

Pirates of Brazil: Integrating the Strengths of Russian and Chinese Hacking Communities

By Insikt Group



Recorded Future's Insikt Group analyzed advertisements, posts, and interactions within hacking and criminal forums to explore the capabilities, culture, and organization of Brazilian hacking communities. Sources include the Recorded Future® Platform as well as open web, dark web, and underground forum research.

This report, which is part of a series that started with [Russia and China](#), [Japan](#), and [Iran](#), will be of greatest interest to organizations seeking to understand the criminal underground to better monitor financial vertical and company-specific threats, as well as to those investigating the Brazilian criminal underground.

Executive Summary

Each country's hackers are unique, with their own codes of conduct, forums, motives, and payment methods. Recorded Future's Portuguese-speaking analysts, with a long-standing background in the Brazilian underground, have analyzed underground markets and forums tailored to the Brazilian Portuguese audience over the past decade and discovered a number of particularities in content hosted on forums, as well as differences in forum organization and conduct.

The primary target of Brazilian hackers is Brazilians. Hackers in Brazil range from the entry-level hackers and security researchers who disclose vulnerabilities in private conferences to black hat hackers who sell illicit products and services. Brazilian hackers are always in search of the next opportunity for easy money. When companies react to their activity by increasing security controls, they move to another business. The abilities of high-level hackers are illustrated through Brazilian law enforcement efforts like [Operation Ostentation](#) and the ATM malware by Prilex gang.

Brazilian forums are not necessarily based on web forums. The Chinese underground is more similar to Brazil's than Russia's in that way, but Chinese cybercriminals rely on local apps such as QQ and Wechat. The Brazilian forum platform of choice is dynamic, changing based on broader social trends and law enforcement efforts. At this time, the forums of choice are WhatsApp and Telegram. Access to Brazilian forums is not as strict as in the Russian-speaking underground. However, because the Brazilian underground is scattered among Telegram and WhatsApp groups, the collection sources are varied. Information in Brazilian forums is not as well organized as in Russian-speaking forums, where threads for products or services are fixed, with well-structured posts including features and pricing.

Key Judgments

- Carding is strong in the country. There is a strong activity of credit cards generated by algorithms — “geradas” in the local slang. This is not observed by Insikt Group in the other geographies covered by this series, at least not explicitly.
- Spam, through email, SMS, social media, and messengers, is still one of the primary methods of malware and phishing distribution. Local actors are taking advantage of less strict security mechanisms in SMS to distribute URLs or malware samples.
- Mass pharming attacks involving vulnerable customer-premises equipment (CPE), observed for the first time in 2014, are still an important method of credentials collection. Typical targets are financial institutions, streaming services, and web hosting companies.
- Brazilian cybercriminals are not intimidated by two-factor authentication (2FA). While the majority of entry-level hackers move to another activity, high-level hackers insist — and succeed — in bypassing this security control. Techniques observed by Insikt Group include SIM-swap attacks, full compromise of desktops used for internet banking, and hackers’ direct interaction and interference with banking sessions.



BRAZIL

Brazilian cybercriminals hold one thing above all else: money. They change their TTPs and platforms at any time, depending on where the easy money is and what law enforcement and security researchers are doing to collect information on them. Their targets are usually other Brazilians.

The platforms of choice for Brazilians changes often, but web forums have never played a significant role, and mobile apps like Whatsapp and Telegram are much more popular venues to advertise products and services. Communications are largely in Brazilian Portuguese.

RUSSIA

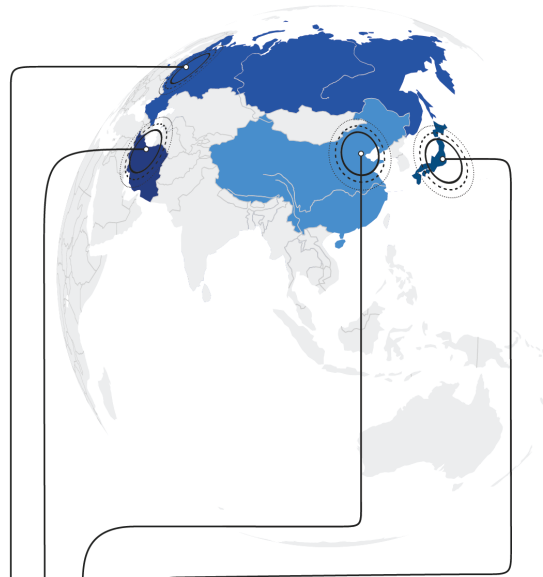
Russian forums, which are largely Russian- and English-speaking, leave little room for socialization or camaraderie — Russian cybercriminals value money above all else. Russian threat actors rarely ever target victims in Russia or countries allied with it, and politically motivated attacks are less common.

Russian criminal forums are compartmentalized — for example, fraudsters and hackers largely operate on different forums. Among hacking forums, three main tiers have evolved: open, semi-private, and closed.

IRAN

Iranian cyber operations are conducted by contractors that compete for government-sponsored offensive campaigns distributed by ideologically and politically trustworthy middle managers. This creates unique trade-offs — ideological devotion and strong hacking skills are often mutually exclusive.

