-hacer-tramites-su-noi

EL OBSERVADOR / CIENCIA Y TECNOLOGÍA / DGI

Para demostrar la veracidad de su oferta, los atacantes publicaron como muestra una **supuesta cuenta de la DGI perteneciente a Gustavo Penadés**, el exlegislador acusado de explotación sexual infantil.

La respuesta de DGI y Agesic

Desde la DGI aseguraron a El Observador que están investigando el inconveniente junto al Centro Nacional de Respuesta a Incidentes de Seguridad Informática (Certuy).

En el primer análisis realizado por los expertos, aseguran que "es altamente probable" que esas cuentas hayan sido robadas a los propios usuarios.

Desde CERTuy descartaron que se haya adulterado el sitio web de la plataforma. "Ninguna de las dos infraestructuras han sido afectadas", dijeron.

Lo que el hizo ademas de meterse en cuentas individuales, fue editar los documentos y el html con el inspeccionar, después escribió "los datos" de personas conocidas en uruguay

En breachforums no hubo ningún comentario de un usuario porque "expresidents" publico todo en "Other leaks" y no en la sección de ventas del foro... Lo que hizo un moderador fue matar el thread para que nadie pueda comentar y relevo el post a la sección de posts eliminados

BreachForums > Leaks > Other Leaks > Other Leaks Removed Content >

Uruguay dgi and republica afap accounts for sale

Dec 04, 2024, 04:00 PM #2

The link in this thread is dead. Please reply to the PM you were sent to get your thread moved back to the Databases section.

Thanks @zehq for ranks!!!

Tanaka
GOD User

GOD

Posts: 4,574
Threads: 456
Joined: Jun 2023
Reputation: 4,043

🍏 🍊

No es difícil darse cuenta que a “expresidents” no le importa si a los usuarios del foro le compran o si la DGI parchea el SUPUESTO acceso que el tenía. A cualquier vendedor en foros les gusta dejar claro precios mínimos o métodos de contacto, también un hacker decente lo que haría es hacer scripts para robarse la info de cada cuenta y crear una base de datos en base a mandar miles o millones de solicitudes a el servidor de la DGI

Pero el prefirió anunciar que tenía acceso interno a un organismo gubernamental en el que era el foro hacker mas conocido de todo internet, donde esta infiltrada la interpol, periodistas, etc etc.. Algo que solo haría que parchen la vulnerabilidad o neutralizan el acceso del login

Fuentes de todo lo anterior:

- <https://www.elobservador.com.uy/ciencia-y-tecnologia/hackers-accedieron-cuentas-usuarios-la-dgi-y-republica-afap-y-aseguran-poder-hacer-tramites-su-nombre-n5973497>
- <https://archive.ph/Bg8b9>

Otro “hacking del acceso” fue una supuesta entrada a la VPN del correo uruguayo donde el subió un manual de instalación de la VPN y archivos de OpenVPN, cambiandole el nombre de archivos de “OpenVPN” a “VPN-orreo” a los .exe oficiales de OpenVPN.

Uruguay Official Postage Service VPN Access (correo.com.uy)
by ExPresidents - Tuesday March 12, 2024 at 10:56 PM

Mar 12, 2024, 10:56 PM (This post was last modified: Mar 12, 2024, 10:58 PM by ExPresidents.) #1

Hello dears,

Today we bring you VPN access for the Official Uruguayan Postage with users manual in PDF.

Manual Sample

[Image: 9dILRgp]

If IMG tags not working, these are the images links:

<https://imgur.com/9dILRgp>
<https://imgur.com/wHdEQtT>
<https://imgur.com/kPzPgG8>
<https://imgur.com/VF3k11v>

Guest Alert!
Join today to experience everything we have to offer such as Leaks, Database Breaches, Adult Content and much more.

Filelist - Proof

```
vpn:  
Manual_de_instalacion_y_configuracion_remota.pdf  
VPN-Correo-Win10.exe  
VPN-Correo-Win7-Win8-Win8.1.exe  
VPN-Correo_Linux.ovpn  
VPN-Correo_XP_32-bits.exe  
VPN-Correo_XP_64-bits.exe  
  
equipos-anc:  
VPN-Correo-Linux.ovpn  
VPN-Correo-XP-32-bits.exe  
VPN-Correo-Win10.exe  
VPN-Correo-XP-64-bits.exe
```

Download

Hidden Content

You must register or login to view this content.

Los .exe son fácilmente encontrarles en la [pagina oficial de OpenVPN](#) y esto se lo dijeron en los comentarios ademas de que un admin le volvió a eliminar el post de la seccion de Others leaks y lo envió a leaks eliminados... Otra vez repitiéndose el mismo metodo

Los comentarios de usuarios son quejándose por esto mismo y hablando sarcásticamente de que eso lo podían haber descargado desde la pagina de OpenVPN... El otro usuario afirma también que las keys de acceso a la VPN no funcionan... Para luego el tercer comentario es de un ex moderador moviéndolo a la zona de posts eliminados por ser inválidos...

miau28
Apr 09, 2024, 04:02 PM #2
it is just the open vpn client , i can just download from open vpn lol, what a leak!

Breached

MEMBER

Posts: 15
Threads: 0
Joined: Apr 2024
Reputation: 0

Smark
Apr 11, 2024, 05:32 PM (This post was last modified: Apr 11, 2024, 05:33 PM by Smark.) #3
Looks like correo.com.uy changed VPN keys and this config files no longer work. The rest are just OpenVPN client installation files.

Home Databases Upgrades Search Escrow

BreachForums > Leaks > Other Leaks > Other Leaks Removed Content > **Uruguay Official Postage Service VPN Access (correo.com.uy)**

Ningún hacker decente querría filtrar un acceso VPN... Si lo hace es porque no sabe que hacer con el o para llamar la atención.. Un hacker decente subiría de privilegio en el sistema con esa VPN y buscaría vulnerabilidades en los sistemas internos más protegidos... Pero el no...

Fuentes de información:

- <https://archive.ph/qhR3a> [Post de la VPN]

Para los mas curiosos... Es tan facil encontrar manual de VPNs para conectarse a la mayoría de organismos públicos y públicos privados como buscarlos en Google...

Google search results for "vpn manual gobierno uruguay".

GUB.UY
https://www.gub.uy > documentos > publicaciones PDF
Anexo I – Instalación de servicios VPN Introducción
Lo aquí descrito no intenta ser una guía exhaustiva de instalación, ni un manual de ... conexión VPN, accedé a. Remote Access y agregá una nueva conexión "Add a ...
34 pages

BPS
https://www.bps.gub.uy > bps > file > manual-para... PDF
manual para conectarse de forma remota– windows 7
PASO 1 (IMPORTANTE): Anotarse el nombre del PC de BPS y dejarlo prendido ya que sino no será posible realizar la conexión. Para saber el nombre de su equipo ...
6 pages

Acá una captura de pantalla del manual de VPN de Fortinet para conectarse a los servidores de la **DNIC**... Incluso con la IP y Puerto exacto para entrar.. Con un usuario de ejemplo.. Porque los inútiles de AGESIC no ocultan bien sus archivos internos y los dejan regalados

Pero nosotros no hacemos publicaciones al respecto... Porque si nos importa preservar datos de acceso que nos pueden ayudar a subir de privilegio en sistemas... Pero a expresidentes no?

manual conexión VPN con FortiClient.pdf 6 / 17 100%

Configuración de la conexión.

En la configuración, completaremos con los datos de conexión para DNIC, algunos fijos y otros dependiendo de nuestros usuarios:

Edit VPN Connection

VPN: SSL-VPN | IPsec VPN | XML

Connection Name: **DNIC**

Description:

Remote Gateway: **https://190.64.73.66:31443**

+Add Remote Gateway

Customize port: 443

Single Sign On Settings: Enable Single Sign On (SSO) for VPN Tunnel

Authentication: Prompt on login **Save login**

Username: **angelo.modena**

Client Certificate: None

Enable Dual-stack IPv4/IPv6 address

Buttons: Cancel Save

Dirección: **https://190.64.73.66:31443**

Sumando a las practicas sospechosas.. El hizo un post donde pone un enlace desbloqueable con 3 monedas de breachforums de un antiguo formulario publico del MTSS que rellenaba datos automáticamente por una api DNIC, aveces compartiendo direcciones o correos electrónicos gracias a una api antigua del MTSS que consultaba los datos a su base de datos

Uruguay government site to easy dox person via its document number
by ExPresidents - Thursday September 12, 2024 at 04:02 PM

Sep 12, 2024, 04:02 PM (This post was last modified: Sep 12, 2024, 04:04 PM by ExPresidents.) #1

hello dears,

today we bring you a vulnerable government site who allows you to find full name, date of birthing and sometimes email and address with just the ci number

it takes the info directly from another official source the direccion nacional de identificacion civil .

works for exposed political people (the very rich) and kids too! see example in thread and can also be automated becoss in uruguay ci are less than 7 million numbers to today so super easy to mass dox

[Image: oT4KA6j]

[Image: H2C29Hg]

images links in case not working

<https://imgur.com/oT4KA6j>

<https://imgur.com/H2C29Hg>

Hidden Content

<https://regobras.mtss.gub.uy/registroObras2ProtWEB/JSF/formularios/registroApoderado.xhtml>

ExPresidents
Breached
MEMBER
Posts: 28
Threads: 20
Joined: Feb 2024
Reputation: 21

Un hacker normal screpearia ese formulario a mas no poder para recrear la base de datos en base a millones de solicitudes... Pero el no, el lo publica mientras menciona que se puede encontrar a gente de la política, muy millonarios y “también niños” que es la mezcla de 3 conceptos perfectos para que venga alguien de AGESIC y elimine ese formulario publico

Que fue lo que paso, a las horas sospechosamente el enlace estaba caido.. Ni siquiera un comentario de un usuario agradeciéndole ya que recordemos que estaba bloqueado a menos que tengas monedas del foro... El único comentario es uno de un admin.. a las pocas horas del post.. Notificándole que el enlace estaba muerto y moviendo su post a la sección borrada

Sep 12, 2024, 11:57 PM #2

The link in this thread is dead. Please reply to the PM you were sent to get your thread moved back to the Databases section.

This forum account is currently banned. Ban Length: Permanent (N/A Remaining)
Ban Reason: Legend

IntelBroker
BreachForums Operative
Posts: 2,402
Threads: 248
Joined: Jun 2023
Reputation: 5,065

🍏 🍌 🍊 🗡️

🔍 Find

🚩 Report

Sumando a las actitudes sospechosas de "Expresidents"... Es que tiene los mensajes directos via el foro **totalmente desactivados** [no es una configuración por defecto], lo puso asi a proposito y la única razón de esto es no tener contacto con otros miembros del foro.. Comparando la cuenta en el foro de ExPresidents y BogotaLeaks, es facil ver que falta esto.

The screenshot shows the profile page for user 'ExPresidents' on PwnForums. The browser address bar shows the URL: <http://pwnfrm7rbf6kyerigxi677lcz5ifmoagdbqqknwdu2by27wfdst5qmqd.onion/User-ExPresidents>. The navigation bar includes links for Databases, Upgrades, Search, Hidden Service, Escrow, Wall of Shame, and Extras. The profile header shows the user's name 'ExPresidents' and status 'Offline (Last Visit: 04-07-2025, 11:14 PM)'. Below this are two main sections: 'ExPresidents's Forum Info' and 'ExPresidents's Forum Statistics'. The forum info section includes a 'MEMBER' badge, a 'Joined' date of 02-13-2024, and 'Time Spent Online' of 7 Hours, 30 Minutes, 48 Seconds. The forum statistics section shows 'Total Threads: 20 (0.02 threads per day | 0.03 percent of total threads)' with a 'Find All Threads' link, 'Total Posts: 28 (0.03 posts per day | 0 percent of total posts)' with a 'Find All Posts' link, and 'Reputation: 21' with a 'Details' link.

