INTSIGHTS
Defend Forward™

The Dark Side of Latin America:

Cryptocurrency, Cartels, Carding, and the Rise of Cybercrime

THREAT BRIEF
LATIN AMERICA

www.intsights.com

Executive Summary

Latin America boasts some of the most sophisticated hackers and organized crime groups in the world, but enterprise security teams without a presence in the region often overlook it. In 2019, the IntSights research team began investigating persistent phishing campaigns launched against customers in the retail and financial services sectors in Colombia and Brazil. The findings were astounding. Very persistent cybercriminals were operating extensive schemes targeting banks, hospitality services, and retail businesses for their credentials and their financial assets. It was not hard to determine where the threats were coming from because the threat actors spent more time changing their infrastructure and tactics than they did hiding their identities.

In one case, the IntSights research team was able to pinpoint a threat actor's location in Colombia, his social media profiles, various avatar names, and phishing methods (see section: Phishing, page 7). Deeper exploration into the life of this threat actor revealed a more complex threat landscape, an escape from poverty and government censorship in Venezuela, and a move over the border to Colombia to pursue cybercrime as a career. This discovery prompted our researchers to address these findings in a report on the political-economic devastation in Venezuela and forces that drive citizens to the underground to make money through cybercrime.

The Dark Side of Latin America is an exploration of the larger threat landscape throughout the region, defined by geopolitical dynamics, government corruption, organized crime, and persistent attacks on industries such as retail, finance, and hospitality services worldwide.

Methodology

Tactical intelligence in this report is derived from several proprietary sources through our ThreatCommand™ platform, including:

- Closed-access databases
- Hundreds of underground sources (deep web and dark web)
- Thousands of open source sites through various search tools
- Manual and automated searches in hundreds of messaging platform conversations and group forums that are used exclusively by hackers and cybercriminals

In addition, the IntSights team of expert researchers and intelligence analysts contribute operational and strategic-level intelligence to enable our users to make important decisions and form strategies for defending against emerging threats in Latin America.

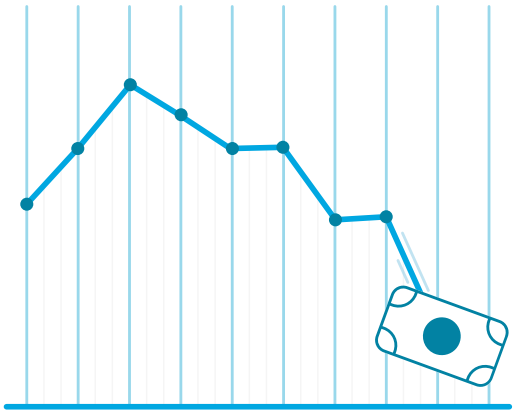
IntSights is proud to have partnered on this report with regional cybersecurity experts CipherTrace and Scitum. Our shared expertise in serving Latin American enterprises with incident response, information security, and intelligence makes this report the first of its kind to address multiple aspects of criminal behavior, its effects on enterprises worldwide, and practical methods for protecting organizations against these threats.

Some identities have been sanitized for purposes of continued anonymity in undercover investigations.

Threat Landscape

The area known as Latin America includes Mexico, Central America, and South America. The diversity in the region is celebrated worldwide as a melting pot of cultures, languages, geographic landscapes, economies, and governments. However, while the region has many universal cultural components, individual nations experience unique successes and challenges defined by their unique political landscapes, dictatorships and democracies, economic diversity, and the sharp increase in the adoption of digital technologies. 2019 was a difficult financial year for all of Latin America as economic growth nearly halted.

On October 30, 2019, the International Monetary Fund (IMF) published its World Outlook Report, which noted a significant downgrade in economic status for the entire Latin America region, highlighting significant difficulties in Venezuela as a result of hyperinflation and a humanitarian crisis. The IMF largely blames social factors for this downgrade, including depreciating consumer confidence around the world, political and economic uncertainty, and Venezuela's role as a catalyst for regional instability.



Economic struggles, political corruption, internet censorship, and the rise of organized crime in Latin America all contribute to the growth of cybercrime. Companies across the region and beyond are struggling to keep up with threat actors that are financially motivated, coordinated, and persistent in their efforts to fraud, scam, and steal from consumers and businesses alike.

Rapid digitization and widespread adoption of digital technology make Latin America a ripe target for cybercrime. In 2019, there were 453.7 million internet users in Latin America – about 69 percent of the total population, with users based in Brazil and Colombia making up the vast majority. One global survey of screen time ranks Brazil and Colombia second and fourth, respectively. In 2018, retail e-commerce sales totaled more than $50 billion, and native retail giant MercadoLibre was the most popular online retailer in Latin America. Other major retailers in the region include Amazon, B2W Digital, and Alibaba.