The main Iranian security forum, Ashiyane, had known connections to the Islamic Revolutionary Guard Corps and was a key source for contractors to identify talent and share information until it was shut down in August 2018. The Iranian hacker community has since then largely split into two distinct forums, all conducted in Farsi.



JAPAN

The Japanese underground is less mature and consists of largely collaborative, anonymous forums mostly housed within Japanese-language, general-purpose bulletin board systems. Illegal drug sales dominate, and the adoption of cryptocurrency lags, with transactions mostly using prepaid gift cards.

Members will also register accounts on non-Japanese message boards to gain information or access to tools and services not readily accessible within domestic forums.

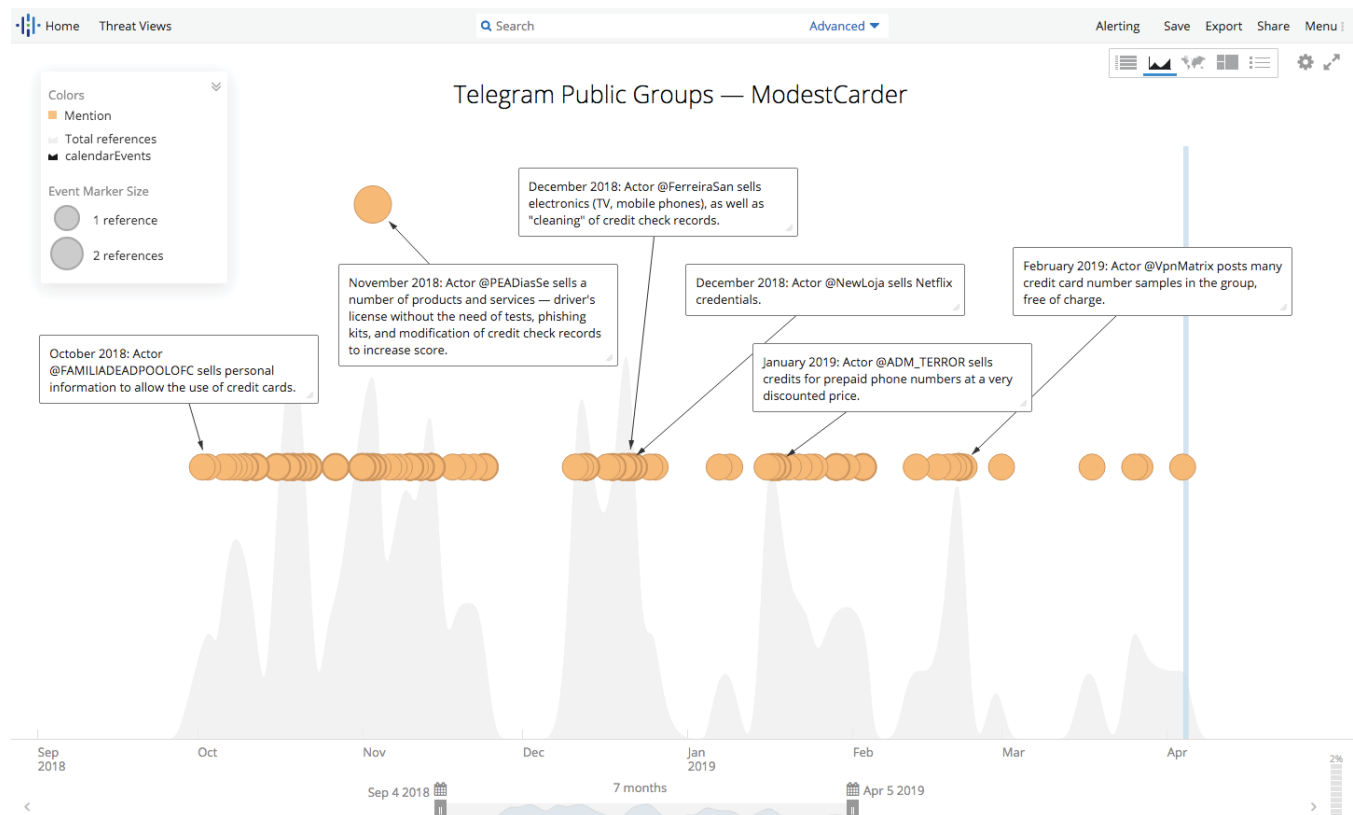
CHINA

Chinese forum members feel an overwhelming sense of community and patriotism. The term “geek spirit” (极客精神) is used to denote forum culture and refers to groups of technical individuals who hope to create a more ideal society.

Many forums require members to engage with a post, either through a comment or personal message. Many hackers also rely on invite-only chat groups or forums within Chinese social media apps QQ, Baidu, or WeChat. Chinese forums and marketplaces are organized similarly to the three tiers (open, semi-private, and closed) of Russian forums.

Brazilian Communities: Pirate Spirit

Similar to Russian-speaking cybercriminals, Brazilian cybercriminals hold one thing above all else: money. Hacker communities in Brazil differ in their neighborhoods, motivations, goals, and communication platform of choice.



Telegram, a very relevant source to Brazil that was recently added to Recorded Future.