The screenshot shows the profile page for user 'BogotaLeaks' on PwnForums. The browser address bar shows the URL: <http://pwnfrm7rbf6kyerigxi677lcz5ifmoagdbqqknwdu2by27wfdst5qmqd.onion/User-BogotaLeaks>. The navigation bar is identical to the previous screenshot. The profile header shows the user's name 'BogotaLeaks' and status 'Offline (Last Visit: 08-10-2025, 04:46 AM)'. Below this are three main sections: 'BogotaLeaks's Forum Info', 'BogotaLeaks's Contact Details', and 'BogotaLeaks's Forum Statistics'. The forum info section includes a 'MEMBER' badge, a 'Joined' date of 12-19-2024, and 'Time Spent Online' of 4 Hours, 51 Minutes, 12 Seconds. The contact details section shows a 'Private Message' button and the text 'Send BogotaLeaks a private message.' The forum statistics section shows 'Total Threads: 2 (0 threads per day | 0 percent of total threads)' with a 'Find All Threads' link and 'Total Posts: 9 (0.02 posts per day | 0 percent of total posts)' with a 'Find All Posts' link.

- <http://pwnfrm7rbf6kyerigxi677lcz5ifmoagdbqqknwdu2by27wfdst5qmqd.onion/User-BogotaLeaks>
- <http://pwnfrm7rbf6kyerigxi677lcz5ifmoagdbqqknwdu2by27wfdst5qmqd.onion/User-ExPresidents>
- <http://pwnfrm7rbf6kyerigxi677lcz5ifmoagdbqqknwdu2by27wfdst5qmqd.onion/Thread-Uruguay-government-site-to-easy-dox-person-via-its-document-number>

Otro “hackeo” de expresidents [XSS] que básicamente es facil hacerlo en casi todas las paginas del estado porque a nadie en agestic le importa este tipo de vulnerabilidades.. El hackeo al “Partido nacional” fue el poniendo codigo html en la url y formularios de la pagina...

Uruguay Partido Nacional New HTML Injection
by ExPresidents - Thursday November 21, 2024 at 05:45 AM

Nov 21, 2024, 05:45 AM #1

Hello dears,
today we bring you new injection on partido nacional de uruguay web page
elections this sunday and do not wanted to go without saying hi to our friends at partido nacional
good to use with svg or something more
also php scripts look like are run but we cant confirm

Sample:

Breached

MEMBER

Posts: 28
Threads: 20
Joined: Feb 2024
Reputation: 21

LA MESA CHICA
Penadés creó grupo de investigación de seis hackers y cuatro policías para armar "trama"
El exsenador mantuvo una reunión en su casa con los involucrados. Uno de ellos podría ser el nexo con el exdirector del Comcar, Taroco.

Guest Alert!
Join today to experience everything we have to offer such as Leaks, Database Breaches, Adult Content and much more.

ELECCION?

Esto no le afecta a nadie que no tenga el enlace con xss... Ningún usuario del partido nacional fue afectado de ninguna manera visualmente en la pagina.. Nadie se entero hasta que esta persona puso el xss valido en la pagina.. <https://archive.ph/OAtJm> [link del post]

Entrevista a Expresidents:

Ademas de “hackeos” basicos, leaks inventadas y otras practicas... Cuando le hicieron una entrevista sobre el “hackeo” al Partido nacional se vivieron contradiciendo. Primero eran **hacktivistas en contra de penades** y la red de pedofilia, después mencionan que el PN nunca desmintió haber trabajado con ellos [recuerda que en el **post de BF hacian referencia a la noticia de hackers trabajando para penades**, para encontrar info de victimas de pedofilia]

¿Son uruguayos? ¿Por qué atacan solo Uruguay?

Si pero todos vivimos afuera hace muchos años. Hackeamos en Uruguay para concientizar la tragedia que estamos viviendo estos últimos años porque afuera del país nadie conoce a Penadés o preguntás por Washington Balliva y te dicen "Poder y Sociedad", no te dicen "el hijo de puta del juez que tenía que cuidar a los botijas y se los cojía en un telo". Nicolás Ortiz dio clases en el liceo a los chiquilines hasta que lo formalizaron, de eso no se habla y por eso sigue pasando.

También llamaron “ajero en sus servidores” hacer un XSS que solo afecta al frontend...

Una víctima recurrente fue el Partido Nacional ¿Por qué?

Porque son una manga de mentirosos y corruptos, prometieron muchas cosas y no cumplieron. Son tan sucios que dijeron tres veces que habían arreglado el agujero de sus servidores (¡y era mentira!) pero en ninguna de esas oportunidades desmienten haber trabajado con nosotros o que tengamos información confidencial.

luego de contradecirse en sus acciones y afirmaciones... + mandarle fruta con lo del XSS, diciéndole “aujero en el servidor” cuando solo afecta al frontend.. [mintiendo] cambian de nuevo de narrativa diciendo que están en contra del PN porque no les interesa el pueblo.... Utilizando el término “blancos pillos” que es lo que recurrentemente usa la izquierda uruguaya

Nadie decente con ideas de izquierda, trabajaría para el partido nacional y menos en buscar datos de víctimas de un pedofilo.. A menos que esta persona este “roleando” ;)

Dentro del PN lanzaron amenazas a funcionarios específicos ¿por qué ellos?

Son personas peligrosas porque a pesar de su poder no les interesa el pueblo, solo los buscan para su beneficio y una vez que lo consiguen no se acuerdan más de ellos. Se callaron con lo de Penadés hasta que fue insostenible, pero para denunciarnos a nosotros por el hackeo a una paginita fueron rapidísimos los blancos pillos.

Podríamos seguir mucho más con esto pero el punto ya está, tiene actitudes muy extrañas que no van con un hacker real... Incluso en los últimos hackeos como el SQL injection al GOB de rocha, las respuestas son quejándose de que el enlace no funciona “desde el primer momento” que ExPresidents publicó el post... Queja recurrente al parecer

05-04-2024, 10:33 AM

ExPresidents Wrote:

hello dears

today we bring you a sql injection on one uruguay rocha government website

it uses postgres backend and has 333 tables with city information about everything: schools, cables, water p lanes, streets, beaches, taxis and bus stops, electric and water stations, parcels and even plans from the mi works with more details for every single block on the city

dears it is a lot of information to dump and the server is slow so we only share the injection here have much

tables list here

```
as_polonio_ranchos_x_padron
as_punta_diablo
as_ranchos_polonio_por_padron_junio2020
```

The link didn't come to life from the first minute of your post. upload to a file hosting service

Resumen sobre todo lo anterior sobre el accionar de expresidents:

- Se contradicen en declaraciones y afirmaciones
- Subían data leaks falsas en breachforums
- Subían data leaks con los enlaces invalidos
- Se inventaban hackeos con usuarios individuales victimas de stelears...
- Hacían supuestas “ventas” sin decir precios y en las secciones invalidas
- No les importaba la reacción negativa de usuarios en foros
- No actúan acorde a un hacker de verdad tratando de proteger sus accesos
- No son conocidos en los foros ni en comunidades a pesar de que salen en las noticias
- Se inventaron una pelea falsa entre nuestro grupo y el suyo...
- No acepta mensajes de otros usuarios de foros
- Subían posts desbloqueables por monedas del foro [dificultando accesos]

Birmingham Cyber Arms LTD [BCA LTD]

Esta es una empresa registrada en Reino Unido por el residente de argentina de nombre Caseres Mauro Francisco [DNI 36006534] que es la responsable de hacer la investigacion sobre "El lider de PampaLeaks" y mintiendo tratando de crear una narrativa donde Expresidents se enoja con LaPampaLeaks y filtra quien es a todo el mundo...

Vamos a demostrar como "Expresidents" es una operacion psicologica / ingenieria social para infiltrarse en comunidades hackers y usarlo de excusa para dar de que hablar con BCA LTD mientras gana dinero, aparece como "el salvador" y vende servicios asustando a la gente

Quien dio a conocer a Expresidents?: BCA LTD fue la primera en hacer un post al otro dia del primer post de Expresidents en BF, el primer post recordemos era una una "DB" que pesaba solo unos KB. Lo mismo con el Club de futbol que pesaba unos pocos KB. BCA LTD en el caso del club de futbol saco la captura **tan solo 1 hora después** del post original en el foro

← Post

 **Mauro Eldritch** 
@MauroEldritch

Show translation

 **#Uruguay:** Publican una base de datos perteneciente a la Intendencia de Flores. Contiene usuarios y claves en texto plano.

#Ciberseguridad #Cibercrimen

 **BCA LTD** 
@BirminghamCyber · Feb 14, 2024

New #cybercrime intelligence.



 **#Uruguay:** Database belonging to Intendencia de Flores was shared. Contains users and plaintext passwords.

...







6:08 PM · Feb 14, 2024 · 26.4K Views

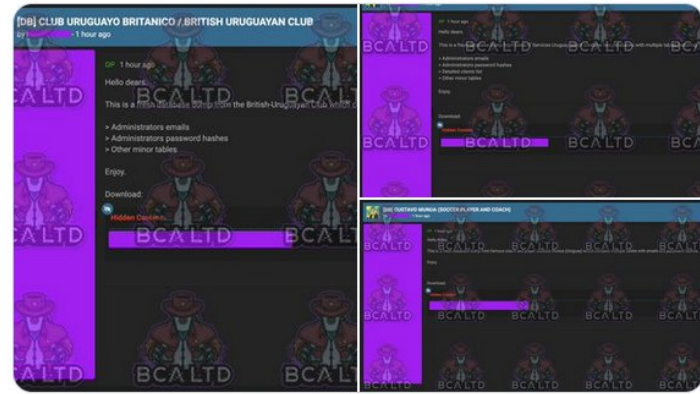
← Post

 **BCA LTD** 
@BirminghamCyber

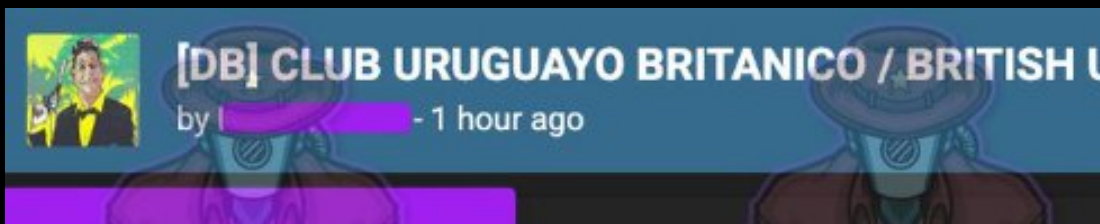
New #cybercrime intelligence.


 **#Uruguay:** New Threat Actor publishes 3 full DB leaks which contain password hashes and emails:

-  Club Uruguayo Británico.
-  Saico (Software Company).
-  Gustavo Munúa's (soccer player and coach) website.



