Blueliv.

Threat Landscape Report

April 2019

1. INTRODUCTION

If 2017 was the year businesses around the world started to smell the smoke, 2018 was the year they realized they were on fire. Cybercriminal activity ramped up in 2018.And with increased legislative protections for customers, many businesses were forced to improve their cybersecurity controls and processes - and started to feel the burn.

Organizations in all sectors faced increasingly virulent and sophisticated cyberthreats on a weekly, if not daily basis. On an individual level, incidents such as the Facebook/Cambridge Analytica scandal showed just how fast and loose people play with their data. As a watershed moment, the general public – not just those working in cybersecurity – started to realize just how powerful personal data really is, and its potential for manipulation and malicious use. Blueliv's threat Intelligence team observed an increase of 50% in the amount of stolen data from one year to another.

The general public – not just those working in cybersecurity – started to realize just how powerful personal data really is, and its potential for manipulation and malicious use.

Blueliv's Threat Intelligence team observed an increase of 50% in the amount of stolen data from one year to another.

1.1. A CULTURAL SHIFT

Since there were more major cyber incidents, 2018 was also the year IT security teams and other business departments began to interact on a greater scale. Now more than ever, it is critical to create a strong culture of cybersecurity within organizations. This trend has become more mainstream in the past twelve months, and will continue in 2019 and beyond.

This culture of cybersecurity should extend past the management team, and move throughout the enterprise. As the workforce becomes more aware about certain risks and good security hygiene, cybersecurity steadily becomes baked into company culture. Enterprises have increased company-wide training and grown their security-related onboarding procedures. Overall, there is a more robust understanding of risk – and this will help to develop more interaction between departments as well as smooth the flow of information.

1.2. DIGITAL TRANSFORMATION

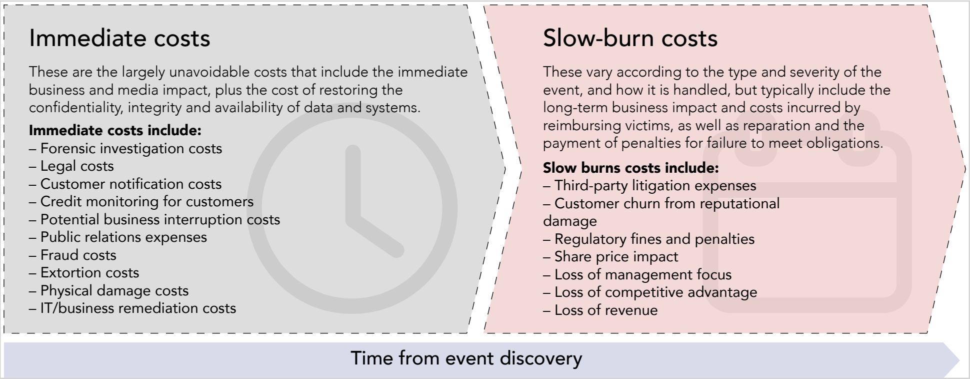
Meanwhile, digital transformation is no longer a choice; it is a something all firms must go through in order to survive. Businesses must stay agile while causing minimal disruption. But as companies transform and take advantage of technologies such as mobility, IoT and the cloud, there are security risks to consider. As the infrastructure changes and the attack surface increases, there is a greater chance that vulnerabilities may emerge and be exploited by cybercriminals. This was the case with a number of breaches this past year, and something Aadhaar in India, for example, experienced on more than one occasion.

In order to accelerate transformation, many companies are signing outsourcing agreements to specifically hand over control of important assets and data to third-party providers. While this may provide business benefits, it increases the risk of these assets being compromised, since the security protocols of the third-party suppliers may not be as robust as the supplied company.

1.3. BUSINESS PERFORMANCE AT RISK

The attack surfaces of governments, enterprises, SMBs and individuals all increased in 2018 – it is clear that the vulnerabilities accessible to cybercriminals are no longer simply limited to entry points. And the risks online have never been higher.

In response, organizations have become more proactive in strengthening their security postures. After all, there are significant business costs associated with a successful cyberattack – both immediately and in the long term. The following illustration depicts the immediate and slow burn costs that generates a cyber security incidents. This analysis is still accurate to today´s challenges and impacts that must face organizations.



Immediate costs

These are the largely unavoidable costs that include the immediate business and media impact, plus the cost of restoring the confidentiality, integrity and availability of data and systems.

Immediate costs include:
– Forensic investigation costs
– Legal costs
– Customer notification costs
– Credit monitoring for customers
– Potential business interruption costs
– Public relations expenses
– Fraud costs
– Extortion costs
– Physical damage costs
– IT/business remediation costs

Slow-burn costs

These vary according to the type and severity of the event, and how it is handled, but typically include the long-term business impact and costs incurred by reimbursing victims, as well as reparation and the payment of penalties for failure to meet obligations.

Slow burns costs include:
– Third-party litigation expenses
– Customer churn from reputational damage
– Regulatory fines and penalties
– Share price impact
– Loss of management focus
– Loss of competitive advantage
– Loss of revenue

Figure 1: This graphic from KPMG illustrates the impact of a successful cyberattack on a business.

We have observed almost a 77% year-over-year increase in the number of credentials belonging to Latin American markets in 2018.

1.4. LATIN AMERICA – A NEW TESTING GROUND FOR CYBERCRIME

We observed a new and interesting trend that emerged in Latin America in 2018 (defined as Mexico and all countries south of it). The cybercriminal ecosystem in Latin America has been growing steadily in recent years, due to increased internet penetration, increased digital transformation, high levels of outside investment and weak or nonexistent cybercrime legislation.

A bellwether for this trend is usually the number of credentials our infrastructure detects geolocated to the region. We have observed almost a 77% year-over-year increase in the number of credentials belonging to Latin American markets in 2018. Compared to the second half of 2017, we observed a jump of nearly 200% in the second half of 2018.

This suggests that certain pieces of malware have seen success in the region – which will be outlined later in this report. We also saw increased attack activity by the Lazarus Group in Latin America this year. These were both successful and thwarted attacks at Mexico's Bancomext, Banco de Chile, and Chile's RedBanc.

In this report, we take a special look at Brazil– the largest economy in the Latin America and one that has made much of its digital modernization in recent years. Well over half of the country is connected to the internet, but Brazil has faced severe cyberattacks targeting individuals and businesses.[1] As of the beginning of 2018, almost two thirds of internet-connected Brazilians had been targeted, generating losses of $22 billion.[2] Internet-connected critical infrastructure in the developing region – like nuclear energy, water treatment plants and electrical transmission systems – is also extremely vulnerable to attack, however the Brazilian government is yet to set basic ground-rules to prevent exposure or mitigate risk.

We have concluded that Latin America is becoming an important component of the global cybercriminal ecosystem. It is unique as threats tend to be less country-specific than on other continents. A common language and similar infrastructure across much of the region allow for the easy flow and exchange of ideas, encouraging a truly regional threat landscape.

Generally, the cybersecurity infrastructure in Latin America is relatively fragile compared to more mature regions like Europe and North America. Research has suggested that the market for cybersecurity products is anticipated to grow at an overall compound annual growth rate (CAGR) of 12.3% and will be worth $20.7 billion by 2023.[3]

Research has suggested that the market for cybersecurity products is anticipated to grow at an overall compound annual growth rate (CAGR) of 12.3% and will be worth $20.7 billion by 2023.

Because of this, we have dedicated a section of this report to Latin America: We believe that sharing intelligence and collaborating is the best way to fight cybercrime.

1.5.PURPOSE OF THE REPORT

This report is intended to be a reference document for CISOs and their security teams, but also for executives interested in how cybercrime affects enterprises today.

The report contains a selection of the most important cybercriminal events of the 2018, including intelligence on specific threat actors and the TTPs (techniques, tactics and procedures) they deploy.

Tactical information and analysis is derived from data extracted from Blueliv's modular cyberthreat intelligence platform, Threat Compass. It is complemented by strategic and operational threat intelligence gathered by Blueliv's in-house analyst team, who offer guidance around how to combat certain attack techniques and improve an organization's overall security posture in 2019 and beyond.

Summary overview

This section highlights some of the most important cyber-related events of 2018.
Many of the incidents highlighted are covered later in the report.

CORPORATE INTRUSIONS

The number of corporate intrusions, breaches and leaks reported in 2018 was higher than ever before. We take a look at the implications of these attacks for the companies and the world. Internally there remains a need to improve IT security skills to prevent attacks and limit the business impact when one happens.

TRENDING MALWARE AND TTPs

Cybercriminals have been deploying more sophisticated tactics, techniques and procedures to attack businesses. Improvements in stealth, encryption and obfuscation have been hammering individuals and enterprises. We explore some of the advances and provide intelligence on how to combat them in 2019.

THREAT ACTOR ACTIVITY

Advanced threat actors on the scene caused some serious damage to enterprises and government institutions in 2018. It is important to highlight their activity in order to better defend against them this year.

LAW ENFORCEMENT OPERATIONS

A number of takedowns and arrests last year demonstrated a continued and coordinated response to cybercriminal activity. Meanwhile, new regulations continue to have a significant impact on the businesses affected by cybercrime – which is all of them.

2018 timeline

JANUARY

India's Aadhaar is compromised, with access to the data subsequently being available for purchase

Mexico's Bancomext is targeted by Lazarus

FEBRUARY

Russian hacking group breached Germany's foreign and interior ministries and exfiltrated 17GB data

MARCH

Information on 150 million users of Under Armor's fitness and nutrition tracking app MyFitnessPal is compromised

Cobalt Group leader is arrested in Spain

APRIL

Hudson's Bay Co. is breached, exposing over five million payment cards

MAY

Mexico's SPEI system is targeted by unknown threat actors, resulting in the loss of between $18 and $20 million from Mexican banks

AdvisorBot is used in several malspam campaigns

JUNE

Exactis suffers an intrusion, exposing the information of 340 million people and businesses

Dixon's Carphone suffers a data breach

Bank of Chile gets hit by Lazarus

JULY

BitPaymer ransomware hits the Matanuska-Susitna borough government in Alaska

AUGUST

Several members of Fin7 are arrested

During the first half of August, the FBI warned all worldwide banks of a possible global ATM cashout blitz

Ar3s is released in Belarus after arrest in 2017

Marap is discovered in a large malspam campaign composed by millions of messages

TSMC became the latest victim of a variant of the WannaCry ransomware

SEPTEMBER

Indictment of North Korean hacker Park Jin Hyok by US DOJ

ZeroEvil: New credential stealer evolution of ARS Loader appears

Trial for Mirai authors ends with no prison time

AirNaine starts distributing phishing via Onliner Spambot

OCTOBER

Data from 9.4 million passengers of Cathay Pacific and one of its units, the Hong Kong Dragon Airlines, was leaked in a data breach in March

NOVEMBER

Breach of Starwood/Marriott is reported

Quora discovered a hack on one of their systems which led to the exposure of approximately 100 million user's data