Whereas we used "thieves" and "geeks" to define Russian and Chinese undergrounds, respectively, we describe Brazilian hackers as "pirates" because they are not just specialized thieves like the Russian-speaking actors, but are ready to change their TTPs and forum platforms at any time, depending on where the easy money is and what law enforcement and security researchers are doing to collect information on them. At the same time, a very select group of Brazilian cybercriminals resemble their Chinese counterparts, in that they can bypass strict internet banking security controls and ATM security in an impressive way.

History of the Brazilian Underground

Commercial internet was introduced in Brazil between 1995 and 1996. In the late '90s, Internet Relay Chat (IRC) networks and ICQ messenger — as well as bulletin board systems (BBS), web-based forums, and chats — became the main chat platforms in Brazil.

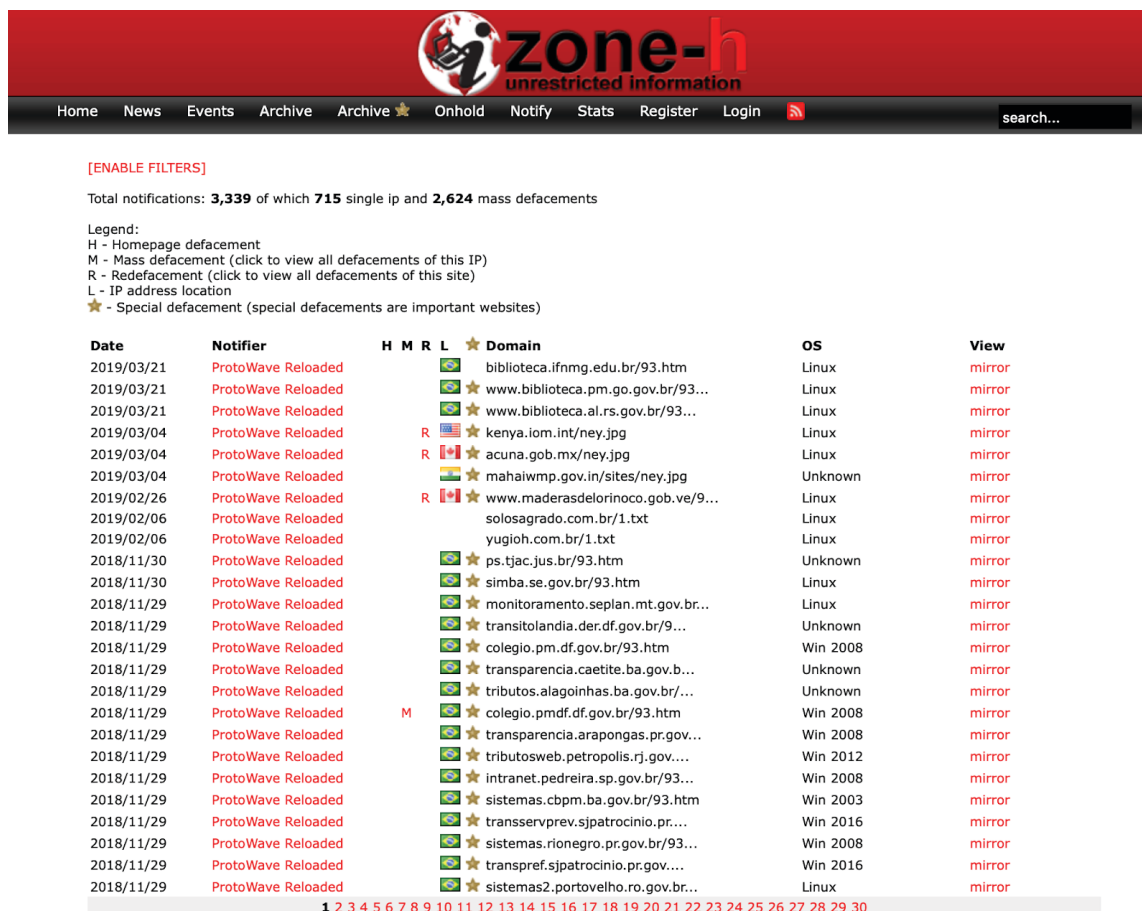
IRC channels were the forums of choice for professional hackers in the 2000s and early 2010s. Activity included advertisements of products and services, bulk credit card information, and discussions — none of it organized by topic. For example, IRC servers operated by the groups Silver Lords and FullNetwork — better described as an IRC network than as a group — ruled the underground for years.

“mIRC” — the name of a very popular IRC client that became synonymous with the Brazilian term for IRC client — became very popular among all types of users. Brasirc and Brasnet were the most popular IRC networks, and from its channels emerged some of the first-known threat activity in Brazil: intentional IRC flooding attacks (a kind of denial-of-service attack) against the IRC server host, takeovers of usernames, and coordinated attacks.

IRC protocol was a favorable environment for hacking discussions, with features including controlled access to channels and servers, the ability to grant specific privileges to each user, and bots. At first, hackers met in public IRC networks like Brasirc and Brasnet, but over time they began hosting their own IRC servers. It was harder to find those servers, which gave users and administrators a certain degree of privacy. Just like in special access web forums found in Russian-speaking countries, there was access control. A registered “nick” (nickname) was required to join channels in certain servers and the bot (service) that managed the nicks (NickServ) was not available at all times.

A common area of interest among Brazilian hackers across many groups, skill levels, and motives is penetration testing. This is one of the main topics of most local hacker conferences and entry-level web forums, where tools and tutorials are shared.

