Thousands of IDs exposed in yet another data breach in Brazil

blog.group-ib.com/brazil-exposed-db

16.06.2022

Unsecured public-facing database allowed anyone to access ID selfies for months

Anastasia Tikhonova

Head of Advanced Persistent Threat Research Team, Group-IB

The blog has been updates at the request of Brazilian cybersecurity authorities

In January 2021, Group-IB Threat Intelligence unit discovered sensitive personal information of over **20,000 Brazilian citizens** on a publicly available server. The data set contained the photos of individuals holding their national IDs. A quick analysis showed that the server had been exposed for at least two months. While not entirely clear if this was a breach or a leak and who was behind it, the data was most likely obtained from one of the Brazilian government portals, as deeper examination revealed.

“

Our first thought was — wow, someone forgot a 55GB directory with sensitive data on a publicly available server. The only right thing to do was to reach out to the relevant Brazilian cybersecurity authorities so they could take the necessary actions to mitigate the risks

Anastasia Tikhonova, Head of Advanced Persistent Threat Research at Group-IB’s Threat Intelligence team

Immediately upon discovery, Group-IB’s Computer Emergency Response Team (CERT-GIB) alerted Brazil's cybersecurity authorities about the incident. The case highlights the importance of rapid threat intelligence exchange and collaboration between the CERTs all over the world – the information provided by CERT-GIB was actioned swiftly. Within ten hours, the server was taken offline.

This was not the first time Brazilians’ sensitive data ended up available to the public. In 2020, personal records of over 243 million Brazilians were exposed. As the world goes digital, the security risks of online identity verification are becoming more pervasive. The incident demonstrates why government and private sector organizations that process sensitive personal data need stringent cybersecurity measures, including threat intelligence and hunting operations in place, to avoid financial losses, reputational damage, and data breaches.

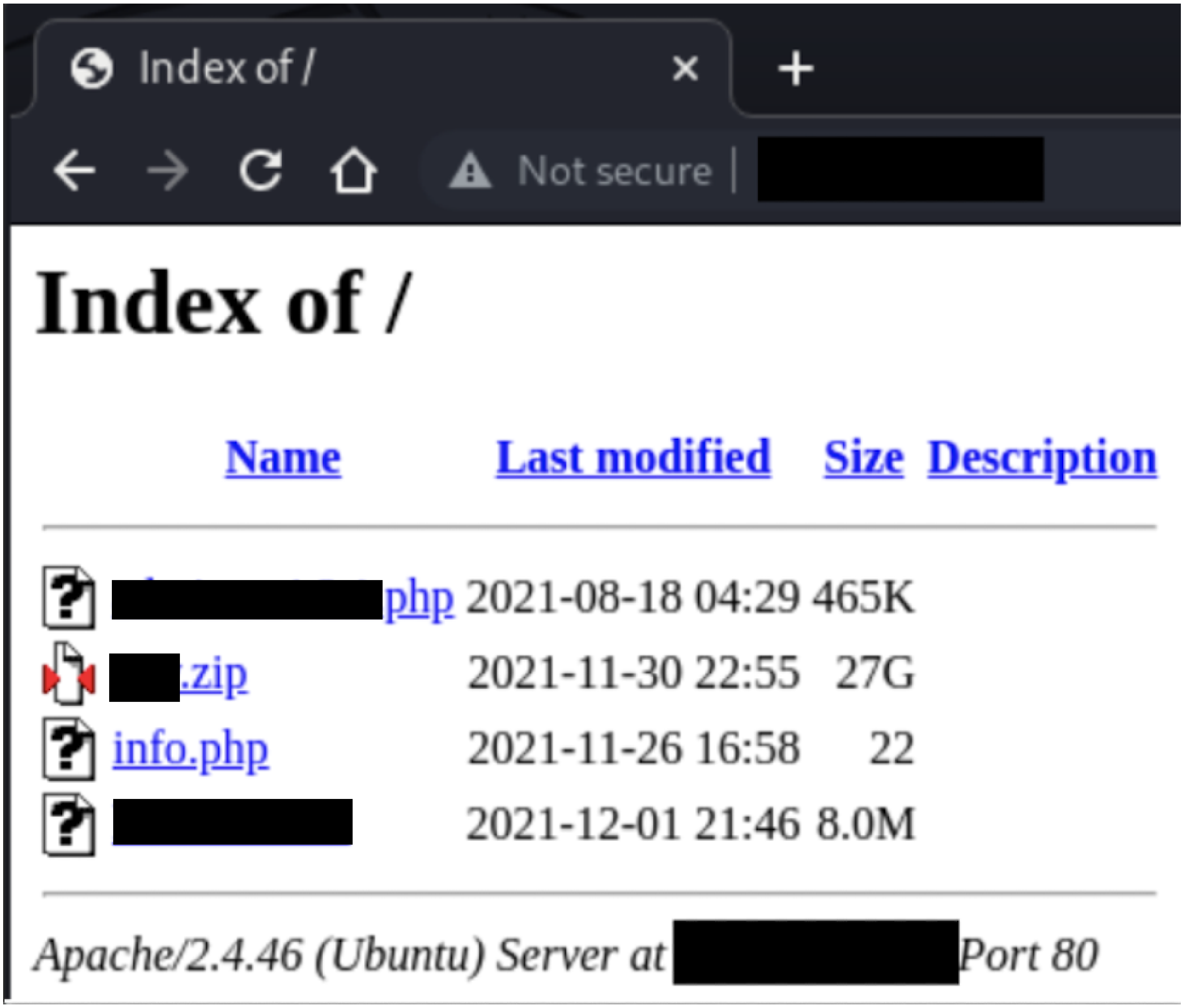
At the end of this post, cybersecurity professionals can find recommendations and remediation techniques to avoid and address similar incidents.

