Insights on Cyber Threats Targeting Users and Enterprises in Brazil

By Threat Analysis Group, Mandiant

Published: 2024-06-12 · Archived: 2026-04-05 13:41:29 UTC

Threat Analysis Group

Mandiant

Written by: Kristen Dennesen, Luke McNamara, Dmitrij Lenz, Adam Weidemann, Aline Bueno

---

Note: A Portuguese-language version of this blog post is available.

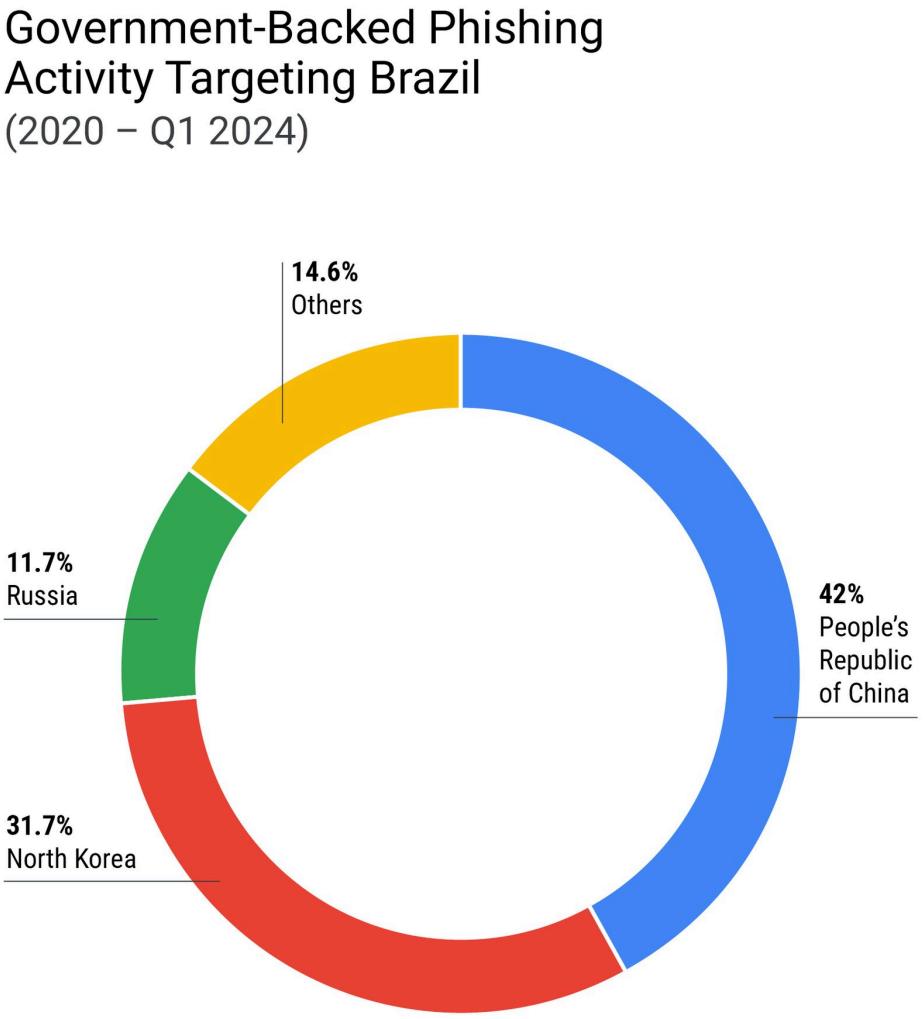
Individuals and organizations in Brazil face a unique cyber threat landscape because it is a complex interplay of global and local threats, posing significant risks to individuals, organizations, and critical sectors of Brazilian society. Many of the cyber espionage threat actors that are prolific in campaigns across the globe are also active in carrying out attempted intrusions into critical sectors of Brazilian society. Brazil also faces threats posed by the worldwide increase in multifaceted extortion, as ransomware and data theft continue to rise. At the same time, the threat landscape in Brazil is shaped by a domestic cybercriminal market, where threat actors coordinate to carry out account takeovers, conduct carding and fraud, deploy banking malware and facilitate other cyber threats targeting Brazilians. The rise of the Global South, with Brazil at the forefront, marks a significant shift in the geopolitical landscape; one that extends into the cyber realm. As Brazil's influence grows, so does its digital footprint, making it an increasingly attractive target for cyber threats originating from both global and domestic actors.