Emotet restarts spamming after ~1 month of inactivity

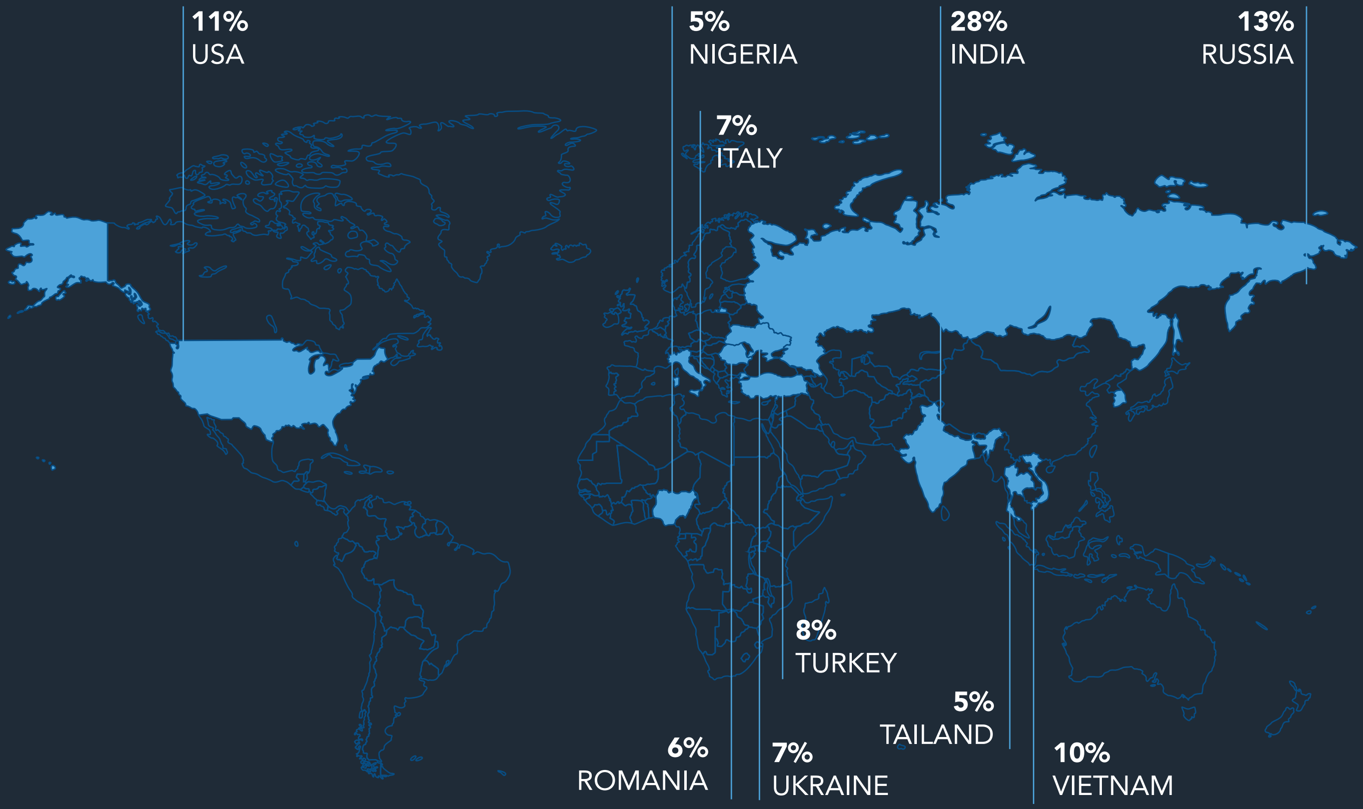
DECEMBER

AZORult author announces retirement

Global incident highlights

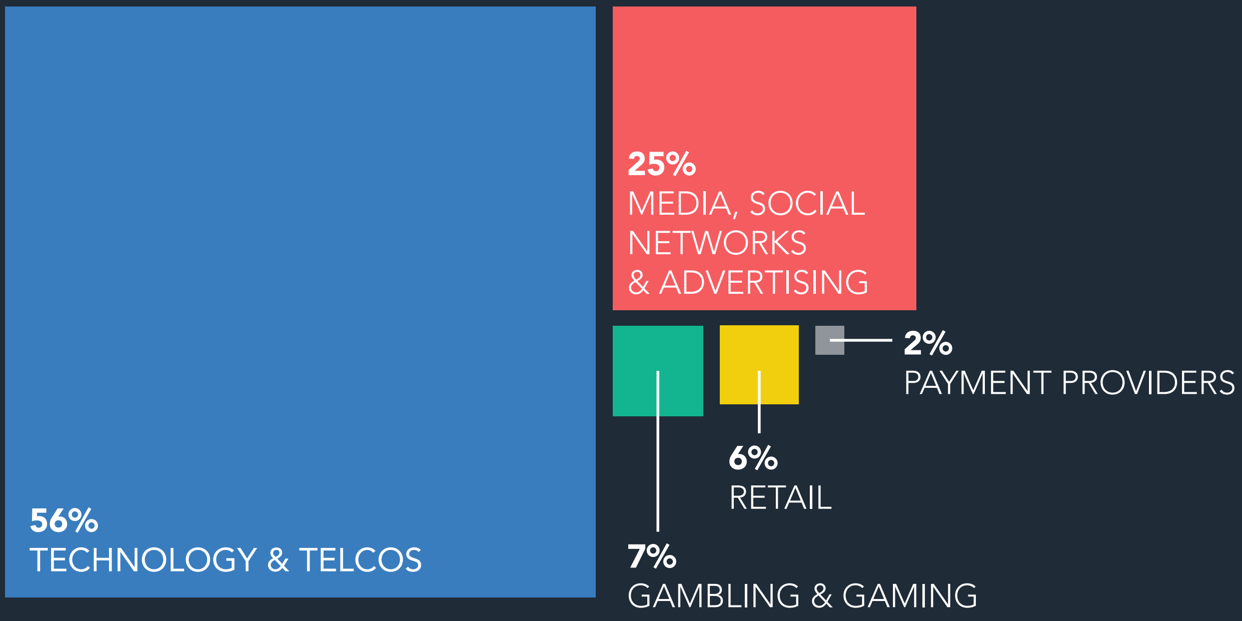
COUNTRIES THE MOST IMPACTED BY CREDENTIAL THEFT

Europe represents 20% of the total number of detected stolen credentials. A fairly similar number to last year

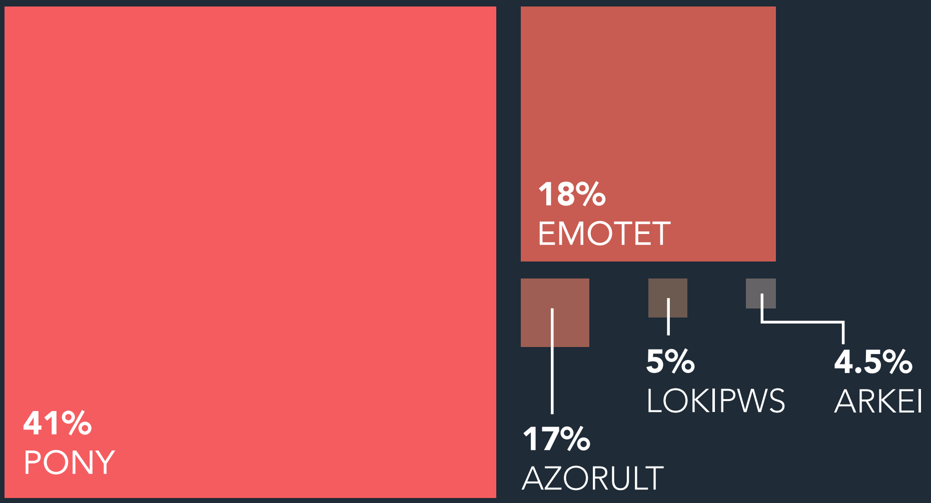


#Blueliv has observed a 50 % growth in the number of stolen credentials from botnet between 2017 and 2018.

90% OF THE TOTAL NUMBER OF STOLEN CREDENTIAL DETECTED ARE FROM 5 INDUSTRIES:

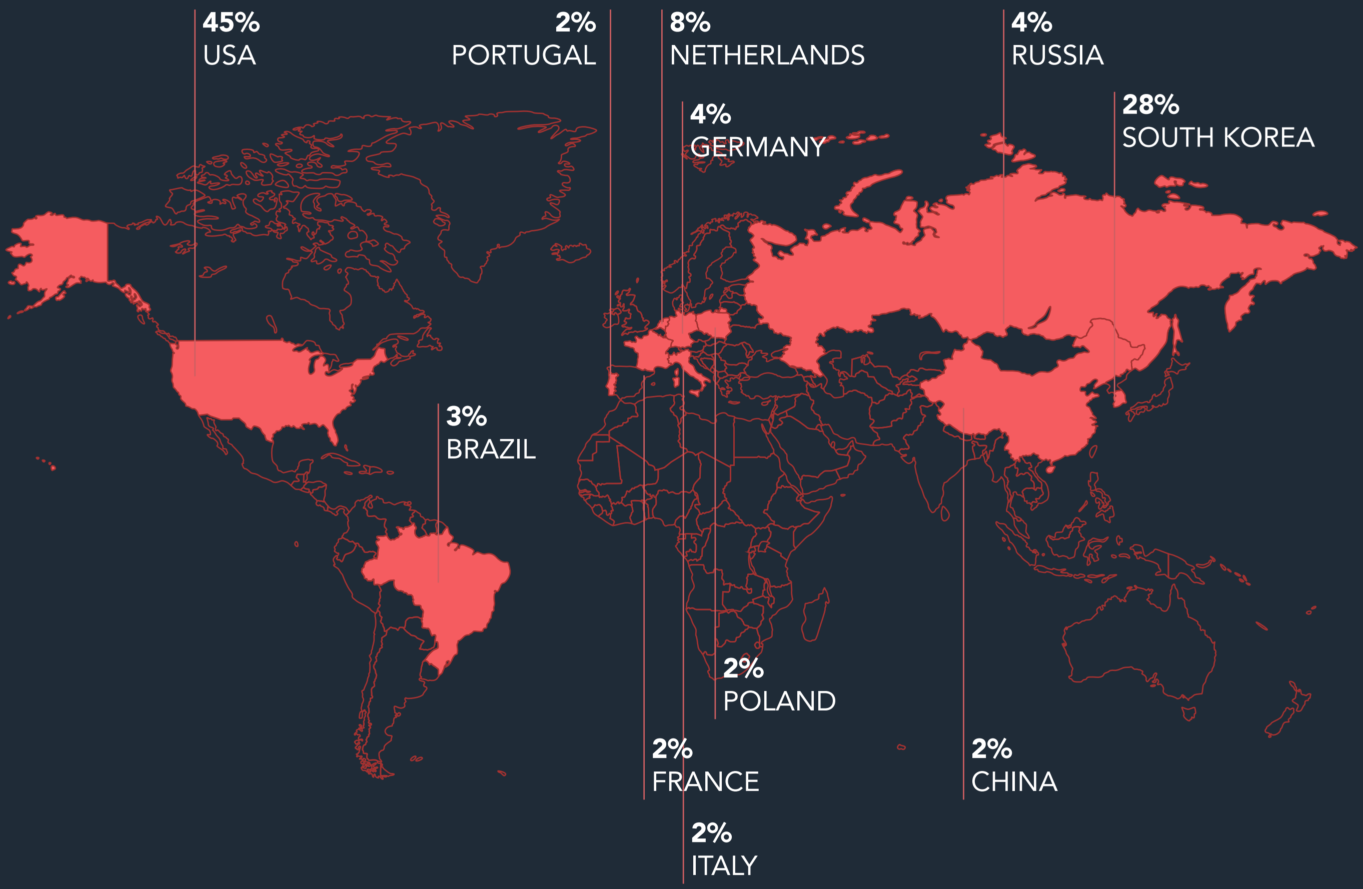


TOP 5 CREDENTIAL STEALING BOTNETS



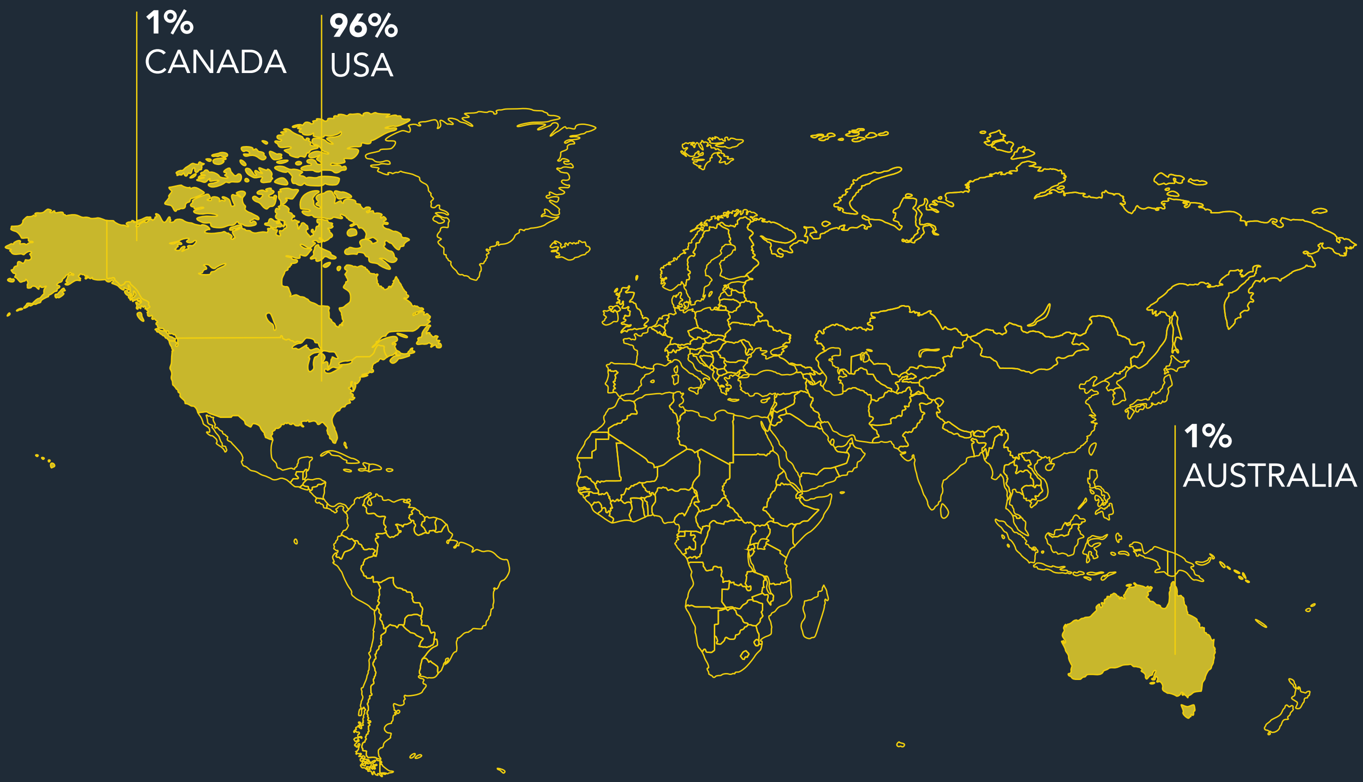
TOP 10 GEO-LOCATIONS OF MONITORED CRIME SERVERS IN 2018

The number of geolocated crime servers in the US decreased from 65% to 45% in the period between 2017 and 2018. Still, more than 90% of the geolocated crime servers come from the following countries: the United States, South Korea, the Netherlands, Germany, and Russia.

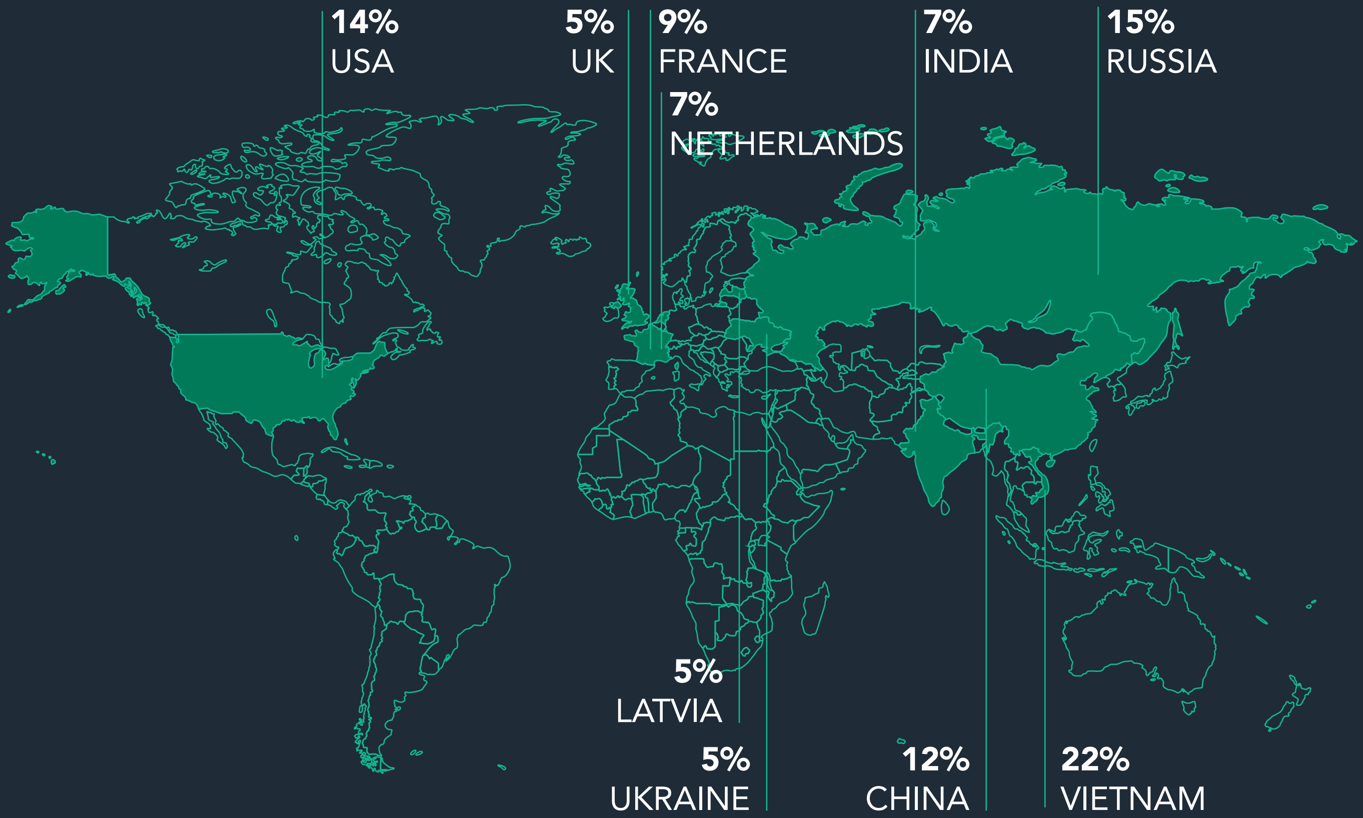


These were picked up by our live cyberthreat map throughout the year.