As with most regions or countries that experience a combination of rapid digitization, high internet usership, and myriad political challenges, data privacy legislation in Latin America is lagging. Brazil leads the way in this effort, having already enacted over 40 different data privacy regulations. It is currently consolidating these into one overarching policy called Lei Geral de Proteção de Dados (LGPD), forecasted to be implemented in August 2020. This law will be similar to Europe's GDPR and will focus on keeping companies accountable for their customers' data. Non-compliance could result in a 2 percent annual revenue penalty, which would be crippling for retailers and banks that are already struggling to fight fraud and cybercrime. Data privacy laws will help streamline expectations for protecting customer and employee data across the region but could pose economic hardship on struggling companies at the beginning.

Threat actors in Latin America vary from other regions of the world. Unlike some of the world's largest powers and militaries, Latin America does not boast state-sponsored Advanced Persistent Threat (APT) groups. While Russia, the United States, China, North Korea, and Iran have developed military powers and established offensive hacker teams, the developing areas in Latin America have focused efforts on stability, economic growth, national defense, and fighting organized crime. The combination of these factors has created a ripe environment for financially motivated hackers, persistent fraudsters, and even drug cartels working with cybercriminals.

Threat Finance: The Catalyst for Cybercrime

Threat finance is evolving in Latin America as organized crime groups turn to cryptocurrency to launder large amounts of money and dive into the dark web to find hackers for hire. Latin American countries top the list of the world's worst money laundering nations. The constant flow of money in the organized crime community feeds into dark web markets and into the cybercrime ecosystem. Organized crime groups and drug cartels in Latin America are taking advantage of technological advances in digital banking and money transfers. In April 2019, agents from Brazil's Department of Narcotics Investigation (Departamento de Investigações sobre Narcóticos – DENARC) apprehended a criminal running a crypto-mining operation in Porto Alegre. The agents seized 25 cryptocurrency mining machines, which operated around the clock and are each valued at approximately $65,000 US.

There are several ways that threat actors are conducting these operations. CipherTrace, the world's first blockchain forensics team, shares their insights:

Mixing Service "Mixer", "Tumbler", "Fogger": A cryptocurrency tumbler or mixer is a service that offers to mix potentially identifiable or "tainted" cryptocurrency funds with others. The intention is to confuse the trail back to the fund's original source and forward to any potential exchanges or other cryptocurrency entities. This operation can include transferring funds between clear web cryptocurrency wallets and dark web crypto wallets. Each transfer, called a "hop," creates an extra layer of obfuscation. From the dark web account, the funds are then split at randomized intervals to TOR-hosted crypto addresses so the transactions cannot be easily correlated. Once the tumbling is complete, threat actors then deposit the freshly washed coins to a cryptocurrency exchange to be traded for other cryptocurrencies. Mixers take a small percentage transaction fee of the total coins mixed to turn a profit, typically 1 to 3 percent.

Source: gauchazh magazine

Launder Through Unregulated Exchanges:

Most "legitimate" cryptocurrency exchanges are required to follow "know-your-customer" (KYC) and anti-money laundering (AML) policies. These exchanges are generally more trusted. However, as with any new financial endeavour, criminals are taking advantage of unregulated exchanges that do not require registration information and proof of identification for tracking purposes. These illegal exchanges are appealing to criminal groups that are looking to move large amounts of money through untracked channels. The method used here is similar to mixers, where the actor will deposit Bitcoin into the exchange account and trade it for various Altcoins. Each time a trade is made, it further distances that original payment from its source account. The privacy and anonymity of this process depend highly on the exchange's monitoring capabilities. Researchers estimate that after cryptocurrencies have been cleaned on exchanges, 97 percent end up in countries that have extremely lax KYC/AML regulations, with Latin American economies topping the charts.

Peer-to-Peer Exchange of Goods and Services

Mass amounts of money are flowing through large organized criminal groups. Despite the many other methods used to launder and mix the money, some still go to trusted networks or illegal peer-to-peer (P2P) exchanges to launder their cryptocurrency. Although this method is not novel, it is evolving with the introduction of cryptocurrencies in the criminal underground and is backed by widespread political corruption in many countries.