This blog post brings together Google's collective understanding of the Brazilian threat landscape, combining insights from Google's Threat Analysis Group (TAG) and Mandiant's frontline intelligence. As Brazil's economic and geopolitical role in global affairs continues to rise, threat actors from an array of motivations will further seek opportunities to exploit the digital infrastructure that Brazilians rely upon across all aspects of society. By sharing our global perspective, we hope to enable greater resiliency in mitigating these threats.

Google uses the results of our research to improve the safety and security of our products, making them secure by default. Chrome OS has built-in and proactive security to protect from ransomware, and there have been no reported ransomware attacks ever on any business, education, or consumer Chrome OS device. Google security teams continuously monitor for new threat activity, and all identified websites and domains are added to Safe Browsing to protect users from further exploitation. We deploy and constantly update Android detections to protect users' devices and prevent malicious actors from publishing malware to the Google Play Store. We send targeted Gmail and Workspace users government-backed attacker alerts, notifying them of the activity and encouraging potential targets to enable Enhanced Safe Browsing for Chrome and ensure that all devices are updated.

Cyber Espionage Operations Targeting Brazil

Brazil's status as a globally influential power and the largest economy in South America have drawn attention from cyber espionage actors for several years, including targeting by government-backed groups from the People's Republic of China (PRC), Russia, and North Korea.



Since 2020, cyber espionage groups from more than a dozen countries have targeted users in Brazil; however, more than 85% of government-backed phishing activity is concentrated among groups from the PRC, North Korea, and Russia. The Brazil-focused targeting of these groups mirrors the broader priorities and industry targeting trends we see elsewhere. North Korean government-backed groups, for example, have shown a keen interest in Brazilian cryptocurrency firms, aerospace and defense, and government targets. PRC groups, meanwhile, have targeted Brazilian government organizations, as well as the energy sector. Russian cyber espionage groups have targeted users in Brazil regularly dating back more than a decade; however since the start of Russia's war in Ukraine, Russian activity targeting Brazil has scaled back considerably - likely an indication of Russia's efforts to focus resources on Ukrainian and NATO targets in the context of the Russia-Ukraine war.

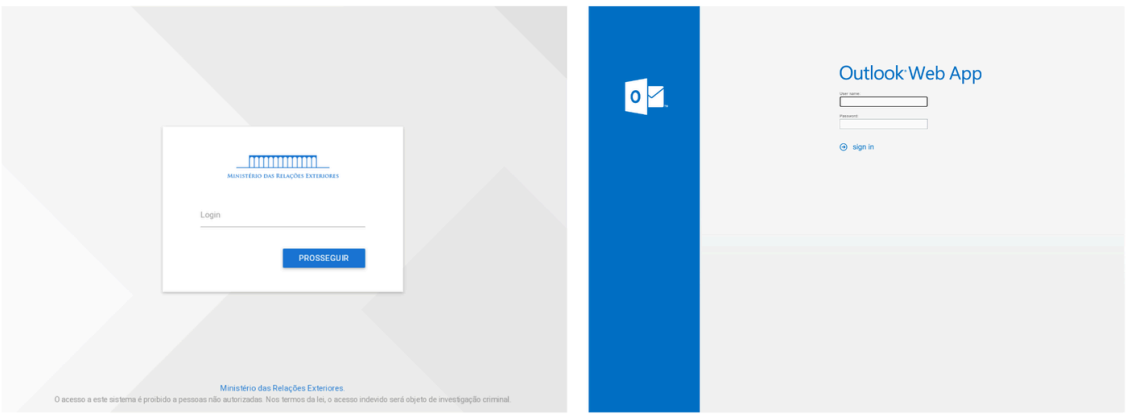
The examples here highlight recent and historical examples where cyber espionage actors have targeted users and organizations in Brazil. It should be noted that these campaigns describe targeting and do not indicate successful compromise or exploitation.

PRC Cyber Espionage Activity Targeting Brazil

Cyber espionage activity linked to the People's Republic of China (PRC) targeting Brazil dates back more than a decade. Since 2020, we have observed 15 PRC cyber espionage groups targeting users in Brazil, and these groups have accounted for over 40% of government-backed phishing activity targeting Brazil. As the largest recipient of Chinese investment in Latin America, this volume of PRC cyber espionage is reminiscent of activity in other regions where Chinese government investment has been focused, such as countries within China's Belt and Road Initiative. In addition to activity targeting Gmail users, PRC groups have targeted Brazil's military, national government, diplomatic organizations, and the provincial governments of multiple Brazilian states. These groups have targeted users in Brazil using tactics ranging from phishing to malware distribution and exploitation of known vulnerabilities.