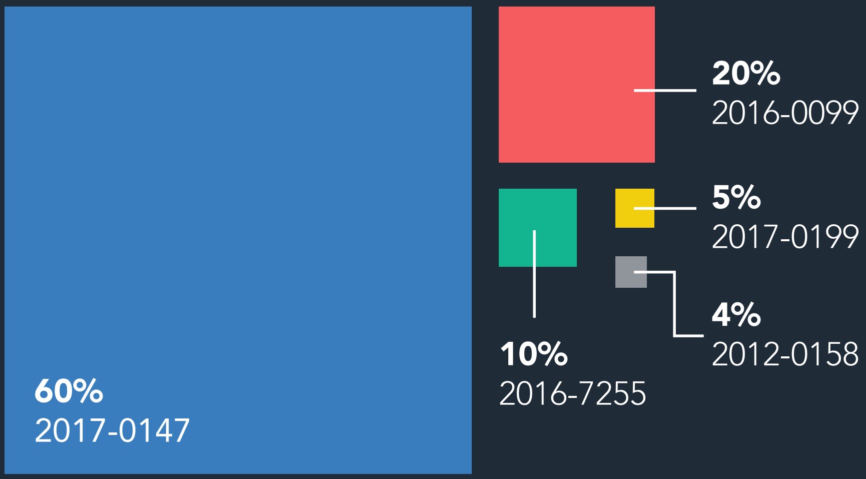
SIMILARLY TO THE PREVIOUS YEAR, 96% OF ALL STOLEN CREDITS CARDS BELONG TO AMERICAN BANKS IN 2018.



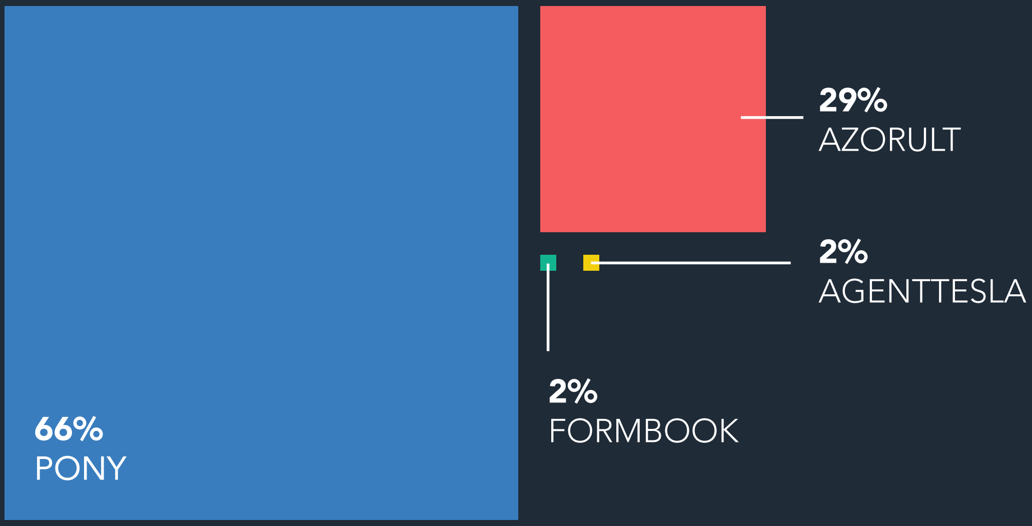
65% OF CYBER ATTACKS SEEN IN OUR HONEYPOTS CAME FROM 5 COUNTRIES: VIETNAM, RUSSIA, UNITED STATES, CHINA, AND FRANCE.



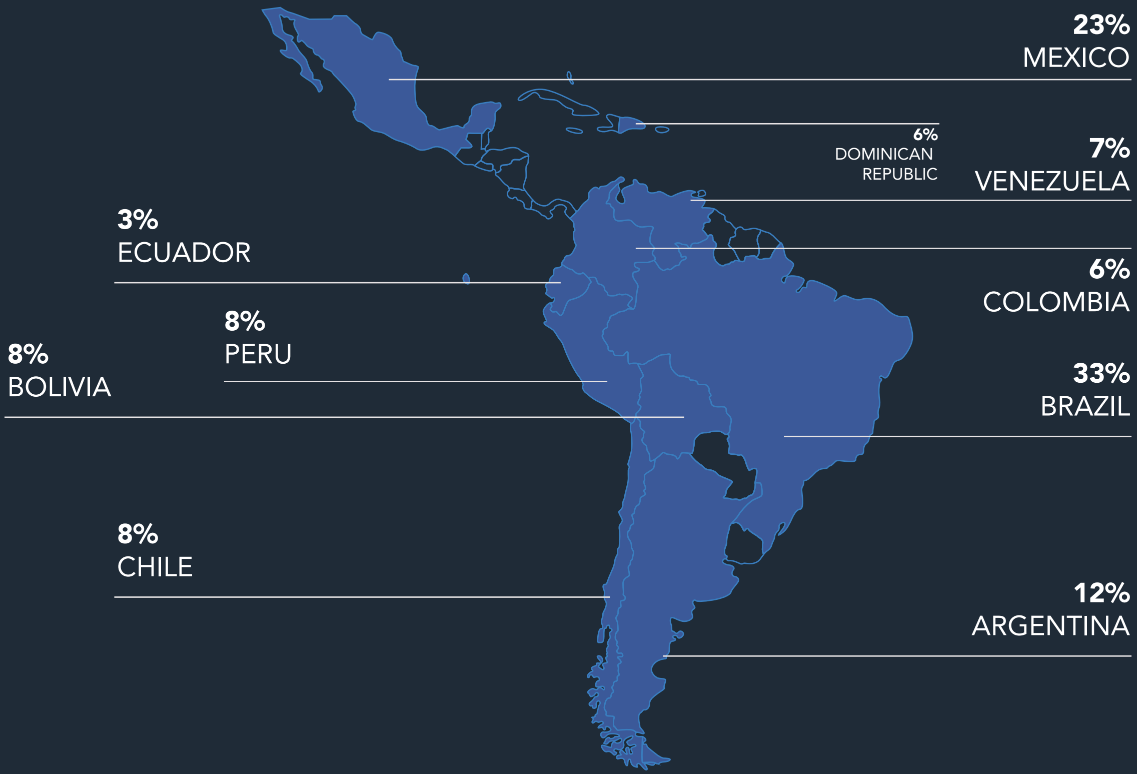
TOP 5 MOST COMMON VULNERABILITIES REFERENCES (CVE) USED IN MALWARE IN 2018



PONY AND AZORULT MAKE UP 95 % OF THE TYPE OF BOTNET STEALING CREDENTIALS IN LATIN AMERICA.



BRAZIL, MEXICO AND ARGENTINA REPRESENTS MORE THAN 2/3 OF THE NUMBER OF STOLEN CREDENTIALS IN LATIN AMERICA FROM BOTNETS IN 2018.



3.CORPORATE INTRUSIONS

Targeted attacks grew in size and scope in 2018, with the objective of stealing valuable information. Many of these attacks appear to be financially motivated, with threat actors seeking to monetize the stolen data by selling it afterwards on the cybercriminal underground. Or in some cases, extorting the victim in the hopes they will pay a ransom instead of having their lack of proper security measures revealed to the public and regulators.

We go into detail on how cybercriminals profit from these attacks in our report on The Credential Theft Ecosystem, available to download here.

It seemed as though every week in 2018 another organization was forced to notify its customers their data may have been compromised. This section delves into some intrusions that occurred throughout the year, and shares lessons that ought to be learned from the incidents.

For Exactis, an enormous 2TB of information was exposed, from names and emails through to intimate personal data like personal characteristics, religious beliefs and interests – enough for identity thieves to potentially make some serious gains.

3.1.EXACTIS

Reports emerged in June that Exactis, a marketing company based in Florida, exposed information on around 230 million Americans and another 110 million record related to US businesses. Security researcher Vinny Troia sought to test out ElasticSearch, a widely-used database type, by leveraging the search tool Shodan, and uncovered a number of unprotected databases.

For Exactis, an enormous 2TB of information was exposed, from names and emails through to intimate personal data like personal characteristics, religious beliefs and interests – enough for identity thieves to potentially make some serious gains. The fact that this was not even part of a concerted effort by cybercriminals to exfiltrate the data was pure chance, and once Troia accessed the data he alerted both Exactis and the FBI. Organizations must remain constantly vigilant, using DLP modules to detect if any information held on servers has become publicly accessible.

3.2.AADHAAR

The Indian government's Aadhaar is the largest biometric ID system in the world, and handles most of India's 1.1 billion citizen's fingerprints, photographs, home addresses and other personally identifiable information (PII). Throughout the year it was plagued by security issues, many of which were denied by the government. In January, a report in Indian newspaper The Tribune alleged that Aadhaar access – advertised on WhatsApp groups – could be bought for as little as $7 USD.[4] In the subsequent months, other incidents demonstrating security issues with the Aadhaar system were exposed. For example in March, a New Delhi-based security researcher detected a vulnerable endpoint and shared it with ZDNet.[5] In July, a government official tweeted his Aadhaar number to challenge the internet to do him harm, with predictable results.[6]

The intrusions here highlight a potentially worrying development, and are notable for their scale and the number of people affected. Biometric authentication and other PII can be used by governments to streamline services, but in the wrong hands it becomes a major concern.

3.3. HUDSON'S BAY CO.

At the beginning of April it was reported that around 5 million credit and debit card numbers were compromised at Saks and Lord & Taylor stores – which are owned by Hudon's Bay Co. – in North America. By the end of the month, it was confirmed that threat actors had access to the data for around nine months, from July 2017 to April 2018. This is a clear demonstration that these sort of breaches can go undetected for a considerable amount of time if the right threat intelligence is not deployed to find the holes and plug them before it is too late.

The breach has been attributed to the Eastern European crime syndicate Fin7, and the data was subsequently offered for sale on the underground card shop Joker's Stash.

The company said that two separate incidents led to the theft of around 1.2 million general user data files – including information such as names, addresses and email addresses - and 5.9 million payment card details.

3.4. DIXONS CARPHONE

On June 13th Dixons Carphone publicly stated they had suffered a data breach. The company said that two separate incidents led to the theft of around 1.2 million general user data files – including information such as names, addresses and email addresses - and 5.9 million payment card details. However, 5.8 million of those cards were PIN-protected and the attackers could neither obtain the PIN nor the CVV of any card, leaving the attackers unable to use them for traditional cybercrime. The banks responsible for the remaining 105,000 unprotected cards were informed. The retailer said that while the data breach was only discovered that week, it occurred in July of the previous year. With that in mind, even though this was the first major data breach to occur after the implementation of the GDPR, its fines would not be applied.

3.5. MARRIOTT

On September 8th, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database in the United States. On November 19th2018, the investigation determined that there was unauthorized access to the database and thereby the information of up to 500 million customers who had stayed at these hotels between 2014 and the day of detection were stolen.

For approximately 327 million customers, the breached data included some combination of name, birth date, email address, phone number, mailing address, passport number, preferred account information, gender, arrival and departure information, reservation date, and communication preferences.

For approximately 327 million customers, the breached data included some combination of name, birth date, email address, phone number, mailing address, passport number, preferred account information, gender, arrival and departure information, reservation date, and communication preferences. For some of these customers, payment card numbers and expiration dates were also exposed, albeit they were encrypted with AES-128. For the remaining guests, the information was limited to name and other data such as mailing address and email address.

Marriott's security experts determined that the unauthorized party had copied and encrypted the data before extracting it, and was taking steps to remove it. To compensate and help the affected customers, Marriott has opened a dedicated Website and a Call Center, has notified the victims and has given them a free one-year WebWatcher Enrolment.

3.6. QUORA

Quora discovered one of their systems had been compromised, which led to the exposure of approximately 100 million users' data on November 30th. The stolen data included contained account information (names, email addresses, encrypted passwords with a specific salt for each user, and dates imported from liked networks if the users had authorized it), public content (publications and upvotes) and non-public content and actions (requests, downvotes or direct messages). Fortunately, no financial information was breached.

Upon discovery, Quora launched an internal investigation to try and determine the identity of the attacker and how the breach occurred. They also informed law enforcement officials and notified the affected users. Quora also logged out all users that may have been affected and invalidated their passwords, and they fixed what they think was the root cause of the breach.

3.7. CATHAY PACIFIC

Cathay Pacific is a Hong Kong flag airline carrier that covers more than 190 destinations in 60 countries worldwide. On October 24th, they reported data of about 9.4 million of its passengers, as well as passengers from one of its units, the Hong Kong Dragon Airlines, was leaked in a data breach in March 2018. Cathay announced that the disclosed data included 860,000 passport numbers, about 245,000 Hong Kong identity card numbers, 403 expired credit card numbers and 27 credit cards without a CVV. No passwords were leaked on this breach, but data such nationalities, dates of birth, phone numbers, email and physical addresses were compromised.