12:46 PM · Dec 22, 2023 · 10.1K Views



 **[DB] CLUB URUGUAYO BRITANICO / BRITISH U**
by [redacted] - 1 hour ago

POST EN X SOBRE EXPRESIDENTS Y BCA LTD

Cada post publicado en BreachForums por "Expresidents" fue replicado a las horas o al otro día por BCA LTD en twitter, incluso las que las bases de datos falsas se notaban o post eliminados. No importa porque ellos lo difunden como una noticia de una nueva vulneración

Muchas de estas "vulneraciones" son las que los usuarios de Breachforums se quejaban de que el enlace estaba caído o desde el principio no funcionaba y los enlaces que llevaban a algun archivo con "DBs" eran toda basura inventada que pesaba unos pocos KB

Tweet 1: New #cybercrime intelligence. #Uruguay: Threat actor selling SQL injection for Rocha Government Website. #ThreatIntelligence: @mbec03 (¡gracias!).

Tweet 2: New #cybercrime intelligence. #Uruguay: Threat actor shares a database belonging to Globaltours. It contains 120+ user emails and IP addresses. #ThreatIntelligence: @chum1ng0 (¡gracias!).

Tweet 3: New #cybercrime intelligence. #Uruguay: Threat Actor selling databases belonging to Cerámicas Reinaldo and Guía del Uruguay, containing emails, password hashes, mobile phone numbers, addresses and CIs. #ThreatIntelligence: @teamcopybara_.

Tweet 4: New #cybercrime intelligence. #Uruguay: A threat actor defaced the Partido Nacional website and publicly shared the HTML Injection vulnerability used. #ThreatIntelligence: @teamcopybara_.

Tweet 5: New #cybercrime intelligence. #Uruguay: A threat actor disclosed a Cross-Site Scripting (XSS) and HTML Injection vulnerability on the Partido Nacional's website, accusing them of breaching an agreement and issuing threats. #ThreatIntelligence: @mbec03.

Tweet 6: New #cybercrime intelligence. #Uruguay: A threat actor published a Cross-Site-Scripting vulnerability on Partido Nacional's website and used it to threaten a parliamentarian. #ThreatIntelligence: @chum1ng0.

Tweet 7: New #cybercrime intelligence. #Uruguay: Threat Actor is selling DGI (Dirección General Impositiva) and República AFAP accounts, claiming to have "hundreds". As a sample, they leaked DGI access of ex-parliamentary Gustavo Penadés. #ThreatIntelligence: @teamcopybara_.

Tweet 8: New #cybercrime intelligence. #Uruguay: Threat Actor is selling a database belonging to Universidad de la Empresa, Facultad de Ciencias Agrarias. #ThreatIntelligence: @chum1ng0.

BCA LTD @BirminghamCyber

New #cybercrime intelligence.

#Uruguay: Threat Actor is selling DGI (Dirección General Impositiva) and República AFAP accounts, claiming to have "hundreds". As a sample, they leaked DGI access of ex-parliamentary Gustavo Penadés.

#ThreatIntelligence: @teamcapybara.



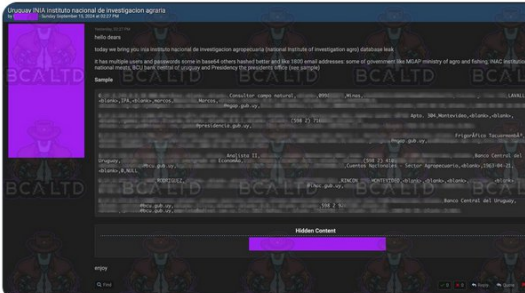
3:58 PM · Dec 4, 2024 · 12.9K Views

BCA LTD @BirminghamCyber

New #cybercrime intelligence.

#Uruguay: TA selling DBs belonging to INIA (Instituto Nacional de Investigación Agraria), containing emails, passwords, CIs, and phone numbers of employees from Presidencia, INAC, MGAP, and BCU.

#ThreatIntelligence: @mbec03 & @chumng0.



BCA LTD @BirminghamCyber

New #cybercrime intelligence.

#Uruguay: Threat actor selling XSS vulnerability in INDT (Instituto Nacional de Donación y Trasplante de Células, Tejidos y Órganos).

#ThreatIntelligence: @teamcapybara.



From sheriff.birminghamcyberarms.co.uk



Hay muchos mas pero no tenemos ganas de seguir capturando todo pero cualquier boludes que "Expresidents" sacaba en BreachForums lo publicaban, sin importar si era una db con 100 supuestos usuarios o con falsos datos y un usuario como con automoviles no se que





Mauro [Dueño de BCA LTD] tiene otra pagina llamada mefiltraron.com que agrega datos de hackers.. Entre los que estamos nosotros y unos cuantos mas de la comunidad pero de alguna manera Expresidents esta en el TOP 1 con "30 incidentes"

 #MeFiltraron

Inicio Países Incidentes Actores Malware Papers Privacidad FAQ Prensa Nosotros


Actores de amenazas

Buscar  

Actor	TTPs	Incidentes
  ExPresidents	Filtración de datos	30
  Actor Desconocido	Filtración de datos	14

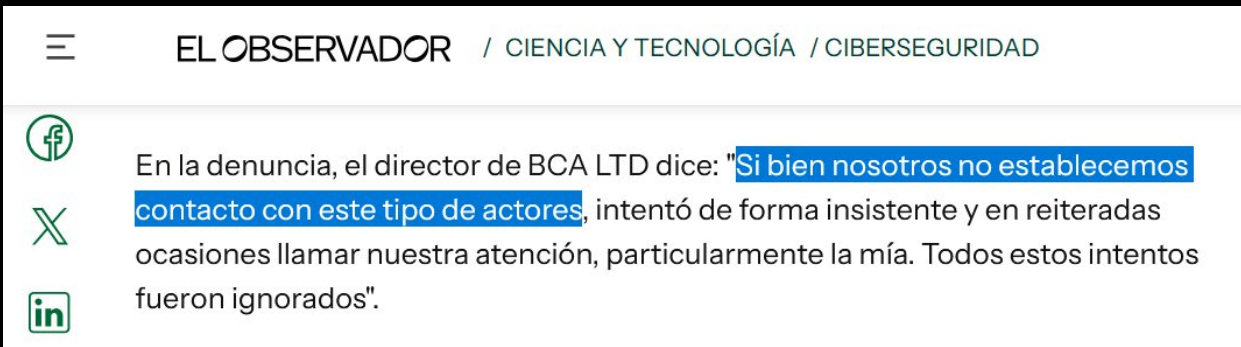
ENTREVISTA A EXPRESIDENTS

Recuerdan la entrevista a expresidents donde se contradecía y parecía mas que estaban actuando / roleando de hackers? Los que le hicieron esa entrevista [La única en la historia] a Expressidents fue una pagina creada por Mauro Francisco Caseres, el mismo dueño de BCA LTD.. No solo lo dio a conocer si no que fueron los únicos en hacerle una entrevista...



The screenshot shows the #MeFiltraron website with a navigation menu including Inicio, Países, Incidentes, Actores, Malware, Papers, Privacidad, FAQ, Prensa, and Nosotros. The main content area features a section titled "7 Ex-Presidents" with a sub-section "2024, Team Capybara". A quote reads: "Nosotros somos la escena". Below this, a paragraph describes Ex-Presidents as a cybercriminal group that attacks Uruguayan entities. A green button asks "¿Cómo nació The Ex Presidents y qué los trajo a esta escena?". A text box contains the quote: "Sentimos la necesidad de mostrar la precariedad del país en seguridad informática y la ineptitud de los que tienen que cuidarnos." Another green button asks "¿Por qué eligieron ese nombre?". A final text box contains the quote: "Es de una película con la que nos identificamos mucho."

La realidad es mas evidente aun cuando el dueño de BCA LTD en la investigación "El Líder de PampaLeaks" cuando Uruguayo1337 le envio un mensaje por telegram [no fuimos nosotros], el nunca le respondió porque "No establecemos contacto con este tipo de actores"..



The screenshot shows an article from EL OBSERVADOR, CIENCIA Y TECNOLOGÍA / CIBERSEGURIDAD. The article text reads: "En la denuncia, el director de BCA LTD dice: 'Si bien nosotros no establecemos contacto con este tipo de actores, intentó de forma insistente y en reiteradas ocasiones llamar nuestra atención, particularmente la mía. Todos estos intentos fueron ignorados'." Social media icons for Facebook, X, and LinkedIn are visible on the left side.

Team Capybara es uno de los nombres a los teams de "investigacion" [sacar captura de lo que sucede en los foros hackers o canales de telegram y subirlo a X / Substack].. Estos son los mismos que si ven en las capturas anterior, son los que mas notifican sobre lo que hacia Expressidents en Breachforums en la cuenta BCA LTD en X

En este Team participa Lara Aniela Caseres [40492286] Familiar de el dueño de BCA LTD

- <https://mefiltraron.com/interviews#expresidents>
- <https://www.nerdear.la/speakers/lara-caseres/>
- <https://www.elobservador.com.uy/ciencia-y-tecnologia/una-pelea-ciberatacantes-expone-la-identidad-del-presunto-lider-pampaleaks-n6044404>

BCA LTD Y SUS SISTEMAS DE STELEARNS LOGS

Tal y como operaba Expresidents [BCA LTD] con el “ataque” a la DGI y otros donde el obtenía credenciales de acceso y las daba al foro [para ser parcheadas], BCA LTD y Mauro tienen sistemas que ellos diseñaron desde 2023 [antes de la existencia de Expresidents] para buscar stelearns logs, una especie de IntelX local dirigido a buscar logins gubernamentales

```
:/h/m/Leaks
#birminghamcyberarms > search_uruguay logs_1.txt
Sheriff-CLI
Search term: Uruguay

> 41 credentials found, including 3 from government websites
> Detected compromised accounts on government websites (displaying first 10):
    4056...
    4056...
    4056...
    [...]

> Affected websites:
    http://campusvirtualcorazonista.uy/moodle/login/index.php
    https://autenticacion.identidaddigital.com.uy/trustedx-authn-passwd/authent[...]
    https://autoservicio.ute.com.uy/SelfService/SSvcController/registration
    https://ingreso.ceibal.edu.uy/login
    https://mi.iduruguay.gub.uy/login
    https://registro.vera.com.uy/nuevaCuenta/0t5F5K5kWySi9Gis9Tps80P-Hxek2fkUH0[...]
    https://scp.bps.gub.uy/my.policy
    https://sucursalvirtual.cablevision.com.uy/
    https://tienda.antel.com.uy/login
    https://viatrabajo.mtss.gub.uy/ViaTrabajoAutogestion/servlet/com.viatrabajo[...]
    https://www.e-sistarbanc.com.uy/ingresar/
    https://www.videocablerivera.com.uy/
    https://za.uy/auth/signin

#birminghamcyberarms >
```

```
~/D/Telegram
mauroeldritch at yharnam in [redacted]
└─$ grep -i "\.uy/" leaks.dat | wc -l
52
mauroeldritch at yharnam in [redacted]
└─$ grep -E -o 'https?://[^\s]+' | sort -u
0 (0.003s) < 14:46:04
mauroeldritch at yharnam in [redacted]
└─$ grep -E -o 'https?://[^\s]+' | sort -u
0 (0.046s) < 14:46:06
http://becas.mec.gub.uy/SolicitarBecas/view/login.php
https://facturas.ose.com.uy/SGCv10WebClient/MenuFacturasYPagos.faces
http://gtm.uy/solicitud.php
https://acceso.anv.gub.uy/
https://acceso.anv.gub.uy/LogIn/LogIn
https://app1.bps.gub.uy/CambioContrasena/CambioContrasena.aspx
https://app.tutasa.com.uy/password/reset/[redacted]
https://auth.midinero.com.uy/authenticationendpoint/login.do
https://auth.redpagos.com.uy/
https://ebanking.brou.com.uy/
https://ebanking.brou.com.uy/frontend/loginStep1
https://familia.ceip.edu.uy/accesofamilia/Login
https://guri2.ceip.edu.uy/
https://guri2.ceip.edu.uy/accesofamilia/Login
https://identityserver.ute.com.uy/Account/Register
https://ingreso.ceibal.edu.uy/login
https://ingreso.claro.com.uy/
https://login.vera.com.uy/login
https://loguno.ose.com.uy/
https://miclaro.claro.com.uy/
https://miclaro.claro.com.uy/web/guest/bienvenido
https://miclaro.claro.com.uy/web/guest/registracion
https://micuentanuevo.oca.com.uy/trx/login
https://pca.ceibal.edu.uy/portal/
https://portalcautivo.ceibal.edu.uy/login.html
https://registro.vera.com.uy/
https://salto.olx.com.uy/login
https://scp.bps.gub.uy/
https://scp.bps.gub.uy/my.policy

~/h/m/PS/Sheriff-CLI
#birminghamcyberarms > search_argentina new_combolist.txt
Sheriff-CLI
Search term: Argentina

> 80288 credentials found, including 364 from government websites
> Detected compromised accounts on government websites (displaying first 10):
    gene...@buenosaires.gob.ar
    alca...@spf.gob.ar
    pvil...@adinq.gov.ar
    jsot...@migraciones.gob.ar
    soli...@adinq.gov.ar
    alej...@iosper.gob.ar
    rica...@abc.gob.ar
    viol...@mpftucuman.gob.ar
    germ...@educacion.gob.ar
    leon...@mec.gob.ar
    [...]

> Affected domains:
+-----+-----+-----+
| abc.gob.ar      | acumar.gob.ar  | ada.gba.gov.ar |
| adinq.gov.ar   | afip.gob.ar    | afip.gov.ar    |
| agcba.gov.ar   | agencia.secyt.gov.ar | agn.gov.ar     |
| ambiente.gob.ar | anac.gob.ar    | anac.gov.ar    |
| anlis.gov.ar   | anmat.gov.ar   | anses.gov.ar   |
| anses.gov.ar   | apn.gov.ar     | ara.mil.ar     |
| arba.gov.ar    | balcarce.inta.gov.ar | bca.gov.ar     |
| buenosaires.gob.ar | buenosaires.gov.ar | c4.pjn.gov.ar  |
| cab.cnea.gov.ar | cae.cnea.gov.ar | caecopaz.mil.ar |
| camdipsalta.gob.ar | cancilleria.gob.ar | cenpat-comicet.gob.ar |
| ceride.gov.ar   | cfee.gov.ar    | chaco.gov.ar   |
+-----+-----+-----+
```