In August 2023, for example, Google detected a campaign from a PRC group that targeted nearly two hundred users in a Brazilian executive branch organization. The phishing emails contained links to an encrypted ZIP archive hosted on a known phishing domain. Organizations in Brazil's state governments have also been a target. In late 2022, PRC actors used an operational relay box (ORB) network to anonymize their activity and attempted to send a mass phishing campaign to nearly two thousand email addresses, including 70 email addresses in the .br ccTLD, the majority of which belonged to Brazilian state government organizations. The mass email, which Gmail blocked, contained a malicious TAR attachment designed to exploit CVE-2022-41352, an n-day vulnerability in the Zimbra Collaboration Suite that enables an attacker to upload arbitrary files and gain unauthorized access to other user accounts. The campaign targeted organizations globally and appeared opportunistic - most of the targeted email addresses were addressed to the domain admin (e.g., admin@[domain].gov.br).

PRC cyber espionage activity against local and provincial entities is of note in light of campaigns by threat actors such as UNC4841 that have focused on similar targets globally, including in Brazil. As part of their exploitation of the Barracuda Email Security Gateway in 2023, UNC4841 targeted a Brazilian business association focused on promoting state-level commerce across several industries.



Phishing pages created by PRC cyber espionage groups targeting Brazil's government

North Korean Government-Backed Groups Targeting Brazil

Since 2020, North Korean cyber actors have accounted for approximately a third of government-backed phishing activity targeting Brazil. North Korean government-backed actors have targeted the Brazilian government and Brazil's aerospace, technology, and financial services sectors. Similar to their targeting interests in other regions, cryptocurrency and financial technology firms have been a particular focus, and at least three North Korean groups have targeted Brazilian cryptocurrency and fintech companies.

In early 2024, PUKCHONG (UNC4899) targeted cryptocurrency professionals in multiple regions, including Brazil, using a Python app that was trojanized with malware. To deliver the malicious app, PUKCHONG reached out to targets via social media and sent a benign PDF containing a job description for an alleged job opportunity at a well known cryptocurrency firm. If the target replied with interest, PUKCHONG sent a second benign PDF with a skills questionnaire and instructions for completing a coding test. The instructions directed users to download and run a project hosted on GitHub. The project was a trojanized Python app for retrieving cryptocurrency prices that was modified to reach out to an attacker-controlled domain to retrieve a second stage payload if specific conditions were met.

coinbase

2. Node.js:

- API Creation: Design a simple REST API in Node.js that supports CRUD operations for managing a list of tasks. Include route definitions and handlers.

Problem Solving

- Given a scenario where your Python script's performance is significantly slower than expected, how would you diagnose and fix the performance issue?
- Describe a situation where Node.js would not be an ideal choice for a project. What alternatives would you consider?

Soft Skills:

- How do you keep up with the latest developments in software engineering and programming languages?
- Can you describe a challenging problem you encountered in a past project and how you resolved it?

Coding and Problem-Solving Skills With Real Project

Test Project (Python): https://github.com/vincentchavez/PythonExam

Problem 1: To get coin BTC/ETH rate by using the project.

Problem 2: As you see in the source code, this project keeps getting BTC/ETH rate from 5 markets every 5 seconds and prints out.

- Please try to find out and add 3 more similar markets API.
- Subscribe how to make graph of the rate by using Python.

Problem 3: Please describe how to improve the speed of the network communication in this code.

PUKCHONG (UNC4899) sent targets instructions to download a trojanized Python app from GitHub

North Korean government-backed groups have also in the past targeted Brazil's aerospace and defense industry. In one example, PAEKTUSAN created an account impersonating an HR director at a Brazilian aerospace firm and used it to send phishing emails to employees at a second Brazilian aerospace firm. In a separate campaign, PAEKTUSAN masqueraded as a recruiter at a major US aerospace company and reached out to professionals in Brazil and other regions via email and social media about prospective job opportunities. Google blocked the emails, which contained malicious links to a DOCX file containing a job posting lure that dropped AGAMEMNON, a downloader written in C++. The attacker also likely attempted to deliver the malware via

messages on social media and chat applications like WhatsApp. The campaigns were consistent with Operation Dream Job and activity previously described by Google. In both campaigns, we also sent users government-backed attacker alerts notifying them of the activity and sharing information about how to keep their accounts safe.

