LOS VENDE HUMO DE BCA LTD Y EXPRESIDENTS

This document shows that Expresidents is an operation created in 2024 by BCA LTD [Birmingham Cyber Arms LTD] to infiltrate hacker forums, where they would upload fake data leaks so that BCA LTD could report the “problem” and provide explanations for what had happened. They created both the problem and the solution until early 2025.

In May 2026, this company “conducted an investigation” filled with lies and distorted facts to claim that they had identified the “Leader of PampaLeaks” and that it all stemmed from a doxxing carried out by “Expresidents.” BCA LTD fabricated a dispute because they thought they actually had the data on “The Leader of PampaLeaks” and that he wouldn’t be able to defend himself

The reality is that they had the information of a former collaborator who was merely an authorized reseller of PampaBot [just as almost anyone with enough tokens to use a command to transfer tokens to another Telegram user could have been]

- **Contributions:** BogotaLeaks, LaPampaLeaks, and 2 other members of PampaLeaks
- **Editors:** BogotáLeaks, Traductor and two other members
- **Investigador:** Researcher

Table of Contents:

2-15: Demonstrating how Expresidents is not a legitimate hacker on forums and how the BCA LTD group operated to create a false issue on forums, deceive users with fake leaks, and post on X before sending it to El Observador to make something false appear real in the narrative...

16-24: Showing how BCA LTD was the one that introduced Expresidents in 2024, even with a one-hour time difference. How BCA LTD, using an alternative project run by the same owners of BCA LTD, conducted an “interview” with Expresidents, and how the Observer helped inflate their image and make a false narrative seem rea

25-29: Debunking the False Hack of HG [An ANTEL Subsidiary] and Tickantel

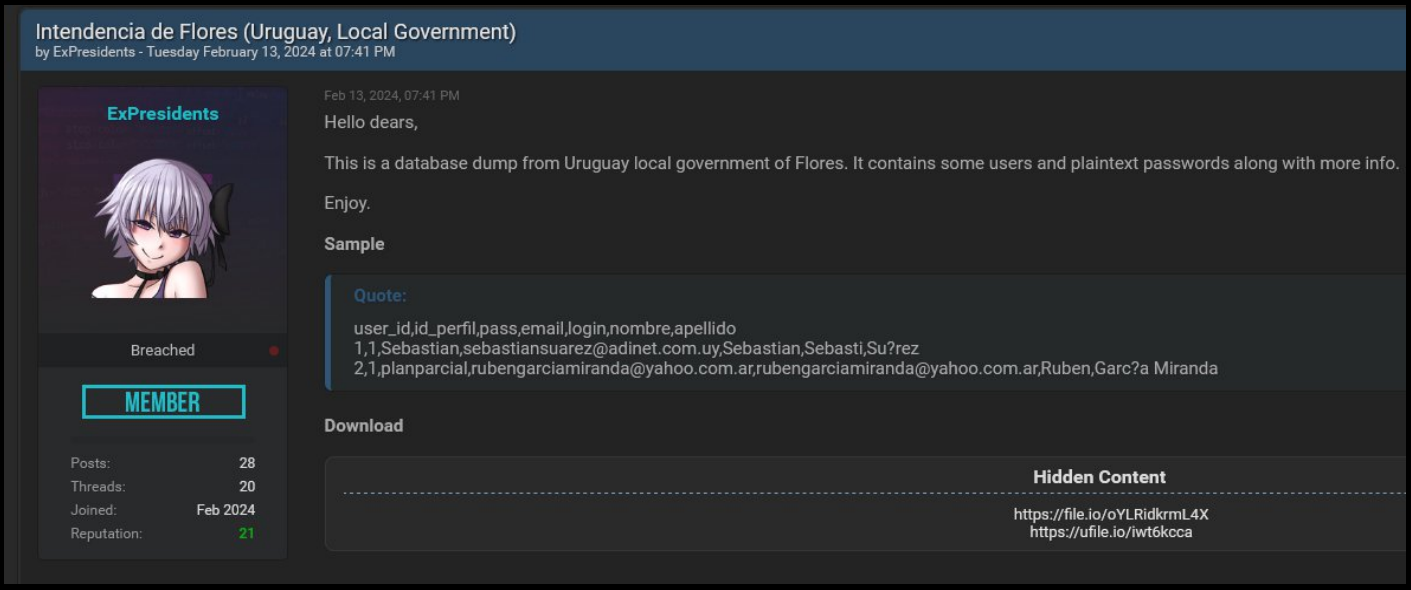
30-31: Debunking the fabricated feud between LaPampaLeaks and Expresidents, as well as demonstrating how it was all intended to build “credibility” for his fake BCA LTD persona on the black markets and in the media... Take down LaPampaLeaks and let only the

32-34: This shows how, for over a year now, Mauro Francisco Caseres [Mauro “Eldrich”], as the owner and founder of BCA LTD, has been obsessed with exploiting the image of *El Observador* by using Juan Pablo De Marco to spread misinformation about us

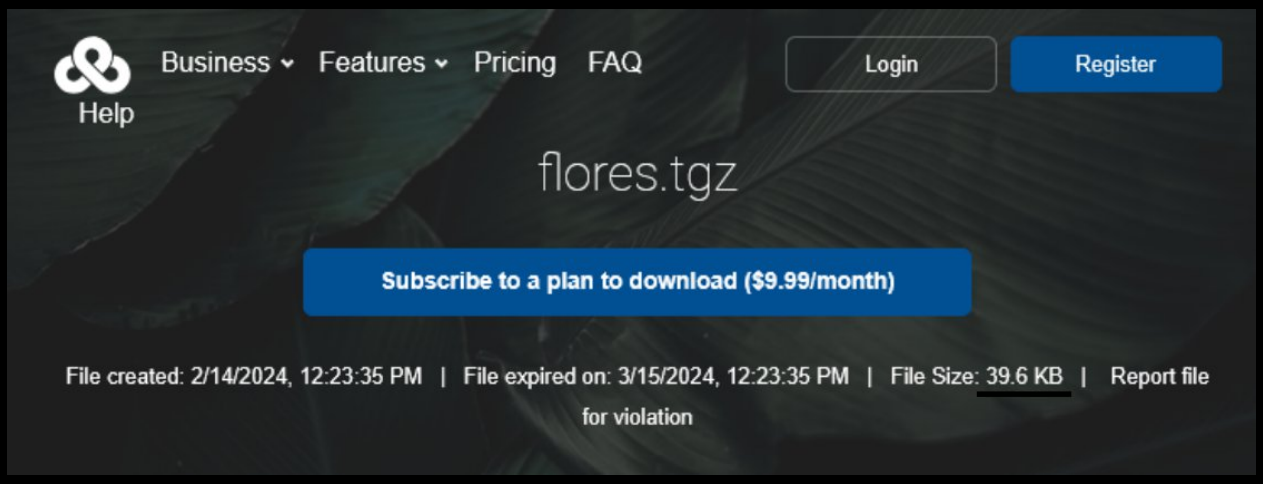
Unlike the investigation titled “The Leader of PampaLeaks at BCA LTD and The Observer,” this one draws on numerous sources and includes screenshots, and everything can be verified by anyone who reads it.

HACKING INCIDENTS INVOLVING DATA LEAKS FROM SUSPICIOUS “DATABASES”

ExPresidents first appeared on Breachforums on February 13, 2024, with a hack of the flower supply department that resulted in a database leak. He claims that the data includes passwords and user information, and has in



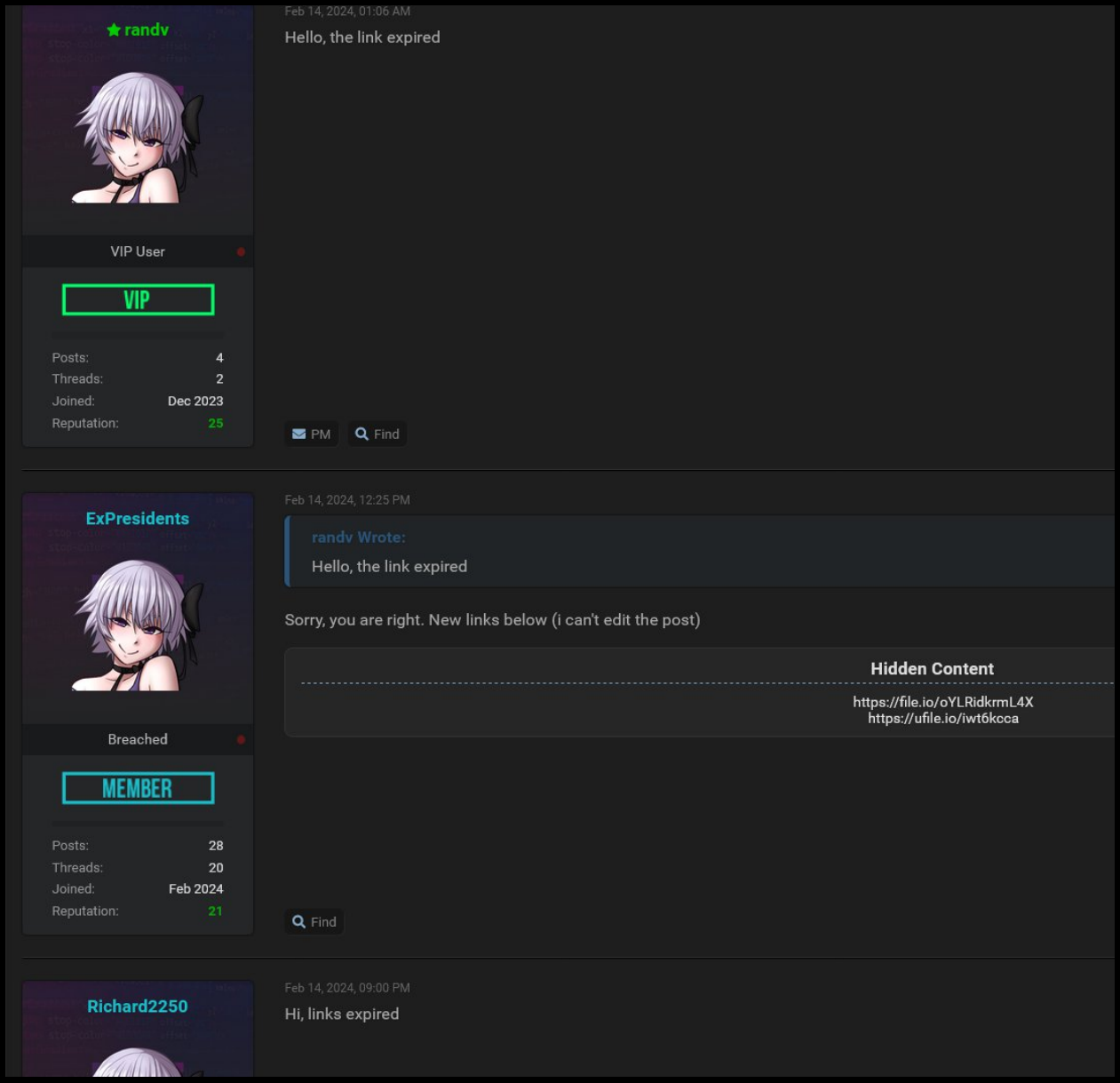
The “DB” is 39.6 KB [not even 1 MB], and since the link is dead / you have to pay, we don’t know what’s inside, but you don’t have to be a genius to know that a decent database isn’t less than 1 MB. None of the samples from LaPampaLeaks ever weighed that little.

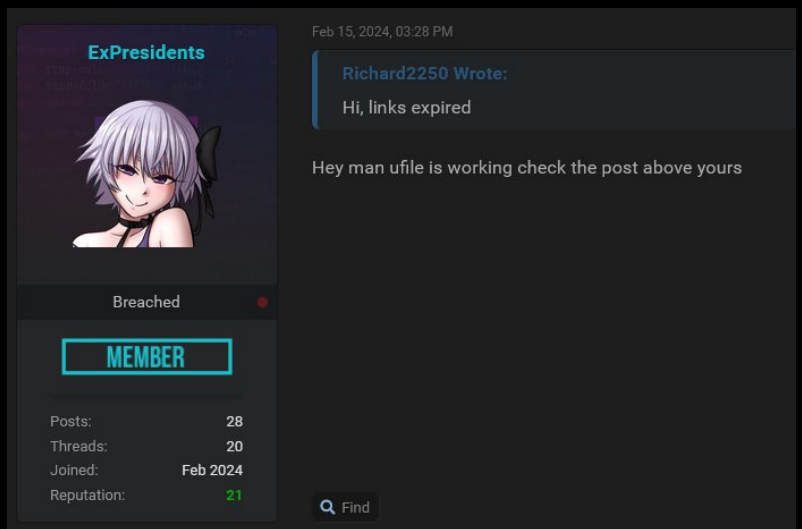


Sources::

- 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

Things get even more suspicious when the first comments come from BF users complaining that the link had expired, and all he did in response was post the same two links he had already shared earlier [he claims he couldn't edit the post].



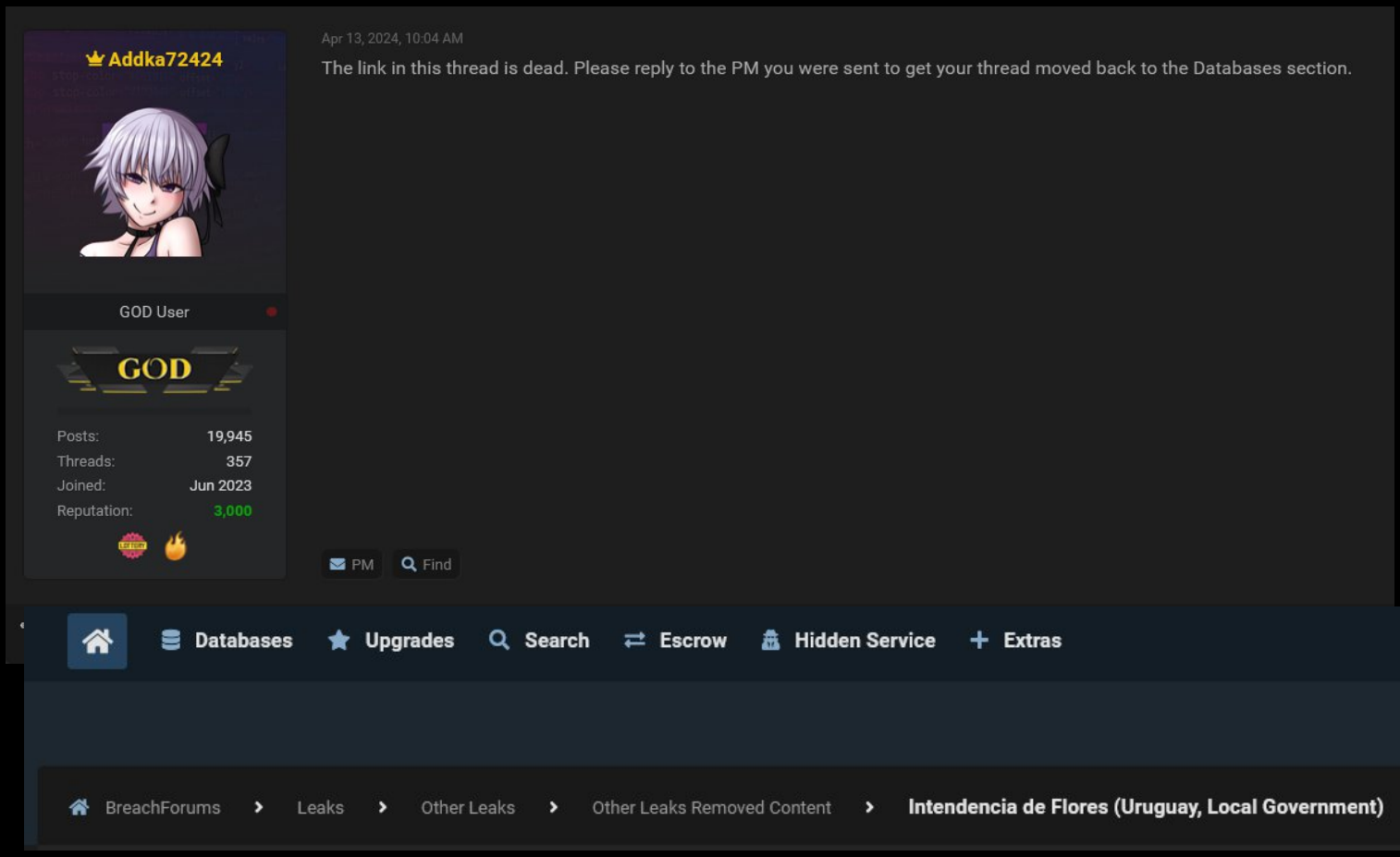


Next, user Richard2250 tells him that the link has expired, and he replies that it works and that the link was right above it.

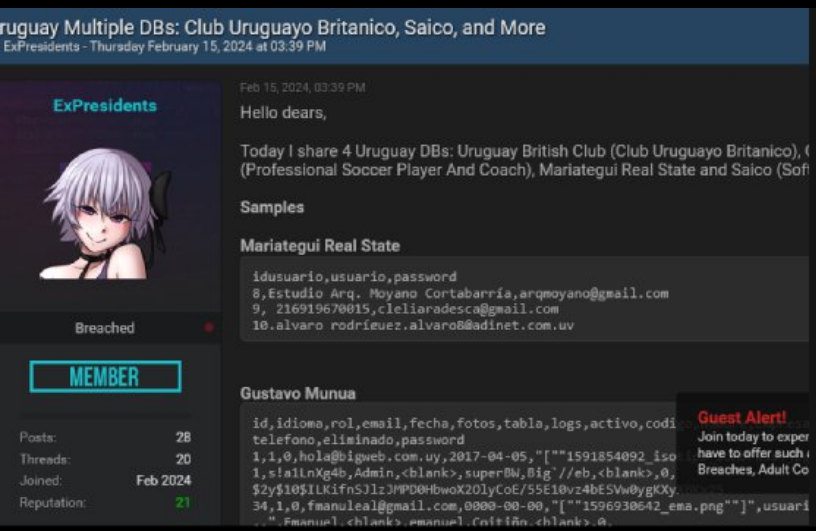
Remember that these are the same links I posted in the original post, so if they were down before... the ones he mentioned are down too, because they're the same...