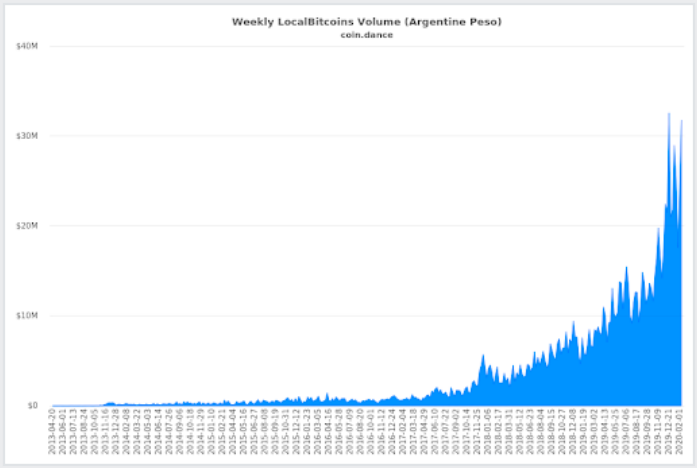
In 2014, nine people were arrested in raids that targeted 75 different locations, including Los Angeles. The US Federal Bureau of Investigation (FBI) seized $90 million, of which most was cash, as part of a money laundering scandal by the Sinaloa Cartel of Mexico. During that time, Los Angeles had become the epicenter of money exchanges for the cartel group in an effort to avoid large wire transfers. The scheme happened as follows: the Sinaloa Cartel was holding a person hostage. The family was in Los Angeles and needed to get $140,000 of pesos to the cartel. The cartel informed the family to take the money to an L.A. clothing shop, which then used the money to pay for shipments of clothing to Mexico. Upon arrival, the importer then paid the Sinaloa cartel the $140,000 of pesos. These types of activities have only become more widespread since the introduction of digital currencies, and criminal gangs are growing and expanding their operations as a result.

Image: LA Times

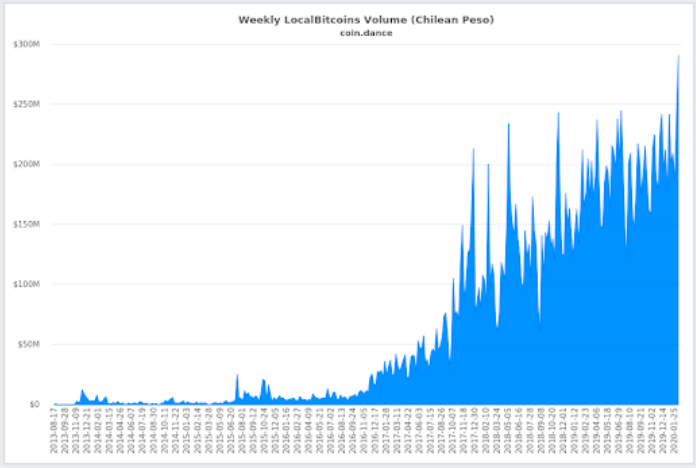
In October 2019, an official of the Panamanian payment processing firm Crypto Capital was arrested as part of a Polish probe for allegedly laundering the proceeds of drug sales on behalf of an international crime group. Ivan Manual Molina Lee was arrested in Greece and extradited to Poland. The Polish Ministry of Justice seized $350 million from a Polish bank, claiming that the funds directly tied to money laundering that Molina Lee conducted for Colombian drug cartels using cryptocurrency.

While there are a host of cryptocurrency exchanges available to serve Latin American customers, the P2P platforms are typically the preferred method of Fiat currency to/from cryptocurrency exchange throughout the region. Throughout 2019 and on into 2020, the well-known P2P platform LocalBitcoins experienced record growth in transaction volume across many Latin American countries. Also seeing a steep growth in volume were other P2P exchangers like Paxful and CCoins. P2P exchangers typically lack AML programs and perform little or no KYC due diligence, which entices criminal actors to utilize P2P versus traditional cryptocurrency exchanges. The following charts demonstrate the rapid growth of LocalBitcoins usage across several Latin American countries.