Si haces zoom en el PDF para ver las imágenes, veras que los nombres de usuario de linux son Mauroeldritch y BirminghamCyberarms [BCA LTD]. Ellos esto lo publicaban en X

No es muy difícil darse cuenta que es el mismo método de ataque de “Expresidents” y que esto es una operación para que le presten mas atención, publicando accesos en el foro y dificultando el acceso rápido a los usuarios de este para que ellos le saquen captura, lo publiquen, salga en las noticias y ellos sean los salvadores que notificaron el problema

- <https://archive.ph/WnCPg>
- <https://web.archive.org/web/20260524135406/https://pbs.twimg.com/media/Fw-QEZ5WAAElaEC?format=png&name=large>

LA COMPLICIDAD DE EL OBSERVADOR

Juan Pablo de Marco usa la imagen de El Observador para promocionar desinformación y realizar afirmaciones sin evidencia a su audiencia como mostramos en el otro PDF, el es parte muy importante de esta operacion de BCA LTD para dar relevancia al hacker inventado y mostrar como “salvadores” y quienes tratan de ayudar a victimas de “Expresidents”



Desde el primer momento que “Expresidents” [BCA LTD] Hizo sus primer post en Breachforums [Post falsos y criticados en el foro] Juan Pablo del observador hizo un artículo promocionando estos supuestos ataques como el de la Intendencia de Flores y de la “VPN” del Correo Uruguayo que demostramos como era info inútil y el post fue removido del foro por admins



Todas las noticias de el observador donde hablan de Expresidents es basado en Birmingham Cyber Arms [BCA LTD] y sospechosamente son ellos los que avisan a las empresas o organismos publicos afectados y saben justamente como logro vulnerarlos...



- <https://www.elobservador.com.uy/ciencia-y-tecnologia/ciberataques-uruguay-2024-el-surgimiento-nuevos-grupos-y-modalidades-delictivas-n5976692>

Es extremadamente evidente como inflan la imagen de “el hacker expresidents” como cuando vimos que hizo fue poner un enlace de un formulario publico del MTSS llamando la atencion que se podia buscar “tambien niños” y a las horas fue parcheado

El mismo que publico “El Lider de PampaLeaks” hizo una noticia de esto, mostrando en el titulo como si Expressidents hubiese echo ese sistema y lo estaban vendiendo en el mercado negro. En la descripcion de la noticia estaban los “Expertos” [BCA LTD] a advertir a todos sobre esto

Hackers pusieron a la venta un sistema que permite saber de quiénes son 7 millones de cédulas uruguayas: ¿cuál es el riesgo?

Los ciberdelincuentes están comercializando un sistema que permite consultar nombres y fechas de nacimiento; expertos advierten de los riesgos

17 de septiembre de 2024 • 8:56 hs



Por Juan Pablo De Marco



EL OBSERVADOR / CIENCIA Y TECNOLOGÍA / CIBERSEGURIDAD

El sistema funciona de manera sencilla: el usuario ingresa la cédula y aparecen los datos de todos los uruguayos, aunque no tengan edad para trabajar, [informó Birmingham Cyber Arms](#), una empresa especializada en reportar incidentes informáticos.

Pasos de la operación que lleva acabo BCA LTD con su personaje “Expressidents:

1. “Expressidents” [BCA LTD] publica vulnerabilidades reales o ficticias en foros [esto lo hacia antes] o en paginas en la red tor que nadie conoce
2. Informa Birmingham Cyber Arms [BCA LTD] en X sobre esto y lo envía a periodistas
3. El observador [Juan Pablo de Marco] publica una noticia al respecto con lo que le dicen que decir desde BCA LTD y mostrando como “expertos” a BCA LTD
4. El articulo toma notoriedad y otros medios lo replican, mostrando a BCA LTD como la que notifico del problema desde el primer momento y la que ayuda dando explicaciones de lo que paso realmente como sucedió con el “Hackeo” HG de ANTEL

Con esto entendemos las “rarezas” de expresidents en los foros hackers, con los mensajes privados desactivados para no hacer contacto con usuarios [otros ciberdelincuentes para BCA LTD], como no le importaba quedar mal ni que le borrarán los posts o publicar accesos que eran evidentemente que iban a ser parcheados como sucedió con el post de MTSS o la VPN

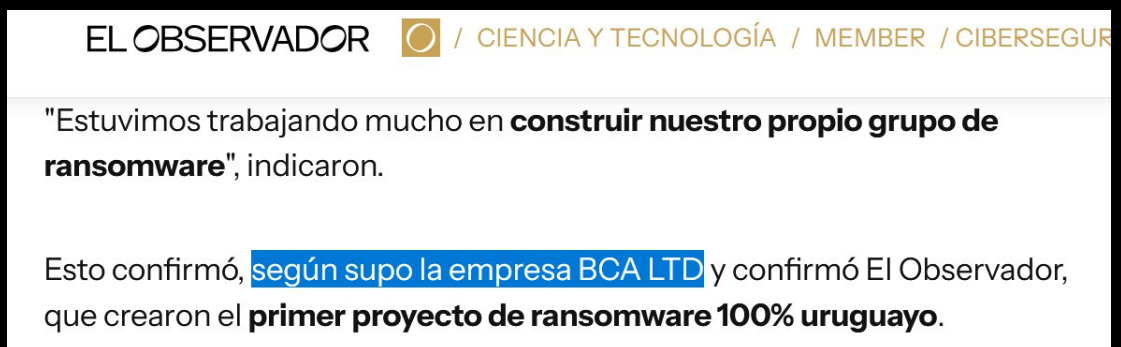
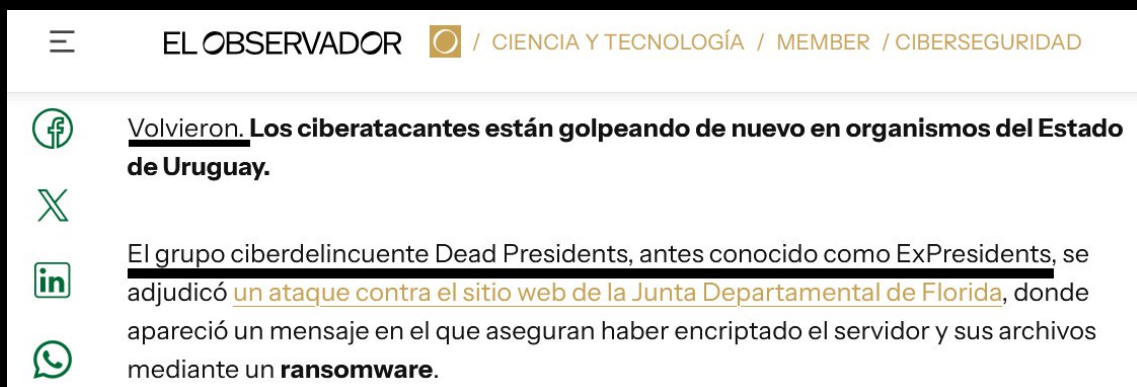
Porque la misión de BCA LTD con esto es darse a conocer y quedar como los salvadores

LAS “EXCLUSIVAS” DEL OBSERVADOR CON EXPRESIDENTS Y BCA LTD

Esta operación viene desde 2024 y a principios de 2025, Expressidents [BCA LTD] detuvo toda su operativa justo en la llegada de PampaLeaks [Dinacia, Masoneria, Fiscalia] y en la de Tacuara [Mides, Ministerio del interior] en BreachForums. Luego desaparecieron y fueron a craxpro.net envés de otro foro conocido como DarkForums, luego de eso Expressidents desapareció de los foros hackers y “se hizo su propio sitio web en la red tor”



Nadie en los mercados ni en los foros hackers sabia que estaba haciendo expresidents pero de alguna manera Juan Pablo de Marco tenia la exclusiva de que estaba haciendo Expressidents, gracias a “la empresa BCA LTD” [Otra vez repitiéndose lo mismo]



- <https://www.elobservador.com.uy/ciencia-y-tecnologia/ciberatacantes-crean-el-primer-ransomware-100-uruguayo-n6036845>

La operación en El Observador y BCA LTD es tan grande que cuando sucedió el hackeo en ANTEL por LaPampaLeaks, en la plataforma TuID y autoridades de la empresa lo confirmaron, la respuesta del Observador **fue decir que el ataque era del grupo “Dead Presidents”** lo que muestra en claro que **no les importa desinformar** mientras beneficie a su personaje



The screenshot shows a news article from 'EL OBSERVADOR' under the 'NACIONAL / SEGURIDAD' section. The main headline is 'Torre de Antel. Fachada'. A highlighted paragraph reads: 'Las autoridades de **Antel** reconocieron que el **portal de identidad digital TuID** fue **objeto de un ciberataque** —atribuido al grupo Dead Presidents— pero **aseguraron que el hackeo no afectó "la operativa ni los mecanismos de autenticación actualmente utilizados por la plataforma"**.' To the right, there is a vertical list of related topics with numbered icons: '3 Ciberinformación', '4 Gobierno la Arranca', and 'OPV'.