Cathay announced that the disclosed data included 860,000 passport numbers, about 245,000 Hong Kong identity card numbers, 403 expired credit card numbers and 27 credit cards without a CVV.

Rupert Hogg, the executive chief of Cathay Pacific, stated that they acted immediately to contain the event and determine the cause with a cybersecurity firm's assistance. They also guaranteed that there was no impact on flight safety. This incident came just a month after British Airways apologized for a heist they suffered, during which payment card details from hundreds of thousands of its customers were compromised in a cyberattack to its website and app.

4. TRENDING TTPS

4.1. MALWARE AND CYBERCRIME SERVICES

Ransomware campaigns decreased in popularity from 2017, but classic malicious campaigns like malware downloaders and trojans were still a trend in 2018. During the last quarter, several malspam campaigns were discovered, proving how a well-planned and professional attack can stay under the radar for months on end. These kinds of campaigns are not new, but they still pose a dangerous threat to businesses in any sector.

During the last quarter, several malspam campaigns were discovered, proving how a well-planned and professional attack can stay under the radar for months on end.

The security of a system is as strong as its weakest link, and more often than not, that link tends to be a human being. That is the reason why hackers are still using malicious email campaigns in order to breach systems and organizations. These emails try to trick victims into performing harmful actions, like giving their credentials to a phishing website or downloading and executing malware. The most popular vector consists of attaching a file of the receiver's interest with the malicious payload embedded on it. Once said file is opened, the malware infects the system. The main type of malware chosen for those attacks are loaders, a type of trojan that secretly downloads, installs and executes other malicious software from a remote server on the host machine. This conduct allows the attackers to choose which kind of malware will be installed, giving them full control over the botnet's state.

The security of a system is as strong as its weakest link, and more often than not, that link tends to be a human being.

We expect this type of infection to continue, due to how easy it is to target these campaigns towards a specific victim, making infections stay under the radar by selecting the desired hosts. Also, they can increase their infection's life expectancy by upgrading the installed modules, as long as the attackers have full control over the malicious payload.

4.1.1. MARAP

On August 10th, a new malware loader named Marap was discovered by Proofpoint in a large malspam campaign composed of millions of messages. Initial research indicates that it was aimed mainly against financial institutions. Marap's main functionality is to download other modules and payloads, allowing the attackers to install any feature they want after the initial infection has succeeded, expanding its capabilities as they see fit. Presently, Marap has only shown a single module with system fingerprinting capabilities, used to gather and send data about the host device to the C&C server. This activity is likely done to identify the infected device and its capabilities, and detect if it is a target of interest or not. The malicious emails are disguised as messages from "sales" or "major banks" containing malicious Word documents, PDF files or password protected ZIP files. This campaign has been attributed to TA505, due to the similarities shared with previous campaigns from the threat actor.

4.1.2. ADVISORSBOT

This malware downloader was first seen by Proofpoint in May 2018 and it was used in several malspam campaigns attributed to TA555. Just like Marap, AdvisorsBot's first stages of infection consists of identifying if the host device is an interesting target or not by using its fingerprinting module. The campaigns are disguised in different ways to target victims. The first campaign was aimed at hotel employees, and was themed as a complaint from a fictitious hotel client who claimed to have been charged twice, attaching a malicious Word document as a card statement. The second and third campaigns, disguised as food poisoning incidents and fake catering orders, targeted restaurant workers. The last detected campaign was disguised as a resume of someone interested in applying for positions at telecommunication companies. AdvisorsBot evolved along with those campaigns, indicating that this malware is currently under development and new different strains may appear in the next months.

Throughout November 2018, Emotet was dispatching approximately 185,000 spam messages a day, using over 50,000 different sender emails.

4.1.3. EMOTET

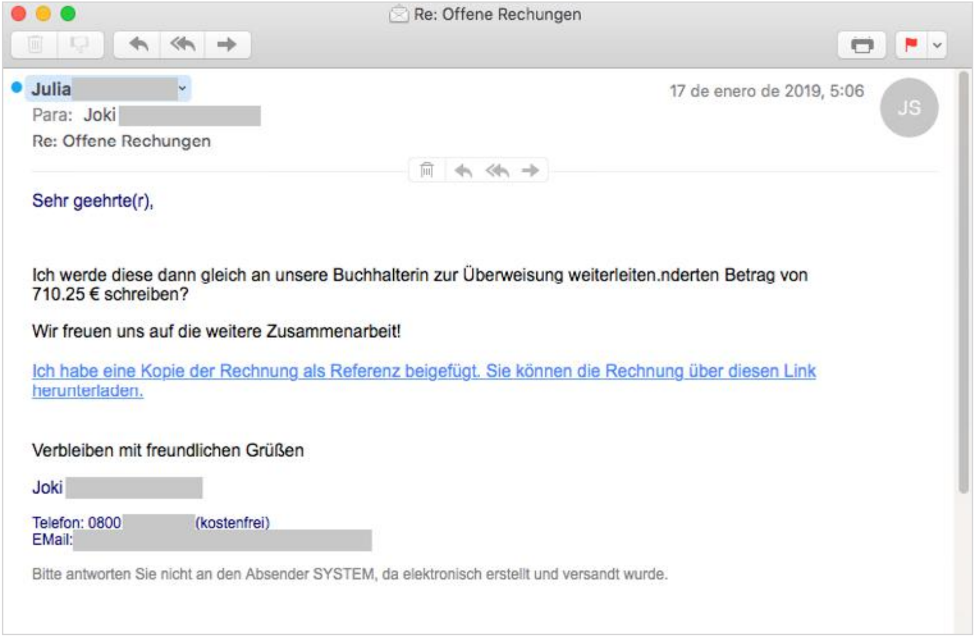
Emotet, also known as Geodo, is a piece of code deployed as a malware distribution service (spam botnet). However its past is a little more complex. This trojan is an evolution of the banking trojan Feodo (also known as Cridex and Bugat).After this version, a new evolution of the banking trojan appeared and was renamed Dridex, the now infamous banker.

Emotet was previously deployed as a banking trojan before disappearing in the middle of 2015. Emotet resurfaced again in December of 2016 with substantial changes: no banking module was detected in this new wave, and its main purpose was now to be used as a spambot to spread additional malware. This latest version is also known as Emotet v4.

In 2018, researchers uncovered a long-running cyberespionage campaign against Android users in the broader Middle East and North Africa.

In 2018 Emotet primarily used PDFs and DOCs as droppers, with payloads of TrickBot, Botbot/IcedID, or PandaBanker. In many instances, the malware is self-propagating as Emotet itself.

The stealer module of Emotet collects credentials as well as email addresses to use in future spam campaigns. Throughout November 2018, Emotet was dispatching approximately 185,000 spam messages a day, using over 50,000 different sender emails. These sender emails represent 15,000 unique domains, of which ~8% belong to countries in Latin America and around 6% were German domains. The recipients of this campaign are largely corporate email addresses, representing 1,200,000 different mail domains, with ~10% of them being corporate German addresses.



Re: Offene Rechungen

Julia [redacted]

17 de enero de 2019, 5:06

JS

Para: Joki [redacted]

Re: Offene Rechungen

Sehr geehrte(r),

Ich werde diese dann gleich an unsere Buchhalterin zur Überweisung weiterleiten.nderten Betrag von 710.25 € schreiben?

Wir freuen uns auf die weitere Zusammenarbeit!

Ich habe eine Kopie der Rechnung als Referenz beigefügt. Sie können die Rechnung über diesen Link herunterladen.

Verbleiben mit freundlichen Grüßen

Joki [redacted]

Telefon: 0800 [redacted] (kostenfrei)
EMail: [redacted]

Bitte antworten Sie nicht an den Absender SYSTEM, da elektronisch erstellt und versandt wurde.

Figure2: Emotet campaign targeting a German business address

4.1.4. THREADKIT

First seen in June 2017, ThreadKit is an exploit builder kit that generates weaponized RTF documents. It bears similarities to Microsoft Word Intruder (MWI), causing some researchers to hypothesize that ThreadKit may be an evolution of MWI. ThreadKit is able to report statistics to a control panel, using the "INCLUDEPICTURE" field, a technique also used by MWI.

While it first debuted in 2017, ThreadKit exploded in popularity in 2018. The kit was employed by advanced threat groups such as the Cobalt Gang. ThreadKit has also been used to distribute various malware families, including Smoke Loader, TrickBot, Chtonic, Formbook, LokiPWS, Neutrino Bot, AZORult, and Ursnif.

ThreadKit is continuously updated and improved upon by its author, who operated under the alias "mrbass." This threat actor integrated newly discovered vulnerabilities – such as CVE-2018-0802 – into their product in 2018. This tool is available for sale on the cybercriminal underground at a cost of $970.

4.1.5. ZOOPARK

In 2018, researchers uncovered a long-running cyberespionage campaign against Android users in the broader Middle East and North Africa. Malicious applications masquerading as legitimate apps were distributed in countries such as Morocco, Egypt, and Iran. These app carry a spying malware dubbed Zoopark, which offers several malicious capabilities to the attackers, including: filtration of contacts' data, GPS location and keylogging. This malware also collects information from messaging applications like Telegram and WhatsApp, and tries to steal their internal databases, which contain all the stored conversations, thus dangerously compromising the victims' privacy. The attackers seem to be especially focused on Egypt, Jordan, Morocco, Lebanon and Iran as targets, as well as employees of the United Nations Relief and Works Agency. The increasing use of mobile devices for personal and professional communication is turning them into important spying objectives for nation-state sponsored actors.

4.1.6. IOT MALWARE

Internet of things (IoT) devices have been garnering more attention among cybercriminal communities due to their harmful potential and their poor security measures. New strains of malware like Mirai Sora or Torii have features that allow them to infect devices from different architectures, such as routers, IP cameras and Android devices. This enormously expands the number of potential victims. The primary objectives weaponized armies leveraging IoT devices are to offer denegation of service attacks for hire, also known as DDoS-for-hire, and trying to mine crypto currencies.

The destructive potential of IoT botnets turns them into an important tool to perform large scale attacks. DDoS-for-hire turned them into a profitable business, so this will raise more attention from criminal groups. On the other hand, even though some malicious developers are still doing this, the use of IoT botnets for mining crypto currencies is not worth the effort and risk, due to the low income margin.

4.2. CRYPTOMINERS AND CRYPTOJACKING

The huge price increase of cryptocurrencies in late 2017 – which led Bitcoin to be worth around $20,000 – caused a surge in interest, including among the criminally minded. In 2018, cryptojacking moved from the fringes of the cybercrime world into center stage. According to research conducted by Skybox Security, cryptojacking accounted for 37% of all malware attacks last year.

The primary impact of cryptojacking is performance-related, though it can also increase costs for individuals and businesses affected. Potential impacts for device owners include:

- A slowdown in device performance
- Overheating batteries
- Devices becoming unusable
- Reduction in productivity
- Higher costs due to increased electricity usage, and for businesses operating in the cloud that are billed based on CPU usage
- Unlike threats like ransomware, which immediately disrupt victims' access to their devices, cryptojacking could be quietly carried out on a victim's device for a long time before they realize what is happening.
- Routers hijacked to mine cryptocurrency

There were a ton of blockbuster-like cryptojacking headlines in 2018, too. Researchers uncovered over 400,000 routers that had been hacked and infected with malware, designed to use their computing power to mine Monero – and the number of impacted devices may be growing. Threat actors elsewhere have surreptitiously infected websites in order to mine cryptocurrencies on visitors'

There were a ton of blockbuster-like cryptojacking headlines in 2018, too. Researchers uncovered over 400,000 routers that had been hacked and infected with malware, designed to use their computing power to mine Monero – and the number of impacted devices may be growing.

computers. This happened in November 2018 when hackers exploited a publicly known Drupal vulnerability to compromise the Make-A-Wish Foundation's website. Other payloads using the same Drupal vulnerability were described by Blueliv analysts last year.

4.3. THE USE OF RANSOMWARE HAS DECREASED OVER THE PAST YEAR

The use of ransomware has decreased over the past few months. It became popular in 2017 after the WannaCry incident, encouraging malicious developers to create new ransomwares. When a ransomware malware successfully infects a machine, it encrypts all important files and data. It then asks for a ransom, in return for the key victims must use to decrypt their files. Those ransoms are often asked for in bitcoin or any other cryptocurrency, and it is highly advised that victims not pay. t Not only does this promote more ransomware attacks, but it is possible the data might never be recovered anyway. Despite numerous warnings, victims still pay the ransoms and, as recent research has shown, the ransomware business is still profitable for some threat actors. One of the most popular ransomwares in 2018, SamSam, has already collected almost $6 million dollars.

Despite numerous warnings, victims still pay the ransoms and, as recent research has shown, the ransomware business is still profitable for some threat actors. One of the most popular ransomwares in 2018, SamSam, has already collected almost $6 million dollars.

Threat actors are losing interest in ransomware attacks due to how hard it is to bring in cash. In order for the attackers to get their hands on any money, the victim must be vulnerable and have quick access to cryptocurrency. Yet, although they've decreased, ransomware attacks must still be considered a dangerous and destructive threat for companies in any sector. But keep in mind: the real economic threat is often not the ransom itself, however either the side effects the attacks incur.

4.3.1. MATANUSKA-SUSITNA ATTACK

In July 2018, the borough of Matanuska-Susitna, Alaska, fell victim to a cybercriminal campaign using the BitPaymer ransomware. The attack impacted all of the borough's desktop computers and the majority of their servers, forcing government employees to rely on typewriters to continue functioning. Analysis of the attack revealed that Matanuska-Susitna infrastructure had been infected since May, with the ransomware "lying dormant" until the borough's IT team began to take measures to remove the malware. Official reports say that it had been a multi-pronged, multi-vectored attack, compounded by a set of malware and tools used in conjunction with each other. Those tools and malware included, but may not be limited to, trojan horses, worms, the BitPaymer crypto locker, and an external hacker logging in the victim's network.

This attack has been considered an Advanced Persistent Threat (APT) - in other words, a set of sneaky and persistent hacking processes targeted at a specific entity. None of the affected employees' anti-virus software detected and blocked the infection, meaning that a new malware strain had been used. The borough did not state whether or not they had paid the ransom in order to recover the data. BitPaymer, which is tied to the gang behind Dridex, had reportedly affected other victims both before and since the attack.