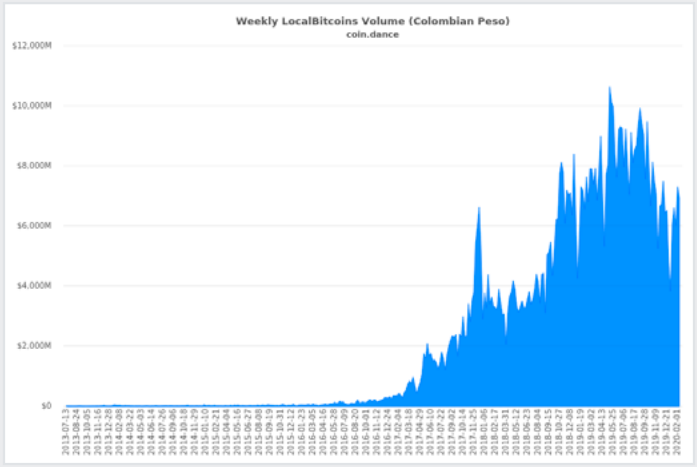
Argentina



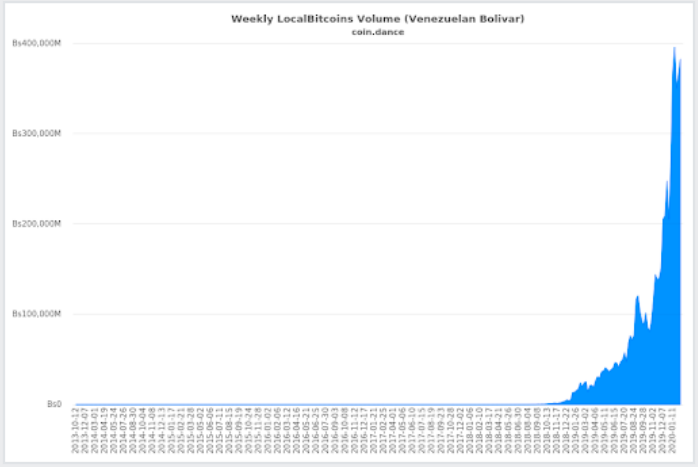
Chile



Colombia



Venezuela



Very few countries in Latin America have established laws to counter money laundering and those that do have them are not enforcing them effectively. According to studies by Basal Institute on Governance, an expert on AML, Colombia tops the list of the five worst deteriorated AML scores. Experts believe this is not due to recent degradation of the policies but a longstanding struggle to enforce the laws. Basal Institute experts also point out that corruption and bribery are often predicate offenses to money laundering, and Venezuela ranked as the worst in 2019 for corruption and bribery. The IntSights Venezuela Threat Brief covers more on the geopolitical issues in the country that contribute to this corruption problem.

Emerging Threats

Hackers Gang Up With Cartels

The marriage of violent drug gangs and the underground hacking community is a significant emerging threat as we move into 2020. The two worlds are combining their influence, skills, and experience to achieve common goals, primarily of the financial variety.

In 2019, a criminal gang called "Bandidos Revolution Team" and their leader, Héctor Ortiz Solares – known as "El H-1" or "Bandido Boss" – was apprehended by law enforcement in León, Mexico. Solares was known for recruiting technically skilled hackers who could write malware code to infect banks and ATMs. His hackers wrote malware that extracts money from banks using the Interbanking Electronic Payment System (SPEI) system and then deposits it to third-party accounts. Once the money is deposited, the gang then withdraws cash and makes large purchases, such as real estate and luxury cars.

Authorities reported that Solares was bringing in between 50 and 100 million pesos per month ($2.6 to $5.2 million). In 2018, the head of Mexico's central bank reported the gang had conducted a cyberattack that cost five financial institutions 300 million pesos (US $15.2 million) in fraudulent transfers.

On May 16, 2019, the Fiscalía General de la República (Attorney General Office of Mexico) announced on Twitter that it had searched 11 homes and confiscated 27 luxury vehicles, drugs, firearms, computer equipment, and telephones from the safe houses of this notorious cyber-cartel. One of the confiscated vehicles was a $30 million Aston Martin, which drew admiration and attention from hackers all over the world who wanted to get a piece of the profits.

Mexico's Attorney General's Twitter account showing the luxury vehicles confiscated in a raid.

This is one example of a much larger problem plaguing law enforcement in Mexico and neighboring countries as digitization and access to the dark web enable organized crime groups to hire hackers for large-scale hacks.