Hay párrafos tan jugosos como el que afirma que Dead Presidents [Expresidents] fue el que hizo el ataque y LaPampaLeaks [Fundador del PampaLeaks] lo publicó después. Haciendo que la narrativa sea que Expresidents atacó TuID y LaPampaLeaks solo lo “divulgo”

La plataforma TuID permite a ciudadanos uruguayos **identificarse para realizar trámites ante el Estado**. El ataque atribuido a Dead Presidents fue divulgado el jueves por el grupo LaPampaLeaks.

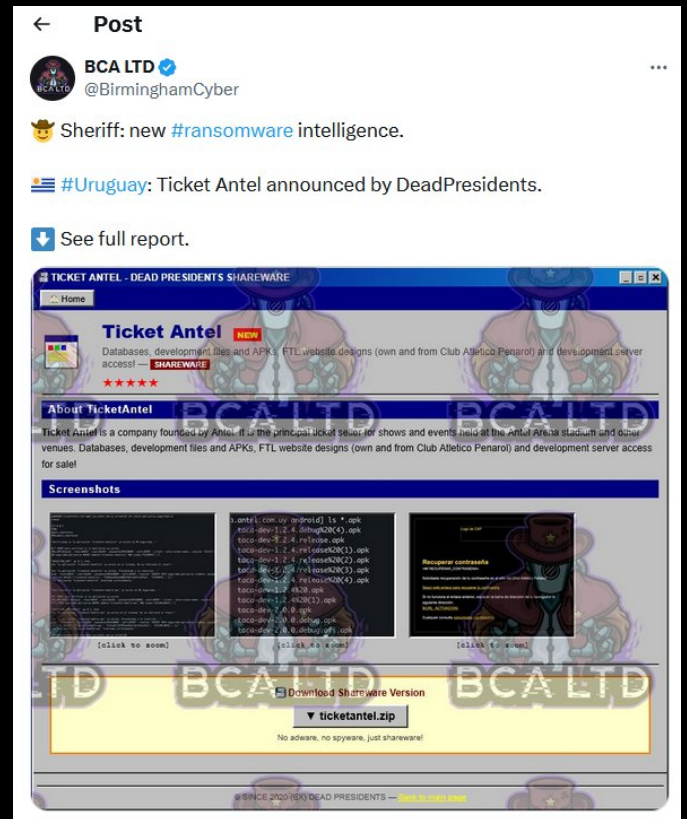
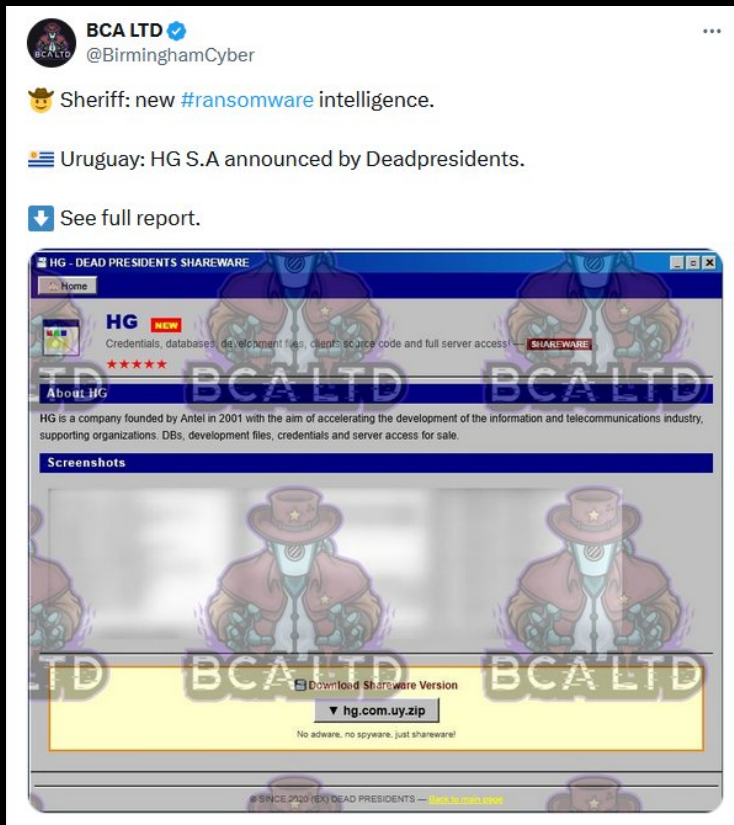
Desmentir esto es tan fácil como ir a DarkForums y comparar fechas de cuando se publicó el post de TuID y cuando apareció Expresidents con el hackeo a “HG” y “Tickantel”

- <https://www.elobservador.com.uy/nacional/antel-asegura-que-ciberataque-plataforma-identidad-digital-no-afecto-operativa-ni-mecanismos-autenticacion-n6044188>
- <https://darkforums.su/Thread-uruguay-Antel-TuID-Digital-8GB-Data-Leak-Government>

EL FALSO HACKEO A HG Y TICKANTEL

Después de que nosotros hiciéramos publico el hackeo a ANTEL, en el servicio TuID lo que sucedió 1 semana después es que “Expresidents” [BCA LTD] volvió de repente y también afecto a servicios de ANTEL por una empresa privada donde antel es 100% propietaria

Nuevamente el origen de la primera noticia al respecto proviene de BCA LTD y no hay mas fuente detrás que esa, nadie que conozcamos tiene acceso a la supuesta pagina en tor que es donde seria esa captura de pantalla [con marca de agua de BCA LTD]..



Apenas unas horas después del Twitt original de BCA LTD.. Juan Pablo de Marco usando la imagen de EL OBSERVADOR, publica la noticia de que filtraron accesos a servidores y que hay expuestos códigos fuentes, etc que en total seria unos 12GB. Unos días después, hacen la noticia de Tickantel con 1GB de supuestos datos filtrados en alguna parte de “la dark web”?

Ciberdelincuentes filtran accesos a servidores de una empresa de Antel

La filtración incluye credenciales, código fuente y documentación técnica de HG, empresa tecnológica de la que el ente estatal es dueña

12 de mayo de 2026 • 12:52 hs

Por Juan Pablo De Marco



LAS MÁS L

- 1 El posteo de N a la tarde, luego Bielsa no lo cit el Mundial 202
- 2 La estrategia de turistas uruguay precios: nuevo mirador en las

Ciberdelincuentes filtraron 1 GB de información de servidores de Tickantel: ¿cómo afecta a los usuarios?

El grupo cibercriminal DeadPresidents puso a la venta 1 GB de información robada a Tickantel, incluyendo las plantillas con las que Peñarol envía los mails de confirmación de compra de entradas a sus hinchas

15 de mayo de 2026 • 12:41 hs

Por Juan Pablo De Marco

LAS MÁS I

HG S.A respondió con un comunicado interno en base a las “notas de prensa” [El Observador] sobre la data leak y según su “análisis exhaustivo” no detectaron “compromiso” [hackeo] de ningún dato y siguieron operando con normalidad... Recuerdas todos los falsos hackeos y filtraciones de Expresidents antes? Bueno exactamente lo mismo sucede aqui

Estimados Clientes y Socios,

HG S.A. informa que ha tomado conocimiento de notas de prensa sobre una posible filtración de información vinculada a nuestra organización. De forma inmediata el equipo de Ciberseguridad ha iniciado los protocolos de respuesta a incidentes, notificando a las autoridades competentes (Unidad de cibercrimen del Ministerio del Interior / CERTuy). Reafirmamos nuestro compromiso con la protección de datos y mantendremos la transparencia durante este proceso.

Situación Actual: El equipo se encuentra realizando un análisis exhaustivo. Hasta el momento, las verificaciones técnicas internas no han identificado evidencia alguna de un compromiso de nuestra infraestructura, sistemas o bases de datos. Tampoco se han detectado indicadores de compromiso en los activos de información de nuestros clientes ni socios de negocios.

Acciones en Curso: Nos mantenemos en una fase de análisis y monitoreo reforzado. Estamos trabajando en analizar la información externa para validar autenticidad, origen y antigüedad, así como para descartar el uso de datos históricos o intentos de desinformación. En paralelo, hemos ampliado los niveles de registro y trazabilidad, activado búsquedas específicas de indicadores de compromiso y reforzando la vigilancia. Estas tareas se realizan en coordinación con CERTuy, la Unidad de Cibercrimen del Ministerio del Interior, nuestra casa matriz y los especialistas técnicos correspondientes.

Nuestros servicios continúan operando con normalidad, priorizando la seguridad y la continuidad operativa. Los mantendremos informados oportunamente ante cualquier actualización relevante que surja.

Atentamente,
HG S.A.

Días después lo que procedió a hacer el tonto util de BCA LTD es tratar de mentirosos a los del equipo de ciberseguridad de HG S.A diciendo que si le habían filtrado datos [“confirmado por ex empleados de H.G que vieron sus credenciales de acceso filtradas”]

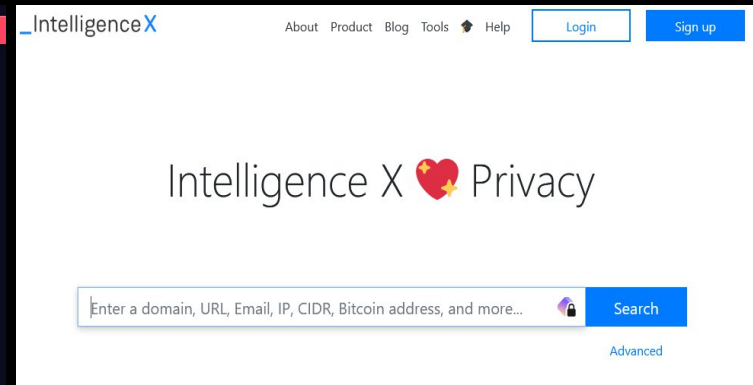
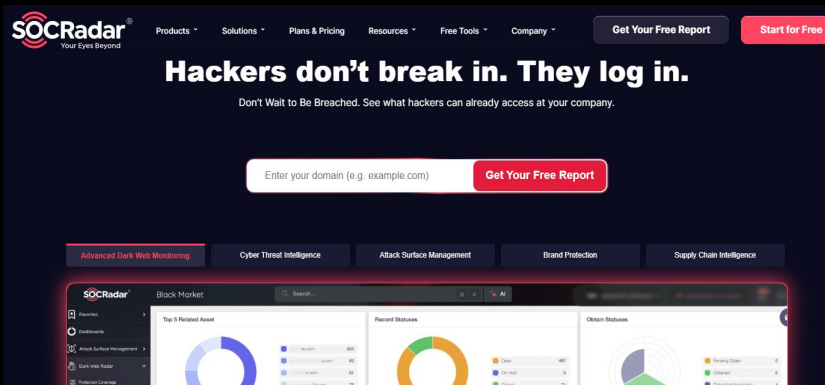


En la proxima pagina desmentiremos lo que afirma este periodista mitomano [otra vez]

La respuesta de el periodista de cuarta de el observador:

"es una cosa muy contradictoria cuando habían ex empleados de H.G que me dijeron "mis credenciales estaban ahí" había otra gente que uso otras plataformas como "SOC RADAR" que son plataformas que detectan que credenciales están dispersas por la dark web" – marc1.mp4

SOCRadar es un sistema para empresas y gobiernos donde con pagar se pueden ver las filtraciones de credenciales segun dominio y otros filtros [Stealers Logs], es lo mismo que IntelX pero legal en todo el mundo y dirigido a entornos profesionales