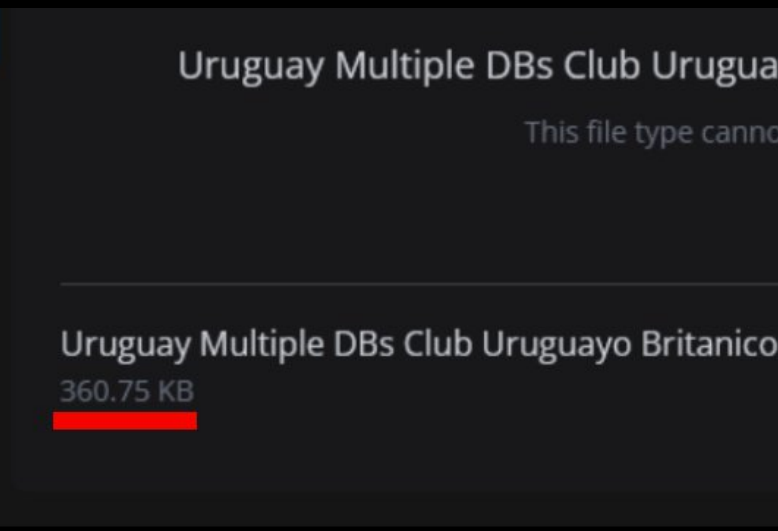
So, not only does it seem like they aren't interested in users downloading their database... but the database itself is surprisingly small for a government database.

Then some people said they worked, others said they didn't... And in the end, the thread for Expresidents' post was locked by an admin to prevent further comments and moved to “Other Leaks Rem....” because the links were broken. The admin told him to contact him to move the thread back [to update the broken link]. It's May 2026, and the post is still in the same state...

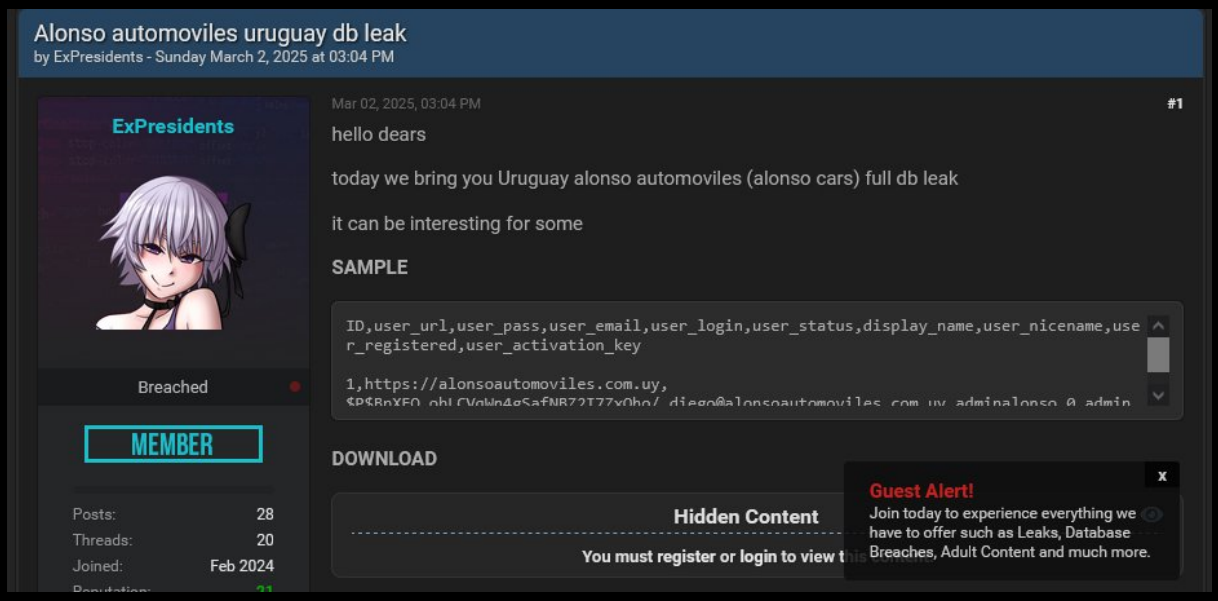


The following post allegedly leaks several databases from Uruguay at once. All of these databases combined, in a 7z file, weigh in at just 360 KB. If someone were to gain access to a private system containing many databases

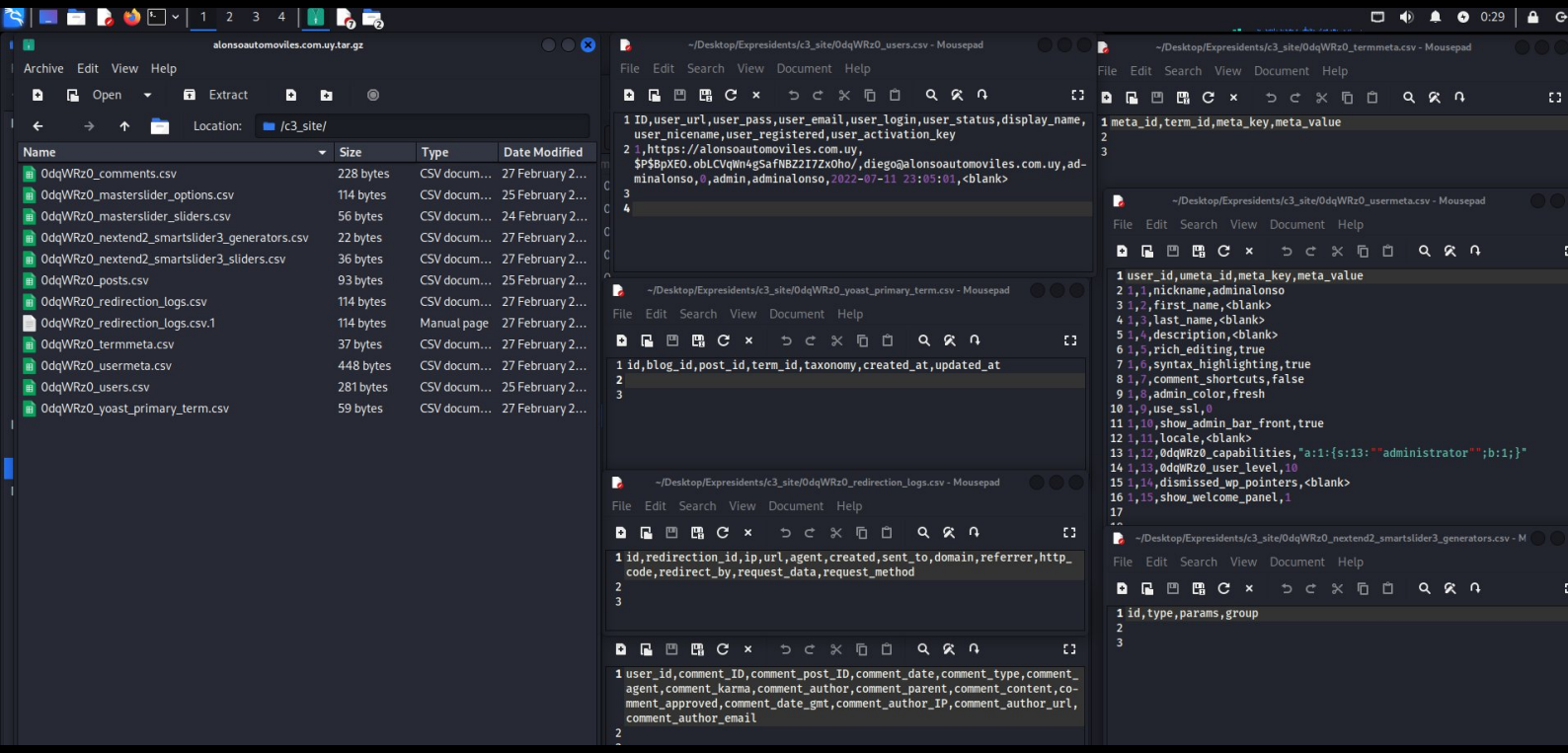




In the post where the only reply is from LaPampaLeaks... He posted about a hack of a car website in Uruguay, along with a download link and another link where you had to pay with forum coins to download. The only one who did that was LaPampaLeaks



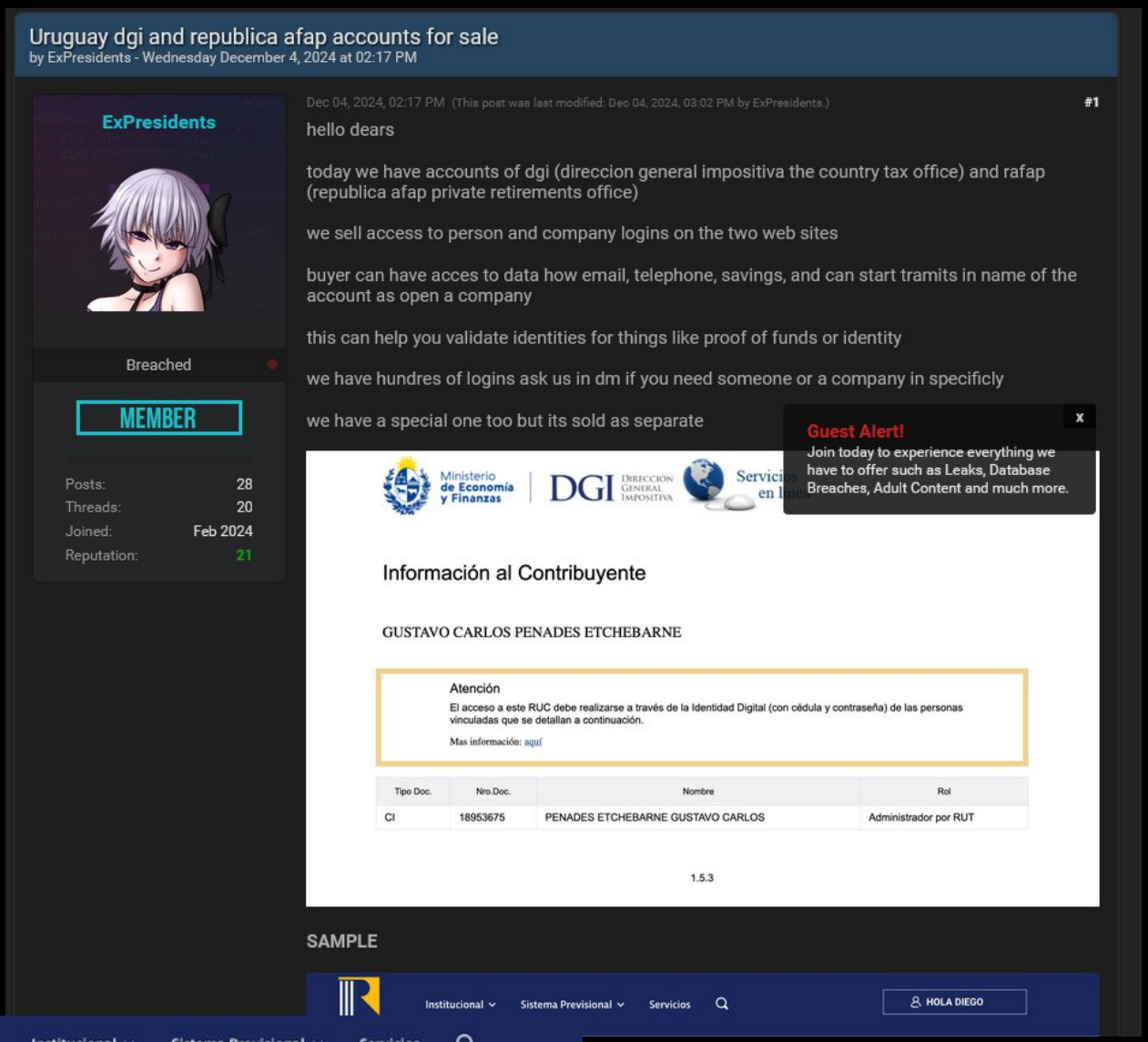
All I found were a few .csv files containing nothing more than frontend information, and in the sample database, there was only one user [the same one shown in the example]. Below is a screenshot sent by LaPampaLeaks showing all the files from that “hack” and “leak.”

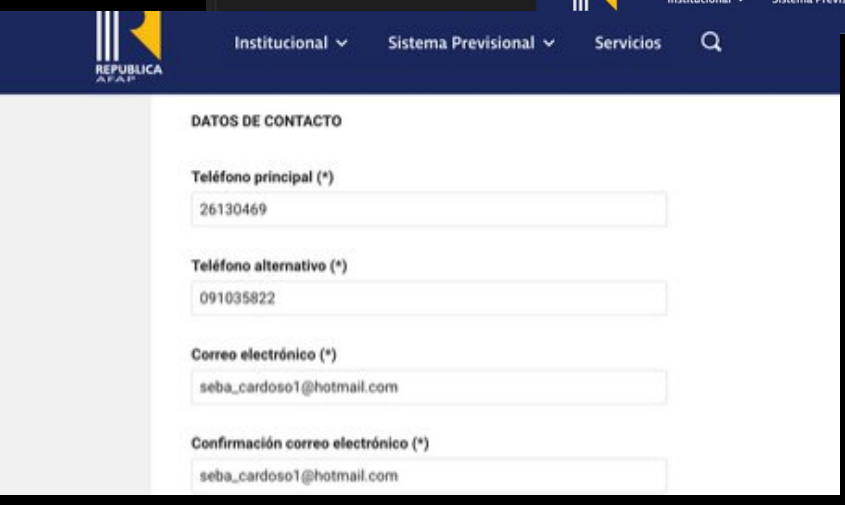


- https://archive.ph/UUFPq [Post en clon de BF]
- El zip esta en la misma carpeta que los pdfs de todo esto
- https://archive.ph/i6Eoy [Post del hackeo a Club de futbol uruguayo]
- https://archive.ph/tqyaX [archivo de descarga del hackeo a Club de futbol uruguayo]

Expresidents operates by uploading databases of highly dubious legitimacy, even making it difficult to download them by forcing users to pay with the group's own currency [to obtain these coins, users must pay the forum or post messages] or by creating temporary links.

Later on, we'll see what interests they might have in acting this way... Now we'll look at how Expresidents pretended to hack the DGI and how they allegedly "sold access" to DGI and República Afap accounts... And how they allegedly added information about "sanctions"...





As people who are in the market, we're very good at spotting what's wrong here...

First of all, it's in the "other leaks" section instead of the sales section... Second, it doesn't list any price for selling access to the accounts... Third, it doesn't provide any contact information or mention that you should message the forum administrator to purchase access to the accounts

It's also clear that someone hacked into an account [more info belowLo que hizo

“Expresidents” involves gaining access to the account of a user infected with a keylogger, something that can be easily detected using Intelx and other tools. After analyzing the “hack,” AGESIC and the DGI stated that it is most likely that the users’ accounts were stolen directly from them.


www.elobservador.com.uy/ciencia-y-tecnologia/hackers-accedieron-cuentas-usuarios-la-dgi-y-republica-afap-y-aseguran-poder-hacer-tramites-su-nor

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

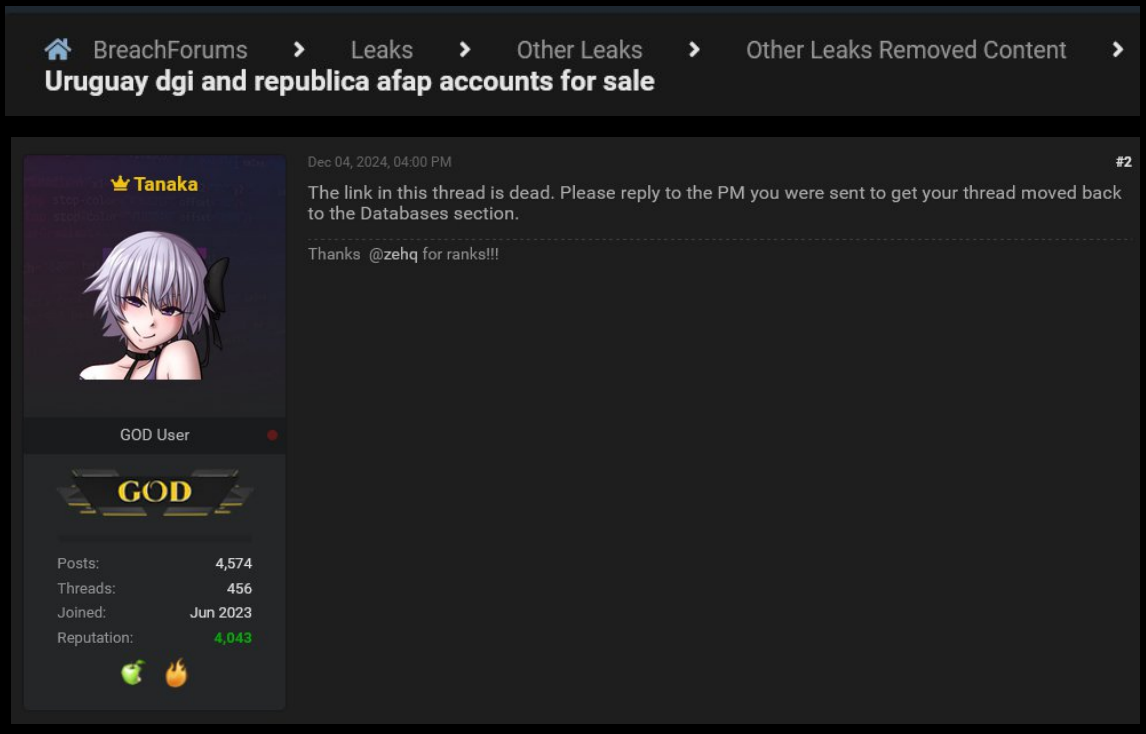
Desde la DGI aseguraron a El Observador que están investigando el inconveniente junto al Centro Nacional de Respuesta a Incidentes de Seguridad Informática (Certuy).

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.

In addition to accessing personal accounts, he used the inspection tool to edit the documents and HTML code; he then entered the personal information of people he knew in Uruguay.

There were no user comments on Breachforums because “expresidents” posted everything in “Other leaks” rather than in the forum’s sales section... A moderator closed the thread so that no one could comment and moved the post to the deleted posts section.


BreachForums › Leaks › Other Leaks › Other Leaks Removed Content ›

Uruguay dgi and republica afap accounts for sale

Tanaka

GOD User

GOD

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

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!!!