How Group-IB uncovered the breach

As part of Group-IB’s threat intelligence gathering processes, the entire IPv4 internet space is scanned continuously for anomalies, signs of suspicious and malicious activity, misconfiguration causing digital assets to be exposed to a wider public. Automated tools assess online resources and identify high-risk infrastructure that requires further evaluation.

In this case, a publicly accessible server hosted in the US with the directory listing function enabled was discovered on **8th January**. Disabling directory listing on a web server is a normal security precaution to avoid the exposure of sensitive information. However, this was not the case. Anyone on the internet could access the server’s contents.

Within the directory, several files were found, including a **27 GB zip-archive** containing more than **20,000 Brazilian citizens’ ID selfies**, a custom web crawling script written in Python, and an open source web tunneling tool.



Index of /

Name	Last modified	Size	Description
[redacted]php	2021-08-18 04:29	465K	
[redacted].zip	2021-11-30 22:55	27G	
info.php	2021-11-26 16:58	22	
[redacted]	2021-12-01 21:46	8.0M	

Apache/2.4.46 (Ubuntu) Server at [redacted] Port 80

Server directory

Based on the archive's last modification date, Group-IB's analysts concluded that the file had been uploaded to the server no later than November 2021.

A crawler script, used for data collection, also caught Group-IB team's attention. As its code examination revealed, the crawler connected to one of the Brazilian government portals. The crawler's developer left a little more in the source code. Group-IB analysts spotted a phrase in Portuguese which says *“Deu erro aqui nessa merda!” (ENG: “You got this s*** wrong”).*

```
else:
 print("Deu erro aqui nessa merda!", requestResult.status_code)
open("log_processo_1", 'wb').write("PAROU EM: "+str(s)+"\n")
```

The server in question was located outside of Brazil.

Given all the above evidence, it is fair to assume that the server appears to have been used by an authorized third party as a staging area while they gathered sensitive personal information with unclear but most likely malicious intent. However, it is not clear what was the end goal of the party that collected sensitive data.

The privacy dangers of digital verification

Personal ID discovered on the server is the Cédula de identidade, the national identity document in Brazil, commonly referred to as ‘carteira de identidade’ or simply “RG” (from Registro Geral, General Registry). The card contains the name of the bearer, filiation, place of birth, date of birth, signature and thumbprint of the bearer and, optionally, CPF number (‘Cadastro de Pessoas Físicas’), the country’s individual taxpayer registry identification.

The identity card is used for a number of private and public purposes including obtaining a driver's license, opening a bank account, buying or selling real estate, financing debts, applying for a job, giving testimony in court, and entering some public buildings. The card can also be used for travel between Mercosur member countries and associates (except Guyana and Suriname).
Around the world, many organizations are implementing digital verification processes as they undergo digital transformation, making the services available via mobile apps or web portals. For the end-user, this model can be appealing; it is a fast and easy way to sign up for services, completely removing the need to visit a physical point of presence. However, when the data is not managed properly without cyber security considerations in mind, it is almost inevitable that personal information will be exposed. Digital Verification based on selfies has been gaining momentum in recent years and is used on everything from dating apps to tax returns. Just in February, the US IRS had to walk back their use of selfie-based ID.ME amidst a storm of privacy concerns.