De los "12GB" en venta y de los "1GB" de Tickantel su única defensa fue hacer referencia a que estaban mintiendo porque se veian credenciales de empleados de HG.. Que estaban filtradas porque alguno se habrá comido un spyware que le robo todas las contraseñas... Recordemos que Mauro y BCA LTD tienen un sistema que tambien hace justo eso...

```
#birminghamcyberarms > search_argentina new_combolist.txt
Sheriff-CLI
Search term: Argentina

> 89288 credentials found, including 304 from government websites
> Detected compromised accounts on government websites (displaying first 10):
gene...@buenosaires.gov.ar
alca...@spf.gov.ar
pvil...@adinqn.gov.ar
jsot...@migraciones.gov.ar
eoli...@adinqn.gov.ar
alej...@losper.gov.ar
rica...@abc.gov.ar
viol...@mftucuman.gov.ar
germ...@educacion.gov.ar
leon...@ec.gov.ar
[...]

> Affected domains:
-----+-----+-----+
| abc.gov.ar      | acumar.gov.ar  | ada.gba.gov.ar |
| adinqn.gov.ar  | afip.gov.ar    | afip.gov.ar    |
| agcba.gov.ar   | agencia.secyt.gov.ar | agn.gov.ar     |
| ambiente.gov.ar | anac.gov.ar    | anac.gov.ar    |
| anlis.gov.ar   | anmat.gov.ar   | anses.gov.ar   |
| anses.gov.ar   | apn.gov.ar     | ara.mil.ar     |
| arba.gov.ar    | balcarce.inta.gov.ar | bcra.gov.ar    |
| buenosaires.gov.ar | buenosaires.gov.ar | c4.pjn.gov.ar  |
-----+-----+-----+

#birminghamcyberarms > search_uruguay logs_1.txt
Sheriff-CLI
Search term: Uruguay

> 41 credentials found, including 3 from government websites
> Detected compromised accounts on government websites (displaying first 10):
4056...
4056...
4056...
[...]

> Affected websites:
http://campusvirtualcorazonista.uy/moodle/login/index.php
https://autenticacion.identidaddigital.com.uy/trustedx-authn-passwd/authent[...]
https://autoservicio.ute.com.uy/SelfService/SSvcController/registration
https://ingreso.ceibal.edu.uy/login
https://mi.iduruquay.gub.uy/login
https://registro.vera.com.uy/nuevaCuenta/0t5F5K5kWySi9GiS9Tps80P-Hxek2fkUH0[...]
https://scp.bps.gub.uy/my.policy
https://sucursalvirtual.cablevision.com.uy/
https://tienda.antel.com.uy/login
https://viatrabajo.mtss.gub.uy/ViaTrabajoAutogestion/servlet.com.viatrabajo[...]
https://www.e-sistarbanc.com.uy/ingresar/
https://www.videocablerivera.com.uy/
https://za.uy/auth/signin

#birminghamcyberarms >
```

Esa afirmación de que si fueron "comprometidos" porque fueron credenciales expuestas es absurdo.. Es como que nosotros digamos que por tener credenciales de AGESIC [ya no validas] pero tenerlas igual.. Comprometimos agestic sin meternos en ningun sistema

Lo segundo.. Desde el 12 de mayo de 2026 El Observador gracias a una investigación de "BCA LTD" ya sabian como "Expresidents" habia accedido y incluso datos que como que el acceso fue vendido por un "IAB" que en palabras normales es alguien que hace un stelear y se dedica a infectar a miles de personas para crear una base de datos de eso y después venderlo



Según una investigación realizada por BCA LTD, una empresa que se dedica a analizar ciberataques y actores de amenazas, el



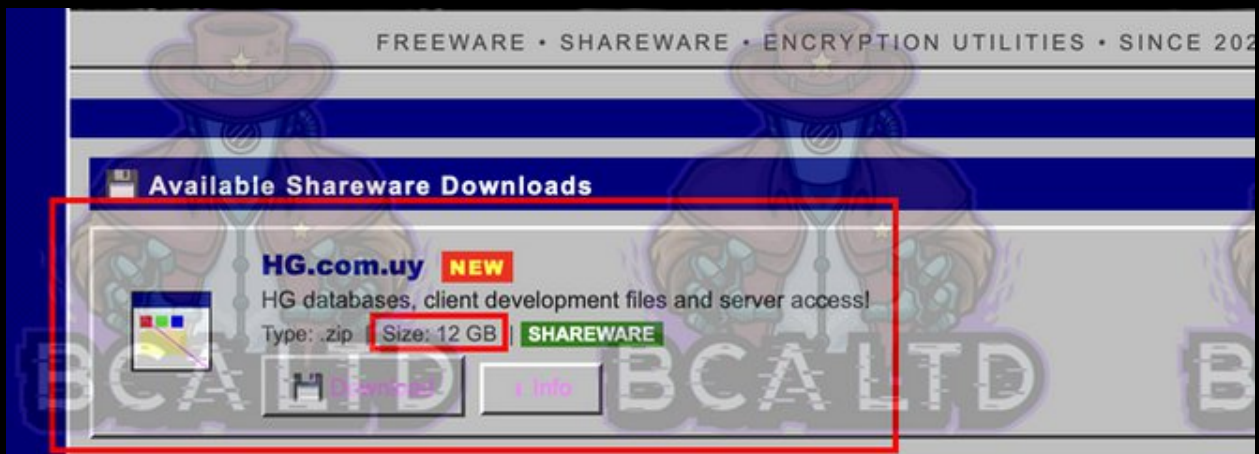
acceso inicial a HG fue vendido por un IAB, sigla en inglés que significa Initial Access Broker (vendedor de accesos iniciales). Se trata de un actor que se especializa en vulnerar sistemas y luego revender esa puerta de entrada a otros grupos criminales.



DeadPresidents (anteriormente ExPresidents) compró ese acceso a un tercero y, desde adentro, extrajo el material.

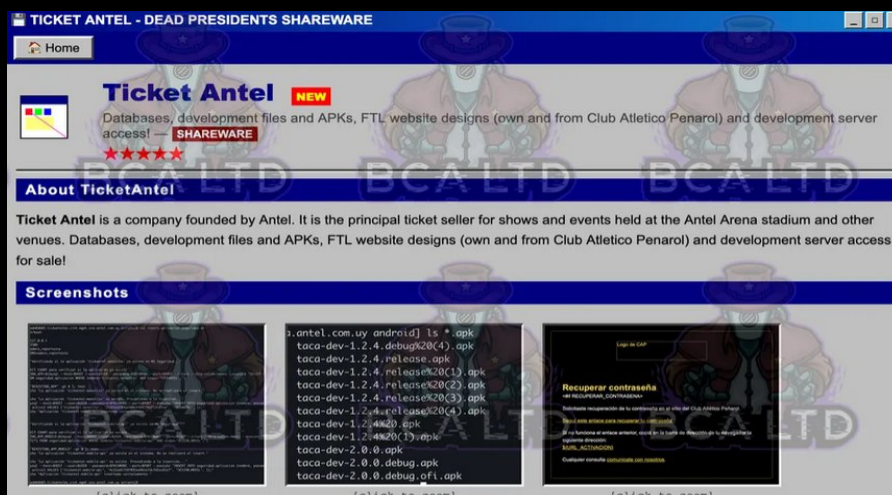


Otros datos como que en las noticias de El Observador se afirma que están vendiendo esos 12GB en la “dark web” pero en la captura [la única en todo internet] de BCA LTD se muestra para descargar.. No dice nada de sample y se afirma haber accedido a bases de datos y mas



luego el “1GB” de Tickantel [basado en una única captura en internet de BCA LTD] solo muestran info del frontend de una APK.. Todas las APK son descomprimibles fácilmente y filtrar esos archivos es igual a ver el código fuente de una página web y decir que es un “leak”

Lo segundo, los diseños de mail [FTL Desings] son fáciles de recrearlos con registrarte o poner “recuperar contraseña” [como se muestra en una de esas capturas] y descargar el código fuente del mail para recrearlo en un archivo “FTL” y decir que hackeaste Tickantel...



Resumen de la operacion del hackeo a HG y Tickantel:

- Los unicos ejemplos de “leak” por Expresidents [DeadPresidents] son credenciales de acceso [Stelear logs] y archivos del frontend de APKs y de mails oficiales
- La defensa del tonto util de el observador es hacer referencia a que HG estaba mintiendo es usar de ejemplo bases de datos de Stelears logs y tools
- Usaron de ejemplo “12GB” porque era mucho mas grande que “8GB” que fue el real hackeo a ANTEL en TuID por parte de el equipo de PampaLeaks

operación para usar la imagen de HG S.A y ANTEL y en que beneficia a BCA LTD:

En ciberseguridad la clave para vender mas es usar el miedo para que contraten tus servicios.. Los de BCA LTD hacen justamente eso y es la verdadera razon de porque inventaron el personaje “Expresidents”, para ellos ser los salvadores cuando este “grupo” ataca llegar a dañar infraestructuras ni filtrar bases de datos con millones de registros

En los ejemplos mas atras mostramos como usaron a la DGI, MTSS, Intendencias departamentales y otros organismos publicos uruguayos para hacer exactamente esto. Ellos notifican y quedan como los salvadores y los “expertos” que dan explicaciones

En este caso usaron la imagen de ANTEL porque ya habia un hackeo confirmado y el mas grande hasta ahora siendo noticia nacional.. Asi que usaron la ola mediática para que Expresidents vuelva con un “Hackeo” a servicios tercerizados de ANTEL.. Haciendo una jugada bastante grande de operacion psicologica para mostrarse como los salvadores

Intereses de BCA LTD y porque hacen esto: Venden servicios de investigación de “amenazas” [hackers], acceso a un sistema de busqueda de credenciales filtradas que lellaman Domain Data Breaches Monitor y “Exposed Credentials” [Stealers Logs] a precios altos