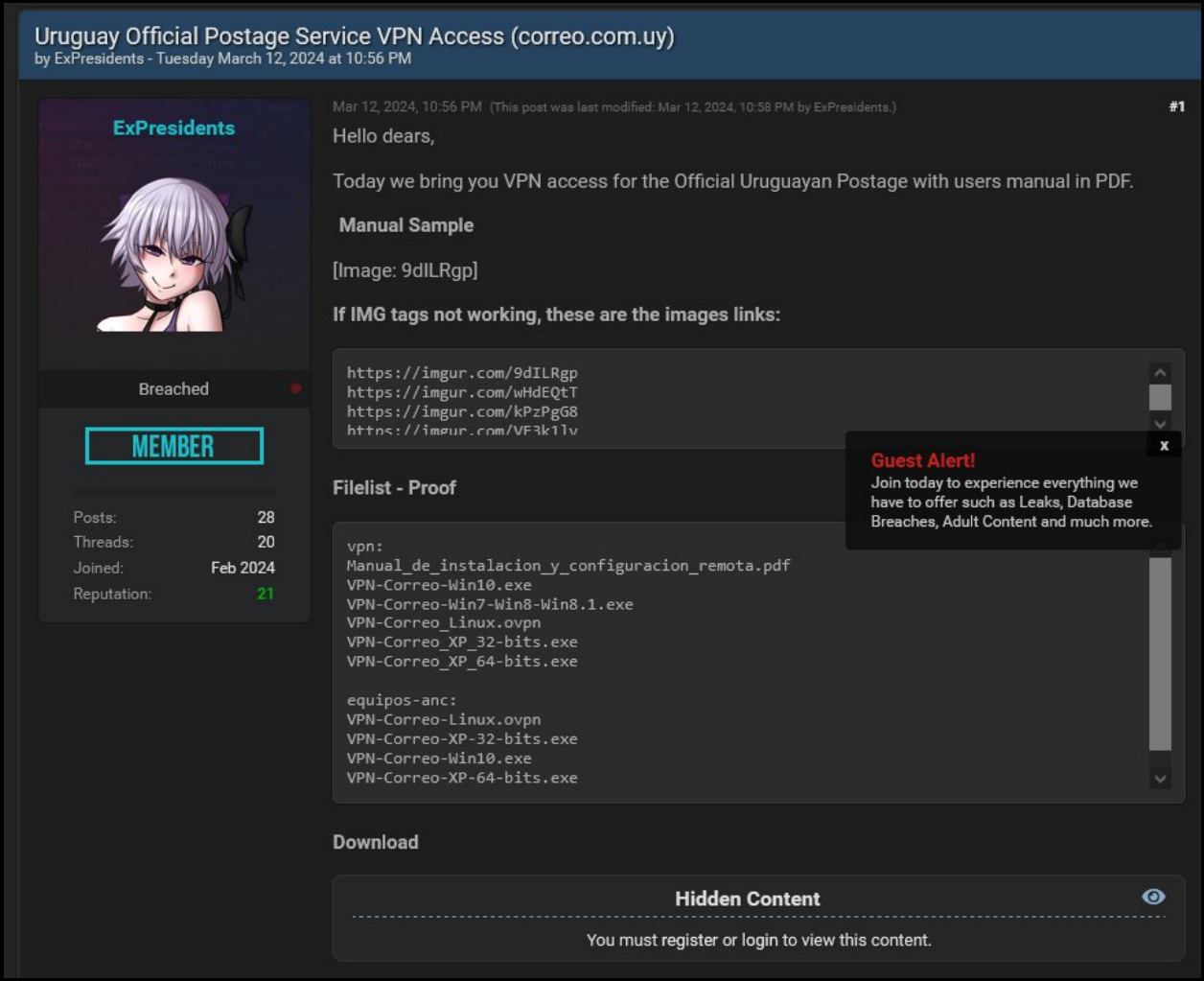
It’s not hard to see that “expresidents” doesn’t care whether forum users buy from him or whether the DGI blocks the ALLEGED access he had. Any seller on forums likes to make minimum prices or contact methods clear; furthermore, what a decent hacker would do is create scripts to steal information from each account and build a database by sending thousands or millions of requests to the DGI server.

But he chose instead to announce that he had insider access to a government agency that was the most well-known hacker forum on the entire internet—one that had been infiltrated by Interpol, journalists, and so on. This would only lead them to patch the vulnerability or block his login access.

Sources for all of the above:

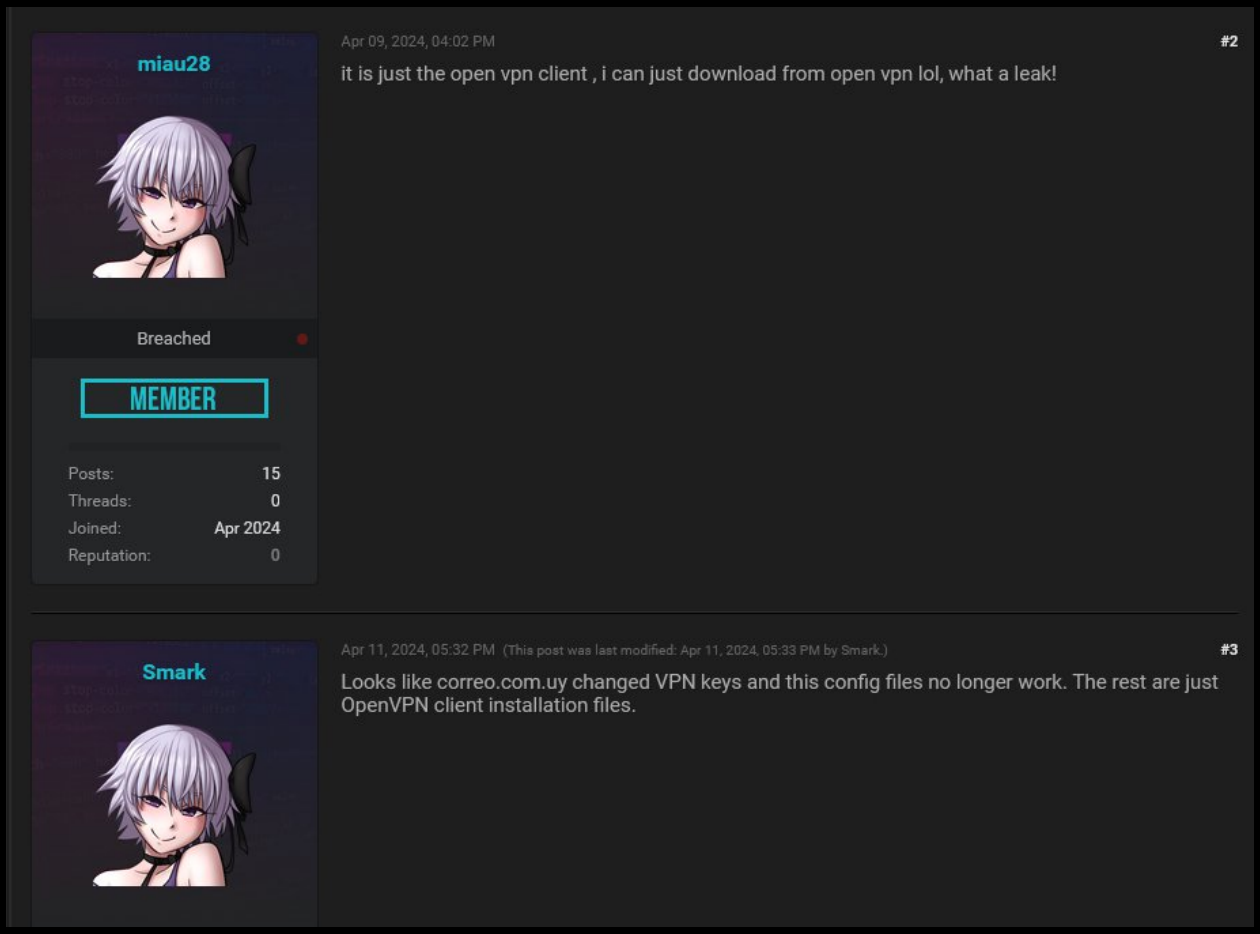
- https://www.elobservador.com.uy/ciencia-y-tecnologia/hackers-accedieron-cuentas-usuarios-la-dgi-y-republica-afap-y-aseguran-poder-hacer-tramites-su-nombre-n5973497
- https://archive.ph/Bg8b9

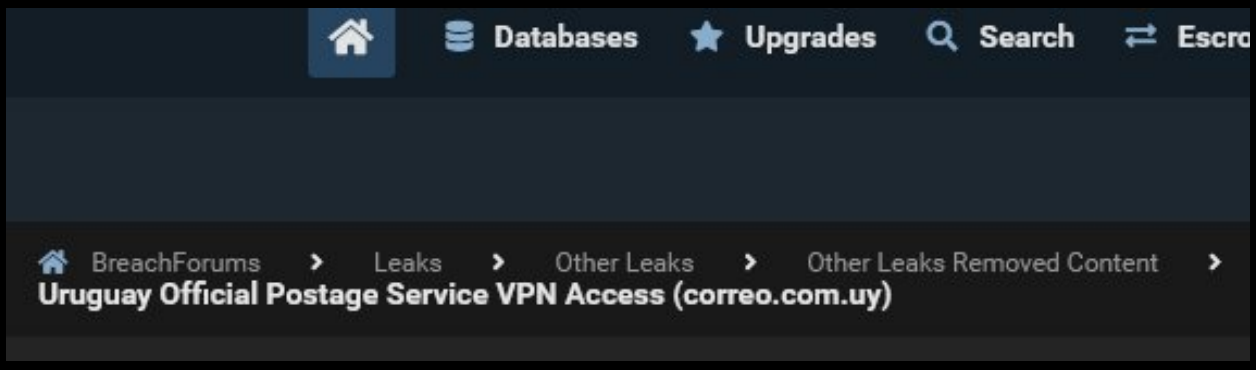
Another “access hack” involved an alleged breach of the Uruguayan email service’s VPN, where the hacker uploaded a VPN installation guide and OpenVPN files, renaming the official OpenVPN .exe files from “OpenVPN” to “VPN-orreo.”



.exe files can be easily found on the official OpenVPN site, and this had already been pointed out in the comments; furthermore, an admins deleted the post again from the “Other leaks” section and moved it to “Deleted leaks”... Once again, the same procedure is being repeated.

Users are complaining about this very issue and sarcastically pointing out that they could have downloaded it from the OpenVPN website... Another user also claims that the VPN access keys don't work... Then the third comment is from a former moderator moving it to the section for posts deleted for being invalid...



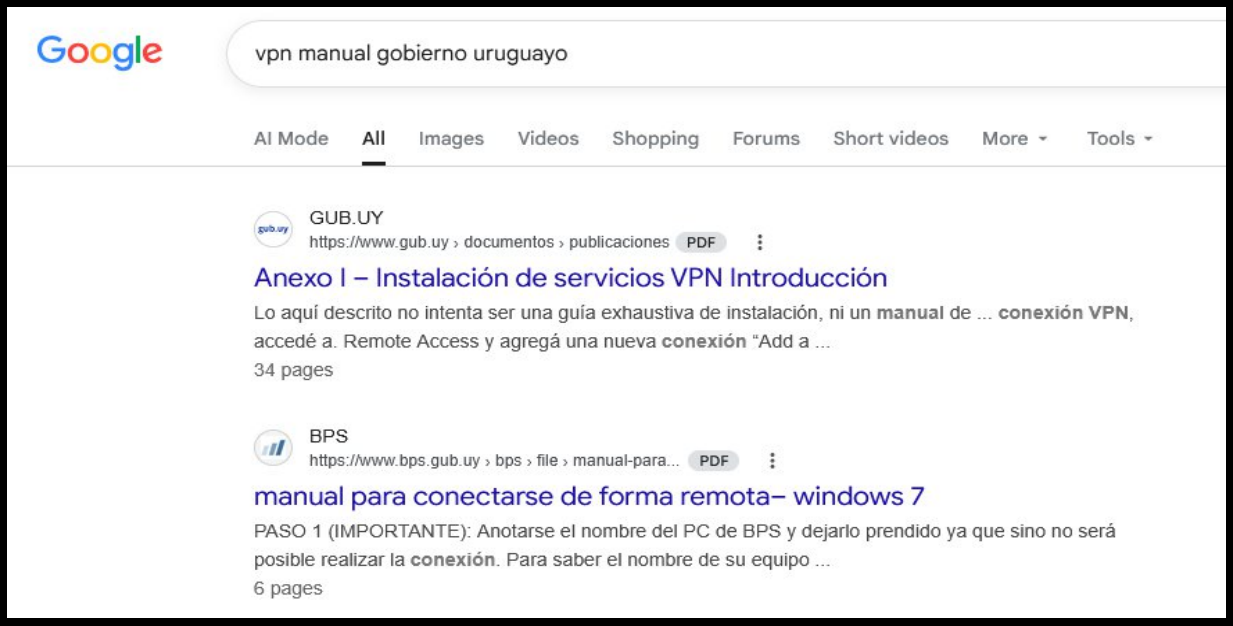


No self-respecting hacker would ever leak a VPN connection... If they do, it’s either because they don’t know what to do with it or to draw attention to themselves... A self-respecting hacker would use that VPN to elevate their privileges on the system and search for vulnerabilities in the most heavily protected internal systems... But not him...

Fuentes de informacion:

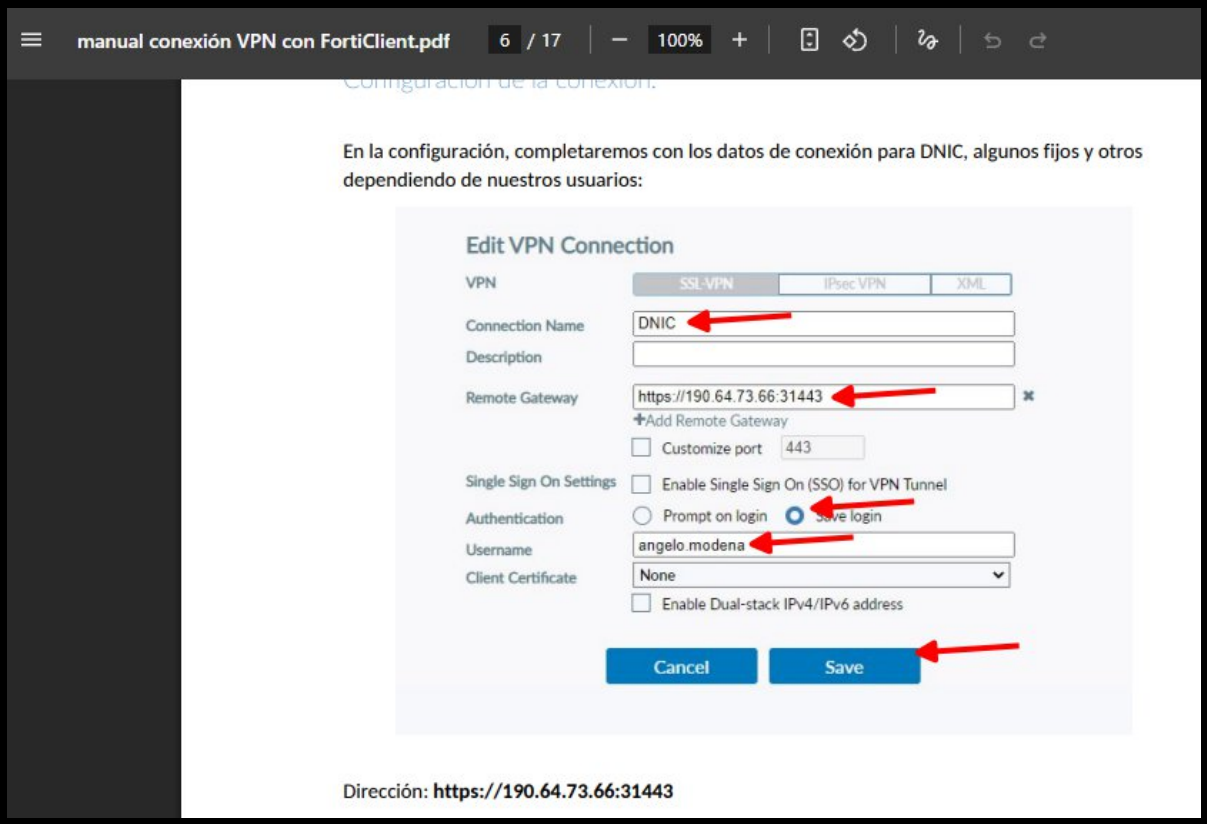
- https://archive.ph/qhR3a [Post de la VPN]

For those who are curious... It's as easy as Googling them to find VPN guides for connecting to most public and private organizations...

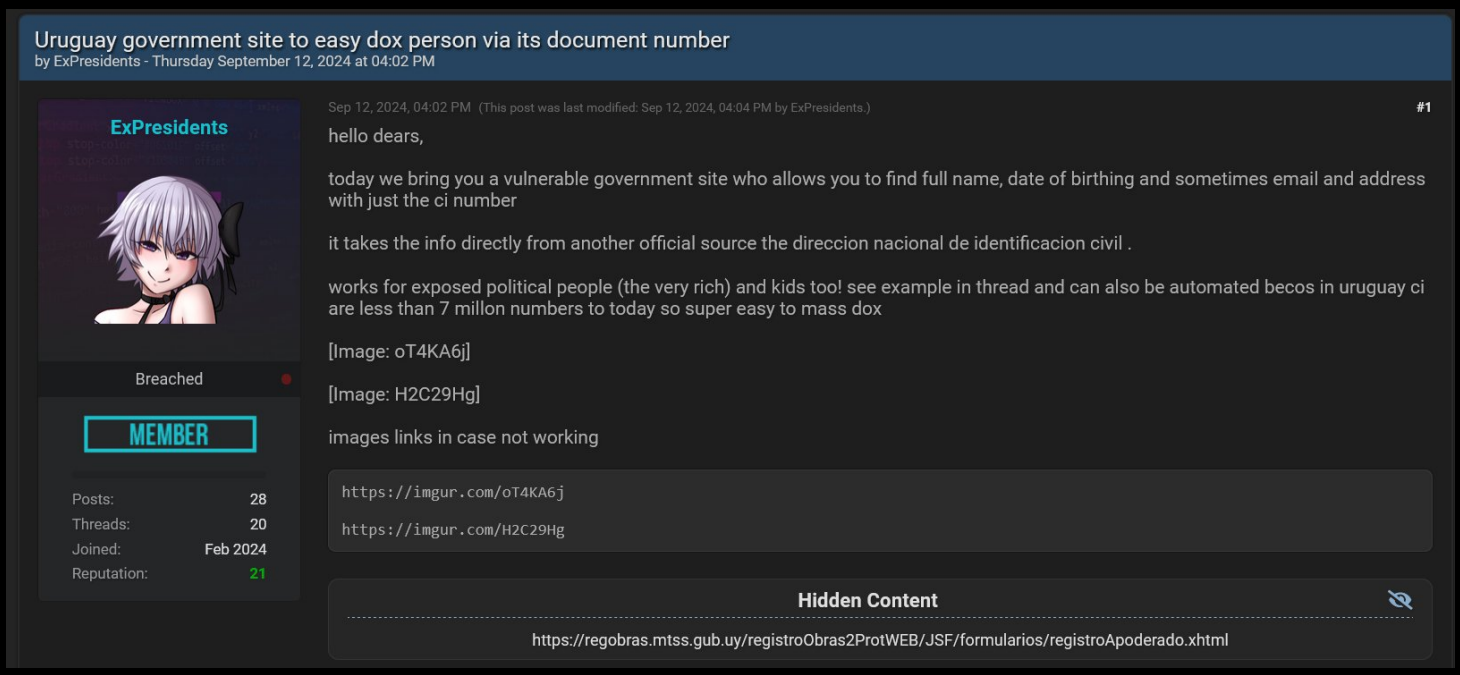


Here's a screenshot from Fortinet's VPN manual showing how to connect to the DNIC servers... It even includes the exact IP address and port for logging in... With a sample username... Because those incompetents at AGESIC don't hide their internal files very well and just leave them out in the open

But we don't post about it... Because while we care about preserving login credentials that could help us escalate privileges on systems... Expresidents don't?