In Brazil, website defacement was always one of the main types of hacking activities. Brazilians always were — and still are — one of the top reporters of website defacements to the popular defacement archive zone-h[.]org.



Date	Notifier	H	M	R	L	★	Domain	OS	View
2019/03/21	ProtoWave Reloaded						biblioteca.ifnmg.edu.br/93.htm	Linux	mirror
2019/03/21	ProtoWave Reloaded						www.biblioteca.pm.go.gov.br/93...	Linux	mirror
2019/03/21	ProtoWave Reloaded						www.biblioteca.al.rs.gov.br/93...	Linux	mirror
2019/03/04	ProtoWave Reloaded	R					kenya.iom.int/ney.jpg	Linux	mirror
2019/03/04	ProtoWave Reloaded	R					acuna.gob.mx/ney.jpg	Linux	mirror
2019/03/04	ProtoWave Reloaded						mahaiwmp.gov.in/sites/ney.jpg	Unknown	mirror
2019/02/26	ProtoWave Reloaded	R					www.maderasdelorinoco.gob.ve/9...	Linux	mirror
2019/02/06	ProtoWave Reloaded						solosagrado.com.br/1.txt	Linux	mirror
2019/02/06	ProtoWave Reloaded						yugioh.com.br/1.txt	Linux	mirror
2018/11/30	ProtoWave Reloaded						ps.tjac.jus.br/93.htm	Unknown	mirror
2018/11/30	ProtoWave Reloaded						simba.se.gov.br/93.htm	Linux	mirror
2018/11/29	ProtoWave Reloaded						monitoramento.seplan.mt.gov.br...	Linux	mirror
2018/11/29	ProtoWave Reloaded						transitolandia.der.df.gov.br/9...	Unknown	mirror
2018/11/29	ProtoWave Reloaded						colegio.pm.df.gov.br/93.htm	Win 2008	mirror
2018/11/29	ProtoWave Reloaded						transparencia.caetite.ba.gov.b...	Unknown	mirror
2018/11/29	ProtoWave Reloaded						tributos.alagoinhas.ba.gov.br/...	Unknown	mirror
2018/11/29	ProtoWave Reloaded						colegio.pmdf.df.gov.br/93.htm	Win 2008	mirror
2018/11/29	ProtoWave Reloaded						transparencia.arapongas.pr.gov...	Win 2008	mirror
2018/11/29	ProtoWave Reloaded						tributosweb.petropolis.rj.gov....	Win 2012	mirror
2018/11/29	ProtoWave Reloaded						intranet.pedreira.sp.gov.br/93...	Win 2008	mirror
2018/11/29	ProtoWave Reloaded						sistemas.cbpm.ba.gov.br/93.htm	Win 2003	mirror
2018/11/29	ProtoWave Reloaded						transservprev.sjpatrocinio.pr....	Win 2016	mirror
2018/11/29	ProtoWave Reloaded						sistemas.rionegro.pr.gov.br/93...	Win 2008	mirror
2018/11/29	ProtoWave Reloaded						transpref.sjpatrocinio.pr.gov....	Win 2016	mirror
2018/11/29	ProtoWave Reloaded						sistemas2.portovelho.ro.gov.br...	Linux	mirror

ProtoWave Reloaded group's verified submissions to Zone-H, a notorious web defacement archive. To date, this Brazilian group has defaced more than 1,250 webpages.

Historically, most Brazilians involved with website defacement were teenagers learning how to exploit software vulnerabilities and badly configured internet-facing systems. Defacement was considered a learning experience in the absence of security frameworks — from reconnaissance to penetration testing and vulnerability exploitation.

From 2005 to the present day, there is still a significant website defacement community in the Brazilian underground, and the motive has evolved from warning administrators to hacktivism. In Brazil, the theme of defacements also corresponds to the current headlines in newspapers: natural disasters, political scandals, and so on.

Some of the most notorious hacker groups of the early 2000s emerged during the IRC era:

- **Website Defacement:** Prime Suspectz¹, Silver Lords, Insanity Zine, HFury, DataCha0s, Crime Boys
- **Hacking:** Unsekurity Scene, or just “unsek,” and its “spin off” groups Clube dos Mercenários (CDM), Front The Scene (FTS)

In the context of hacking, the activity was mainly security research on reconnaissance, penetration testing, and known vulnerability exploitation. Given the limitations of that time — no vast penetration testing literature, frameworks like Metasploit, or tools like Kali Linux — it is possible that some of those researchers began as web defacement actors.

In a series of articles published in 2001, investigative journalist Giordani Rodrigues [interviewed](#) the main web defacement groups of that time. In most of them, actors were between 15 and 22 years old. Most likely, that age range has not changed significantly. Actors in that age range tend to act irresponsibly — maturity and ethics are what separate a web defacer who becomes a security professional from one who moves to other outcomes of an intrusion, like data exfiltration or lateral movement.

In 2010, when Anonymous activity began worldwide, the same activity was observed in Brazil. It began as a support to Wikileaks in the second half of 2010, and continues in various forms to the present day. The highest level of Anonymous activity occurred between 2011 and 2015, when most global operations had support from local groups. Targets were mostly political, and distributed denial of service (DDoS) was the primary type of attack. In 2011, Brazilian Federal Police [probed](#) the activity of Anonymous in Brazil, as multiple government websites were targets.