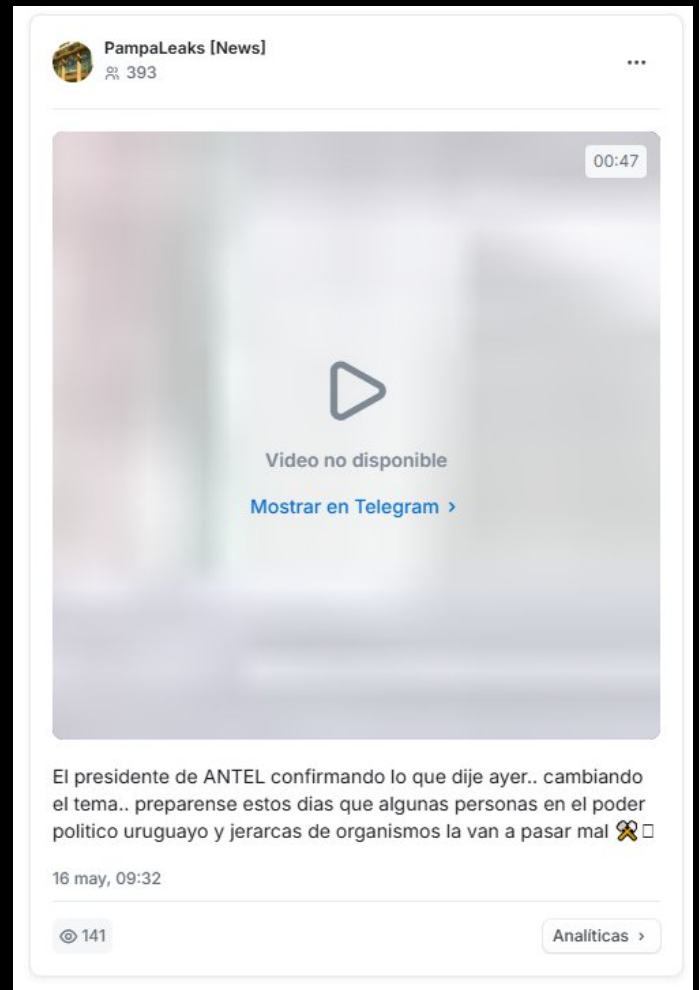
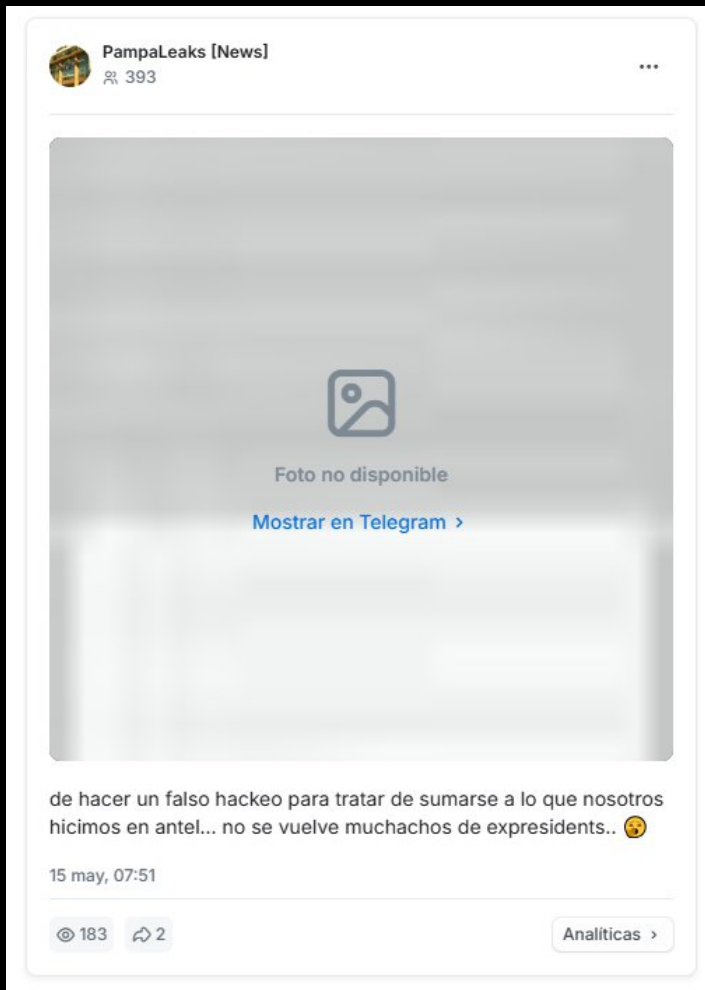
Premium Small Businesses & Teams	Enterprise Large Companies
<ul style="list-style-type: none">Access to our Threat Intelligence FeedAccess to our Ransomware Intelligence FeedAccess to our Curated Cyber News FeedAccess to our Latest Alerts FeedAccess to our Attacks & Leaks FeedAccess to our Crypto Crime & News FeedAccess to our Crypto Transactions FeedAccess to Threat Actors ProfilesAccess to our Exploits FeedAccess to Adversary Websites & Channels FeedAccess to Adversary Infrastructure FeedAPI Access with Slack & Telegram IntegrationsPriority support from our engineers <p>KYC required. Partial refund if verification fails.</p>	<ul style="list-style-type: none">Access to our Threat Intelligence FeedAccess to our Ransomware Intelligence FeedAccess to our Curated Cyber News FeedAccess to our Latest Alerts FeedAccess to our Attacks & Leaks FeedAccess to our Crypto Crime & News FeedAccess to our Crypto Transactions FeedAccess to Threat Actors ProfilesAccess to our Exploits FeedAccess to Adversary Websites & Channels FeedAccess to Adversary Infrastructure FeedAPI Access with Slack & Telegram IntegrationsAccess to Domain Data Breaches MonitorDaily notifications for Exposed CredentialsComplimentary monthly Intelligence ReportsPriority support from our engineers

<p>\$7,500 per year</p> <p>Subscribe</p>	<p>\$14,500 per year</p> <p>Subscribe</p>	<p>\$29,000 per year</p> <p>Subscribe</p>
---	--	--

PELEA INVENTADA ENTRE PAMPALÉAKS Y EXPRESIDENTS [DEADPRESIDENTS]

Las únicas referencias de PampaLeaks fue por LaPampaLeaks en 2026 cuando se confirmó que el hackeo a HG y Tickantel era falso, en 2025 fue la respuesta a el post donde el subió una base de datos falsa con tan solo un usuario y archivos .csv del frontend de una web

Los que afirman que fue una “pelea” y que Expressidents doxéo al “Lider de PampaLeaks” es BCA LTD, esta investigación se hizo publica unos días despues de que LaPampaLeaks con su antigua cuenta @lapampaleaksbf en telegram mostro lo siguiente en telegram:



Días despues de que LaPampaLeaks hiciera un doxx a figuras politicas de Uruguay y le suspendieran las cuentas y todos los canales, nos quedamos sin comunicación y 2 días despues apareció la investigacion que revela “El Lider de PampaLeaks” y una de las narrativas es que nosotros sabiamos que esto iba a pasar por culpa de expresidents y borramos todo..

Los intereses de BCA LTD aqui: Estabamos yendo contra su narrativa y la de su personaje “Expressidents” asi que usaron a Juan Pablo de el observador para hacer publica una investigación “Que revela el lider de pampaleaks” para destruirnos y pensando que ibamos a desaparecer por ende que no nos ibamos a desmentir nada de las afirmaciones

Una pelea entre ciberatacantes expone la identidad del presunto líder de PampaLeaks

Su falta de conocimiento de Telegram, sumado a un insulto a otros atacantes develó la identidad de un joven de 19 años apuntado en una denuncia

19 de mayo de 2026 • 20:30 hs



Por Juan Pablo De Marco

Juan Pablo de Marco... El mismo que desde 2024 viene promocionando "investigaciones" de BCA LTD, que promociono a "Expresidents" desde el principio basado en BCA LTD.. Y persona del mismo medio que afirmaba que TuID habia sido vulnerado por expresidents, 2 dias despues de nosotros estar en contra de la narrativa de BCA LTD.. Sale con esto...

El otro documento destinado y desmentir la investigación:

- BCA LTD afirma que nosotros desde el 2024 venimos atacando a expresidents "en diferentes foros" con insultos y consignas políticas [desmentido]
- BCA LTD afirma que expresidents durante todo el tiempo que LaPampaLeaks lo insulto y lo atacaba.. El lo ignora hasta que un día se canso y "lo doxeo" con todos sus datos personales como direcciones, info dnic, etc y ahí "BCA LTD comenzo a investigar".. ;)
- Ellos afirmaban que nos borramos nosotros las cuentas de TG para escapar porque "sabian lo que se les venian" cuando realmente las cuentas fueron suspendidas
- Mostramos como Juan Pablo de Marco junto a BCA LTD, se dedico a mentir en el pasado en otras noticias y no verificar absolutamente nada de lo que afirmaba

Lo que pensaba por la mente de Mauro de BCA LTD al hacer esto:

Ellos pensaban que uruguayo1337 era el lider de PampaLeaks y que LaPampaLeaks solo era un alias de una misma persona, de esta forma cuando nos suspendieron las cuentas de TG a todos, días después de desmentir a expresidents.. Ellos vieron que podian usar al tonto util de el periodista de El Observador para quitarse a la competencia de "expresidents" [ellos]

De esta manera se hace un hito historico para Juan Pablo de Marco, descubriendo la identidad del líder de el grupo hacker mas buscado de Uruguay basado en una investigación de BCA LTD que seria un antes y un después para sus "investigaciones a actores de amenaza"

Ademas de quitarse la "competencia" y que el único "actor de amenaza" sean ellos mismos, controlando la narrativa de todos los futuros hackeos del pais [falsos] y haciendo que el grupo DeadPresidents o Expresidents [ellos] tenga mucha reputación por derribar a PampaLeaks

BCA LTD Y LA REPUTACION DE PAMPALEAKS

Esta empresa que controla "Expresidents" viene desde hace mas de 1 año tratando de bajar la reputación de PampaLeaks.. Sin importar si es mentira, intentan manipular al ojo publico lo cual a NOSOTROS NO NOS IMPORTA porque ya somos los malos.. Una vez después de eso solo es intentarlos bajar la reputación para que "expresidents" [ellos] estén en alto

es muy evidente esto con solo leer "la entrevista" que le "hicieron" a "expresidents", desde el titulo "Nosotros somos la escena" o como los describen "Este grupo que lidera hoy el ranking de incidentes en uruguay" o la primera pregunta que perfectamente podría ser el lema de BCA LTD con "sentimos la necesidad de mostrar la precariedad del pais en segur..."

"Nosotros somos la escena"

Ex-Presidents, el grupo cibercriminal que ataca entidades uruguayas habló con nosotros. Compuesto por miembros que adoptan nombres de ex funcionarios, como *r3agan*, *Cl1nton*, *Nix0n*, *Gorb4chov*, *2anguinetti* y *bu5h*, este grupo lidera hoy el ranking de incidentes en Uruguay y en #MeFiltraron. En esta oportunidad, dialogamos con *r3agan* y *Cl1nton* sobre sus planes.

¿Cómo nació The Ex Presidents y qué los trajo a esta escena?

Sentimos la necesidad de mostrar la precariedad del país en seguridad informática y la ineptitud de los que tienen que cuidarnos.

Hace un año esta misma empresa de "ciberseguridad" intento hacernos lo mismo haciendo que el tonto util del periodista del observador saque una nota donde apunta a personas que no tienen nada que ver con nosotros [los "hackers" con *intelx* de buquebus] que eran solo unos adolescentes tratando de llamar la atención haciendo todo desde "sus celulares" y redes

Quiénes están detrás del hackeo a la web de la Dinacia y cómo una persona los delató

Usaban seudónimos, operaban desde sus propios celulares y se jactaban de sus delitos en redes sociales

15 de abril de 2025 • 13:41 hs



EL OBSERVADOR / CIENCIA Y TECNOLOGÍA / CIBERSEGURIDAD



La investigación



Una investigación de la empresa de ciberseguridad Birmingham Cyber Arms reveló la forma de operar de este joven de 18 años junto a otro uruguayo.



Los expertos descifraron que disfruta de vanagloriarse en redes sociales de sus hechos delictivos, lo que aportó "evidencia en forma constante y trivial". También descubrieron que la crítica o la competencia lo enfurecen.