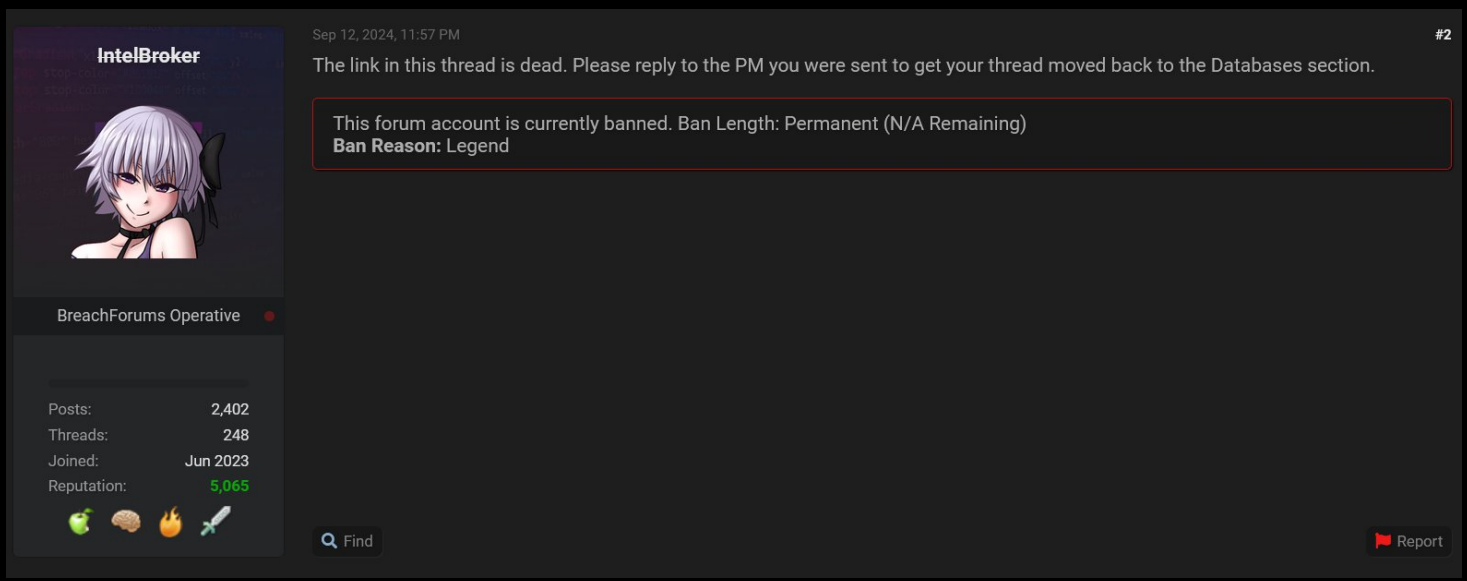


In addition to these suspicious practices... He posted a message that included a clickable link with three Breachforums coins obtained from an old public MTSS form that automatically populated data using a DNIC API, sometimes sharing addresses or email addresses thanks to an old MTSS API that queried data from its database.



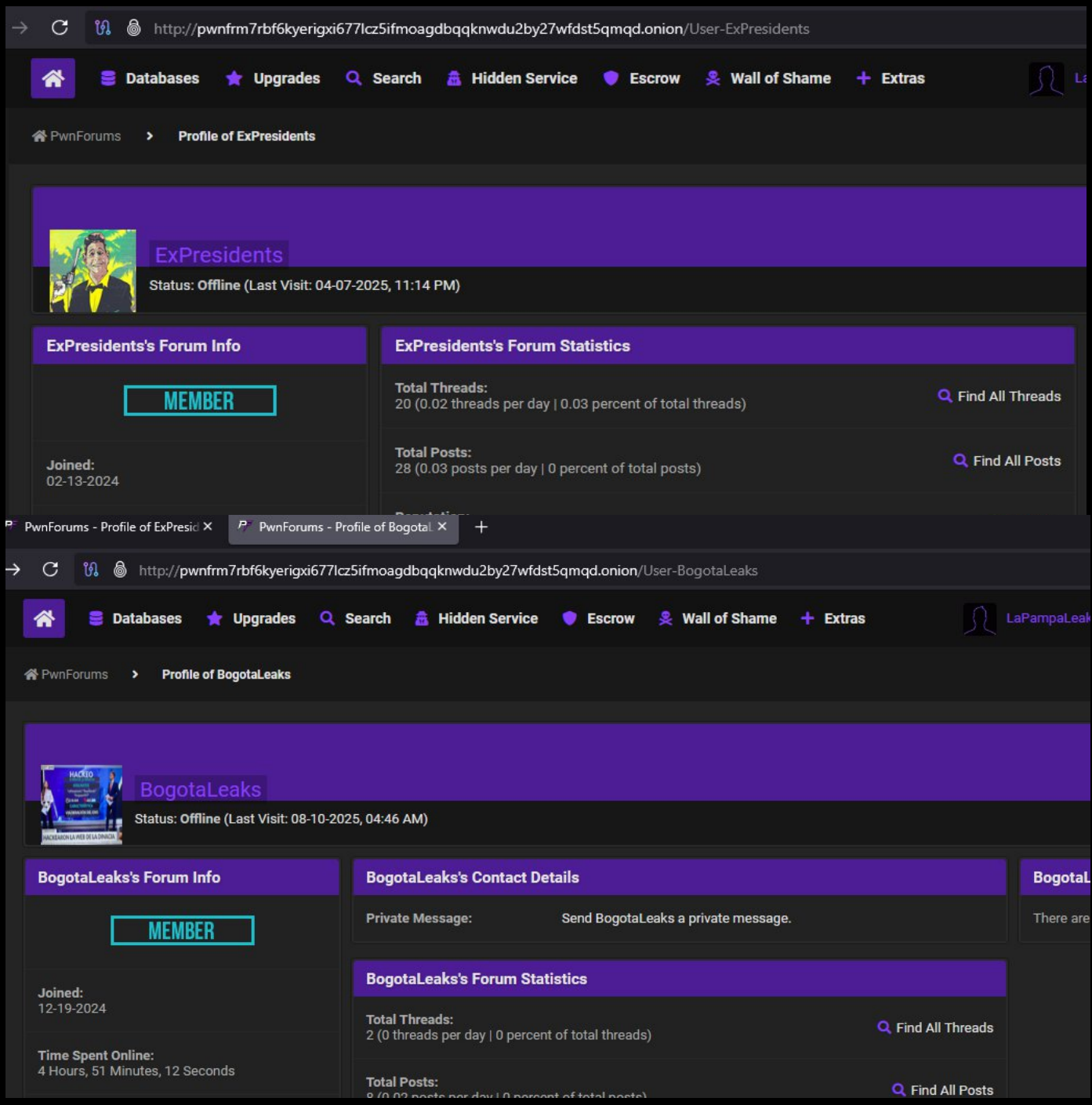
A typical hacker would scrape that form relentlessly to recreate the database based on millions of requests... But not him—he posts it online while mentioning that you can find politicians, millionaires, and “even children” on it, which is the perfect mix of three concepts to get someone from AGESIC to come along and take down that public form.

What happened? A few hours later, the link was no longer working... There wasn't even a single comment from a user thanking him, since, as we know, the forum was locked unless you had forum coins... The only comment was from an administrator... a few hours after the post... notifying him that the link was no longer working and moving his post to the deleted section.

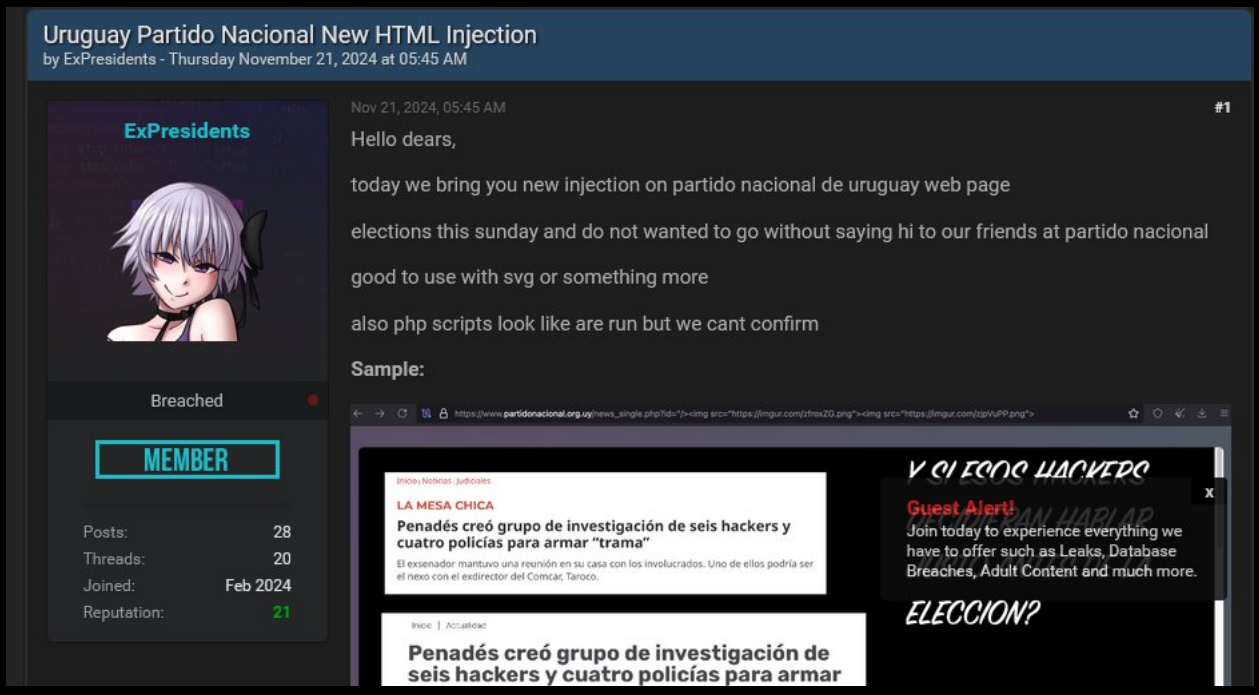


In addition to the suspicious behavior of Expresidents... The fact is that direct messages via the forum are completely disabled [this isn't the default setting]; he set it up that way on purpose, and the only reason for this is to avoid contact with other forum members. Comparing the forum accounts of ExPresidents and BogotaLeaks, it's easy to see that this feature is missing.

- 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



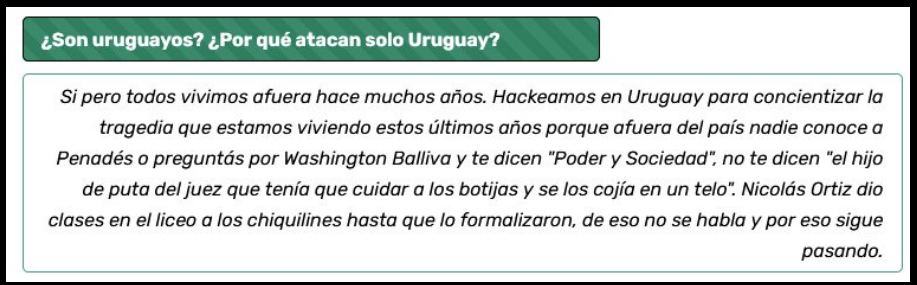
Another “hack” targeting expresidents [XSS]—it's basically easy to pull off on almost any government website because no one at AGESIC cares about these kinds of vulnerabilities... The hack against the “Partido nacional” involved inserting HTML code into the URL and the website's forms....



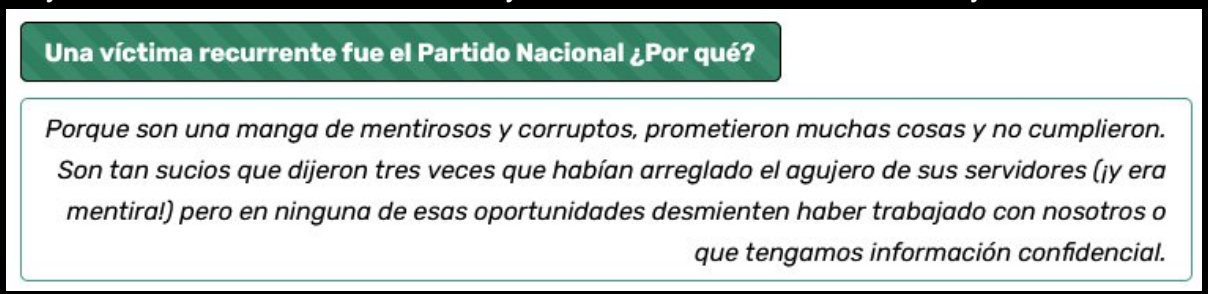
This doesn't affect anyone who doesn't have the link with the XSS... No user of the National Party was affected in any way visually on the page... No one knew about it until this person posted the valid XSS on the page... https://archive.ph/OAtJm [post link]

Interview with Ex-Presidents:

In addition to basic “hacks,” fabricated leaks, and other practices… When they were interviewed about the “hack” of the National Party, they kept contradicting themselves. First they claimed to be hacktivists opposing Penades and the pedophile network, then they mentioned that the PN never denied having worked with them [remember that in the BF post they referred to the news about hackers working for Penades to find information on victims of pedophilia].

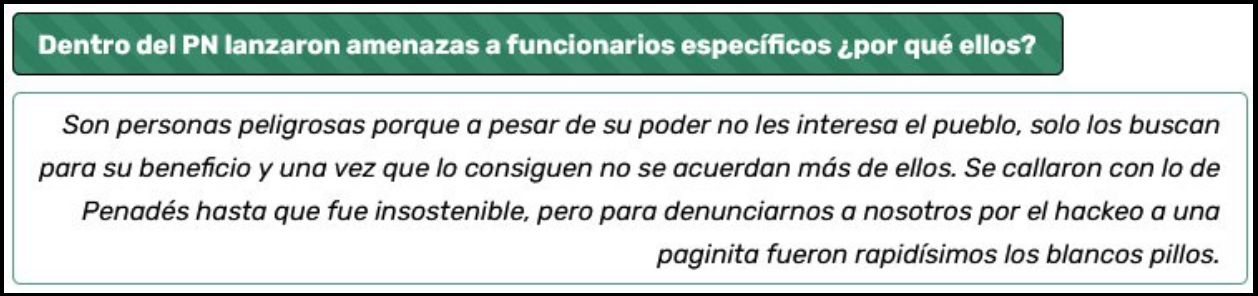


They also called an XSS attack that only affects the front end a “vulnerability in their servers”...

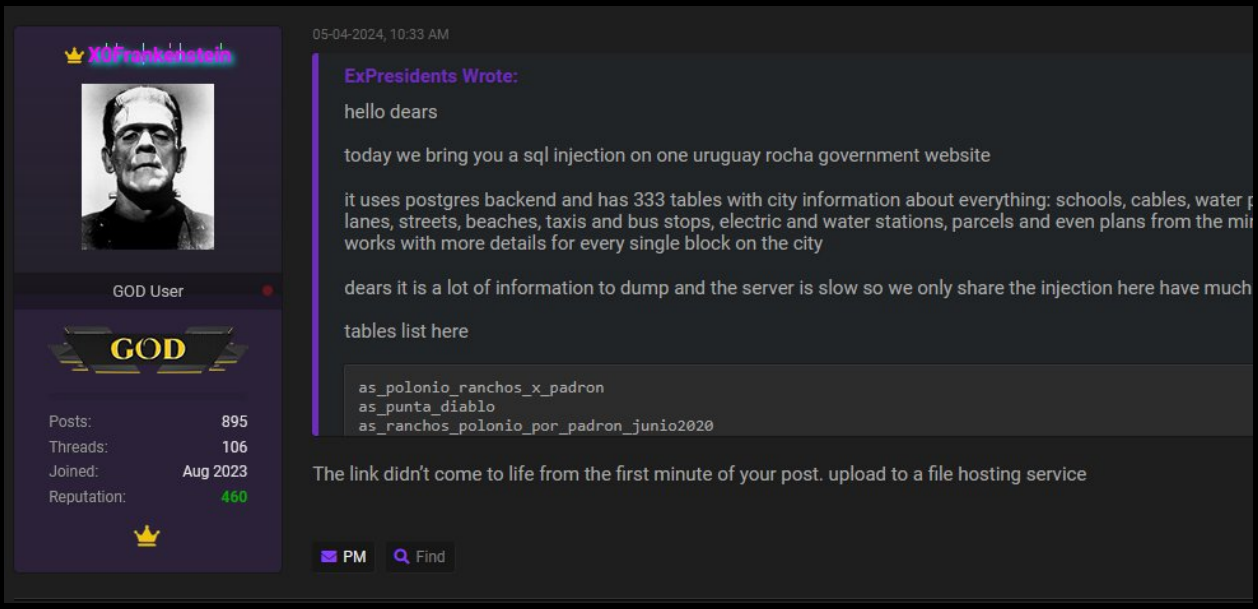


After contradicting themselves in their actions and statements... + throwing shade at them over the XSS issue, calling it a “server vulnerability” when it only affects the frontend... [lying] they’ve changed their tune again, claiming they’re against the PN because they don’t care about the people.... Using the term “white crooks,” which is a phrase the Uruguayan left frequently uses

No one in their right mind with left-wing views would work for the Partido Nacional, let alone gather information on the victims of a pedophile... Unless that person is “up to their old tricks” ;)



We could go on and on about this, but it’s already clear: he has some very strange habits that don’t fit with those of a real hacker... Even in the latest attacks, such as the SQL injection on Rocha’s GOB, his responses consist of complaining that the link didn’t work “from the very moment” Expresidents published the post... A recurring complaint, it seems.