Since 2016, groups that claim to support Anonymous’s cause have targets that vary with the headlines of local news and public opinion. Corrupt politicians, companies involved in corruption scandals, candidates in elections, the 2016 Summer Olympics in Rio de Janeiro, the 2014 FIFA World Cup in Brazil — any target or topic is eligible for a local Anonymous campaign. After DDoS attacks became ineffective, the most typical attack became — and still is —

¹ Defacements authored by Prime Suspectz [archived](#) in Zone-H.

leak of breach data. In the past year, Anonymous activity primarily focused on political targets. In the last incident, AnonOpsBR, one of the only groups with recent and recurrent activity, has attacked the Brazilian Ministry of Defense and now president Jair Bolsonaro, as well as the vice president.

Organization of the Brazilian Underground

In Brazil, any platform used for interaction could be considered a hacker forum. As we stated before, the typical organization of Russian-speaking criminal underground communities does not apply to what we observe in Brazil, as each forum does not have a singular purpose, nor are they well organized, lacking fixed threads for products or services or well structured posts with features and pricing. This makes a big difference in terms of understanding the local underground.

Unlike in Russian-speaking countries, Jabber/XMPP was never a popular chat platform for Brazilian hacker forums. We can state with a high level of confidence that communities of interest jumped from IRC to the modern mobile chat platforms, such as Telegram, WhatsApp, TeamSpeak (gaming), and Discord (gaming), beginning in 2015. Privacy-oriented messengers like Wickr and Signal are more frequently seen in Tor dark web forums and markets.

Orkut, by Google, was the first popular social network in Brazil. From 2004 to 2010, it was the center of the internet — along with the hacking scene — for Brazilians. Private Orkut groups were created for selling hacking products and services. The organization of advertisements was very similar to what we see in Russian-speaking web forums. Around 2010, users started to migrate to Facebook, including the hackers. In 2014, Orkut was discontinued by Google.

The use of social networks for cybercrime shows how unprofessional certain groups of Brazilian hackers are. Any actor from Russian-speaking or Chinese-speaking forums would know that social networks are a risky place to conduct illicit business. The companies who own those networks are generally obliged to cooperate with local authorities, making it easier for law enforcement to investigate and detain hackers.

In Brazil, cybercrime actors started to use Facebook for advertisement as soon as the social network became popular in the country in 2011. Groups were closed, but there was no strict review or vetting process — it was just a matter of requesting access and having it granted.

In 2011, Kaspersky Lab found a website created for hackers to check if another hacker they were doing business with was reliable or a “ripper” (scammer). The service was dubbed “SPC dos Hackers,” which essentially means “Hacker’s Credit Report,” and it was a database of usernames, the contact information associated with each of those usernames, and assessments of those users — positive or negative.

On average, Brazilian cybercriminals from entry to medium level do not demonstrate concerns about operational security (OPSEC) and law enforcement. It is common in the country to see criminals detained for cybercrime only to be released days or weeks later.

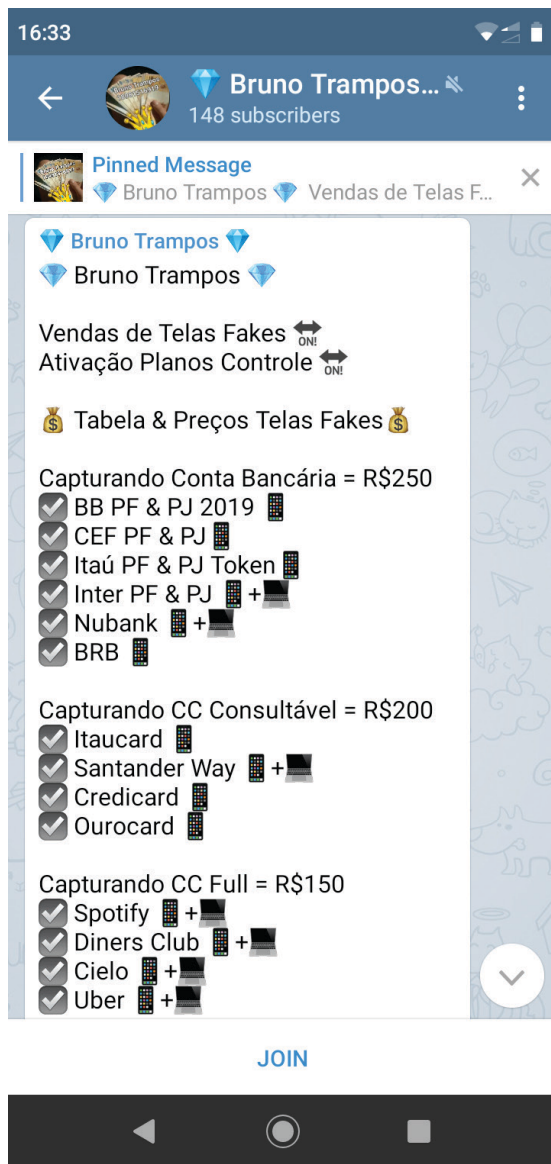
Current Landscape

Brazilian web forums do not have a significant role in the Brazilian underground. They never did, and most likely never will. In 2010, the most prominent hacker web forums were essentially the same as the most active ones in 2019: Fórum Hacker and Guia do Hacker. Some forums emerged and were voluntarily taken down in the meantime, like Perfect Hackers, which was taken down in 2018. However, those prominent forums remain the main hacker communities, open to the public. There is no vetting process or payment required to register — anyone can join these forums.