4.4. DIGITAL SKIMMERS ON THE RISE

Digital skimmers received an explosive amount of attention this year. The number of threat actors operating under the umbrella term "Magecart" and leveraging digital skimmers increased significantly.

Digital skimmers are scripts designed to steal data entered into online payment forms, and threat actors use these on the compromised websites of e-commerce entities or third-party suppliers. Research suggests that the actors often use vulnerabilities in the website/CMS, or take over the hosting/CMS accounts to facilitate their crimes.

Magecart groups first started appearing in 2015, attacking the e-commerce platform Magento. Later on in 2016, they hacked numerous e-commerce websites. The groups would inject Javascript code into the sites thereby allowing the attackers to capture the credit card information introduced in the payment form. Since these attacks, it seems that the group established the modus operandi of injecting Javascript code to exfiltrate the customer's' payment data.

The year 2018 ushered in an era of Magecart megabreaches, including breaches at Ticketmaster, British Airways, and Newegg.

Cash-out attacks, also known as Jackpotting or black box attacks, consist of manipulating ATMs to make them dispense cash, potentially causing financial institutions to lose thousands of dollars in a single heist.

4.5.HACKING ATMS

ATMs are still one of the most profitable targets for criminals, who do not hesitate to use every possible method and technique in order to take money from the devices. Malware infections are getting more and more popular, leaving physically destructive techniques more deprecated. Cash-out attacks, also known as Jackpotting or black box attacks, consist of manipulating ATMs to make them dispense cash, potentially causing financial institutions to lose thousands of dollars in a single heist. We saw a rising number of cash-out heists in 2018, performed using a range of approaches.

Most ATM models share the same structure; a vault with a cash dispensing mechanism controlled by a computer operating system. Each one of these components is vulnerable to different kinds of violations - classified as physical, logical or hybrid attacks depending on how to access the device. What makes this type of heist popular is the fact they require a low level of technical knowledge to execute; step-by-step guides can even be easily found on the dark net. Within the several sub-categories that compound logical ATM attacks, malware attacks have gained steam within the criminal community.

Many techniques require the criminal to manipulate the ATM physically to some degree, potentially exposing the threat actor. But there are also completely remote attacks that can empty an ATM the same way without compromising the attacker's identity. An attacker can infect and manipulate ATMs through the financial institution network itself, gaining access to the device and turning it into a slave machine, this allows the attacker to use the ATM not just to dispense money, but to also gain full control of the device.

India's Cosmos Bank lost $13.4 million in an aggressive malware attack, uncovering the poor measures that banks use against targeted cyberattacks.

4.5.1.COSMOS BANK

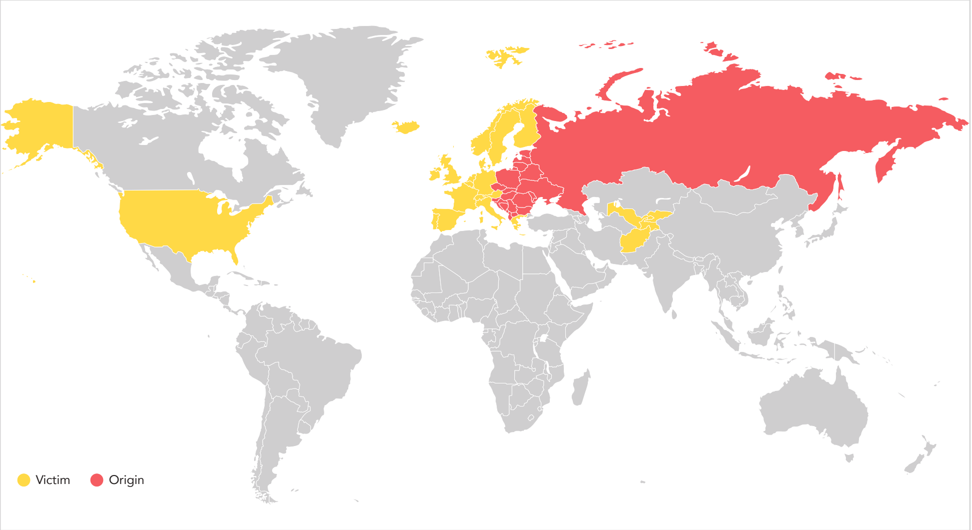
In the first half of August 2018, the FBI warned all worldwide banks of a possible global ATM cashout blitz. A few days later, India's Cosmos Bank lost $13.4 million in an aggressive malware attack, uncovering the poor measures that banks use against targeted cyberattacks. It is unclear how the hacker group breached Cosmos

Bank's network, but it is fairly possible that they broke in through phishing email campaigns. After the initial compromise, the attackers turned the ATMs into malicious proxy switches, possibly by installing a malicious version of their firmware or by modifying their current software. At this point, Cosmos Bank ATMs were modified to steal customer's payment card information and SWIFT codes required for transactions.

The heist took place in two stages; the first stage involved the subtraction of $11.5 million in transactions from 22 different countries; followed by the second one, where the criminals stole $2 million through debit card transactions across India. Much of the stolen loot was later transferred to Hong Kong through fraudulent SWIFT transactions. Subsequent reports indicate that this was not the first attempt to compromise the bank's system, but no alert was issued after the previous attempts and they did not set any additional protection measures despite detected suspicious activity.

5.THREAT ACTOR ACTIVITY

5.1.FIN7



FIN7 is a financially-motivated threat group. It has primarily targeted the retail and hospitality sectors, but has an eye on financial information. The group uses phishing techniques to distribute point-of-sale (POS) malware, often combined with remarkably bold social engineering techniques, such as calling up victims to ensure they open malicious files. Since appearing in 2015, the group has compromised hundreds of companies, thousands of POS terminals, and millions of payment cards. FIN7 has been linked to high profile breaches at Arby's, Chili's, Chipotle, Red Robin, Jason's Deli, and Sonic. After a successful breach, FIN7 typically offers the compromised cards for sale on the underground card shop Joker's Stash.

Researchers have uncovered that in addition to compromising payment cards, FIN7 occasionally elects to also pivot towards finance departments. Even more, US law enforcement has reported FIN7-linked phishing emails posing as the US Security and Exchange Commission (SEC), targeting individuals with access to documents that may prove useful in the stock market.

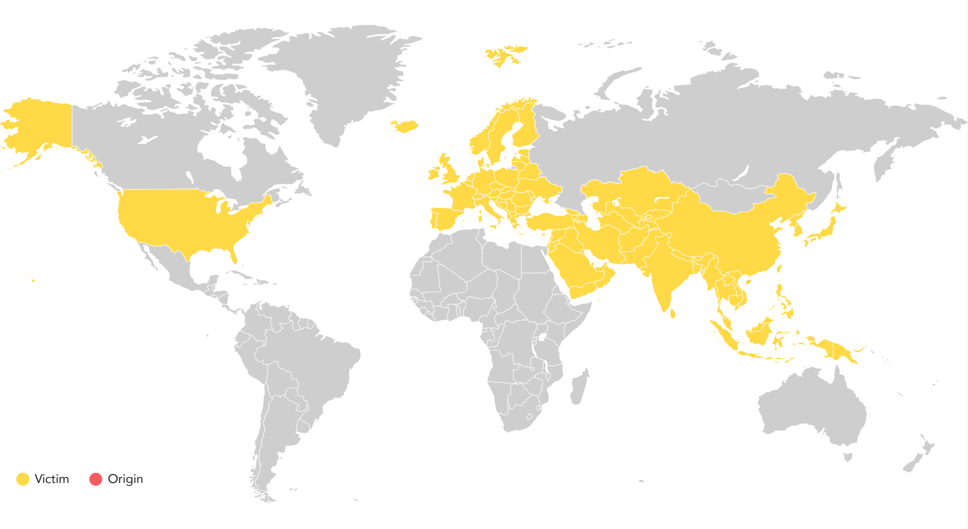
In August 2018, the US Department of Justice (DOJ) announced that three members of FIN7 had been arrested. In the announcement, the DOJ revealed that FIN7 used a front company called "Combi Security" to carry out at least a portion of their activities. Combi Security masquerades as a legitimate company headquartered in Russia and Israel and has posted on job recruitment boards in Eastern Europe and Central Asia. Membership of the group is primarily Eastern European.

FIN7 should be considered a dangerous APT because of its rigorous and sophisticated procedures, proving in several occasions the ability to quickly evolve new strategies and adapt tools. The group has shown to be a particularly professional and disciplined organization, working following a regular office schedule, with nights and weekends off.

FIN7 should be considered a dangerous APT because of its rigorous and sophisticated procedures, proving in several occasions the ability to quickly evolve new strategies and adapt tools.

This group seems to choose its objectives carefully, planning the strikes in advance after studying the potential victims for some time.

5.2. ORANGEWORM

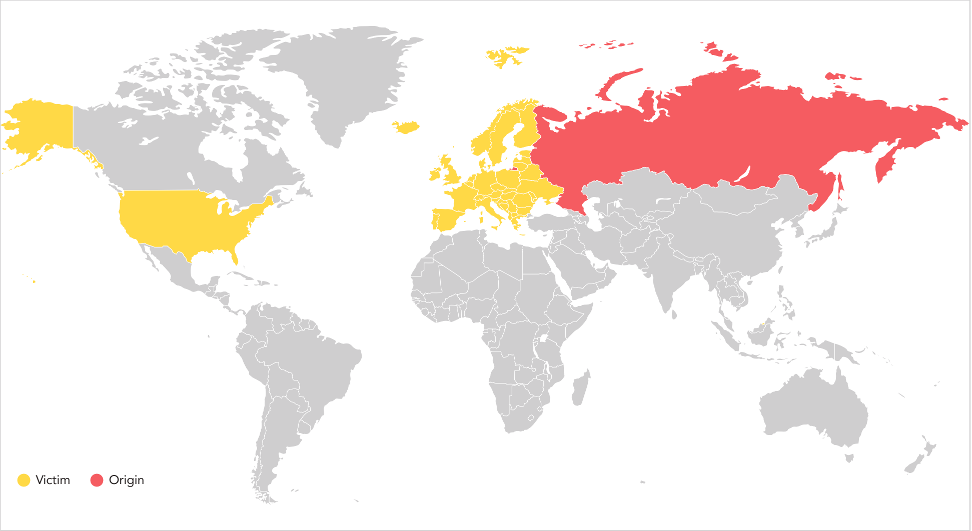


The timeline for each compromise may vary but, in general, they manage to exploit the targeted network within a week, with ongoing access maintained for months.

A new hacker group named Orangeworm has been discovered deploying a custom backdoor into large international corporations, most of them related to the healthcare sector in the United States, Europe and Asia. There is no evidence of this group working for any nation or fighting for any political cause. Rather, Orangeworm could be a lone criminal or a small group of individuals working in their own interest. This group seems to choose its objectives carefully, planning the strikes in advance after studying the potential victims for some time.

The malware they use consists of a custom Trojan backdoor called Trojan.Kwampirs. This Trojan prowls in medical devices - think X-ray devices and MRI machines - but it has also been detected in machines used to assist patients in completing consent forms for medical procedures. In order to get access to healthcare corporations, Orangeworm develops a large supply chain-attack, striking industries related with the healthcare business. The malware they deploy, Kwampir, uses some obfuscating techniques and ensures its persistence on the infected system, avoiding antivirus detection by inserting randomly generated strings into the middle of the payload. In spite of that, this malware shows a notably noisy behavior due to the way it propagates and communicates with its command and control servers. It tries to infect all the devices inside the victim's network by copying itself over the network shares, and communicates with the C&Cs servers by cycling connections through a large list of servers. Those methods are easily detectable and they indicate that Orangeworm is not concerned about being discovered. Kwampir collects basic information about the compromised device, such as the language settings, system version and network adapter information, and it may use that data in order to determine if the infected system is potentially worthy. Then, Kwampir opens a backdoor and allows the attackers to access the victim's device remotely, allowing them to steal confidential data.

5.3. ENERGETIC BEAR

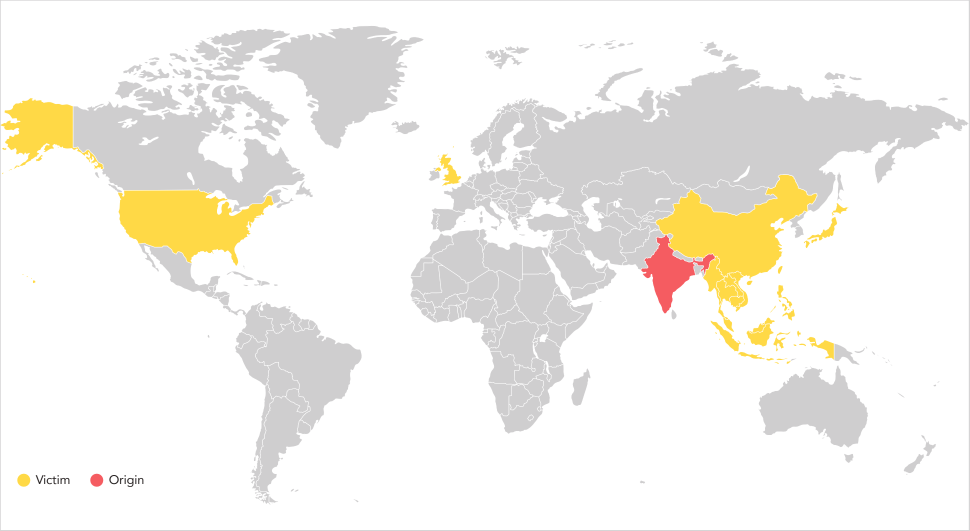


Energetic Bear (or Dragonfly) is a threat actor aligned to the Russian government's interests that has been active since at least 2010. In 2018 it was especially interested in targeting multiple government entities and infrastructure sectors from Europe and United States within the energy, nuclear, water, aviation and critical manufacturing industries. This group seems focused on learning how energy facilities operate, and in finding ways to gain access into the operational systems themselves.

The energy sector has turned into an area of interest for cybercriminals, due to the large repercussion that would be seen upon achieving a successful attack. For example, the disruptions in Ukraine's power system in 2015 and 2016 performed by the APT Sandworm affected hundreds of thousands of people. In 2018 several attack attempts on the electricity grids in European countries have been reported, and some US nuclear facilities have been compromised by hackers, as well.