Summary of the above regarding the actions of expresidents:

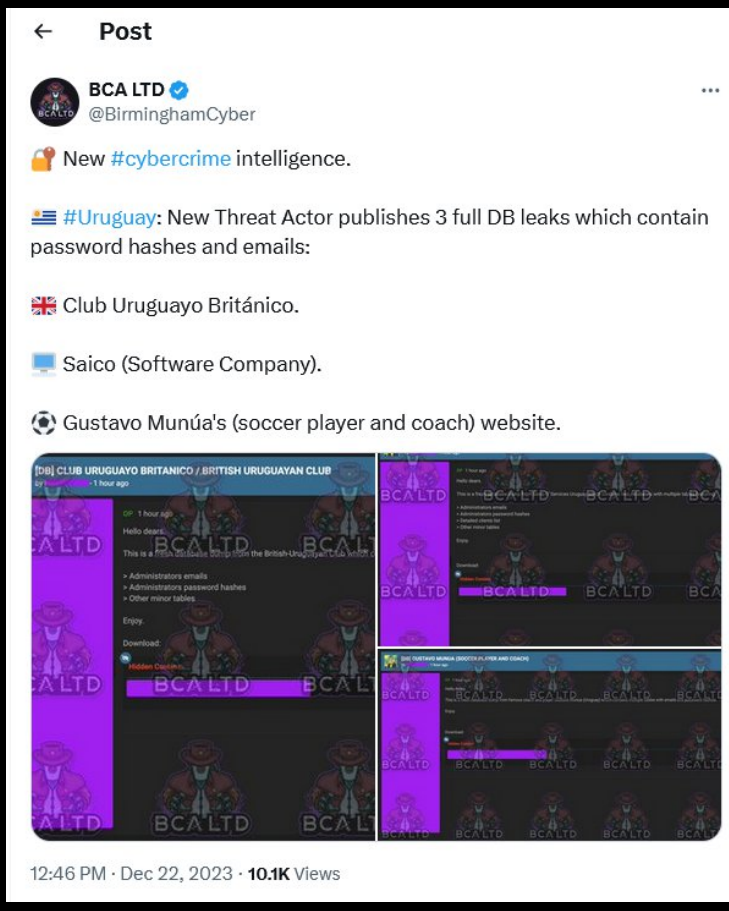
- Their statements and claims contradict each other
- They posted fake data breaches on Breachforums
- They were uploading data leaks with invalid links
- They held so-called “sales” without listing prices and in the clearance sections
- They didn't care about the negative reaction from users on the forums
- They don't act like a real hacker who tries to protect their access
- They aren't well-known in forums or online communities, even though they appear in the news
- They made up a fake fight between our group and theirs...
- Does not accept messages from other forum users
- Messages were posted that could be unlocked using forum coins [which made access difficult]

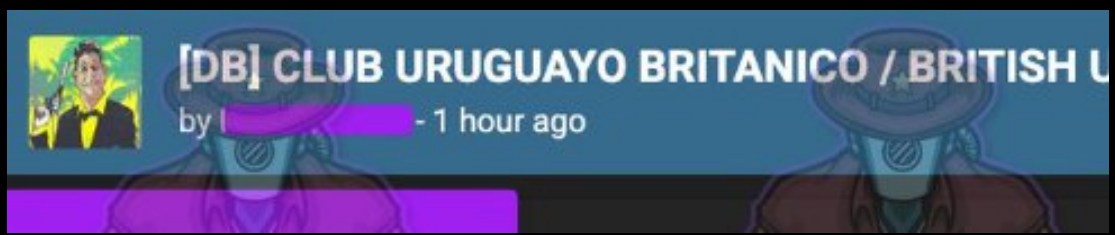
Birmingham Cyber Arms LTD [BCA LTD]

This is a company registered in the United Kingdom under the name of Argentine citizen Caseres Mauro Francisco [ID No. 36006534], which is tasked with investigating the “leader of PampaLeaks” and, through falsehoods, attempts to create a narrative in which Expresidents becomes angry with PampaLeaks and reveals his identity to the world...

We’re going to show how “Expresidents” is a psychological operation/social engineering scheme designed to infiltrate hacker communities and use that as an excuse to generate buzz around BCA LTD while making money, positioning itself as “the savior,” and selling services by scaring people

Who brought Expresidents to light?: BCA LTD was the first to post the day after Expresidents’ first post on BF; as we recall, that first post was a “DB” file that was only a few KB in size. The same goes for the soccer club file, which was also just a few KB. In the case of the soccer club, BCA LTD posted the screenshot just one hour after the original forum post.





POSTS ON X ABOUT EXPRESIDENTS

Every post published on BreachForums by “Expresidents” was reposted within hours or the next day by BCA LTD on Twitter, even those where the fake databases were obvious or the posts had been deleted. It doesn’t matter, because they spread it as news of a new breach.

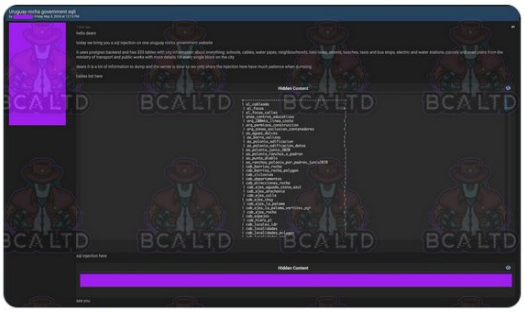
Many of these “breaches” were the ones that Breachforums users complained about—saying the link was down or hadn’t worked from the start—and the links leading to files labeled “DBs” were all fabricated junk that weighed in at just a few KB.

BCA LTD ✓
@BirminghamCyber

New #cybercrime intelligence.

#Uruguay: Threat actor selling SQL injection for Rocha Government Website.

#ThreatIntelligence: @mbec03 (¡gracias!).

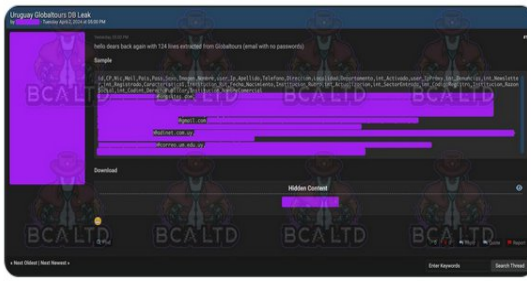


BCA LTD ✓
@BirminghamCyber

New #cybercrime intelligence.

#Uruguay: Threat actor shares a database belonging to Globaltours. It contains 120+ user emails and IP addresses.

#ThreatIntelligence: @chum1ng0 (¡gracias!).

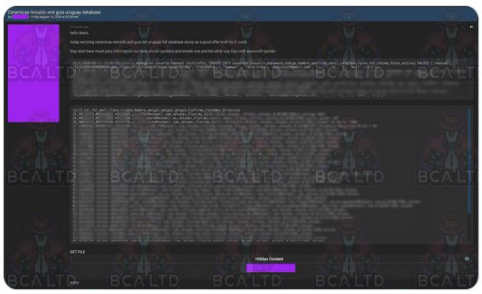


BCA LTD ✓
@BirminghamCyber

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: @teamcapybara_.



BCA LTD ✓
@BirminghamCyber

New #cybercrime intelligence.

#Uruguay: A threat actor defaced the Partido Nacional website and publicly shared the HTML Injection vulnerability used.

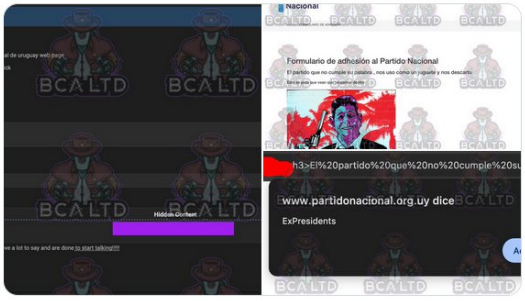
#ThreatIntelligence: @teamcapybara_.

BCA LTD ✓
@BirminghamCyber

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.

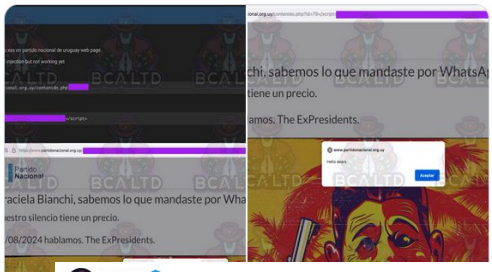


BCA LTD ✓
@BirminghamCyber

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.

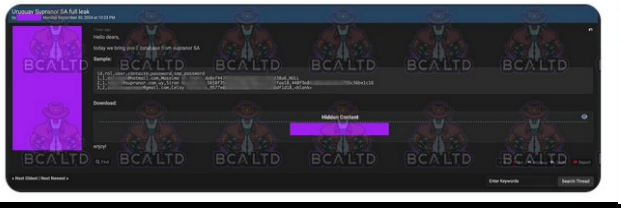


BCA LTD ✓
@BirminghamCyber

New #cybercrime intelligence.

#Uruguay: Threat Actor selling databases belonging to Supranor SA.

#ThreatIntelligence: @teamcapybara_.



BCA LTD ✓
@BirminghamCyber

New #cybercrime intelligence.

#Uruguay: A threat actor is selling a database belonging to Universidad de la Empresa, Facultad de Ciencias Agrarias.

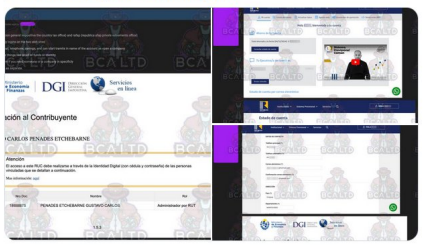
#ThreatIntelligence: @chum1ng0.

BCA LTD ✓
@BirminghamCyber

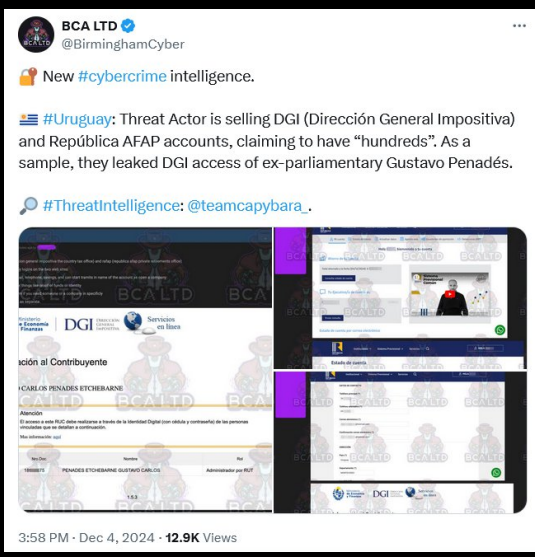
New #cybercrime intelligence.

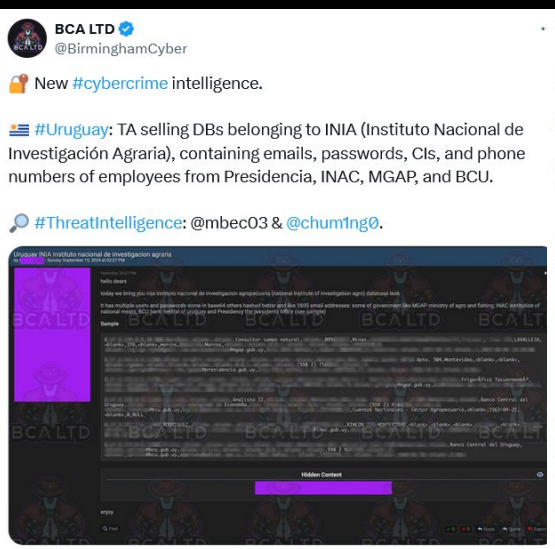
#Uruguay: Threat Actor is selling DGI (Dirección General Impositiva) and República AFAP accounts, claiming to have “hundreds”. As a sample, they leaked DGI access of ex-parliamentary Gustavo Penadés.

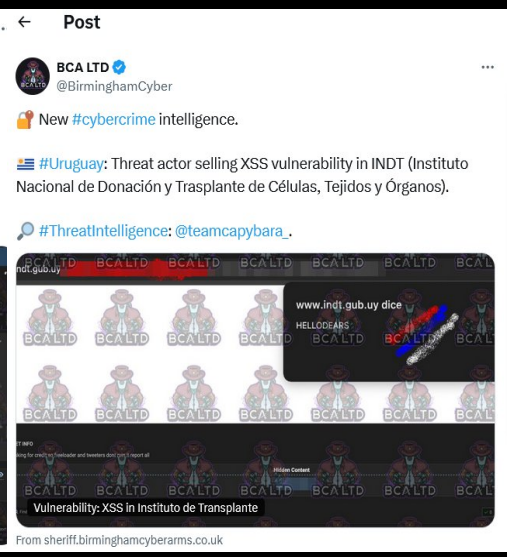
#ThreatIntelligence: @teamcapybara_.



3:58 PM · Dec 4, 2024 · **12.9K** Views







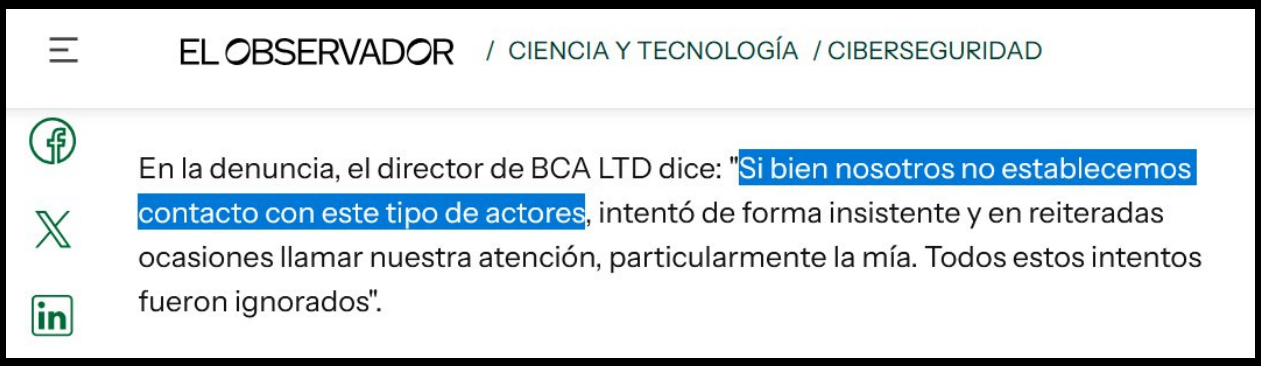
There are many more, but we don't feel like compiling them all; whatever nonsense "Expresidents" posted on BreachForums, they published it, regardless of whether it was a database with 100 alleged users or fake data, and a user like with the cars, I don't know what...

Mauro [Owner of BCA LTD] has another website called mefiltraron.com that compiles data on hacking incidents. It includes us and a few others from the community, but for some reason, Expresidents is ranked #1 with "30 incidents."

INTERVIEW WITH EXPRESIDENTS

Do you remember the interview with Expresidents where they contradicted themselves and it seemed more like they were acting or playing the part of hackers? The people who conducted that interview [the only one ever] with Expresidents were a website created by Mauro Francisco Caseres, the same owner of BCA LTD. Not only did they publicize it, but they were the only ones to interview them...

The reality is even more evident when, in the investigation “The Leader of PampaLeaks,” the owner of BCA LTD—after Uruguayo1337 sent him a message on Telegram [it wasn’t us]—never replied because “We do not make contact with this type of actor.”



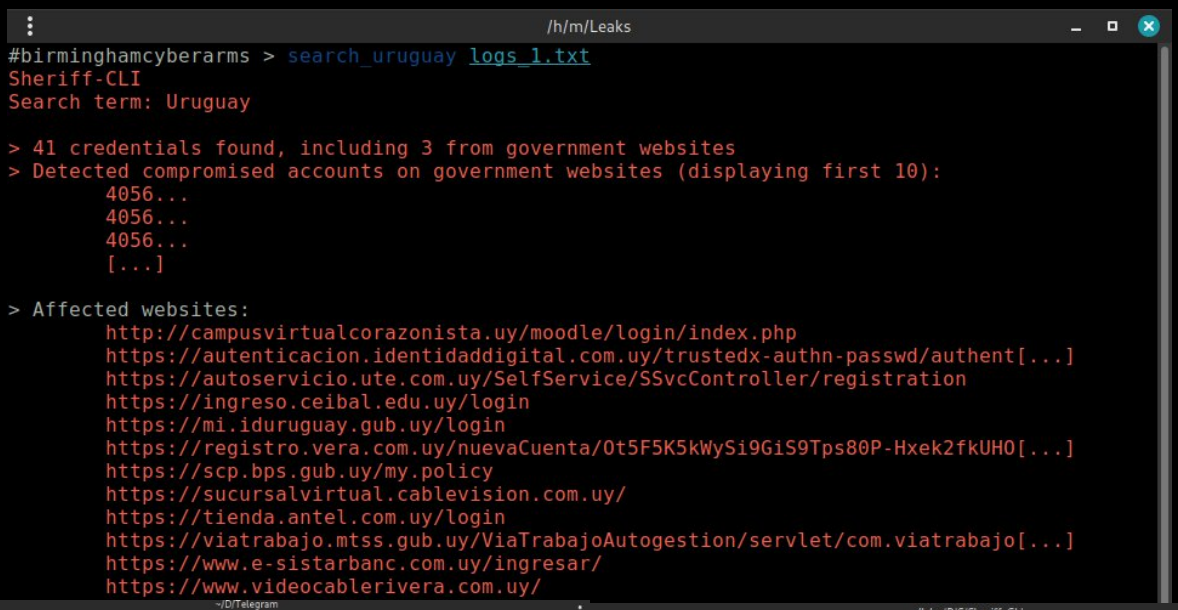
Team Capybara is one of the names of the “research” teams [taking screenshots of what's happening on hacker forums or Telegram channels and posting them on X / Substack]... These are the same people you see in the previous screenshots; they're the ones who post the most about what Expresidents was doing on Breachforums under the BCA LTD account on X

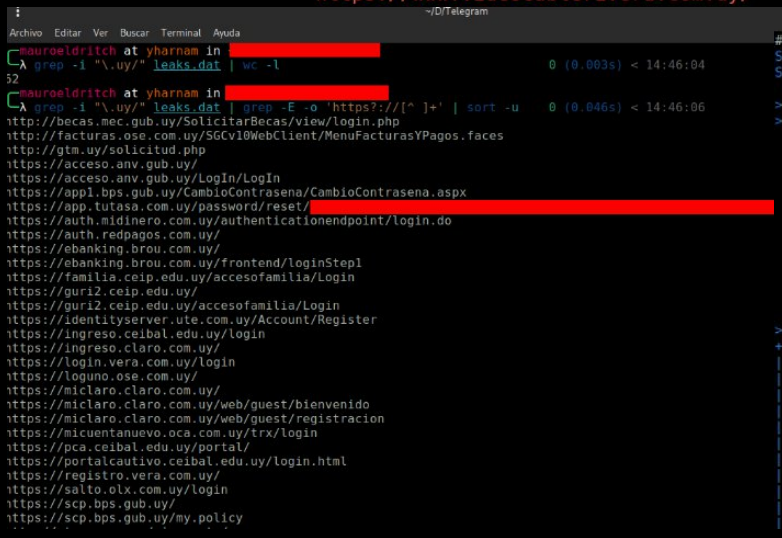
Lara Aniela Caseres [40492286], a relative of the owner of BCA LTD, is part of this team