One North Korean group, PRONTO, concentrates on targeting diplomats globally, and their targets in Brazil follow this pattern. In one case, Google blocked a campaign that used a denuclearization-themed phishing lure and the group's typical phishing kit - a fake PDF viewer that presents the users with a login prompt to enter their credentials in order to view the lure document. In another case, PRONTO used North Korea news-themed lures to direct diplomatic targets to credential harvesting pages.

One of the emerging trends we are witnessing globally from North Korean threat activity today is the insider threat posed by North Korean nationals gaining employment surreptitiously at corporations to conduct work in various IT roles. Though we have not yet observed direct connections between any of these North Korean IT workers and Brazilian enterprises, we note the potential for it to present a future risk given the growing startup ecosystem in Brazil, historical activity by North Korean threat actors in Brazil, and expansiveness of this problem.

Diminished Activity From Russia Since Start of Ukraine War

Activity by Russian government-backed groups targeting Brazil has diminished significantly since the start of the war in Ukraine. Of the seven Russia-backed groups observed targeting Brazil, over 95% of the phishing activity targeting users in Brazil comes from one group, APT28 (aka FROZENLAKE). APT28's targeting of Brazil dates back more than a decade, and Brazilian users have regularly been a target in the group's frequent phishing campaigns. In late 2021, more than 200 Brazil-based users were targeted in large scale phishing campaigns by APT28. In those campaigns, which took place over several days between September and October 2021, APT28 sent credential phishing emails to over 14K recipients globally. Following late 2021, Russian groups have not targeted Brazil on a regular basis - a shift likely due at least in part to Russia's efforts to prioritize cyber operations focused on Ukraine and NATO.

Brazil's Unique Cybercrime Ecosystem

Financially motivated threat activity represents a constant, serious threat to users and organizations in Brazil. Notably, we have observed a variety of operations, including ransomware and data theft extortion as well as underground forum and social media advertisements for access to malicious insiders, databases, sensitive information, and specialized tools to compromise Brazilian users and institutions.

Although cybercriminal actors focused on financial gain represent a transnational threat and emanate from all corners of the globe, particular communities sometimes spring up with more localized characteristics. For example, Russian-language only forums in the eastern European underground market ecosystem shape the flow of malware, data offered for sale, and formation of criminal relationships. Similarly in Brazil, Brazilian Portuguese-specific cybercriminal communities enable a localized and domestic threat.

Brazilian Cybercrime Communities

Mandiant's insights into advertisements and discussions within Brazilian Portuguese-language underground marketplace over the past year illustrate that these actors have access to a variety of malicious tools and products, including the compromise and sale of payment card data, credentials, and sensitive databases; phishing; development and sale of remote access trojans (RATs); insider access; and mobile threats.

Notably, these actors rely significantly less on traditional underground forums, which are the most common platforms used in other regions, and tend to rely on alternatives such as mobile apps and social media, particularly Telegram and WhatsApp.

In general, the technical capability of actors engaged in cybercrime activity is generally low to moderate relative to underground communities in other regions. Consistent with past trends, we continue to see threat actors from Latin American underground communities primarily advertise products designed to target their own region. Notably, more experienced members of Brazilian Portuguese-language cybercrime underground often appear willing to teach and mentor less skilled and/or new actors. While some actors charge for this, others offer this help and support for free. Teaching less experienced members for free can help the mentor improve their reputation, grow their group's membership, and demonstrate their own skills and knowledge.

Malware Targeting PIX Interbank Transfer System

We have observed Latin American-based threat actors leverage and target country-specific payment platforms, either to facilitate sales of services or to target payment information from victims. In the case of Brazil, such activity has focused on Pix, an instant payment platform created and managed by the Brazilian Central Bank. Pix enables instant payments and transfers between bank accounts within seconds using a key, and it is one of the most common methods of payment in Brazil.