Brazilian web forums are an environment for learning how to become a hacker and the sharing of information and tools. In Brazil, forums have been home to entry-level hackers (script kiddies) since at least 2010. They stay in the forums while it is useful for them to learn hacking methodologies. Camaraderie is praised and encouraged. There are products and services for sale. Mobile forums — specifically, Telegram channels — became the preferred environment to advertise products and services.

More recently, when groups moved to Telegram, it was observed that most of the channels have minimal access control — a defined

username is the necessary and sufficient condition to gain access to some channels. Brazilian public Telegram channels are available in the platform.



Telegram channel with advertisements for phishing kits

In the screenshot above, the administrator of a Telegram group advertises “telas fake” — a local slang for phishing kits. In this particular case, there are three different types of product: capturing the bank account credentials for 250 BRL (66 USD), capturing basic credit card information for 200 BRL (53 USD) and capturing full credit card information (including name and address) for 150 BRL (40 USD). Cell phone icons indicate the kit is compatible with mobile phones.

Web forums like Forum Hacker and Guia do Hacker are considered by many Brazilians a good way to get immersed in network and information security. The majority of entry-level hackers are not able to enter the white hat and black hat communities in Brazil. This is best shown by the insular, invite-only nature of Brazilian hacker conferences.

[Sacicon](#) is another one-day, invite-only conference that has taken place in São Paulo since 2012. This conference is similar to YSTS, with a focus on highly technical talks and partying. This conference is promoted by the same organizers of the Hackers to Hackers Conference ([H2HC](#)), the first (starting in 2004) and most notorious hacker conference in Brazil. The organizers of [Roadsec](#), a conference targeted at the entry-level security professional or student more than any other audience, also support Sacicon.

You Shot The Sheriff ([YSTS](#)), a yearly one-day invite-only hacker conference that has taken place in São Paulo since 2007, is similar to DEF CON in terms of content and parallel activities, like lockpicking and hardware hacking. The conference venue is always a bar. Tickets for this conference are rarely sold, but when it happens, the prices are not affordable to most local entry-level professionals or students. This is considered one of the best hacker conferences in Brazil from a security research perspective.

[AlligatorCon](#), which takes place in Recife, PE, Brazil, is an invite-only black hat conference. This conference is similar to Sacicon in its goal to present content with a high technical level, but it goes beyond — topics include vulnerability exploitation, new hacking tools, and zero-day vulnerability disclosures. Unlike Sacicon, this conference focuses exclusively on local research, presented in Brazilian Portuguese.

We have mentioned multiple times where Brazilian hackers are not: in web forums. But where are they? The same places the rest of the Brazilians are. The communication platforms of choice are usually the very same ones used by the local population in general. In the current context, this means WhatsApp, Telegram, and Discord. The last of those is also commonly used by gamers, a result of the dominant teenage demographic in the Brazilian hacking community.

Content in Brazilian Underground Forums

Malware

The most common type of software product found in Brazilian web forums is the “crypter,” an obfuscation tool used to pack malicious software in such a way that it goes undetected by antivirus engines. The more “FUD,” or “fully undetectable,” a malware is, the more likely that malware is to reach the user’s email inbox undetected.

This high interest in malware packers is an indicator of one of the main attack vectors of Brazilian cybercriminals: email. Email spam has always been one of the main methods of phishing and malware distribution in Brazil. However, over the years, multiple security controls have increasingly prevented campaigns from reaching victims’ inboxes. Concurrently, new generations changed their relationship with email messaging, and multiple other social media sites and messenger apps emerged and became the primary communication platforms. Cybercriminals had to adapt to those behavioral changes in order to succeed.

The latest quarterly report from the Anti-Phishing Working Group (APWG) shows that phishing campaigns now use paid advertisements in search engines like Google and Bing, social media, rogue mobile apps in official stores, and Smishing (SMS Phishing) to target victims. Many of these attack vectors have ineffective methods for handling spam — SMS in particular — allowing cybercriminals to reach more victims. Even after the malicious link reaches the inbox of a victim, there is still one last phase needed in a successful phishing campaign: the victim must take the bait and click the link. There is a way to not only entice users to click on a phishing link, but also force them to do it technically. That method is known as “pharming.”

Pharming involves the use of malware or technical strategy to subvert the DNS name resolution and force all users of a host or network to visit a known website address at the wrong host (IP address), under the control of the attacker. Pharming is a very common activity of Brazilian hackers. Despite efforts from security companies and internet service providers, occasional attacks are not always detected.

One of the first forms of pharming was local: the attacker would leverage malware to modify the local host address resolution files (“LMHOSTS” for Windows, and “hosts” for Linux). The operating system first checks those files for hostname and IP address pairs. If a bank’s hostname is listed in that file, that resolution has the highest priority. The user visits a website with the correct URL at the wrong server. Local pharming has one weakness: antivirus. Malware can be detected by signature or heuristics, and any application trying to modify the local name resolution file is considered suspicious. Local pharming is convincing because the URL looks legitimate to the victim, but with today’s anti-malware controls, an attacker successfully changing the file with malware is unlikely. DNS or network pharming, on the other hand, does not require the complexity of malware.