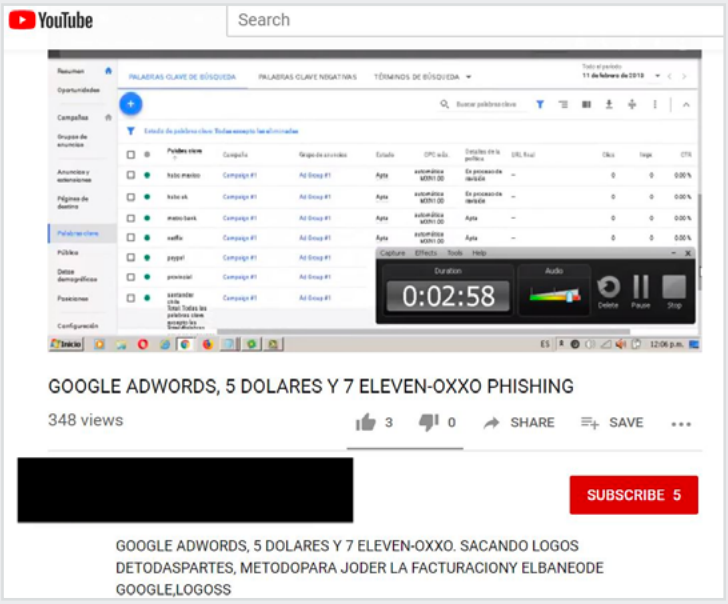
Next-Gen Phishing Campaigns

In mid-2019, IntSights analysts discovered a large-scale phishing campaign being launched against several major banks in North America and Latin America, including a customer. The threat actor had created several websites to mimic the official bank website. IntSights issued takedown notices to the registrars. The threat actor was persistent and pivoted to new registrars and new infrastructure. IntSights researchers started digging into the domain registrations and chatter around these URLs. They discovered that customers were being directed to the phishing sites via fake Google and Bing adwords. These fake advertisements appear as links at the top of the page when the victim does a Google search. When the victim clicks on the link, it opens a phishing website that appears to be identical to the bank's real website.

The victim proceeds to enter his or her credentials to log in to a bank account. The page is then redirected to a second page, which requires the victim to enter personal information when queried. This personal information could be used to answer two-factor authentication questions and also to collect personal information, such as current address and contact information. In one dark web forum, the threat actor referred others to read about the technique in a news article. This type of media helps the subject to build a reputation in the underground community.

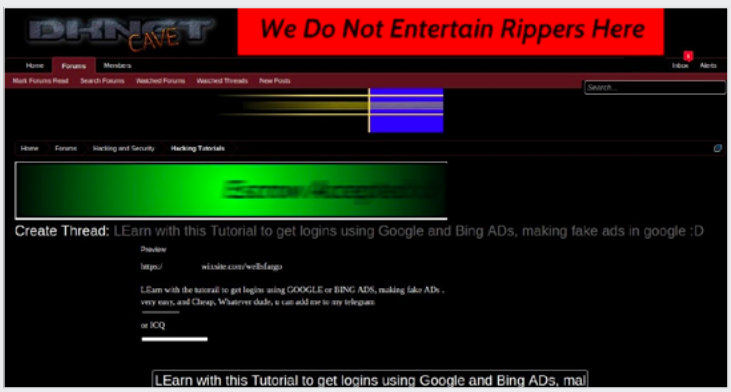
The general sentiment towards this threat actor in forums is positive. Several other people have reached out to him asking for his messaging information and desire to speak to him about this method and how to make it work. The threat actor has also revealed through several interactions in private chats that he has hackers working for him that create the phishing kits.

This leads us to believe that this type of phishing campaign is not limited to one individual but, instead, involves many hackers using this same method. In this case, it would enable the hacker community to simultaneously spin up many different phishing domains and websites. This would explain the influx of suspicious domain registrations and phishing website registrations that have been affecting these banks and their customers.



YouTube tutorial for how to conduct phishing attack

Threat actor's Wix page advertising his methods



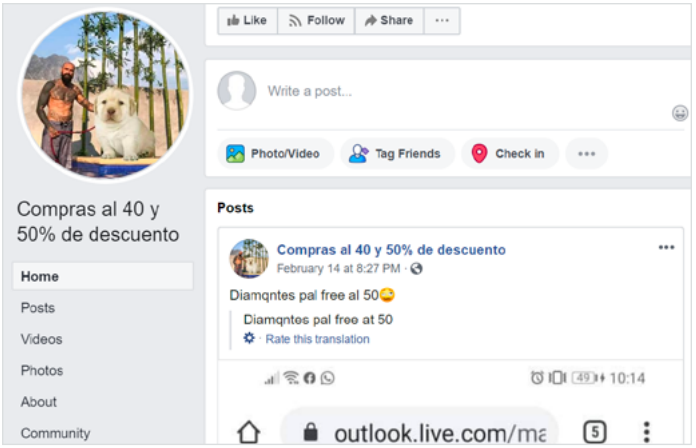
Threat actor's darknetcave.net post advertising tutorials

"Compras" Carding and Insider Threats

Carding is the use of stolen credit cards to make fraudulent purchases. This practice is widespread in the Latin American cybercrime community, and threat actors have made millions of dollars. They call this practice "compras", Spanish for "purchase" or Portuguese for "shopping."