This campaign affects two types of victims: staging and intended targets. This group infects peripheral companies, such as trusted third-party suppliers with less secure networks, in order to use those networks as pivot points and malware repositories when targeting their final intended victims. They use these staging targets as watering holes, turning trade publications and informational websites related to process control into dangerous sites containing malicious code. This group uses a large set of open source utilities available on GitHub in order to perform and improve their operations, such as Nmap, Sqlmap or Sublis3r. The timeline for each compromise may vary but, in general, they manage to exploit the targeted network within a week, with ongoing access maintained for months.

5.4. PATCHWORK

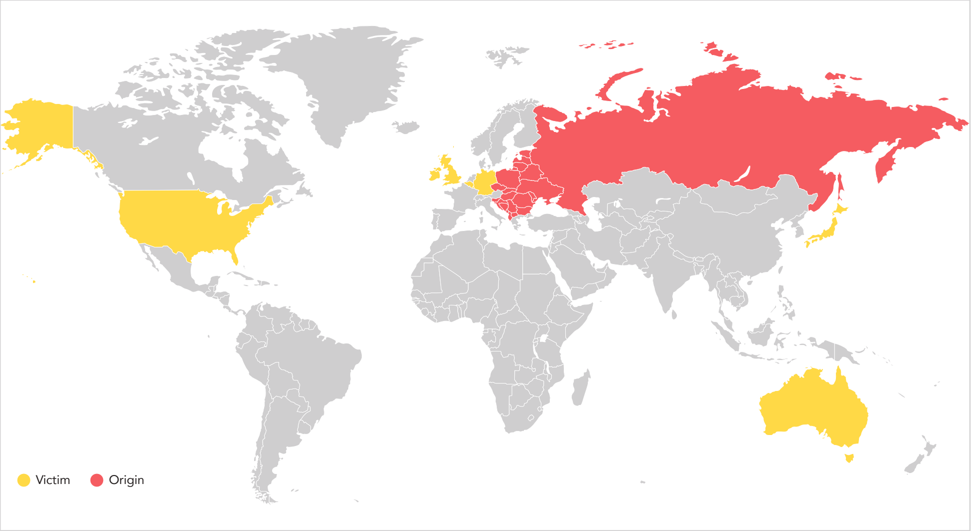


Patchwork (also known as Dropping Elephant) is a group of hackers from the Indian subcontinent first observed in December 2015. Although there are no strong indicators of their motivations, circumstantial evidence suggests that this group may have pro-Indian national interests.

During March and April 2018, several spear-phishing campaigns targeting US-based think tanks have been associated with Patchwork. Part of their methodology consists of deploying phishing campaigns with malware lures, including unique tracking links in their emails in order to identify which recipients opened the malicious messages. During three of their last spear phishing campaigns in 2018, Patchwork mimicked well-known American think tank organizations by using their themes and similar domain names. The group copied the style from publications of the Council on Foreign Relations, the Center of Strategic and International Studies, and the Mercator Institute for China Studies, applied it on their phishing emails and weaponized documents. Each one of those emails contained a link to a .doc file, which was a malicious Rich Text Format document attempting to exploit CVE-2017-8570 by using a publicly available exploit code. If the exploit worked successfully, they would try to execute an open source RAT named QuasarRat on the infected device. This malware has several useful functionalities to the attackers, such as key logging, file management, remote desktop access and reverse proxy.

This groups is trying to grow by acquiring techniques and habits from other important APT groups, such as tracking the effectiveness of their campaigns by recording which recipients have opened the message.

5.5. TA505



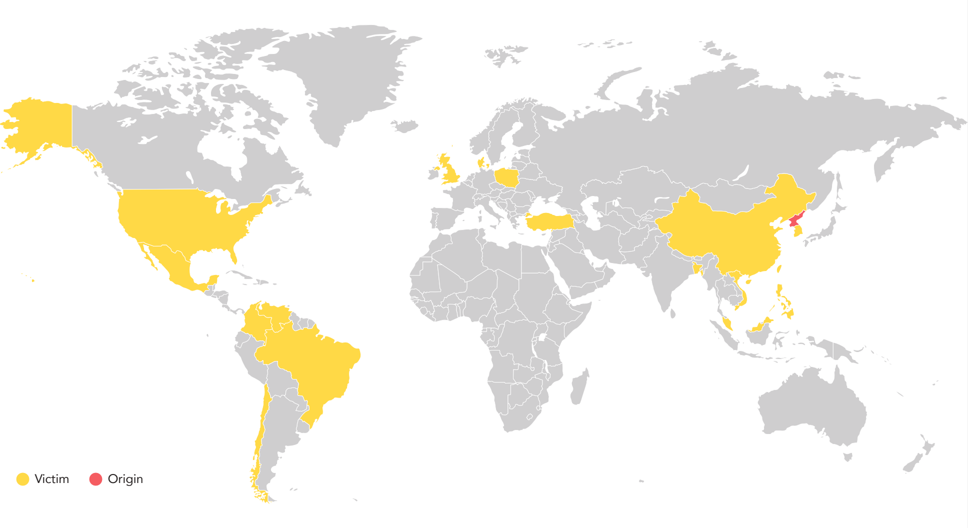
TA505 is one of the most prolific threat actors in recent years. The group has targeted several countries since they have been discovered, and seems to be driven purely by financial motives.

TA505 is one of the most prolific threat actors in recent years. The group has targeted several countries since they have been discovered, and seems to be driven purely by financial motives. They appear to be Eastern European since they have never targeted countries in the Commonwealth of Independent States (CIS), and they cease their activities during Russian Orthodox holidays. The group mainly provides a malware distribution service to other cybercriminal groups and individuals.

TA505 was discovered for the first time in 2014 during a campaign against the US, while they were distributing the Dridex banking Trojan using the Necurs botnet to send millions of spam messages with the malware attached. They repeated these attacks against several countries such as the UK, Germany and Australia without much variation until October 2015, when they started using the Shifu banking Trojan against Japanese and British targets (all while they still were launching Dridex campaigns). In 2016 they stopped using banking Trojans, and centered almost all their activities on the Locky ransomware. During this switch of tactics, techniques and procedures (TTPs) and at the beginning of 2017, the group experimented with several other ransomware variants in smaller campaigns such as Bart, Philadelphia and GlobeImposter. In October 2017, TA505 introduced their first geotargeted campaign, dropping either The Trickbot banking Trojan for victims that appeared to reside in the UK, Australia, Luxembourg, Ireland, and Belgium, or Locky if the target was located elsewhere. At the beginning of 2018 their activities were almost halted due to problems with the Necurs botnet but they rapidly changed their TTPs. When the botnet started to recover, they launched a handful of campaigns delivering the Remote Access Tool (RAT) FlawedAmmyy, last seen in June of this year. The last time they were observed was in August 2018 when TA505 sent millions of messages with the Marap malware downloader attached. Marap can be used to subsequently install malware in infected systems.

Their recent foray into large-scale distribution of RATs and intermediate loaders bears furthers the observation that as, unlike with Locky or GlobeImposter infections, victims may not realize they are infected until the group triggers additional malware installations or steals valuable data. The group's willingness to explore new vectors, payloads, sending infrastructure, and other malicious services – even when they do not have access to the Necurs spam cannon – exemplifies their adaptability, making them a threat actor to keep an eye on.

5.6. LAZARUS



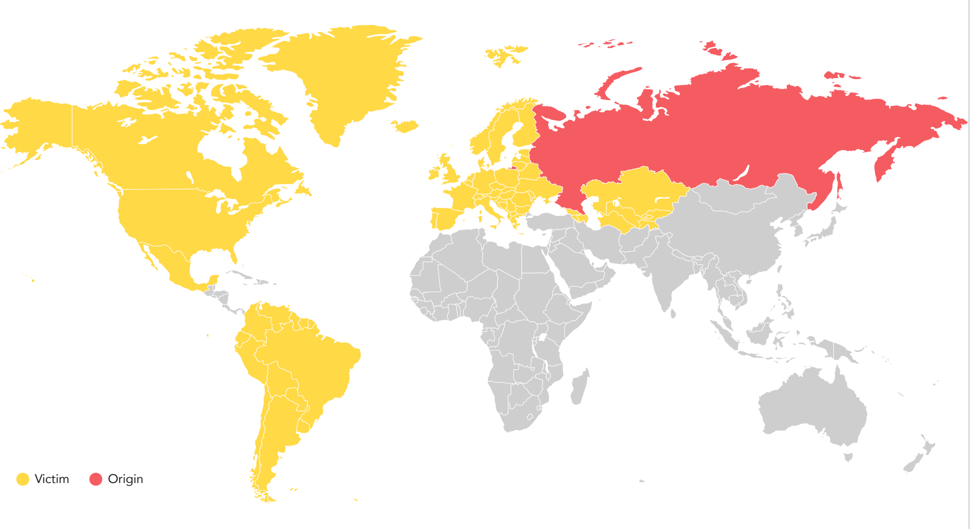
Lazarus Group's activity dates back to 2009, with some analysts suggesting they started as early as 2007. The group has performed some of the most notorious hacks in memory, including the 2014 attack on Sony Pictures Entertainment and the 2017 WannaCry ransomware attack. Some researchers have suggested that Lazarus Group is backed by the North Korean government.

Throughout 2018, Lazarus continued to target financial institutions via unauthorized SWIFT transfers. The results of this campaign were heists – both thwarted and successful – at financial institutions in Mexico and Chile. The group was also observed compromising financial institutions in Turkey in March 2018, though no losses are associated with that activity.

Interestingly, in late 2017 and throughout 2018, Lazarus Group began adding cryptocurrency exchanges to their lists of targets. Using the kind of adaptive creativity long-associated with Lazarus, the group compromised at least one of these exchanges via the use of a trojanized cryptocurrency trading application that pushed a malicious software update. This attack is also remarkable as it represents one of the first times that the Lazarus toolkit was expanded to target beyond Windows machines, in this case targeting MacOS.

Interestingly, in late 2017 and throughout 2018, Lazarus Group began adding cryptocurrency exchanges to their lists of targets.

5.7. FANCYBEAR



FancyBear (a.k.a APT 28, Softcay or Sedint) has been operating since the mid-2000s and is one of the most well-known Russian hacking groups around today. They had been pretty active during the last quarter of 2018, with some campaigns and new malwares being discovered.

5.7.1. LOJAX

LoJax is the first UEFI Rootkit that has been observed in the wild. It owes this name to the LoJack recovery tool, a legitimate software designed to be able to track a stolen computer even if a new OS is installed. The software is installed within the UEFI, the first program to run when a computer is started. The hackers modified a single bit of a version of LoJack for it to connect to their C&C instead of downloading the recovery tool. Then, malware can be easily installed and information can be easily gathered. It doesn't matter if the user restores the system or reinstalls the OS because the rootkit is located in the BIOS's memory and will be able to redownload everything. The only way to get rid of it is to reflash the affected BIOS memory.

5.7.2. DEAR JOOHN

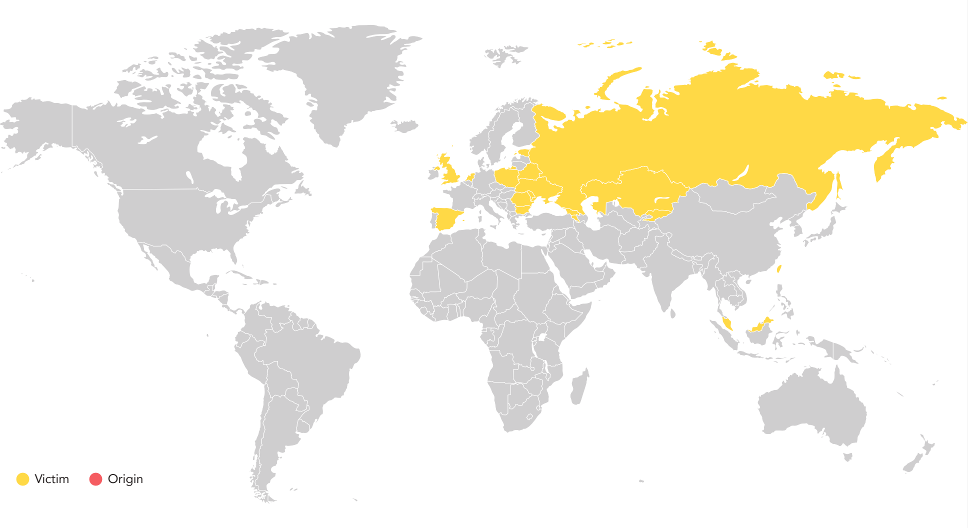
FancyBear launched two big parallel campaigns from mid-October to the beginning of December clustered under the name "Dear Joohn". Both campaigns consisted of a spearfishing attack targeting government organizations form North America, Europe and former USSR nations. They also targeted NGOs, marketing organizations and the medical industry. In the email they sent, the group attached files specifically named after recent events such as an airplane accident or the Brexit in order to attract the victim's attention. All the files were authored by Joohn, hence the campaigns' name. A malicious script that downloads a backdoor is found in a macro linked to a function executed when the file is closed. The difference between the campaigns is the payload they deliver.

Both campaigns consisted of a spearfishing attack targeting government organizations form North America, Europe and former USSR nations.

The first campaign delivers one of the most widely used backdoors by this group, Zebrocy. This is then used to gather information about the victim and install further malware. Something interesting about this backdoor is that it has been written in a wide variety of programming languages, and several versions of it were used in this campaign alone. The most recent was written in Go, a fairly new programming language developed by Google. It is thought that this variety is used to make detection more difficult.

The other campaign delivers a completely new malware, dubbed Cannon. Unlike Zebrocy, Cannon will communicate with its C&C server and receive orders via email and not through regular HTTP traffic. This technique is not new but it is difficult to detect since the hosts it communicates with are from legitimate mailing services.

5.8. COBALT GANG



Cobalt Gang first came onto the scene in 2016, when the group attacked First Commercial Bank in Taiwan and attempted to steal over $2 million. The group is believed to have roots in Eastern Europe.

Cobalt Gang has been observed sending spear-phishing emails to individuals at high-value institutions to distribute their malware. Once a system is compromised, the gang pivots to gain valuable access at the institutions. Using this access, Cobalt Gang carries out a variety of fraudulent money-making schemes.