Network pharming is an attack vector used by Brazilian cybercriminals since as far back as 2014. At first, the strategy was to abuse customer-premises equipment (CPE) — network routers provided by ISPs. Most users receive the same models or routers from the ISP, making the network environment very predictable. The attack involved sending spam with local network URLs that changed the DNS settings of the local router. Succeeding with this attack method required one favorable condition: a default administrator username and password.

Over time, other strategies were used for exploiting CPEs — exploitation of remote software vulnerabilities, for instance. One of those campaigns, [described by Radware in March 2018](#), involved the exploitation of vulnerabilities in MicroTik routers. In September 2018, 360 Netlab reported two incidents (September 4 and September 29) involving more than 85,000 routers in Brazil. Affected companies involved all major local banks, web hosting companies, and Netflix — a common credential for sale in Telegram channels. Spotify was not among the targeted domain names in those attacks but is a typical target as well. Neither service offers two-factor authentication, which makes credential collection and reuse trivial in this context.

Financial Services Targeting Drives High Security Standards

The Brazilian financial system is very advanced in terms of security controls. This is a result of decades of cybercrime, real-world crime, and — no less important — a response to Brazilians' consistent malicious activity. Brazil is a hostile environment for the financial vertical in every aspect, and as a result, security standards are high. Hacker activity and developments in the security of the financial system are strongly related, causing the financial institutions to constantly increase the security.

2FA for logins, 2FA for transactions via QR codes, physical tokens, browser plugins that resemble "rootkits," pre-registration of devices, device fingerprinting, strict limits for wire transfers, pre-registration of wire transfer destination accounts, a dedicated desktop browser for internet banking, and biometry in ATMs are among the vast and ever-growing list of security controls.

Transferring money between Brazilian bank accounts and foreign banks — even within Latin America or MERCOSUR trade bloc — is not trivial. The processing of international payment orders is treated as a currency exchange transaction. As such, additional controls against money laundering and tax evasion are applied, making moving money across country borders harder.

Another important security control relates to credit cards. In most countries, it is necessary to provide basic personal information in card-not-present (CNP) transactions: full name, full address. In Brazil, it is necessary to provide Cadastro de Pessoas Físicas (CPF) — a unique tax ID for every Brazilian citizen in every transaction — and that ID must match the one associated with the credit card. That ID is very similar to a Social Security number (SSN) in the United States. It is considered critical if that information becomes public.

As illustrated above, it's difficult to move money across country borders and security controls are strict. So how can a cybercriminal thrive in such an environment?

Chip-and-PIN technology was deployed in Brazil in the early 2000s. Just like with any new technology, chip-and-PIN was abused in Brazil, and eventually, cybercriminals succeeded in attacking not the EMV system itself, but poorly implemented deployments.

In March 2018, Kaspersky Lab Brazil released [research](#) on malware targeting POS systems with chip-and-PIN (EMV): Prilex. The exploitation of EMV was not something new: other attacks against vulnerable deployments of chip-and-PIN authentication had been seen in the wild over the past few years. The group behind Prilex, which has been active since at least 2015, used many variations of a black box attack, including one involving a Raspberry Pi with 4G data network access capable of exfiltrating data. They also focused on taking control of machine infrastructure. Finally, they added point-of-sale (POS) systems to their attack surface and started targeting chip-and-PIN cards.

Prilex allegedly operates off the limits of web-based forums and social media. According to Kaspersky researchers, they operate their own private WhatsApp groups, which are strictly controlled. For that reason, there is no forum activity from Prilex actors in the platform.

Language and Fraud Drive Targets

The primary target of Brazilian hackers is Brazilians. The Portuguese language is key for explaining that observation, but there are other elements that explain this geographical isolation.

There are other Portuguese-speaking countries — Angola, Cape Verde, Guinea-Bissau, Mozambique, Portugal, and São Tomé and Príncipe — but there is minimal interaction between these countries and Brazil. The country has its own variation of Portuguese — Brazilian Portuguese — with phonetics and vocabulary that are different from the Portuguese spoken in other countries. That unique Portuguese variation, combined with cultural and economical differences, also isolate Brazil from other countries in South America, as it is surrounded by Spanish-speaking countries.

Most of the products and services in the Brazilian underground are related to personal information: access to credit record databases, full information on a certain individuals provided with a CPF (tax ID) and credentials. Those credentials are obtained in many ways: malware, phishing for financial credentials, phishing for credit checks, Serasa Experian credentials, and insider employees at companies of interest. Carding, and the products and services surrounding it, like selling credentials, is one of the main activities of closed hacker groups.

In the past, information was shared in IRC channels, but now it is present in Telegram and other modern platforms. Carding activity is usually not present in major hacker web forums.

Carding is strong in the country's underground. Not all credit cards found in the Brazilian underground were necessarily collected. There is strong activity of credit cards generated by algorithms, referred to as "geradas." They look for companies that don't validate cards appropriately, which they call "cardeáveis," or "susceptible to carding," and exploit them.