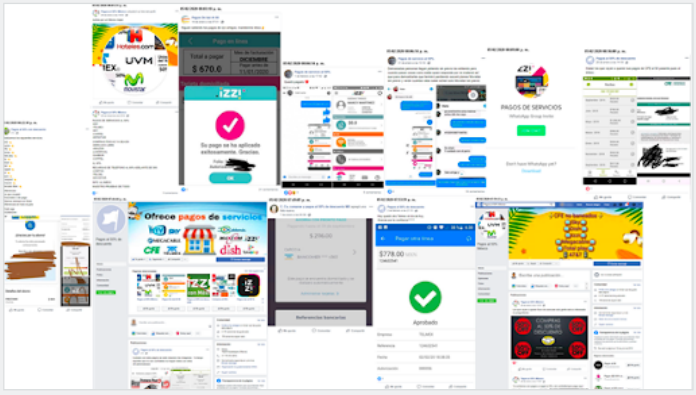
There are currently hundreds of marketplaces in the clear, deep, and dark web that provide services to the general population. The criminals use stolen credit cards to pay bills, purchase airfare, book hotels, and buy goods and services. The process works as follows:

1. Criminals advertise that they will pay a bill for customers at a discounted rate (for example, pay $50 for a $100 electric bill).
2. The customer deposits money into the criminal's bank account. This is usually done through convenience stores, cash stores, or grocery stores.
3. Criminals immediately use stolen credit cards to pay the bill on behalf of the customer. They pocket the money from the customer.



A private Facebook compras group where criminals collaborate and support each others' businesses

Oftentimes, the criminals will advertise these services on social media, Facebook groups, messenger applications, and Twitter. They often use logos familiar to the customer, such as popular booking websites, bank names, and utility companies.



Examples of compras advertisements by criminals on open sources

Criminals have used these methods to book expensive airfare for their "customers." Airlines have started requesting the credit card that was used for booking to be presented upon check-in. If not presented, the customer must pay cash for the ticket in order to board the flight.

Criminals have one primary source for stolen credit card numbers: insider threats. The most common type of credit card acquisition is through employees who work where credit cards are presented. Criminals contact employees through WhatsApp or social media, offering a commission in exchange for customer credit card information. For example, in Mexico, gas station attendants fill your gas tank and process your credit card. The attendants copy the card information and give it to cybercriminals for carding operations. They are often paid for meeting monthly quotas. Other methods for obtaining credit card data are through small hacking jobs on web applications and through social engineering.

BINero Fraud

"BINero" fraud is a widespread fraud tactic in Latin America that has a detrimental impact on banks in the region. A BIN (bank identification number) is the first four to six numbers that appear on a bank card. The BIN identifies the specific bank that issued the card and is key to matching banks to transactions that happen around the world. BIN – or BINero – fraud is the unique practice of finding BINs that are improperly validated by online payment processors, which, in turn, allows fraudulent transactions to occur online. When the criminal actor discovers a misconfigured BIN and online payment processor combination, he or she then fabricates the remaining card information and makes fraudulent online purchases through popular retail sites, such as MercadoLibre or Amazon. BINero fraud is widely discussed in open, deep, and dark web Spanish-language sources. IntSights analysts continuously monitor these sources to keep up with new trends, actors, and schemes related to BINero fraud. Some of the busiest online BINero tutorial forums include Telegram groups, WhatsApp groups, Facebook groups, and dark web underground sources. The scheme is successful and lucrative, and does not seem to be slowing down.

Facebook groups about BINero fraud

Latin America Threat Actors: Communication and Contact

Criminals in Latin America communicate in open-source platforms and often do not put work into hiding their true identities, unless they are tied to cartels or gangs. Despite access to underground forums, the lack of law enforcement enables criminals to use open-source tools to freely communicate with each other. **WhatsApp, Facebook Messenger, and Telegram are the most popular methods for cybercriminals to talk to each other and collaborate.** In the past, ICQ was the most popular communication tool. Over the past few years, WhatsApp has gained popularity as a free messenger platform that allows group chats, video, and more.

IntSights undercover intelligence analysts engage with threat actors in their preferred communication method – usually WhatsApp and Facebook Messenger. They find that threat actors are very comfortable in these platforms because they are allowed by their local governments and are free to use. Facebook Messenger, in particular, offers an easy way for them to pivot from a Facebook group to chatting in Messenger within the same browser window. Facebook Messenger now offers an encrypted chat called "secret" mode. It is simple for criminals to use this platform to switch between unencrypted casual conversations to full encrypted end-to-end messages so they can discuss more clandestine business deals.