In March 2018, Europol announced that one of the leaders of the Cobalt Gang (also, apparently, a leader of the Anunak Gang, to which Cobalt shares several ties) had been arrested. Despite the arrest, the Cobalt Gang continues to be active. In late 2018, for instance, the group was observed targeting financial institutions in a campaign that distributed a malware dubbed "SpicyOmlette." SpicyOmlette is likely used to establish a foothold in a victim's network in order to conduct reconnaissance.

Another well-known tool used by Cobalt Gang is Cobint. Cobint is a backdoor that communicates back to its C&C server and waits for instructions, involving different stages and creating different requests per target so the actors can identify the infected computers easily. So far, Cobalt has been detected using two modules, one that sends screenshots to the server and a second one that sends a list of running processes and names. Both modules seem to be created with reconnaissance purposes.

Researchers have noted the Cobalt Gang's ability increase attack sophistication and evolve to avoid detection.

Cobalt Gang first came onto the scene in 2016, when the group attacked First Commercial Bank in Taiwan and attempted to steal over $2 million.

In late 2018. the group was observed targeting financial institutions in a campaign that distributed a malware dubbed "SpicyOmlette." SpicyOmlette is likely used to establish a foothold in a victim's network in order to conduct reconnaissance.

6.LEGISLATION HIGHLIGHTS AND BUSINESS IMPACT

6.1.GDPR VIOLATIONS

Since GDPR fines are so stiff, Twitter, whose revenue totalled $2.4 billion in 2018, could be fined up to $96 million.

Since the General Data Protection Regulation (GDPR) came into effect on May 25th 2018, several important companies have been fined for violating the new customer data management and permissions policies. Facebook and Google each faced lawsuits of €3.9 billion and €3.7 billion, respectively. This wasn't because the companies exposed or misused sensitive data, rather, it's because both companies forced their clients to choose between using the product and having their personal data collected, not using the product at all. Under the GDPR, companies are allowed to process any kind of customer data, as long as it is strictly necessary for the service. However this data cannot be used without explicit consent.

Several European countries complain about Google and Facebook

Data breaches have continued into the GDPR era, and cybercriminals are now trying to strike harder and mention the regulation in their extortion techniques.

WhatsApp, owned by Facebook, also faced some issues under the GDPR. In order to improve its service, Whatsapp sends every single address book entry from users' smartphone to its servers, located in the United States. This practice is no longer allowed, because data from users who never intended to use the messenger app can now be found in these servers.

Accidents can lead to GDPR infringements as well, as what happened to Ghostery, an ad-blocking tool. The company accidentally leaked hundreds of users email addresses in one of its regular newsletter emails.

6.1.1.SEVERAL EUROPEAN COUNTRIES COMPLAIN ABOUT GOOGLE

In December 2018, Google received complaints from seven European countries due to the way it manages and tracks user location data. Constant location tracking is considered very sensitive information, as it can be used to obtain intel such political interests, health conditions, sexual orientation or even religious beliefs. Google uses several practices to ensure that their users have location tracking services enabled, and keeps these techniques for the most part on the down low. As mentioned above, the consent Google's users provide is not done so freely, given they must accept Google's conditions in order to use its product.

Companies found violating GDPR could be fined up to 4 percent of their total yearly revenue, or up to €20 million, whichever amount is greater. In turn, European countries are taking the GDPR seriously, when it comes to both large scale companies and SMBs alike. However cases in which high profile companies violate their customers' privacy policies still arise, which demonstrates companies themselves might not become aware of how important GDPR policies are until they actually receive a successful complaint against them.

6.1.2.CENTRO HOSPITALAR BARREIRO MONTIJO

In April 2018, a union called Sindicato dos Médicos da Zona Sul communicated that non-medical personnel from Portuguese hospital Centro Hospitalar Barreiro Montijo (CHBM) were able to access to clinical sensitive data through fake profiles on the CHBM's computer system. Subsequently audits, performed by the Comissao

Nacional de Protecçao de Dados (CNPD), reported that 985 users were registered on the system as 'physicians' with access to patient's private data, but just 296 real physicians were working on the hospital. Furthermore, the auditors found that users under the 'technical' profile also had access to sensitive information.

Two fines had been issued after the CNPD concluded their investigation. The first one came to the sum of €300,000 for violating patients' confidentiality by exposing their data to unauthorized personnel. The second one, for failing to "ensure the confidentiality, integrity, availability and permanent resilience of treatment systems and services", totaled €100,000.

6.1.3. AUSTRIA'S FIRST GDPR ISSUE

Four months after the GDPR came into force the Austrian Data Protection Authority (DSB) issued its first fine, against an entrepreneur for€4,800. The entrepreneur had a CCTV camera recording the sidewalk in front of his establishment. This kind of monitoring is considered a violation of the GDPR, since the large-scale monitoring of public spaces is not permitted as it infringes on the pedestrian's privacy. . Additionally, the camera was not marked transparently enough as a surveillance device, which it should have been.

6.1.4. THE TWITTER INVESTIGATION

The Irish Data Protection Commission has started investigating Twitter after its refusal to give details about how it tracks the way users click on links in tweets. Twitter controls the links pasted on their platform by applying its own link-shortening service, called t.co. Twitter claims that t.co is just a system to measure a link's popularity and restrict the spread of malware through its platform. But some specialists suspect it may also be used to track the users' activities and browsing data from their cookies.

The GDPR policies gives customers the right to retrieve and inspect all the personal data that it is being collected from them, but Twitter rejects that kind of requests because of the disproportionate effort it would take to gather it. Researchers also suspect Twitter is recording and monitoring user agents and estimating user location and IP.

The way GDPR handles Twitter's current structure has yet to be settled, but we expect this structure will be adopted by more companies in the following months. Since GDPR fines are so stiff, Twitter, whose revenue totalled $2.4 billion in 2018, could be fined up to $96 million.

Protecting user privacy and respecting their data rights is now a critical task for organizations operating within the European Union and beyond, as companies not following GDPR will inevitably face the penalties. At the same time, ransomware and cryptominers continue to threaten both for individuals and companies. During this quarter new malware targeting routers and mobile operating systems especially made a great impact. Data breaches have continued into the GDPR era, and cybercriminals are now trying to strike harder and mention the regulation in their extortion techniques. To find more specific guidance on how organizations can handle GDPR, read our white paper here.

7.CASE-STUDY: LATIN AMERICA – A NEW TESTING GROUND

Latin America has transformed into an increasingly sophisticated area in recent years, with both internet and mobile internet penetration expanding across the region. Financial technology, or FinTech, offerings are on the rise, revolutionizing the economy with new and accessible ways for people access, move and invest money. People in Latin America are now more likely to own bank accounts – and therefore payments cards that facilitate online transactions – while some FinTech companies are working to fill in the gaps for those that are still unbanked.

Only two Latin American countries (Uruguay and Colombia) ranked above a 3/5 for societal security awareness.

With this growth comes an expanding target population for cybercriminals bent on defrauding residents. Security awareness is low: a 2016 joint report by the Inter-American Development Bank and Organization of American States found that only two Latin American countries (Uruguay and Colombia) ranked above a 3/5 for societal security awareness.[7] This level of security awareness leaves the population vulnerable to simple and unsophisticated cybercrime schemes. This problem is further compounded by weak or nonexistent cybercrime legislation in many Latin American countries, thereby doing little to deter illicit activity.

The same technology that is bringing people together is likewise uniting cybercriminals, who seek partners on underground forums, advertise compromised databases on Facebook groups, and share YouTube tutorials demonstrating how to defraud retailers.

This section contains in-depth situational intelligence to help decision-makers best protect their enterprises regionally, aligning it to their strategic business priorities and making long term calculations about how organizations might be affected by their digital and real-world environments.

7.1.REGIONAL FRAUD SCHEMES

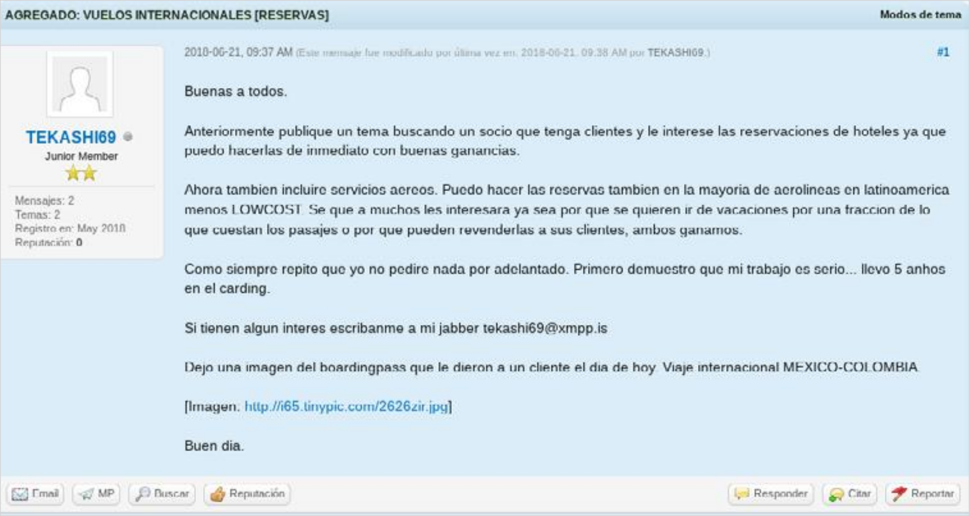
7.1.1.TRAVEL SECTOR

Sharing a common language more or less across the whole of Latin America makes the region unique in the way that cybercriminal ideas can spread quickly from one country to the next.

7.1.1.1.Rewards Points Theft

Illicit 'travel agencies' offering to fraudulently book flights, hotels, cruises, car rentals, tours, and other tourism-related activities are commonplace in the cybercriminal underground. Threat actors offering these services allow their clients the opportunity to plan trips for a fraction of the actual cost; typically these vendors charge clients between 30% and 50% of the actual cost of the trip.

Our analysts have observed these services advertised on English-language marketplaces as well as Spanish, Russian, and French-language cybercriminal forums. The presence of this type of fraud across linguistic communities is striking, highlighting the appeal of these types of offerings. Furthermore, it demonstrates that illicit travel services represent a sort of Goldilocks situation in the world of fraud: not too complicated as to be inaccessible to less-sophisticated threat actors, but complex enough that most threat actors cannot obtain these services on their own.



AGREGADO: VUELOS INTERNACIONALES [RESERVAS]

TEKASHI69

Mensajes: 2
Temas: 2
Registro en: May 2018
Reputación: 0

2018-06-21, 09:37 AM (Este mensaje fue modificado por última vez en: 2018-06-21, 09:38 AM por TEKASHI69.)

Buenas a todos.

Anteriormente publique un tema buscando un socio que tenga clientes y le interese las reservaciones de hoteles ya que puedo hacerlas de inmediato con buenas ganancias.

Ahora tambien incluire servicios aereos. Puedo hacer las reservas tambien en la mayoria de aerolineas en latinoamerica menos LOWCOST. Se que a muchos les interesara ya sea por que se quieren ir de vacaciones por una fraccion de lo que cuestan los pasajes o por que pueden revenderlas a sus clientes, ambos ganamos.

Como siempre repito que yo no pedire nada por adelantado. Primero demuestro que mi trabajo es serio... llevo 5 anhos en el carding.

Si tienen algun interes escribanme a mi jabber tekashi69@xmpp.is

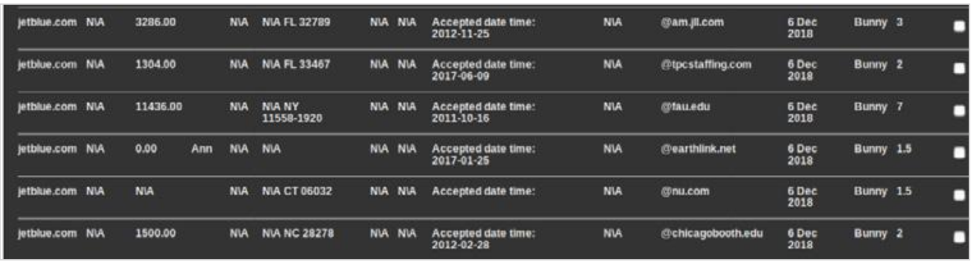
Dejo una imagen del boardingpass que le dieron a un cliente el dia de hoy. Viaje internacional MEXICO-COLOMBIA

[Imagen: http://i65.tinypic.com/2626zir.jpg]

Buen dia.

Figure 3: The threat actor operating under the alias "TEKASHI69" on Cebolla Chan 3.0 seeks a partner with "clients" that may be interested in their hotel and flight booking services.

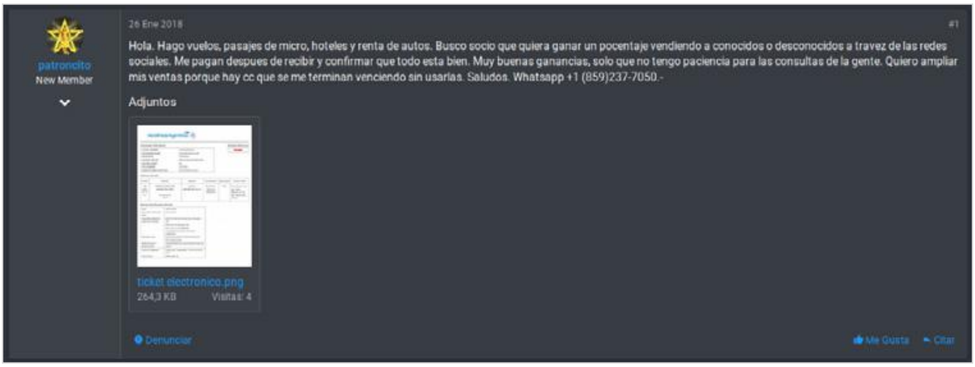
Our analysts think that the majority of the vendors offering these travel services are using compromised rewards points. These rewards points may come from accounts directly related to travel services – such as frequent flyer miles or hotel rewards points accounts – or from other accounts that include travel rewards points as a bonus, such as a bank account with a credit card that earns miles.



jetblue.com	N\A	3286.00		N\A	N\A FL 32789	N\A	N\A	Accepted date time: 2012-11-25	N\A	@am.jll.com	6 Dec 2018	Bunny	3	☐
jetblue.com	N\A	1304.00		N\A	N\A FL 33467	N\A	N\A	Accepted date time: 2017-06-09	N\A	@tpcstaffing.com	6 Dec 2018	Bunny	2	☐
jetblue.com	N\A	11436.00		N\A	N\A NY 11558-1920	N\A	N\A	Accepted date time: 2011-10-16	N\A	@fau.edu	6 Dec 2018	Bunny	7	☐
jetblue.com	N\A	0.00	Ann	N\A	N\A	N\A	N\A	Accepted date time: 2017-01-25	N\A	@earthlink.net	6 Dec 2018	Bunny	1.5	☐
jetblue.com	N\A	N\A		N\A	N\A CT 06032	N\A	N\A	Accepted date time:	N\A	@nu.com	6 Dec 2018	Bunny	1.5	☐
jetblue.com	N\A	1500.00		N\A	N\A NC 28278	N\A	N\A	Accepted date time: 2012-02-28	N\A	@chicagobooth.edu	6 Dec 2018	Bunny	2	☐

Figure 4: JetBlue accounts for sale on an underground account shop display the number of rewards points (third column) associated with the compromised account.