In November 2016, Tesco Bank [announced](#) a security incident involving 20,000 accounts and a loss of 2.26 million GBP (2.95 million USD). The company issued a [new statement](#) a few days later, stating that normal service has resumed. No further information was disclosed in that new statement. In October 2018, the Financial Conduct Authority (FCA) released a "[Final Notice](#)" on the incident that occurred in 2016. According to the 27-page document, the attackers most likely used an algorithm that generated authentic Tesco Bank debit card numbers. It was determined that the majority of fraudulent transactions were coming from Brazil using a payment method known as "PoS 91," an industry code which indicated that the attackers were making contactless MSD transactions. Most likely, this is the most notorious example of the impact of Brazilian hacker activity involving generated card numbers.

Currently, there is no personal data protection regulations in place in Brazil. There are plans to implement one — similar to the European Union's General Data Protection Regulation (GDPR) — but it will not be effective until December 2020. This is bill number 13.709, also known as "Lei Geral de Proteção de Dados," or LGPD.

At this time, a company that suffers a breach is not obliged to disclose it to the public or the Brazilian government. As a result, companies deny breaches at all costs. In October 2018, Brazilian payment-processing company Stone [announced](#) a data breach on the eve of its IPO. It was reported that there was an extortion attempt, though that detail was not confirmed by the company. It could have been cybercriminals or just the competition trying to interfere with the company's IPO. The same kind of [extortion attempt](#) before an IPO happened in April 2018 against financial-tech bank Banco Inter.

Case Study: Law Enforcement Operation Ostentation

One recent Brazilian law enforcement operation, [Operation Ostentation](#), summarizes how a successful cybercrime enterprise in Brazil was carried out. The leader of the gang involved, Pablo Henrique Borges, was arrested on October 11, 2018. According to law enforcement reports and media, he and his gang were able to steal 400 million BRL (about 108 million USD) in 18 months. Borges was 24 years old and was living a life of luxury, with multiple Lamborghinis and Ferraris and expensive trips and habits. Two accomplices were also arrested — Rafael Antonio dos Santos and Matheus Araújo Galvão.



Cars seized in Operation Ostentation (Operação Ostentação) in October 2018.

The gang would offer to pay people's bills with up to a 50 percent "discount" via WhatsApp or Facebook posts. This is a common money laundering technique used by Brazilian cybercriminals — instead of cashing out money from bank accounts, they paid for bills, receiving a portion of it in an unconnected account.

It is still unclear how the gang gained access to the bank accounts — more than 23,000 in total — in order to pay for the bills. Most likely, it was with a combination of malware and phishing campaigns. The person responsible for software development was 24-year-old Leandro Xavier Magalhães Fernandes. Also from humble origins — he has a high school degree but no formal education beyond that — he was responsible for the most important element of the gang's business. His ostentatious lifestyle, with a mansion and expensive cars, attracted attention from the local law enforcement of Goiânia, GO.

Unfortunately, no information on handles, the malware family, sample information, or the forum name was released about this gang. Given the background and profile of the two leaders, it is unlikely that they obtained foreign malware for this operation and likely that they developed their own malware.

We do not have further information on this particular law enforcement operation to make statements on the quality of malware that was involved. What we know from other operations and law enforcement opinion is that Brazilian cybercriminals organize themselves in a structure that resembles terrorist groups, not criminal organizations. Gangs are organized into cells — software development, operations, money laundering — in a way that the disruption of one or more cells does not affect the business. Operators are notified when an infected user opens a session and interacts with them to bypass 2FA and other security controls. In March 2016, Kaspersky [described](#) this particular type of Remote Access Trojan (RAT) that is common in Brazil.

In Brazil, there are very distinct types of hacker groups: “Lammer” — entry-level hackers in the local slang of web forums — and the legitimate researchers and hackers. Sometimes, hackers evolve from web forums, other times they appear to be completely disconnected from both of these circles. They are simply smart people with basic software development skills who found a niche to explore and a way to make money.

Outlook

High-level Brazilian hackers will continue to exploit financial institutions, no matter how rigorous the security controls become. Desktop security is sufficiently high, but local cybercriminals have proven that they are capable of successfully bypassing those controls. However, high desktop security does not mean cybercrime is deterred.

The majority of Brazilians no longer do their internet banking on desktops, but on mobile clients. Transfers, one-time passwords, payments — all major banks allow clients to do practically anything using a mobile app. This change in behavior has already motivated change in cybercrime activity. SMS phishing (Smishing), mobile phishing kits, and malicious mobile applications — the majority for Android — pretending to be popular apps, such as WhatsApp, or mobile banking apps have increased in the past few years.

Android exploitation is already a reality in Brazil and this trend continues, as security hardening for those devices is a challenge. Another very important aspect to consider is that many Brazilians — particularly the ones with low income — don't do internet banking on desktops simply because they don't even own a desktop or laptop.

Use of WhatsApp in the country remains stable. Most likely, this will continue to be one of the attack vectors for cybercriminals. In 2018, WhatsApp announced and deployed person-to-person payments in India in a feature called WhatsApp Payments. [According to WABetaInfo](#), a news website specializing in WhatsApp news, the feature will be extended to Brazil, Mexico, and the U.K. in the near future. It is highly likely that this feature will be exploited in Brazil.

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.