Malware Trends

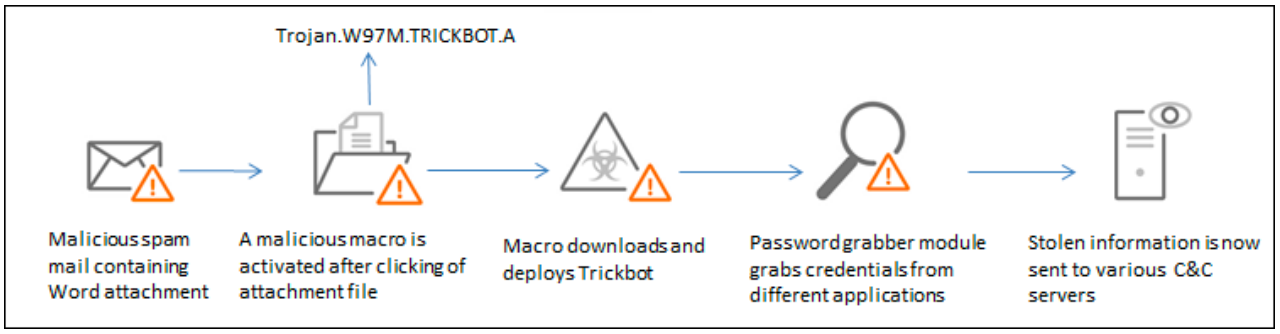
Banking trojans and ransomware top the list of malware threats targeting and coming from the Latin American region. Scitum, the leader in managed security in the Latin America region, contributed this information about the top trending malware affecting their customers in 2019:

1. **Catasia** - Dating back to 2014, the Catasia malware distributed emails impersonating different government organizations in Mexico. The emails initially contained a Word document with macros that downloaded the malware in the background when enabled. The malware was able to access the victim's camera and microphone and enabled voice and video recording. In recent versions, it has sent emails with .zip files instead of a Word document. The most notable characteristic of this malware is that the attacker updates its functionality, often to include man-in-the-middle (MITM) browser attacks. The Catasia malware has found success being hosted on otherwise non-malicious infrastructure, where legitimate business operations are also hosted. During the investigation, it was found that it only focuses on Mexican targets, despite being initially tested in Colombia.

2. **Cosmic Banker** - The Cosmic Banker trojan is a malware that has had a significant impact on banks in Latin America since 2018. Scitum observed it in April 2019 when it was massively distributed. One of the most notable characteristics of this campaign is that the executable contained very specific Portuguese comments that also have been spotted in other reported events. The campaign targets the user credentials of Mexican banking institutions. However, the group behind Cosmic Banker is also the author of another campaign targeting users from Brazil's banking institutions. Some of the attack elements match with a malicious artifact documented by Trend Micro as Banload, which affected some banks in Brazil.

This strengthens the hypothesis that the group started its attacks in South America and later reused the developed malware to attack targets in Mexico. Using the same strain of malware left behind common traces that support the attribution of this campaign to the Brazilian attackers. Even though the indicators of compromise such as hash values, IP addresses, and domains change during each attack, the TTP shown by the cyber group changes less frequently, particularly the clear text transfer from a compressed file, which includes the final toolkit of the attacker.

3. **Trickbot** - Trickbot is a banking Trojan that is used in cyberattacks against small and medium-sized businesses (SMBs). It was created to access online accounts – especially bank accounts – to obtain Personally Identifiable Information (PII) to be used in identity fraud and theft. Over the years, the creators of the Trickbot trojan have added modules and expanded its abilities. Trickbot is delivered through malicious spam containing Word documents, which enables the malware to steal credentials and exfiltrate sensitive and valuable data.