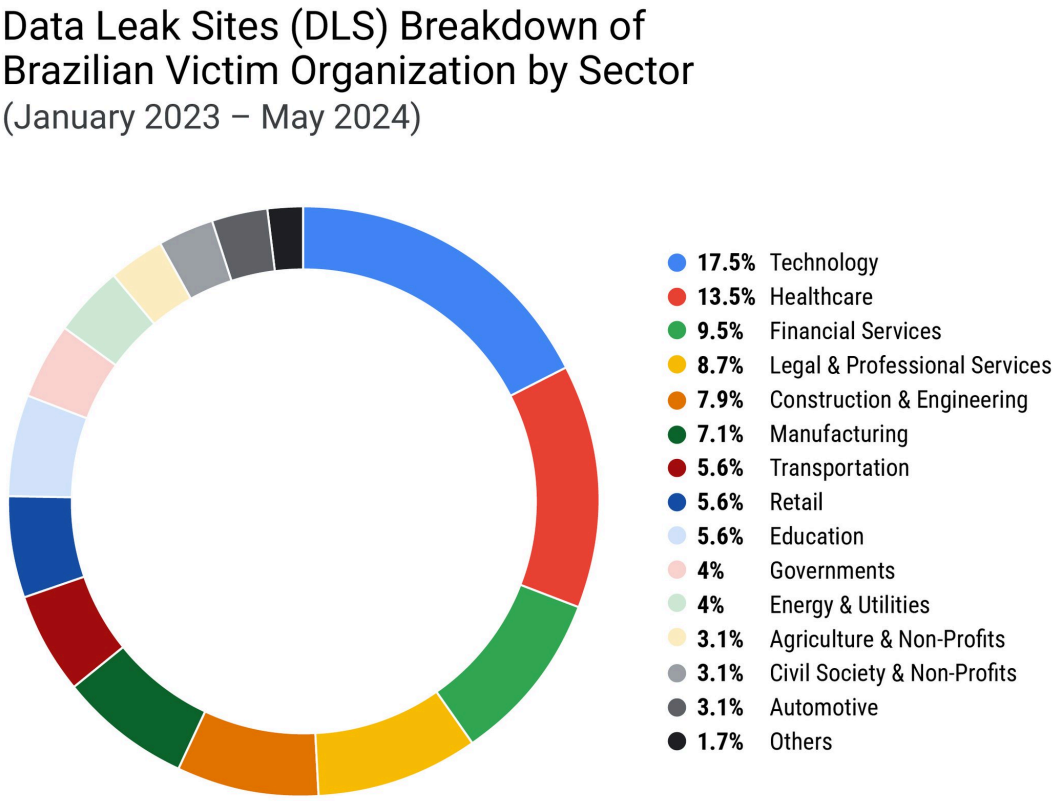
Open source reporting indicates threat actors as recently as late 2023 were involved in distributing malware called "GoPix" to specifically targeted Pix users via malicious advertisement techniques or "malvertising." The reported functionality of this malware includes the ability to hijack clipboard functionality for Pix or cryptocurrency transactions, replacing the Pix string or wallet address with one controlled by the attacker.

UNC5176 Distributes URSA Malware

Another group that has historically targeted users and enterprises across Latin America, is UNC5176, a suspected Brazil-based threat cluster that distributes malware targeting users of Latin American and Spanish banks, including in Brazil. In late April, Mandiant observed an UNC5176 campaign distributing URSA to victim organizations in sectors such as financial services, healthcare, retail, and hospitality. In this recent campaign Mandiant did not observe targeting of entities in Brazil. URSA is a backdoor that is capable of stealing login credentials for various banks, cryptocurrency websites, and email clients. UNC5176 uses emails and malvertising campaigns to compromise users, typically delivering emails that have a ZIP file attached that contains a malicious HTA file. When opened, these HTA files drop a VBS file that connects to a C2 and downloads a second stage VBS file. The downloaded VBS file contains guardrails including anti-VM/Sandbox and OS language checks, if the checks are passed it initiates connections to the C2 and an URSA payload is downloaded and executed.

Beyond Borders: Multifaceted Extortion's Impact on Brazil

While many of the financially motivated cyber threats impacting Brazil originate domestically, Brazil also faces global risks such as ransomware and data theft as a means of extortion. While the most prolific multifaceted extortion campaigns continue to focus on North America and Europe, these threat actors have also exploited Brazil. For example, based on analysis of alleged victims listed on Ransomware as a Service (RAAS) RANSOMHUB's data leak site, their second most targeted country based on listed victims is Brazil, after the United States. RANSOMHUB’s ransomware operations have impacted organizations across multiple geographic regions and spanning almost every industry vertical. Since January 2023, across data leak sites (DLS) that Mandiant tracks, for enterprises based in Brazil, the top most targeted verticals were technology, healthcare, and financial services.