Risks of having personal such information exposed vary for users and companies.

For the individuals that had their personal information exposed, they are at risk of:

- Identity theft
- Account takeover
- Extortion
- Spear phishing attacks
- Theft of money

The organizations that experienced the data breach can also be at risk of:

- Financial loss
- Legal action
- Reputational damage

- Operational downtime
- Response and recovery costs
- Disclosure announcements if there is a breach

Upon the discovery, Group-IB’s Computer Emergency Response Team (CERT-GIB) immediately took steps to remediate the risks, and within 10 hours the server was taken offline by the Brazil's cybersecurity authorities.

Why Group-IB reported this breach

Group-IB's mission is to fight against cybercrime. As part of this mission, Group-IB continuously scans the internet for unsecured databases containing private and personal information. When we uncover unsecured data, we immediately take steps to mitigate the risks to users, organizations and government departments.

Under a responsible disclosure protocol, Group-IB always does its best to reach out to the affected parties so they can take the necessary steps to eliminate the threat. Typically, Group-IB launches an investigation to determine who the owner is, what information is at risk, who is affected, and the potential impact on data subjects. After identifying whoever is responsible for an exposed database, we utilize our contacts in the security community, including CERTs, law enforcement partners and threat analysts, to alert the appropriate parties to secure the data as quickly as possible.

Recommendations

How to prevent a similar data breach

Know all of your internet-facing assets

The forgotten server had an HTTP directory listing, which allowed anyone to discover and utilize the information. Inappropriately exposed directory listing is categorized by MITRE as a Common Weakness Enumeration (CWE-548).

Organizations should conduct attack surface management to identify all of their internet-facing assets, including servers that have been forgotten. An audit or vulnerability scan of the identified infrastructure can reveal weaknesses including CWE-548, allowing security teams to remediate them before they are exploited.
Prevent automated tools exploiting known vulnerabilities

Improper authentication (CWE-287) occurs when an unauthorized third party claims to be an authenticated user, such as falsifying cookies to bypass authentication checks. This technique is sometimes used in conjunction with Improper Control of Interaction Frequency (CWE-799) which can allow the attacker to launch brute force attacks, such as repeatedly guessing the credentials of an administrator until a correct combination is found.

Servers and applications should be penetration tested to identify security issues such as CWE-287 and CWE-799. Dynamic Application Security Testing (DAST) also known as web application vulnerability scanning, is a method for finding externally visible issues and vulnerabilities, and can further help identify issues. Equipping developers with Open Web Application Security Project (OWASP) Top Ten Web Application Security Risks document can help avoid the most critical security risks.
Prevent compromised information from being exploited

By identifying the exposed personal information Group-IB was able to alert Brazilian authorities, allowing them to take steps to prevent the information from being used for fraudulent purposes. For a private organization, a parallel could be identifying administrator credentials for critical infrastructure on the internet, knowing that these credentials have been compromised the organization can revoke the account’s permissions before it is used for malicious purposes.

Scanning the open internet, dark web and closed threat actor forums for compromised information can help prevent it from being utilized by threat actors. This activity is performed by threat intelligence teams that have the resources and skills to find, process and disseminate this information. Timeliness is a factor for preventing compromised information from being used and should be a factor when evaluating threat intelligence solutions.

What to do if you believe you have experienced a breach

If an attack has taken place the first step is to remove the threat actor from your network, revoking account privileges, disabling communications with C2 servers and disrupting any persistence techniques. The anatomy of the attack should then be explored to understand the kill chain that allowed the attacker to gain a foothold within the organization and move laterally. Lastly, remediating steps should be actioned to prevent similar attacks from occurring in the future.

Timeliness is key to minimizing the impact of a breach. If you believe your company may have fallen victim, contact us to get a rapid and complete response from the Group-IB Incident Response team.

Contact our 24/7 incident response hotline
— Call us at +65 3159-3798
— Email us at response@cert-gib.com
— Fill out our incident response form