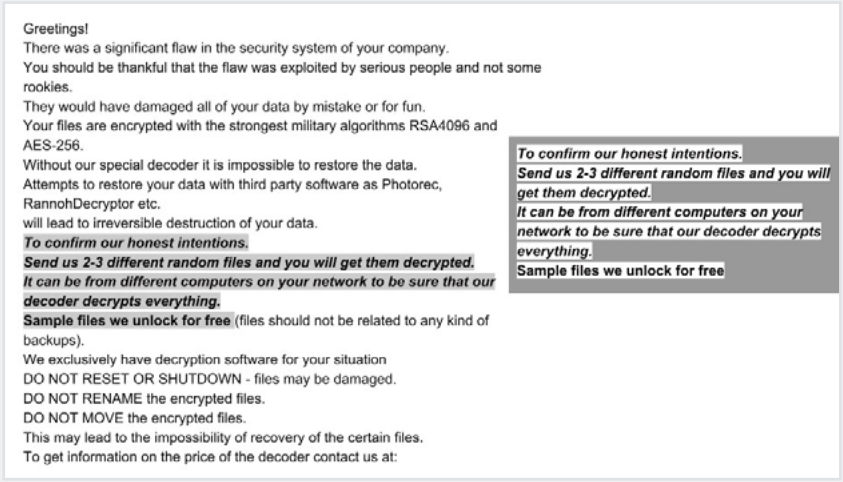


Trend Micro

Trickbot has affected many Latin American organizations, but Mexico was hit especially hard by variants that delivered Emotet. Between late 2018 and late 2019, the number of Emotet-infected bots soared in South America. Infected hosts include organizations in the automotive, finance, energy, construction, retail, entertainment, logistics, and technology sectors.

4. **Phobos Ransomware** - The Phobos ransomware is by far the most common strain at the moment, as it is present in at least 70 percent of ransomware incidents. Attackers are using vulnerable third-party services for entry into the organization. Once inside, the threat actors extract valid credentials and move laterally until they reach the Active Directory server. They disable the Windows firewall and sometimes uninstall EDR and antivirus solutions, before distributing the malware using GPO. They do not encrypt the whole network, focusing only the most critical servers of the company at the same time to cause significant disruption in daily operations.

5. **Ryuk Ransomware** - The Ryuk ransomware was especially effective in 2019 and has hit Latin America especially hard. Mexico's state oil firm, PEMEX corporation, was completely shut down due to a Ryuk ransomware incident in November 2019. Ryuk is especially dangerous because it was created to infect a system and hide undetected for a period of time while the malware seeks out critical network systems to maximize its impact. Countless other organizations throughout the Latin America region have suffered from Ryuk infections in late 2019 as well. Ryuk is believed to be operated by the same group that manages the Trickbot malware, a group dubbed Wizard Spider, based out of Russia. Ryuk is closely tied to other malware groups and is observed as part of a complex infection chain. For example, one report explains that Ryuk is usually the last step in an attack that starts with Emotet malware delivering the Trickbot trojan. Trickbot deploys post-exploit tools such as Mimikatz and Powershell, which enables it to harvest credentials, remotely monitor a system, and move laterally within the network. This process enables the attacker to determine the value of a machine and assess whether it is worth deploying Ryuk.


Greetings!
There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.
Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.
will lead to irreversible destruction of your data.
To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts everything.
Sample files we unlock for free (files should not be related to any kind of backups).
We exclusively have decryption software for your situation
DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.
To get information on the price of the decoder contact us at:

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts everything.
Sample files we unlock for free

Ryuk ransomware letter example

Recommendations

1. **Collect, monitor, and analyze cybercrime intelligence** to understand and proactively defend against threats like those coming from and affecting Latin America. Global, multinational enterprises and financial institutions need to have an in-depth understanding of the adversary and their tactics, tools, and methods. Further understanding of their motivations and lives can shed light on regional or national issues that drive cybercrime in the underground. No matter where your security practice is in maturity, there are ways to build a cyber threat intelligence (CTI) program to get an immediate return on investment (ROI). IntSights offers practical options for CTI solutions and tools, as well as an advisory services team available to come to your company and teach your team the basics of cyber threat intelligence.

2. **Follow security best practices.** Phishing campaigns are becoming more sophisticated, and employees and customers need to be educated on these tactics. Inform customers about phishing threats and advise them on how they should expect your organization to contact them. Recommend that they type in the name of your website instead of clicking on Google or Bing ads that look like your website, and advise them to never enter their credentials or credit card information into a suspicious website.

3. **Prioritize compliance.** Payment Card Industry (PCI) is being targeted more every year. If your company is receiving electronic payments, you should be prioritizing PCI-DSS standards to show your customers that they can trust you with their money and their personal information. Organizations operating in Latin America should prepare themselves for upcoming data privacy legislation.

About IntSights

IntSights is revolutionizing cybersecurity operations with the industry's only all-in-one external threat protection platform designed to neutralize cyberattacks outside the wire. Our unique cyber reconnaissance capabilities enable continuous monitoring of an enterprise's external digital profile across the clear, deep, and dark web to identify emerging threats and orchestrate proactive response. Tailored threat intelligence that seamlessly integrates with security infrastructure for dynamic defense has made IntSights one of the fastest-growing cybersecurity companies in the world. IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo. To learn more, visit: intsights.com or connect with us on LinkedIn, Twitter, and Facebook.

To see the IntSights External Threat Protection Suite of solutions in action, **schedule a demo today.**