Impersonating Official Government Services to Distribute Malware

Malware distribution campaigns targeting Brazilians frequently use tax and finance-themed lures to convince recipients to open malicious links or files. One financially motivated group we track, PINEAPPLE, regularly masquerades as Brazil’s revenue service, Receita Federal do Brasil, in spam campaigns that attempt to convince users to install the Astaroth infostealer. The overwhelming majority of these campaigns were blocked on arrival for Gmail and Workspace users. The campaigns often spoof Receita Federal’s legitimate email address, `receita@gov[.]br`, and use different techniques to convince email gateways the email is authentic - for example, using mail forwarding services, which do not drop messages with failed SPF records, or placing unexpected data in the SMTP `Return-Path` field to trigger a DNS request timeout and cause SPF email authentication checks to fail.

In one recent campaign blocked by Gmail, PINEAPPLE's spam emails impersonated Brazil's finance ministry and directed recipients to a social engineering page that mimicked the Brazilian government's electronic tax document system (Portal da Nota Fiscal Eletrônica). The site directed visitors to click a button to view an electronic tax document generated by the system. If clicked, the link directed users to an LNK payload hosted on an attacker-controlled IP address. In a likely effort to evade detection, the attackers incorporated multiple legitimate services into the campaign. Links on the social engineering site used the `ms-search://` protocol to direct users to the attackers' IP address, and threat actors hosted their site on GCP Cloud Run. Google disabled the malicious Cloud Run site and suspended the associated GCP project.

Social engineering page impersonating the Brazilian government's electronic tax document system (Portal da Nota Fiscal Eletrônica)

Abusing Legitimate Cloud Services to Distribute Astaroth Infostealer

PINEAPPLE often abuses legitimate cloud services in their attempts to distribute malware to users in Brazil. The group has experimented with a number of cloud platforms, including Google Cloud, Amazon AWS, Microsoft Azure and others.

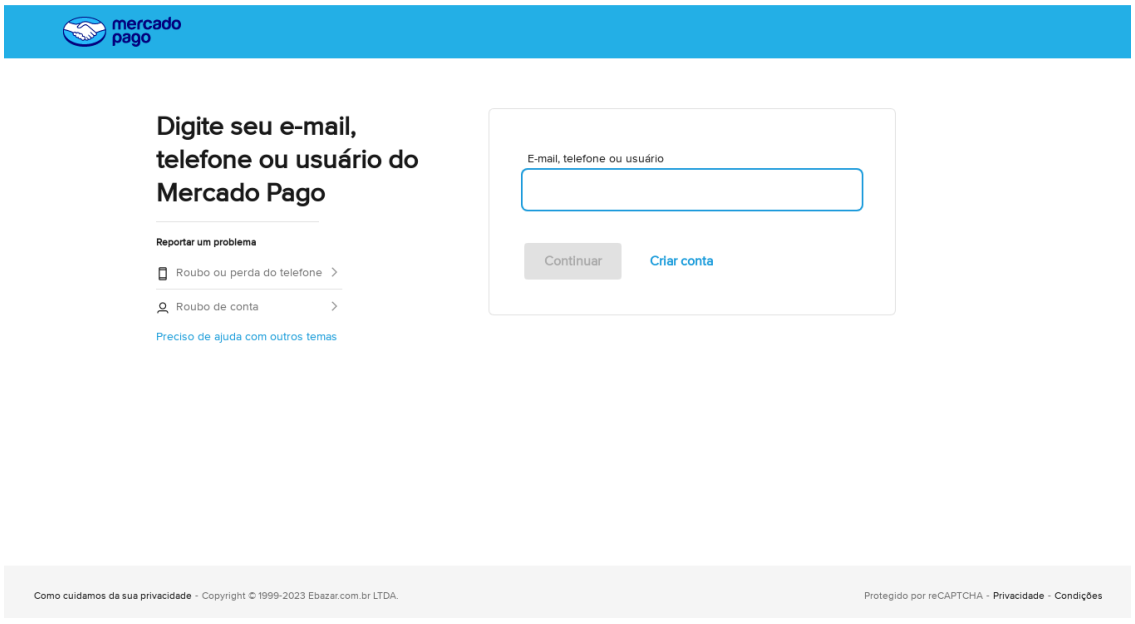
In 2023, teams across Google worked together to disrupt PINEAPPLE's misuse of Google Cloud Run and Cloud Functions. In those campaigns, PINEAPPLE used compromised Google Cloud instances and Google Cloud projects they created themselves to create their own Google Cloud container URLs hosted on legitimate GCP domains such as `cloudfunctions.net` and `run.app`. The URLs hosted landing pages that then redirected targets to malicious infrastructure that dropped the Astaroth infostealer. Upon discovery, Google disabled the malicious Cloud Run and Cloud Functions sites and suspended the associated GCP projects. We also increased our detection and response coverage and implemented product level security improvements to significantly increase the difficulty of our platforms being used by this threat actor. These mitigation measures reduced the volume of the Astaroth campaigns by 99% compared to the campaign's peak.