Ahora mismo mientras estamos escribiendo esto, LaPampaLeaks nos acaba de enviar como Juan Pablo De Marco a las 5 DE LA MAÑANA [esta muy enfermo] hizo una nueva noticia sobre “falsas filtraciones de PampaLeaks” poniendo de ejemplo la base de datos de DNIC publicada en DarkForums y Spear Forums junto a otra de TATA que nosotros no tenemos nada que ver

Uruguay Argentina España Estados Unidos

EL OBSERVADOR / CIENCIA Y TECNOLOGÍA / SEGURIDAD INFORMÁTICA

Estas son las falsas filtraciones de PampaLeaks sobre las cédulas y un supermercado

Expertos cuestionan la autenticidad y el alcance de varias publicaciones del grupo ciberdelincuente, incluida una supuesta filtración de Ta-Ta que fue borrada minutos después y una base de cédulas que ya circulaba desde 2019

26 de mayo de 2026 • 5:00 hs

Por Juan Pablo De Marco

LAS M

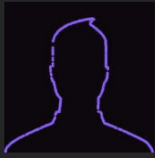
La “primicia” es que esa base de datos ya estaba filtrada.. La pregunta es, que primicia? LaPampaLeaks en todo momento dijo que esa base de datos estaba circulando, que era la “clasica base de datos de DNIC” y que lo hacia mas que nada como un servicio a la comunidad hacker porque personas en telegram la estaban vendiendo a gente ingenua a precios altos

DATABASE uruguay: DNIC [5.8M] [Database] [Citizens] [Leak] [Free]
by LaPampaLeaks - 20-05-26, 05:51 PM

Pages (12): 1 2 3 4 5 ... 12 Next »

20-05-26, 05:51 PM #1


LaPampaLeaks



DarkForums Members

MEMBER

Hello again! Today we're bringing you a free data leak. **This database is circulating in closed Telegram groups, where it's being sold at exorbitant prices. It's one of the classic DNIC databases containing over 5.8 million records** of people born up until early 2020, extracted thanks to the lack of rate limits and security measures in a DNIC API. Surprisingly, this database was shared in very few places, and now lammers are using it to sell it to unsuspecting buyers. As a service to the Uruguayan hacker community, we are uploading it here for free and will constantly update the download links.



Details of the Data breach: Cedula de identidad [ID Number], Citizen's name, Citizen's last name
Number of Citizens: 5.8M

This will make it easier for many people to obtain an ID and complete procedures on government websites that only require an ID and a full name. It is also useful in the event that a hacker gains access to an internal section of the Uruguayan government's network, where they could view citizens' information or extract data from databases, since it contains most of Uruguay's valid ID

Desde el primer momento LaPampaLeaks ya afirma esto pero Juan Pablo [a las 5AM] lo muestra como si fuera la desmentida del año cuando desde el primer momento se dejaba claro esto... Tambien “Expertos cuestionan la..” mas abajo veremos quienes son esos “expertos” ;)

Los otros ataques "falsos" de PampaLeaks

Según el análisis realizado por la empresa de ciberseguridad **BCA LTD**, una de las publicaciones atribuidas al alias "Uruguayo1337" fue una supuesta filtración vinculada a la cadena de supermercados Ta-Ta.

si... Los mismos de siempre que vienen hace mas de 1 año como pulgas atrás de la gente de PampaLeaks y lo mas cercano que han estado es exponiendo a un ex colaborador del grupo que era un revendedor del bot como podía serlo cualquiera si tenia tokens suficientes

Y como era de esperar como mostramos antes.. En la misma noticia que salio justo ahora cuando estamos escribiendo esto.. En la misma noticia referente a des meritir [manipulando y omitiendo información] de PampaLeaks.. También es mencionado Expresidents pero a diferencia de nosotros.. No hay nada negativo al respecto y son totalmente neutrales

☰ EL OBSERVADOR / CIENCIA Y TECNOLOGÍA / SEGURIDAD INFORMÁTICA



El otro ataque a las cédulas



El 12 de setiembre de 2024, **el grupo ciberdelincuente ExPresidents** puso a la venta un acceso a un sitio web gubernamental vulnerable que permitía consultar datos de ciudadanos uruguayos utilizando únicamente el número de cédula de identidad.



Según describieron los atacantes, el sistema devolvía información como nombre completo y fecha de nacimiento, incluidos datos de menores de edad.



Para coronar todas estas afirmaciones.. Tambien afirman que exajeramos el ataque a la pagina web de Buquebus cuando nosotros no tuvimos nada que ver con ese "defacement".. No es tan dificil investigar bien buscando el hackeo a dinacia y el hackeo a buquebus y ver que "LaPampaLeaks, Bogotaleaks, uruguayo1337" y "vladi, gov.eth, etc" no son los mismos



EL OBSERVADOR / CIENCIA Y TECNOLOGÍA / SEGURIDAD INFORMÁTICA



Otro de los episodios señalados por la empresa fue el **ataque reivindicado contra Buquebus**. Según el análisis técnico, no se habría tratado de una intrusión al sitio



principal ni a los servidores centrales de la compañía, como se difundió inicialmente en redes y canales de Telegram.



Lo que mas nos da gracia y es realmente patético es que antes de pensar que fallaron y que se pudieron equivocar afirmando que uruguayo1337 era nuestro lider, lo siguen afirmando después de los comunicados nuestros y nos adjudican no se que de Tata??

Sin mencionar que es la misma empresa y medio de comunicación que prefirió hacer toda una investigacion publica sobre un supuesto lider de una organización criminal sin verficar nada y pudiendo trabar investigaciones serias del ministerio del interior y interpol solo por tratar de obtener un par de clicks en noticias y 2 mil o 3 mil visitas en un podcast de Youtube...

El “periodista” como se refiere a Expresidents: <https://minochinos.com/embed/ucre1bgegfvj>
[“Expresidents, ahora Expresidents se esta sofisticando cada vez mas” “esta montando su propia infraestructura tecnológica y esta atacando con mucha mas relevancia...””]

El “periodista” habla de la pelea falsa: <https://minochinos.com/embed/15ah62b4s92b>
[se inventa toda una historia falsa en “foros” y cambia el contexto de un doxeo hace 1 año como se mostro en el otro PDFs dirigido a desmentir la “investigacion” de BCA LTD]

Exclusiva del “ataque” a HG de el observador: <https://minochinos.com/embed/gutu9tsdh66g>

Relación entre el periodista de el observador y mauro de BCA LTD:
<https://minochinos.com/embed/r0atfv20tf3d> [“Full Trabajo entre los 2”]

Demostracion de como se inventaron una pelea: <https://streamable.com/e/fyz720>
[Desmintiendo en vivo como mienten descartamente siendo datos totalmente verificables]

Mintiendo haciendo referencia a que el arresto de vladi [hacker de buquebus] fue despues de la investigacion de BCA LTD en el observador: <https://minochinos.com/embed/u2xy1wbsi9mi>

Panelista del programa donde se mostro la “exclusiva” del “lider de pampaleaks”, en la mitad diciendo como curiosidad “ese es el logo de expresidents” cuando ese logo era el de BCA LTD y el periodista no supo donde meterse: <https://minochinos.com/embed/q2g1zd8ic9p1>

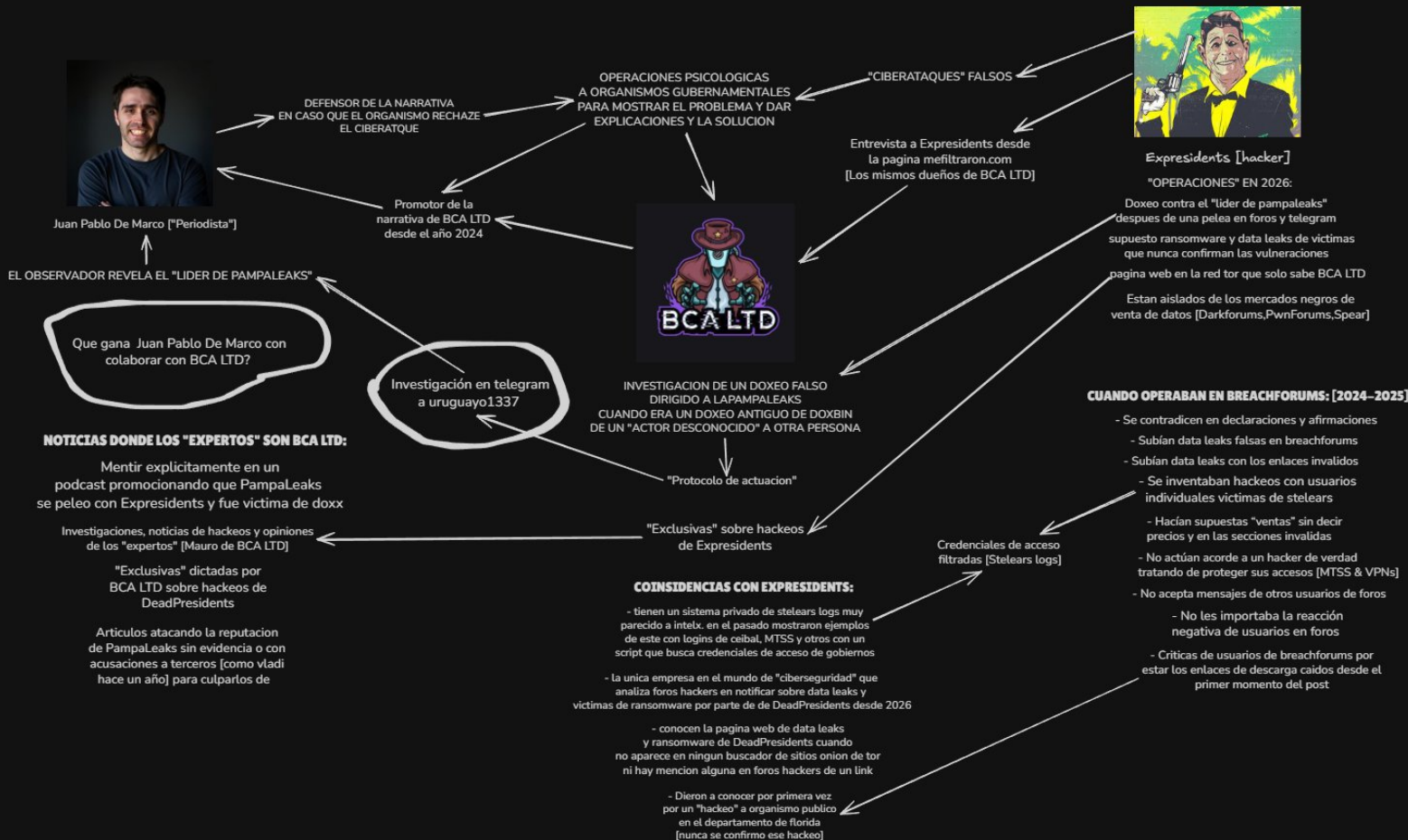
Lista de fuentes de todas las anteriores paginas que faltaron por espacio:

- <https://www.elobservador.com.uy/ciencia-y-tecnologia/estas-son-las-falsas-filtraciones-pampaleaks-las-cedulas-y-un-supermercado-n6045146>
- <https://darkforums.su/Thread-DATABASE-uruguay-DNIC-5-8M-Database-Citizens-Leak-Free>
- <https://telemetr.io/es/channels/2942705940-pampabotrefes>
- <https://sheriff.birminghamcyberarms.co.uk/plans>
- <https://www.elobservador.com.uy/ciencia-y-tecnologia/ciberdelincuentes-filtraron-1-gb-informacion-servidores-tickantel-como-afecta-los-usuarios-n6044143>
- <https://www.elobservador.com.uy/ciberdelincuentes-filtran-accesos-servidores-una-empresa-antel-n6043757>

CASI EL FINAL DE LA INVESTIGACION

Ya a este punto es muy evidente quien esta y quien siempre estuvo detrás de Expressidents y la razón de porque lo utilizan. A diferencia de las anteriores paginas, ahora soy yo LaPampaLeaks quien escribe y sinceramente me parece que Juan Pablo de Marco y BCA LTD la cago bastante metiendo a Expressidents y afirmando lo de "el líder de pampaleaks" en vez de dejar trabajar a la policía en paz.. Decidieron ir por los clicks fáciles y pocos miles de visitas..

Mapa con todas las conexiones antes mencionadas:



Fin de la investigación publica

- Signal: lapampaleaks.33
- Canal de telegram: <https://t.me/lapampanoticiasarg>
- Cuenta de LaPampaLeaks: @pampalix
- Pagina web: lapampaleaks.pages.dev