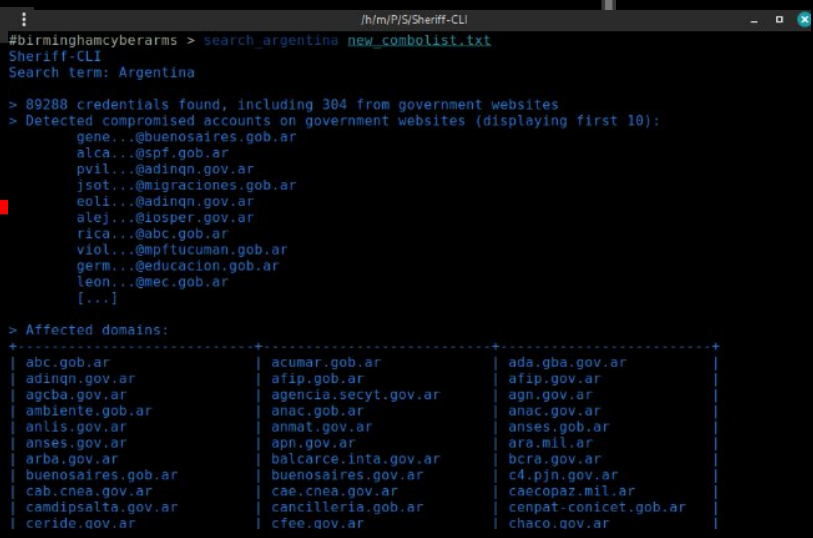
- https://mefiltraron.com/interviews#expresidents
- https://www.nerdear.la/speakers/lara-caseres/
- https://www.elobservador.com.uy/ciencia-y-tecnologia/una-pelea-ciberatacantes-expone-la-identidad-del-presunto-lider-pampaleaks-n6044404

BCA LTD AND STELEARS LOGS TOOL

Just as Expresidents [BCA LTD] did with the “attack” on the DGI and other cases in which it obtained access credentials and shared them on the forum [so they could be patched], BCA LTD and Mauro have systems that they designed themselves starting in 2023 [before Expresidents existed] to search for Stelear records, a sort of local IntelX intended to track government logins







If you zoom in on the PDF to view the images, you'll see that the Linux usernames are Mauroeldritch and BirminghamCyberarms [BCA LTD]. They posted this on X

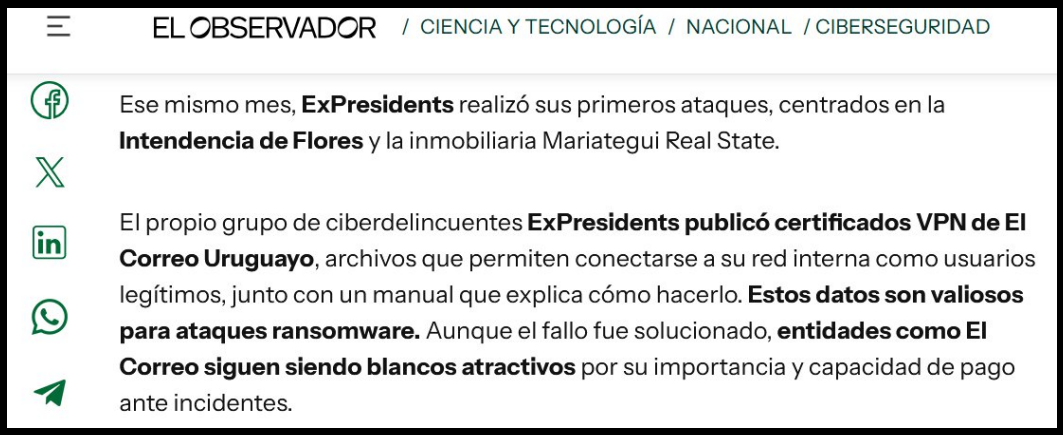
It’s not hard to see that this is the same attack method used by “Expresidents” and that this is a ploy to draw more attention—by posting messages on the forum and making it difficult for users to access the site quickly so they can take screenshots, post them, make the news, and position themselves as the saviors who warned of the problem.

- https://archive.ph/WnCpG
- https://web.archive.org/web/20260524135406/https://pbs.twimg.com/media/Fw-QEZ5WAAEIaEC?format=png&name=large

THE COMPLICITY OF THE OBSERVER

Juan Pablo de Marco uses the image of El Observador to spread misinformation and make unsubstantiated claims to his audience, as we showed in the other PDF. He plays a very important role in this operation by BCA LTD to give credibility to the fabricated hacker and portray them as “saviors” and those who are trying to help the victims of “Expresidents.”

From the very moment that “Expresidents” [BCA LTD] made their first posts on Breachforums [false posts that were criticized on the forum], Juan Pablo from El Observador wrote an article promoting these alleged attacks—such as the one on the Flores Intendencia and the “VPN” of the Uruguayan Postal Service—which we demonstrated to be useless information, and the post was removed from the forum by the admins



All the news reports in *El Observador* that mention Expresidents are based on Birmingham Cyber Arms [BCA LTD], and suspiciously, it is they who notify the affected companies or public agencies and know exactly how to breach their systems.

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

It’s painfully obvious how they’re hyping up the image of “the hacker-turned-president”—just look at what he actually did: he posted a link to a public MTSS form, pointing out that you could search for “children as well,” and within hours it was patched.

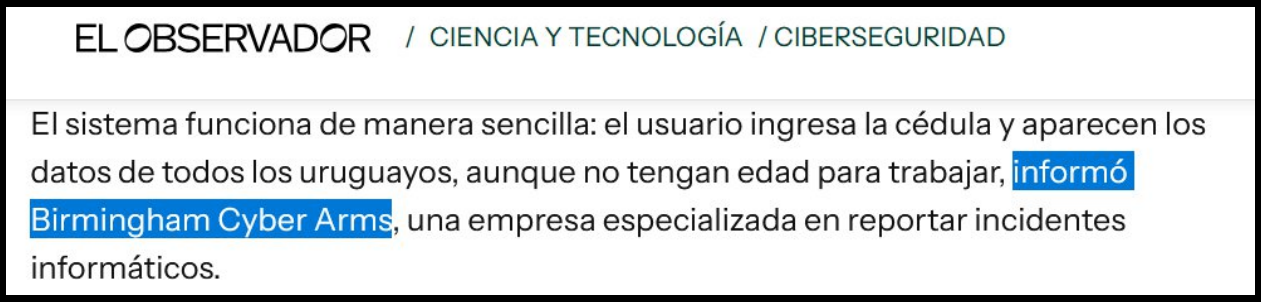
The same person who published “The Leader of PampaLeaks” wrote a news article about this, implying in the headline that Expresidents had created the system and were selling it on the black market. In the article’s description, the “Experts” [BCA LTD] were warning everyone about this.

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.

Steps in the operation carried out by BCA LTD using its “Expresidents” persona:

1. “Expresidents” [BCA LTD] posts real or fictitious vulnerabilities on forums [it used to do this] or on Tor network sites that nobody knows about
2. Birmingham Cyber Arms [BCA LTD] posts about this on X and sends it to journalists
3. The reporter [Juan Pablo de Marco] publishes a story on the subject, including the official statement from BCA LTD and presenting BCA LTD as “experts”
4. The article gains attention and is picked up by other media outlets, portraying BCA LTD as the company that reported the issue from the very beginning and is helping to clarify what actually happened with the ANTEL “HG Hack.”

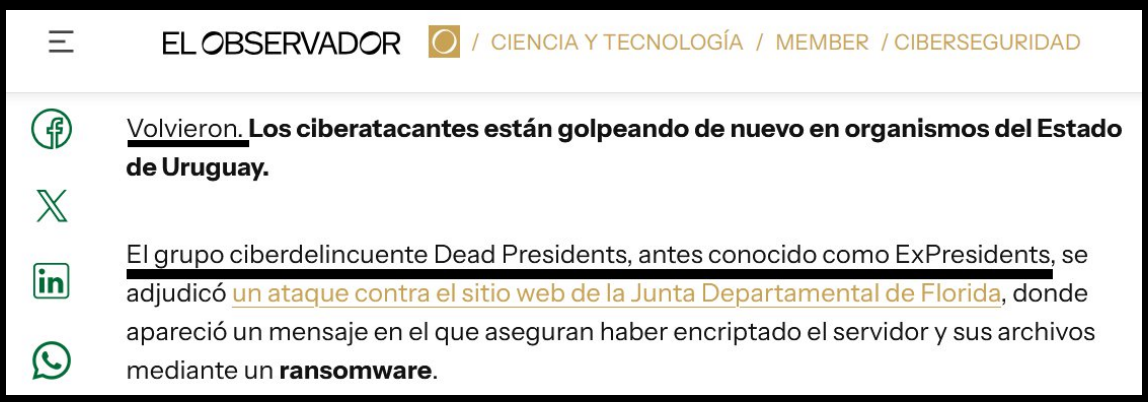
This explains the “odd behavior” of expresidents on hacker forums, such as disabling private messages to avoid contact with users [other cybercriminals, according to BCA LTD], as well as why he didn’t care about looking bad, having his posts deleted, or sharing access credentials that were obviously going to be patched—as happened with the MTSS post or the VPN.

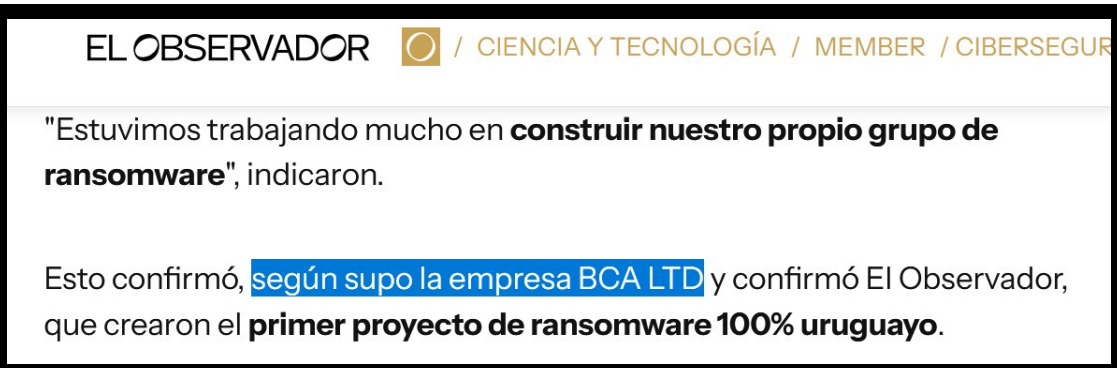
Because BCA LTD's goal here is to raise its profile and be seen as the saviors

EL OBSERVADOR'S “EXCLUSIVES” WITH EXPRESIDENTS AND BCA LTD

This operation dates back to 2024, and in early 2025, Expresidents [BCA LTD] halted all its operations just as PampaLeaks [Dinacia, Masoneria, Fiscalia] and Tacuara [Mides, Ministry of the Interior] appeared on BreachForums. They then disappeared and moved to craxpro.net instead of another forum known as DarkForums; after that, Expresidents vanished from the hacker forums and “created its own website on the Tor network.”

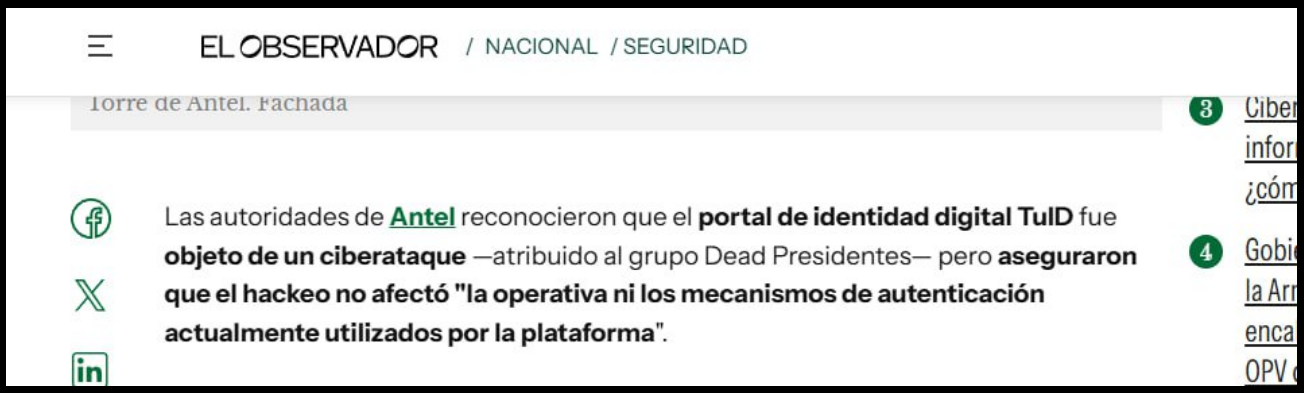
No one in the markets or on the hacker forums knew that he was working on Expresidents, but somehow Juan Pablo de Marco had the inside scoop that he was working on Expresidents, thanks to “BCA LTD” [Here we go again]



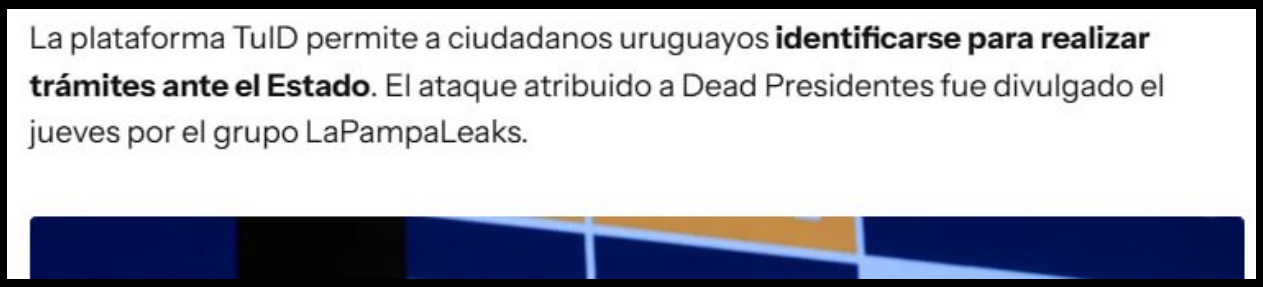


- https://www.elobservador.com.uy/ciencia-y-tecnologia/ciberatacantes-crean-el-primer-ransomware-100-uruguayo-n6036845

The operation at El Observador and BCA LTD is so extensive that when the hack at ANTEL by LaPampaLeaks occurred—as confirmed by the TuID platform and company officials—El Observador's response was to claim that the attack was carried out by the "Dead Presidents" group, which clearly shows that they don't mind spreading misinformation as long as it benefits their own interests.



There are some particularly juicy passages, such as the one claiming that Dead Presidents [Expresidents] carried out the attack and LaPampaLeaks [Founder of PampaLeaks] published it afterward. This creates the narrative that Expresidents attacked TuID and LaPampaLeaks merely "disclosed" it.

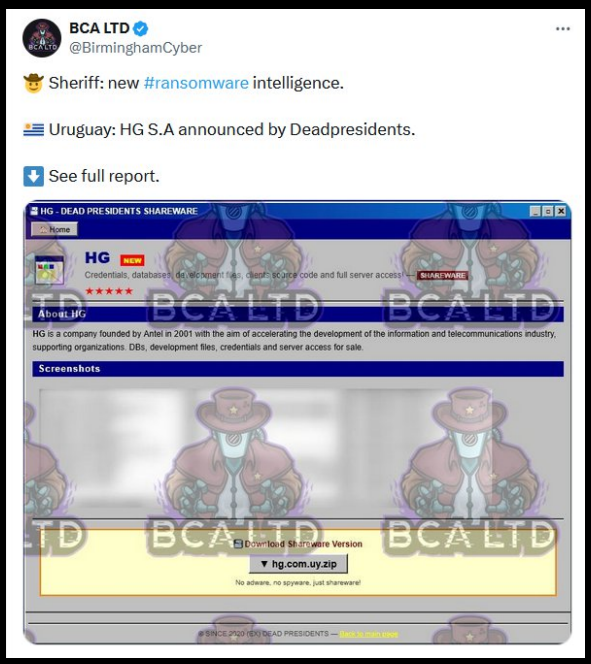


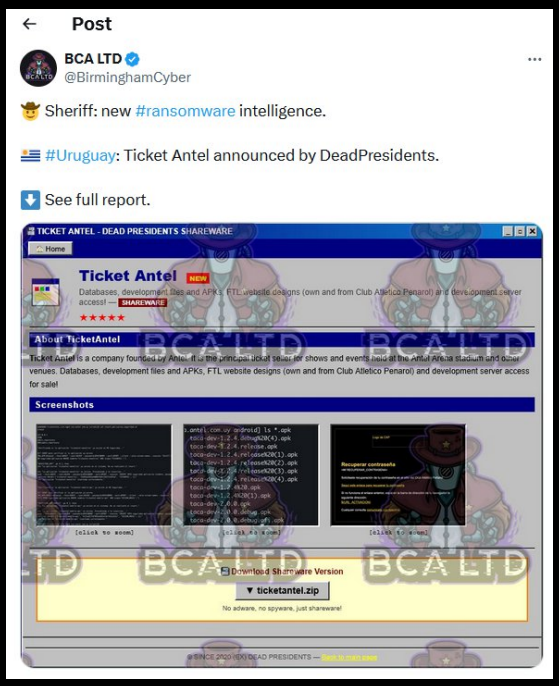
It's as easy as going to DarkForums and comparing the dates when the TuID post was published and when Expresidents appeared with the hack of "HG" and "Tickantel"

- 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

THE FALSE CYBERATTACK ON HG AND TICKANTEL

After we made public the hack of ANTEL's TuID service, what happened a week later was that "Expresidents" [BCA LTD] suddenly reappeared and also affected ANTEL services through a private company that ANTEL wholly owns Once again, the source of the initial report on this matter is BCA LTD, and there is no other source behind it; as far as we know, no one has access to the alleged Tor page where that screenshot [watermarked by BCA LTD] is said to have come from.





Just a few hours after the original tweet from BCA LTD., Juan Pablo de Marco, using an image from EL OBSERVADOR, posted the news that server access credentials had been leaked and that source code and other data—totaling about 12GB—had been exposed. A few days later, they reported on Tickantel, citing 1GB of allegedly leaked data found somewhere on "the dark web"?

HG S.A. responded with an internal statement based on the “press releases” [El Observador] regarding the data leak, and according to their “exhaustive analysis,” they did not detect any “compromise” [hacking] of data and continued to operate normally... Remember all the false hacking claims and leaks from Expresidents before? Well, exactly the same thing is happening here

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.