PINEAPPLE reacts quickly and iteratively adapts their TTPs in response to new detections. Following the disruption of their scaled abuse campaigns, PINEAPPLE's abuse of Cloud Run has continued intermittently at lower volumes. The group has also experimented with other cloud services, including Google Compute Engine. Similar to their past campaigns, PINEAPPLE distributed malicious links via email. The GCE links were configured to serve an unencrypted archive such as a ZIP, LNK, or other, lesser known file types. Google Cloud Trust & Safety suspended PINEAPPLE's attacker-operated GCP projects. Shortly thereafter, the group began experimenting with other cloud platforms including Microsoft and Tencent.

Recent PINEAPPLE campaigns in May and June 2024 continued to spoof Receita Federal and hosted landing pages on dedicated virtual servers created through GoDaddy's reverse IP hostname service. In other recent cases, PINEAPPLE has used mail forwarding services to send emails that appear to come from WhatsApp. We continue to monitor their campaigns and regularly update Google's protections to ensure users are protected.

Credential Phishing

Credential phishing is also a common threat affecting users and organizations in Brazil. In 2023, for example, Google disrupted phishing activity hosted on GCP serverless projects that were being used to harvest credentials for one of Latin America's largest online payment platforms. The pages were operated by Latin America-based financially motivated actor, FLUXROOT, a group best known for their distribution of the Grandoreiro banking malware. Upon discovering the FLUXROOT sites, we updated detection signatures and added the sites to the Safe Browsing blocklist. More recently, FLUXROOT has continued distribution of Grandoreiro, using cloud services such as Azure and Dropbox to serve the malware.



Credential harvesting page hosted on GCP serverless project

Conclusion

As Brazil continues to grow in economic and geopolitical significance, it will remain an attractive target for threat actors driven by diverse motivations. The country's digital landscape is a complex arena, developed and expanded

over the years by a convergence of both global and local threats. Global cyber espionage actors from North Korea, the People's Republic of China (PRC), and Russia as well as multinational cybercriminals pose longstanding threats, and Brazil's domestic cybercriminal market remains a persistent challenge–increasing the complexities of this dynamic landscape.To effectively safeguard Brazilian enterprises and users, it is important to understand this unique interplay of threats and adopt a proactive approach to cybersecurity.

We hope the analysis and research here helps to inform defenders in Brazil, providing fresh insights for collective defense. At Google, we are committed to supporting the safety and security of online users everywhere and will continue to take action to disrupt malicious activity to protect our users and help make the Internet safe for all.

Indicators of Compromise (IOCs)

Host-Based Indicators (HBIs)

Filename	SHA256	Description
Question Sheet.pdf	e9841e5c218611add64c07b6d6e8b2f2a899ee32da2bb0326238b332f34bd045	Benign PDF delivered in PUKCHONG social engineering activity targeting cryptocurrency firms
0tiukr.verdelimp.com518.429006.45528.lnk	38fad88f0fefb385fdfba2e0be28a1fe6302387bc4a0a9f8b010cca09836361d	Malicious LNK dropped in PINEAPPLE campaigns
NFe92759625212697.115112.62531.lnk	57a0a64ff7d5ca462fe18857f552ab186d118a80ecad741be62ee16e500ac424	Malicious LNK dropped in PINEAPPLE campaigns

Posted in

- Threat Intelligence