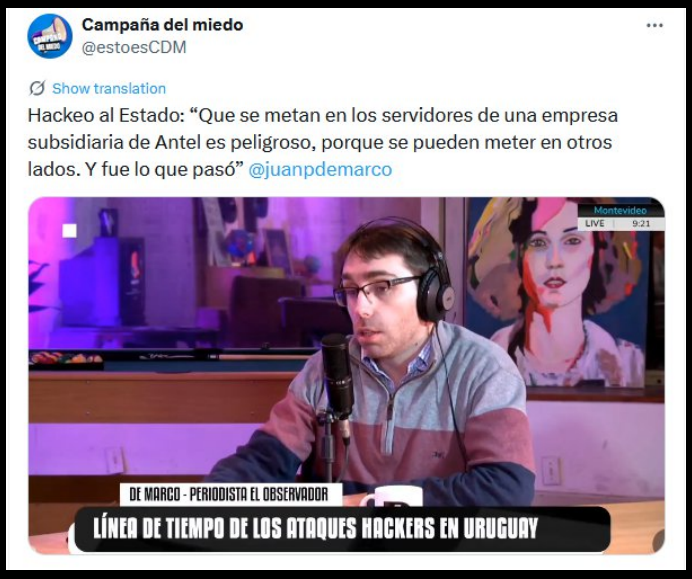
Situación Actual: El equipo se encuentra realizando un análisis exhaustivo. Hasta el momento, las verificaciones técnicas internas no han identificado evidencia alguna de un compromiso de nuestra infraestructura, sistemas o bases de datos. Tampoco se han detectado indicadores de compromiso en los activos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

A few days later, the clueless fool at BCA LTD proceeded to call the members of HG S.A.’s cybersecurity team liars, claiming that their data had been leaked [“confirmed by former HG employees who saw their leaked login credentials”]

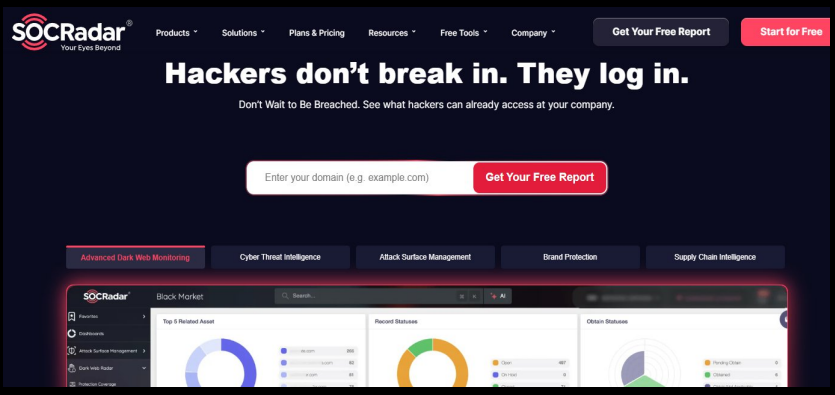


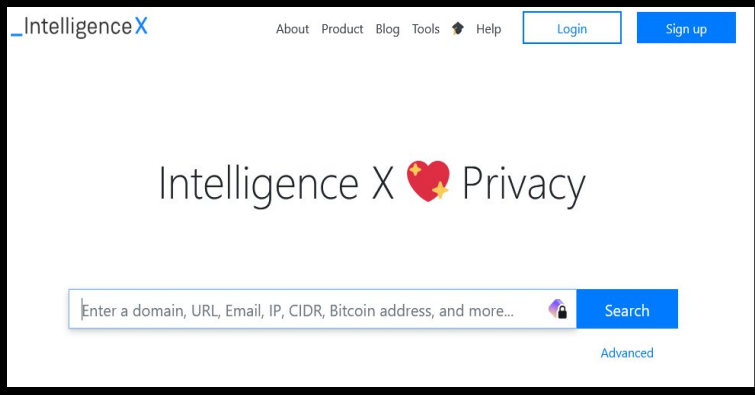
On the next page, we will refute what this myth-spinning journalist claims [again]

The response from the third-rate journalist at *El Observador*:

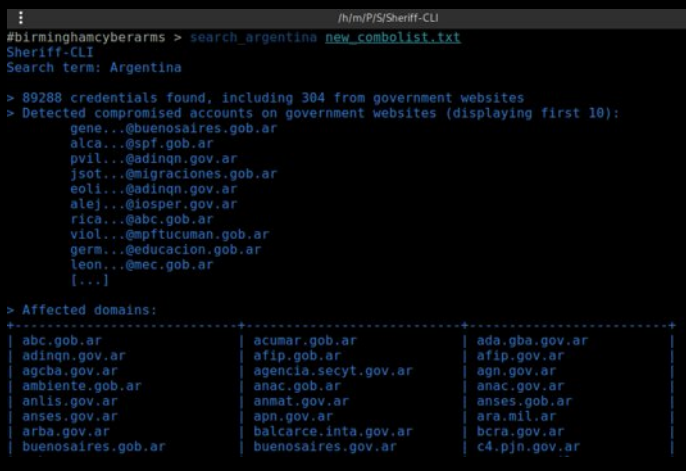
"It's very contradictory: while some former H.G. employees told me, “My credentials were there,” there were others who used platforms like “SOC RADAR,” which are designed to detect which credentials are circulating on the dark web." – marc1.mp4

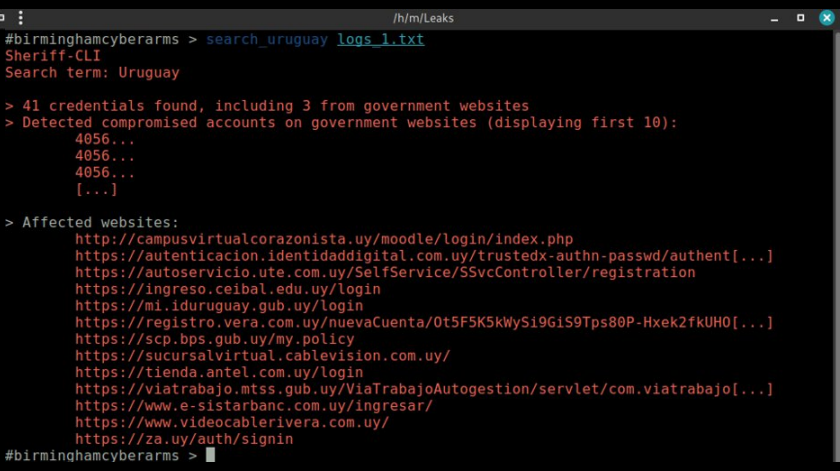
SOCRadar is a system for businesses and governments that, for a fee, allows users to view credential leaks by domain and other filters [Stealer Logs]; it is similar to IntelX but is legal worldwide and designed for professional environments





Regarding the “12GB” files for sale and the “1GB” files from Tickantel, their only defense was to claim that the sellers were lying because HG employee credentials were visible in the files. They claimed the credentials had been leaked because someone must have downloaded spyware that stole all their passwords... Let’s remember that Mauro and BCA LTD have a system that does exactly that...





That claim that they were “compromised” because the credentials were exposed is absurd. It's like us saying that just because we have AGESIC credentials [that are no longer valid]—but still have them—we compromised AGESIC without ever accessing any of its systems.

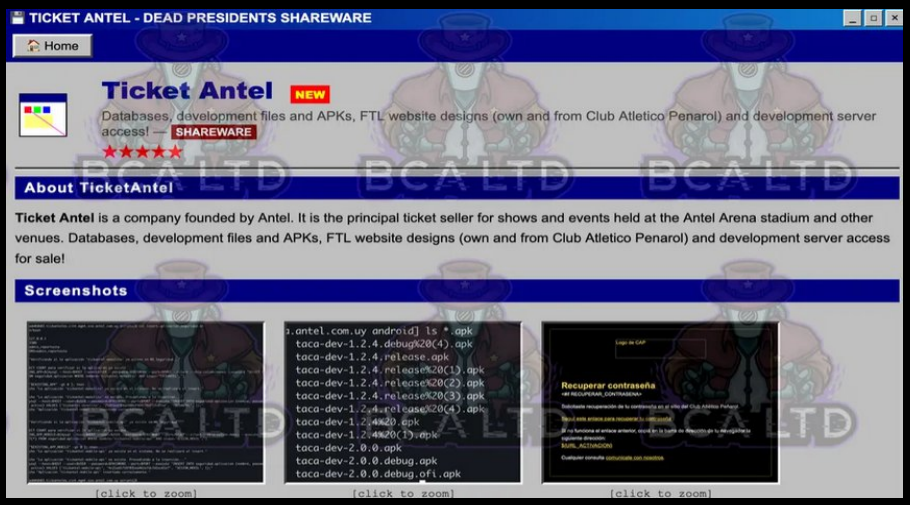
Secondly... Since May 12, 2026, El Observador, thanks to an investigation by “BCA LTD,” already knew how “Expresidents” had gained access and even details such as that the access was sold by an “IAB”—which, in plain terms, is someone who engages in phishing and dedicates themselve

Other details include the fact that a report in *El Observador* claims those 12GB are being sold on the “dark web,” but the screenshot [the only one on the entire internet] from BCA LTD shows them available for download. It makes no mention of a sample and claims to have accessed databases and more.

Then there’s the “1GB” from Tickantel [based on a single screenshot from BCA LTD’s website]—it only shows information from the front end of an APK. All APKs can be easily unpacked, and filtering through those files is like looking at a website’s source code and calling it a “leak.”

Second, the email designs [FTL Designs] are easy to recreate by signing up or clicking “Forgot Password” [as shown in one of those screenshots] and downloading the email’s source code to recreate it in an “FTL” file and claim that you hacked Tickantel...

Second, the email designs [FTL Designs] are easy to recreate by signing up or clicking “Forgot Password” [as shown in one of those screenshots] and downloading the email’s source code to recreate it in an “FTL” file and claim that you hacked Tickantel...



Summary of the hacking attack on HG and Tickantel:

- The only examples of “leaks” by Expresidents [DeadPresidents] are access credentials [Stelear logs] and files from the APK frontend and official emails
- The observer's flimsy defense—that HG was lying—relies on examples from Stelear's logs and tools.
- They used “12GB” as an example because it was much larger than “8GB,” which was the actual hack of ANTEL’s TuID system by the PampaLeaks team

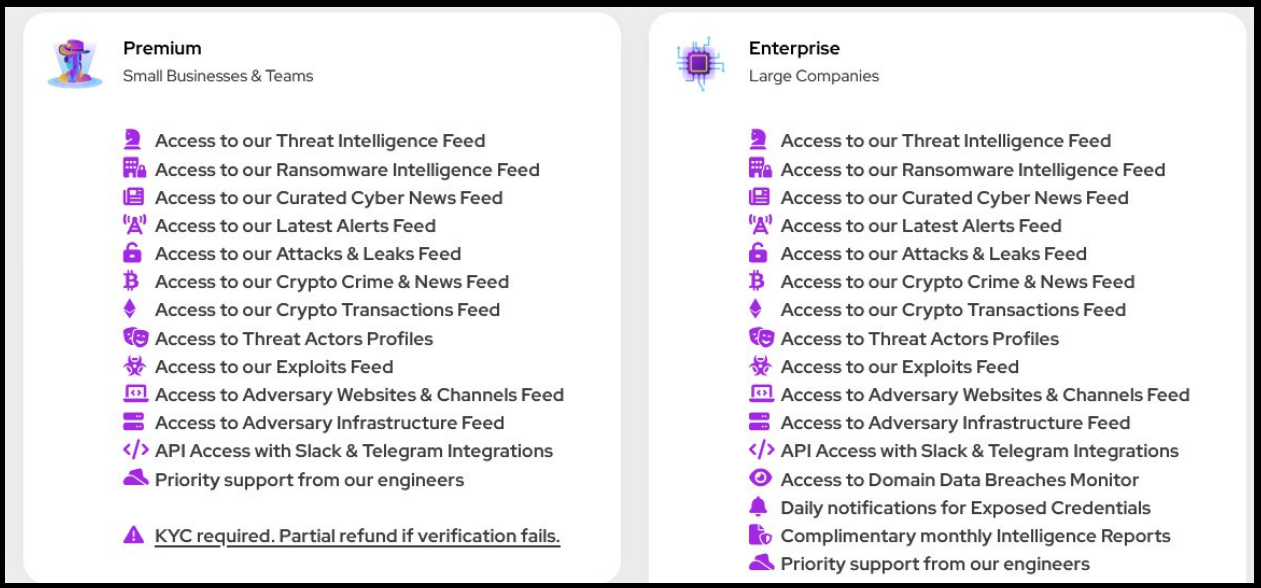
The transaction involving the use of the HG S.A. and ANTEL brands and the benefits it provides to BCA LTD:

In cybersecurity, the key to increasing sales is to use fear to get people to hire your services. The folks at BCA LTD do exactly that, and that’s the real reason they invented the “Expresidents” character—so they can position themselves as the saviors when this “group” attacks, damages infrastructure, or leaks databases containing millions of records.

In the examples above, we showed how the DGI, MTSS, departmental governments, and other Uruguayan public agencies were used to do exactly that. They issue the warnings and come across as the saviors and the “experts” who provide explanations

In this case, they used ANTEL’s image because there had already been a confirmed hack—the largest one to date—that was making national headlines. So they rode the media wave to have Expresidents return with a “hack” targeting ANTEL’s outsourced services, pulling off a major psychological operation to portray themselves as saviors.

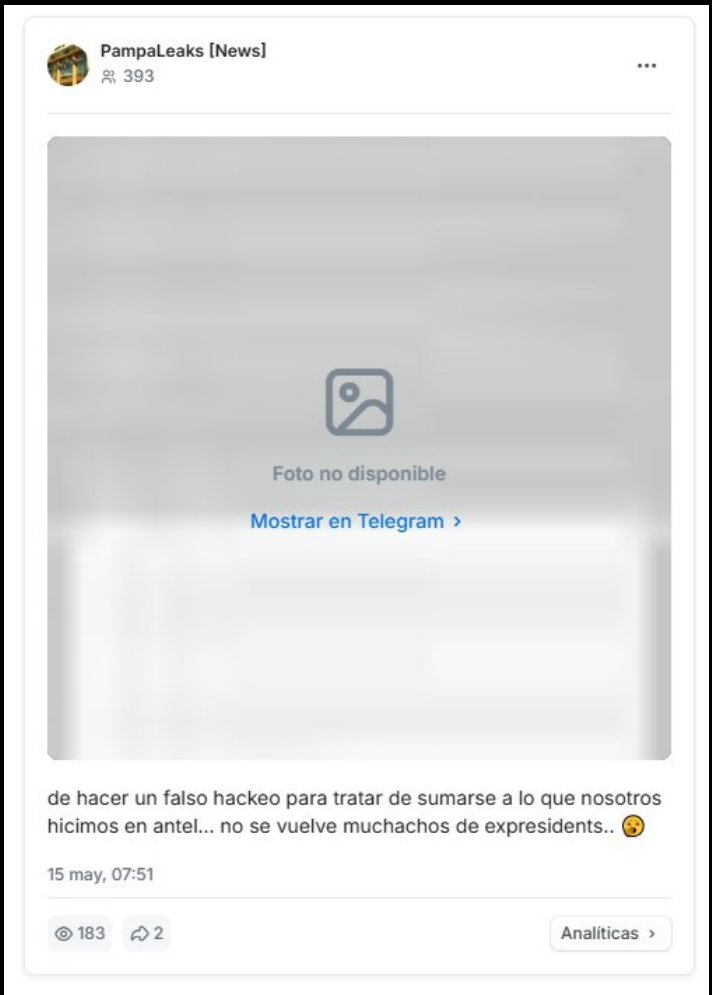
BCA LTD's interests and why they do this: They sell “threat” [hacker] research services, access to a search system for leaked credentials they call “Domain Data Breaches Monitor,” and “Exposed Credentials” [data breach records] at high prices

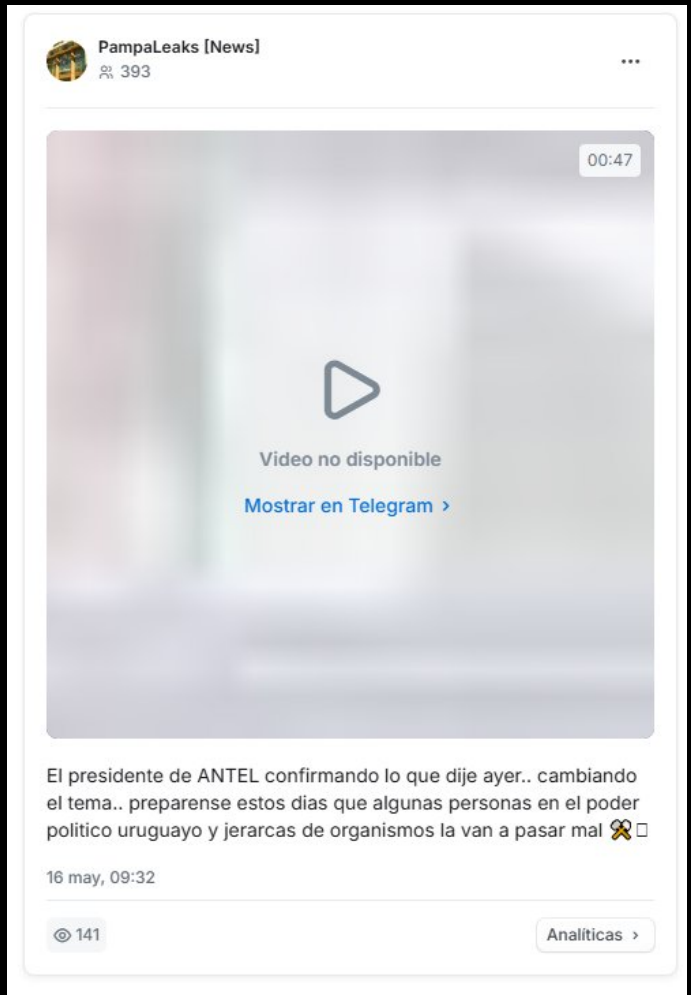


A FAKE FIGHT BETWEEN THE PAMPALEAKS AND THE [DEADPRESIDENTS]

The only mentions of PampaLeaks were by LaPampaLeaks in 2026, when it was confirmed that the hack of HG and Tickantel was a hoax; in 2025, it was a response to a post in which the user uploaded a fake database containing only one user and .csv files from a website's frontend.

Those who claim it was a "fight" and that Expresidents doxed the "Leader of PampaLeaks" at BCA LTD—this investigation was made public a few days after PampaLeaks, using its old Telegram account @lapampaleaksbf, posted the following on Telegram:





A few days after LaPampaLeaks doxxed political figures in Uruguay and had its accounts and all its channels suspended, we lost all communication, and two days later, an investigation was published revealing "The Leader of PampaLeaks," and one of the narratives is that we knew this was going to happen because of expresidents and that we deleted everything...

BCA LTD's interests here: We were challenging their narrative and that of their "Expresidents" character, so they enlisted Juan Pablo from El Observador to publish an investigation titled "Revealed by the Leader of Pampaleaks" in order to destroy us, assuming we would disappear and therefore not refute any of the claims.


EL OBSERVADOR / CIENCIA Y TECNOLOGÍA / CIBERSEGURIDAD

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... The same person who, since 2024, has been promoting “research” by BCA LTD—which has been promoting “Expresidents” from the start based on BCA LTD... And the same person who claimed that TuID had been compromised by Expresidents, two days after we challenged BCA LTD’s narrative... Now he comes out with this...

The other document intended to refute the investigation:

- BCA LTD claims that since 2024 we have been attacking presidents “in various forums” with insults and political slogans [denied]
- BCA LTD claims that LaPampaLeaks insulted and attacked him the whole time... He ignored him until one day he got fed up and “doxed” him, revealing all his personal information—like addresses, etc.—and that's when “BCA LTD started investigating”...
- They claimed that we deleted our Telegram accounts ourselves to escape because “they knew what was coming,” when in fact the accounts were suspended
- We show how Juan Pablo de Marco, along with BCA LTD, has a history of lying in past news reports and failing to verify any of his claims

What I think Mauro from BCA LTD was thinking when he did this:

They thought that uruguayo1337 was the leader of PampaLeaks and that LaPampaLeaks was just an alias for the same person. So when all of our Telegram accounts were suspended—a few days after we debunked expresidents—they saw that they could use the El Observador journalist as a pawn to eliminate the competition from “expresidents” [they]

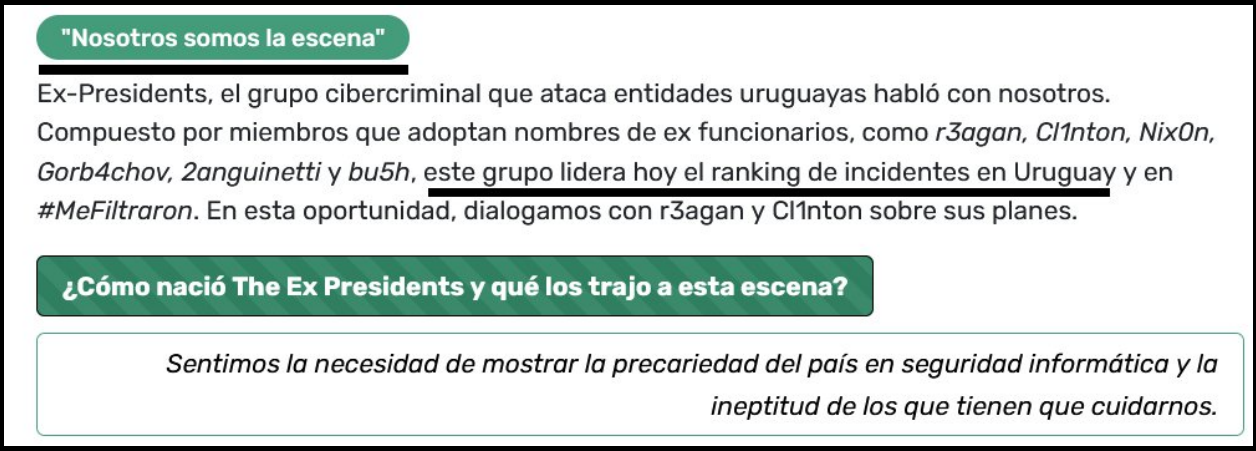
This marks a historic milestone for Juan Pablo de Marco, who uncovered the identity of the leader of Uruguay’s most-wanted hacker group based on an investigation by BCA LTD—a turning point in his “threat actor investigations.”

In addition to eliminating the “competition” and ensuring that the only “threat” is themselves, they control the narrative surrounding all future [fake] hacks in the country and build up the reputation of the group DeadPresidents or Expresidents [themselves] for taking down PampaLeaks

BCA LTD AND THE REPUTATION OF PAMPALEAKS

This company that controls “Expresidents” has been trying to damage PampaLeaks’ reputation for over a year now. Regardless of whether it’s a lie, they’re trying to manipulate public opinion—which WE DON’T CARE ABOUT because we’re already seen as the bad guys. After that, it’s just a matter of trying to damage our reputation so that “Expresidents” [they] can come out on top.

This is very clear just by reading “the interview” that was “conducted” with “expresidents,” from the headline “We Are the Scene” to how they’re described as “the group currently leading the rankings for incidents in Uruguay,” or the first question, which could easily be BCA LTD’s motto: “We feel the need to highlight the country’s precarious security situation...”



"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?

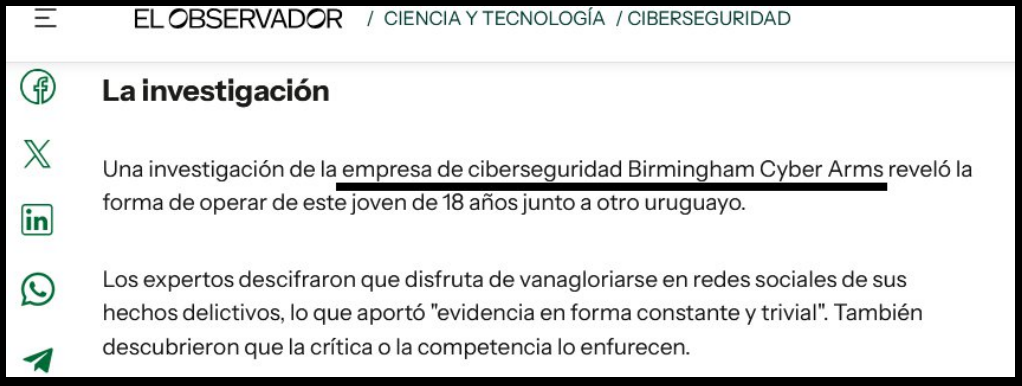
Sentimos la necesidad de mostrar la precariedad del país en seguridad informática y la ineptitud de los que tienen que cuidarnos.

A year ago, this same “cybersecurity” company tried to pull the same stunt on us by getting that dim-witted reporter from *El Observador* to publish an article pointing the finger at people who have nothing to do with us—the “hackers” with the Buquebus intelx—who were just a bunch of teenagers trying to get attention by doing everything from “their cell phones” and social media

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

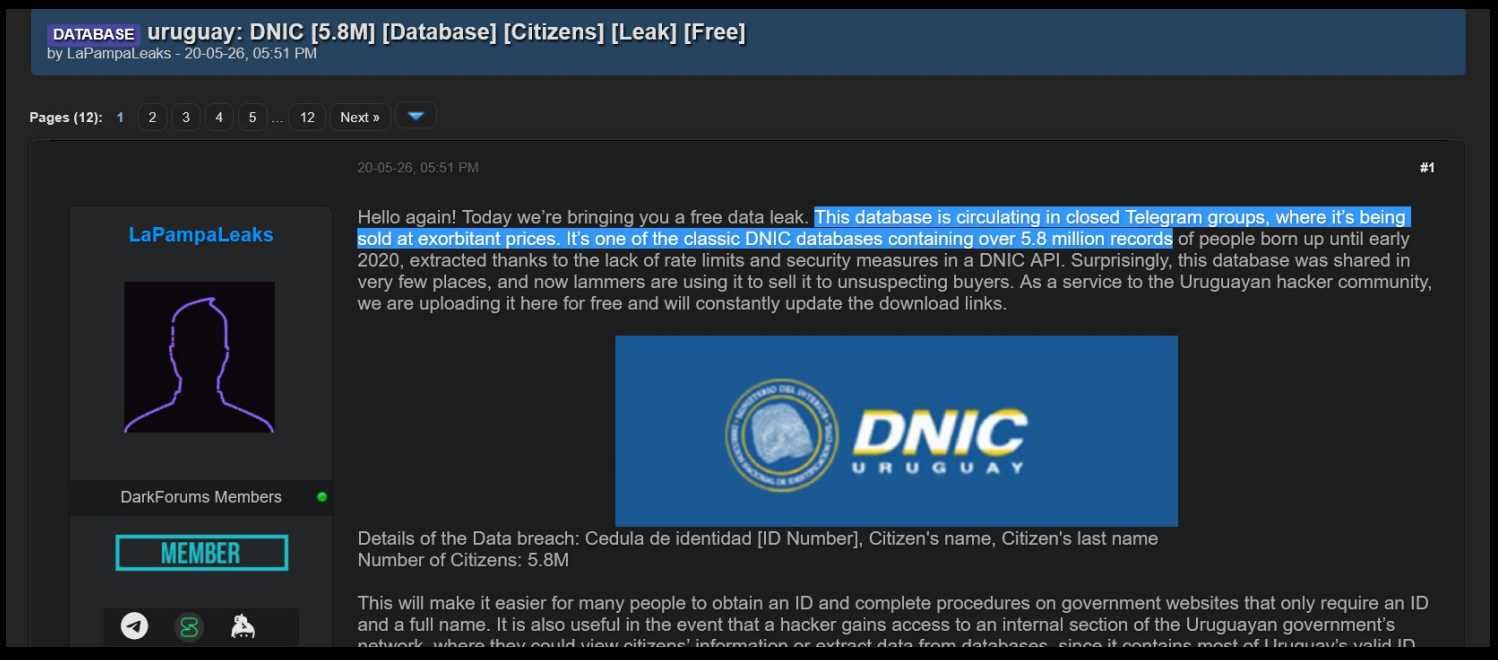
La investigación

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.

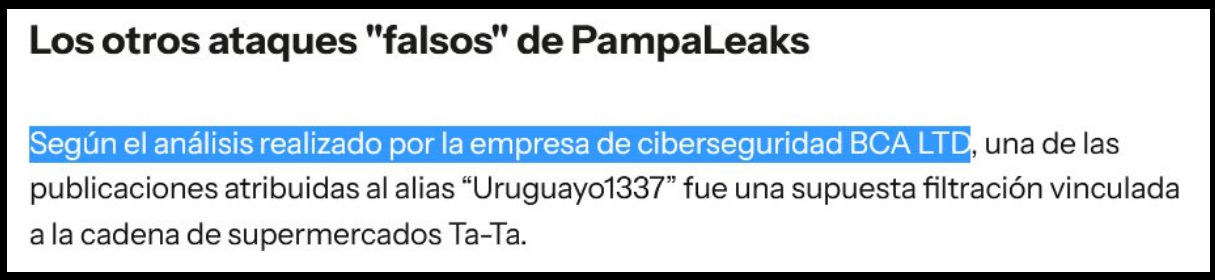
Los expertos descifraron que disfruta de vanagloriarse en redes sociales de sus hechos delictivos, lo que aportó "evidencia en forma constante y trivial". También descubrieron que la crítica o la competencia lo enfurecen.

As we write this, LaPampaLeaks has just sent us a message—like Juan Pablo De Marco at 5 A.M. [he's very sick]—with a new post about "fake leaks from PampaLeaks," citing as an example the DNIC database published on DarkForums and Spear Forums, along with another one from TATA that we had nothing to do with

The "scoop" is that the database had already been leaked. The question is, what's the scoop? LaPampaLeaks has always said that the database was already circulating, that it was the "standard DNIC database," and that they were doing this primarily as a service to the hacker community because people on Telegram were selling it to unsuspecting buyers at inflated prices.



From the very beginning, LaPampaLeaks has already stated this, but Juan Pablo [at 5 a.m.] presents it as if it were the scoop of the year, even though this was made clear from the start... Also, "Experts question the..."—we'll see who those "experts" are a little later ;)



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.

Yeah... The same old crowd that's been following the PampaLeaks folks around like fleas for over a year now, and the closest they've come to anything is exposing a former group member who was a reseller of the bot—just like anyone else could have been if they had enough tokens.

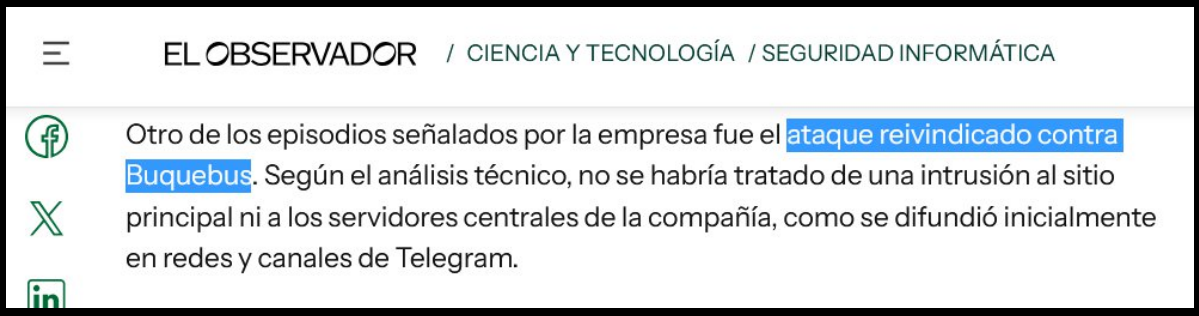
And as expected, as we showed earlier... In the very same news story that just came out as we're writing this... In the very same news story that seeks to discredit [by manipulating and omitting information] PampaLeaks... Expresidents is also mentioned, but unlike us... there's nothing negative about it, and they're completely neutral.

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.

To top off all these claims... They also claim that we exaggerated the attack on the Buquebus website when we had nothing to do with that “defacement.” It’s not that hard to do some proper research by looking into the hack on Dinacia and the hack on Buquebus and see that “LaPampaLeaks, Bogotaleaks, uruguayo1337” and “vladi, gov.eth, etc.” are not the same



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.

W

hat we find most amusing—and truly pathetic—is that instead of acknowledging they were wrong and could have made a mistake by claiming that uruguayo1337 was our leader, they keep insisting on it even after our statements, and they’re attributing some nonsense about Tata to us??

Not to mention that it’s the same company and media outlet that chose to launch a full-scale public investigation into an alleged leader of a criminal organization without verifying anything—and in doing so, risked hindering serious investigations by the Ministry of the Interior and Interpol—just to get a few clicks on news stories and 2,000 or 3,000 views on a YouTube podcast...

The “journalist” as referred to by Expresidents: https://minochinos.com/embed/ucre1bgegfvp [“Expresidents—now Expresidents is becoming increasingly sophisticated,” “it’s building its own technological infrastructure and launching attacks with much greater impact...”]

The “journalist” talks about the staged fight: https://minochinos.com/embed/15ah62b4s92b [A completely fabricated story is being spread on “forums,” and the context of a doxxing incident from a year ago is being distorted, as shown in the other PDFs intended to refute BCA LTD’s “investigation”]

Exclusive report on the “attack” on HG published in El Observador: https://minochinos.com/embed/gutu9tsdh66g

Relationship between the journalist from “El Observador” and Mauro, of BCA LTD: https://minochinos.com/embed/r0atfv20tf3d [“Full Trabajo entre los 2”]

A demonstration of how they fabricated a fight:: https://streamable.com/e/fyz720 [Exposing their blatant lies in real time, even though the data is fully verifiable]

Lying by claiming that vladi’s [Buquebus hacker] arrest came after BCA LTD’s investigation, as reported in *El Observador*: https://minochinos.com/embed/u2xy1wbsi9mi

A panelist on the show that aired the “exclusive” interview with the “leader of Pampaleaks” casually remarked halfway through, “That’s the logo of Expresidents,” even though it was actually the logo of BCA LTD, leaving the journalist at a loss for words: https://minochinos.com/embed/q2g1zd8ic9p1

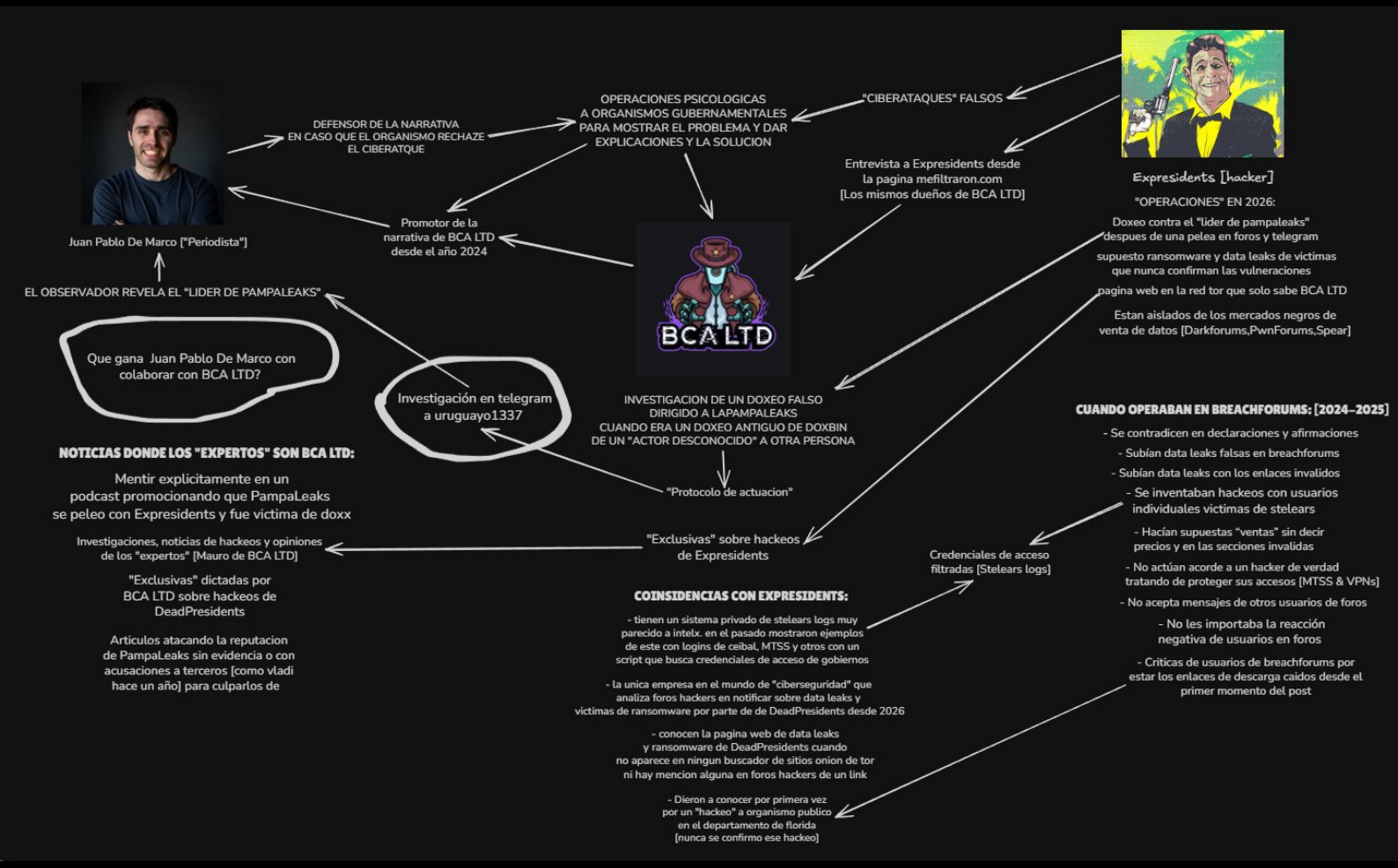
List of sources for all the previous pages that have not been included due to lack of space:

- 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

NEAR THE END OF THE INVESTIGATION

At this point, it's very clear who is behind Expresidents—and who has always been there—and why they're using it. Unlike the previous pages, now it's me, LaPampaLeaks, who's writing, and honestly, I think Juan Pablo de Marco and BCA LTD really screwed up by dragging Expresidents into this and claiming "the leader of Pampaleaks" instead of letting the police do their job in peace. They decided to go for the easy clicks and a few thousand views.

Map showing all the connections mentioned above



Fin de la investigación publica

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