While most threat actors are likely using compromised rewards points, our analysts assess that several vendors might be using compromised payment card information in order to make these purchases.



patroncito
New Member

26 Ene 2018 #1

Hola. Hago vuelos, pasajes de micro, hoteles y renta de autos. Busco socio que quiera ganar un pocentaje vendiendo a conocidos o desconocidos a travez de las redes sociales. Me pagan despues de recibir y confirmar que todo esta bien. Muy buenas ganancias, solo que no tengo paciencia para las consultas de la gente. Quiero ampliar mis ventas porque hay cc que se me terminan venciendo sin usarlas. Saludos. Whatsapp +1 (859)237-7050.-

Adjuntos

ticket electronico.png
264,3 KB Visitas: 4

Figure 5: The threat actor "patroncito" on Carding21 offers clients the ability to book flights, bus tickets, hotels, and car rentals. patroncito includes an example of plane ticket purchase information as evidence of their abilities; the ticket appears to have been purchased with a payment card and not with airline miles

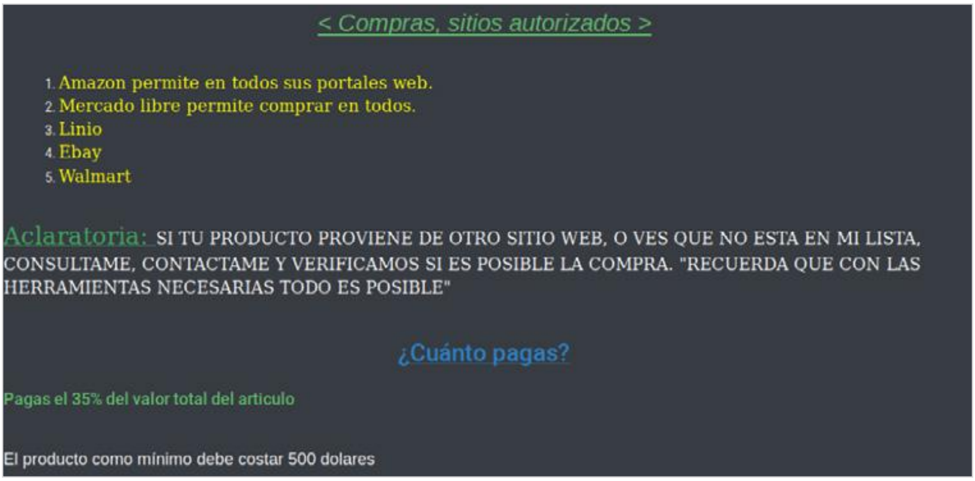
Many travel entities, especially those active in Latin America, do not appear to have the know-how or the resources to effectively combat this type of fraud. As long as this fraud is relatively easy to conduct, profitable, and without serious consequences, threat actors are likely to continue to offer these services. Our analysts envision that this form of fraud will likely continue to proliferate in the cybercriminal underground.

7.1.2. RETAIL SECTOR

7.1.2.1. Compras

Obtaining carded purchases online – a fraud scheme known simply as "compras" in Spanish – is a common topic of interest across various Spanish-language underground communities. The scheme attracts the interest of both novice cybercriminals looking to fraudulently obtain products as well as veteran cybercriminals that have turned obtaining compras on behalf of paying clients into a business model.

Compras are attractive to fraudsters due in part to the low barrier to entry into this type of fraud ecosystem.



< Compras, sitios autorizados >

1. Amazon permite en todos sus portales web.
2. Mercado libre permite comprar en todos.
3. Linio
4. Ebay
5. Walmart

Aclaratoria: SI TU PRODUCTO PROVIENE DE OTRO SITIO WEB, O VES QUE NO ESTA EN MI LISTA, CONSULTAME, CONTACTAME Y VERIFICAMOS SI ES POSIBLE LA COMPRA. "RECUERDA QUE CON LAS HERRAMIENTAS NECESARIAS TODO ES POSIBLE"

¿Cuánto pagas?

Pagas el 35% del valor total del articulo

El producto como mínimo debe costar 500 dolares

Figure 6: The compras vendor "John Lennon," active on the Spanish-language carding forum Carding21, describes their service. John Lennon lists prices in Mexican pesos.[8]

Compras are typically technology purchases, though clothing items are another frequent target. These goods are often obtained from e-commerce sites such as

MercadoLibre and Amazon, though online retailers are also popular targets. Many compras 'vendors' – those offering to secure carded purchases on behalf of paying clients – will only conduct the purchase if the good is more than several hundred dollars, typically charging clients about 30% of the value of the carded product.

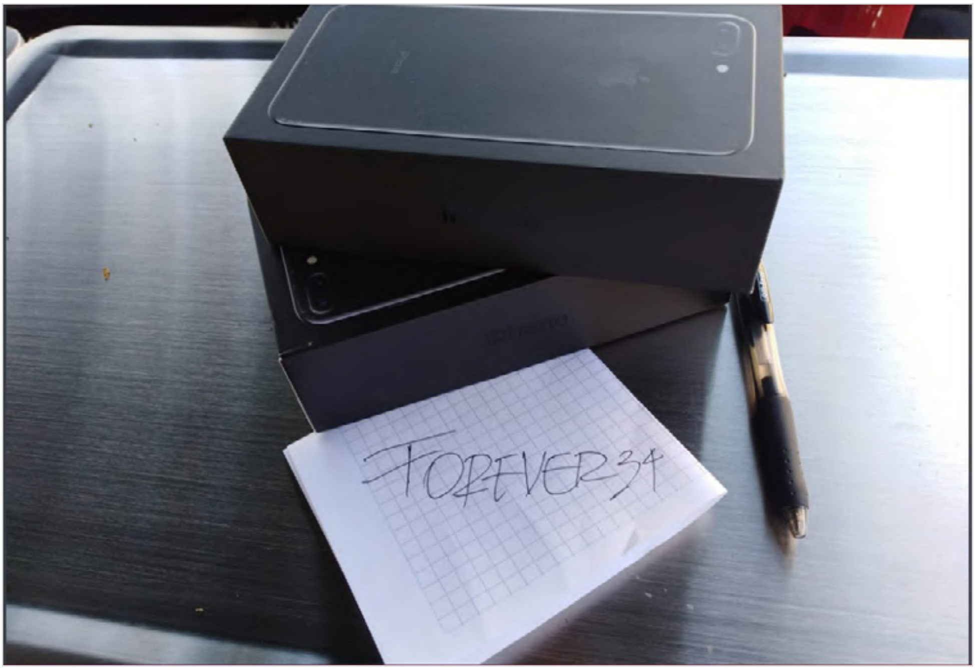


Figure 7: A satisfied customer of John Lennon operating under the alias "FOREVER34" posts a photo to Carding21 vouching for John Lennon's services.

Several prolific carders on the Spanish-language underground have published comprehensive guides on how to conduct compras fraud. In one such guide, authored by the admin of the Spanish-language darknet carding forum "Darkside," includes the following instructions (translated from the original Spanish):[9]

> *Before you make a [fraudulent] purchase, it's important to link the [compromised] card to the account [you have just created] and wait 24 hours. After 24 hours, if the account has not been blocked or anything, we can then conduct the [fraudulent] purchase.*
>
> *If the card is reported as missing or is canceled, the worst that can happen is they will cancel the purchase and we'll [now] know for a fact that that card is not useful to us.*

Many of the cybercriminal guides to compras, such as Darkside's, indicate that the fraudster should use compromised payment card information and newly created accounts. Our analysts believe that there is a realistic possibility that compromised retail accounts may be used for this type of fraud as well, though to a much lesser extent.

Compromised payment cards can be found easily on underground forums or cardshops. Because the purchases are made online, the costs and hassle associated with creating duplicate physical cards is avoided. Statements made by cybercriminals about compras suggest that many retailers operating in Latin America do a poor job at tracking and preventing compras fraud. For instance, many compras guides and vendors state that it is safe to ship multiple carded purchases directly to the fraudster's home address, underscoring a failure on the part of retailers and e-commerce sites to track and flag fraud.

Many retailers operating in Latin America do a poor job at tracking and preventing compras fraud.

Our analysts assess that it is highly likely that both new and old cybercriminals will likely continue to be attracted to committing this type of fraud.

7.1.2.2.Refund Fraud

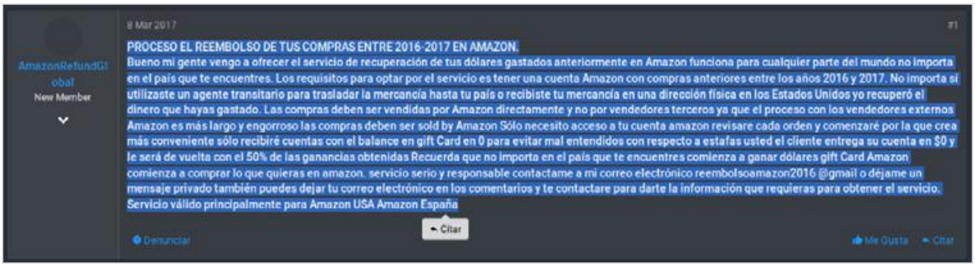
Fraudsters have developed an interest in conducting scams that involve obtaining refunds from major retailers under false pretenses. One renowned member of the English-language forum MPGH (MultiPlayer Game Hacking) – where refund fraud is regularly discussed and vendors offering to secure refunds on behalf of illicit clients are incredibly commonplace – described refund fraud in the following terms:[10]

As North American and European companies become increasingly difficult to defraud, our analysts consider that refund fraud might become more commonplace in the Latin American underground.

> A refund service is a service in which the cost of the item(s) you purchased are refunded to you, as if you never bought the items at all, while being able to keep the items. The typical process you want to follow for pursuing this that I recommend is as follows:
>
> - Contact a refunder [refund vendor] and ask if the item you want to refund is possible (if not specifically outlined in their thread).
> - Purchase and order the item
> - Wait until the item is delivered
> - Contact the refunder to complete the refund, providing the necessary information which differs site to site.
>
> Now, the risks are obvious. Refunding an item is fraud in and of itself however the reason that refunding is possible is because it's plausible. All of the reasons and methods refunders use are public here on MPGH but not everyone is well equipped to talk to the representatives on the phone and actually social engineer them to get the refund done in a safe and elegant way.

Unlike compras fraud, refund fraud does not use compromised payment card information but rather relies on social engineering techniques to secure the refund. Refund fraud vendors endeavor to make customer service representatives believe that there has been an issue in the shipment or delivery of the purchase. Common fabrications used by refund vendors hoping to secure a refund is that the package never arrived, the package was stolen, the package was empty, or that the items within the package were somehow sullied.

Vendors of refund fraud services can be found in a variety of underground cybercriminal communities, including in the English and Russian-language cybercriminal space. Refund fraud is found to a lesser extent in the Spanish-language underground.



PROCESO EL REEMBOLSO DE TUS COMPRAS ENTRE 2016-2017 EN AMAZON.
Bueno mi gente vengo a ofrecer el servicio de recuperación de tus dólares gastados anteriormente en Amazon funciona para cualquier parte del mundo no importa en el país que te encuentres. Los requisitos para optar por el servicio es tener una cuenta Amazon con compras anteriores entre los años 2016 y 2017. No importa si utilizaste un agente transitario para trasladar la mercancía hasta tu país o recibiste tu mercancía en una dirección física en los Estados Unidos yo recuperó el dinero que hayas gastado. Las compras deben ser vendidas por Amazon directamente y no por vendedores terceros ya que el proceso con los vendedores externos Amazon es más largo y engorroso las compras deben ser sold by Amazon Sólo necesito acceso a tu cuenta amazon revisare cada orden y comenzaré por la que crea más conveniente sólo recibiré cuentas con el balance en gift Card en 0 para evitar mal entendidos con respecto a estafas usted el cliente entrega su cuenta en $0 y le será de vuelta con el 50% de las ganancias obtenidas Recuerda que no importa en el país que te encuentres comienza a ganar dólares gift Card Amazon comienza a comprar lo que quieras en amazon. servicio serio y responsable contactame a mi correo electrónico reembolsoamazon2016 @gmail o déjame un mensaje privado también puedes dejar tu correo electrónico en los comentarios y te contactare para darte la información que requieras para obtener el servicio.
Servicio válido principalmente para Amazon USA Amazon España

Figure 8: The threat actor operating under the alias "AmazonRefundGlobal" offers their services in securing Amazon refunds on Carding21. AmazonRefundGlobal indicates that they are capable of securing fraudulent refunds from Amazon anywhere in the world.[11]

Many refund fraud vendors currently target US companies (and to a lesser extent European and Canadian companies) due to the desirability of these products, as well as the huge potential client bases available in those regions. Shipping agreements and standardized regulations across borders in these regions – such as within the European Union or between the US and Canada – also make shipping a lesser concern; oftentimes, Latin American cybercriminals must employ reshipping services to move goods across borders, which adds an additional complication. Many retailers in North America and Europe, however, are starting to crack down seriously on refund fraud, implementing mitigation measures such as requiring signatures upon delivery or weighing packages through transit.

e-commerce will become increasingly prevalent in Latin America as internet penetration increases along with the banked population.

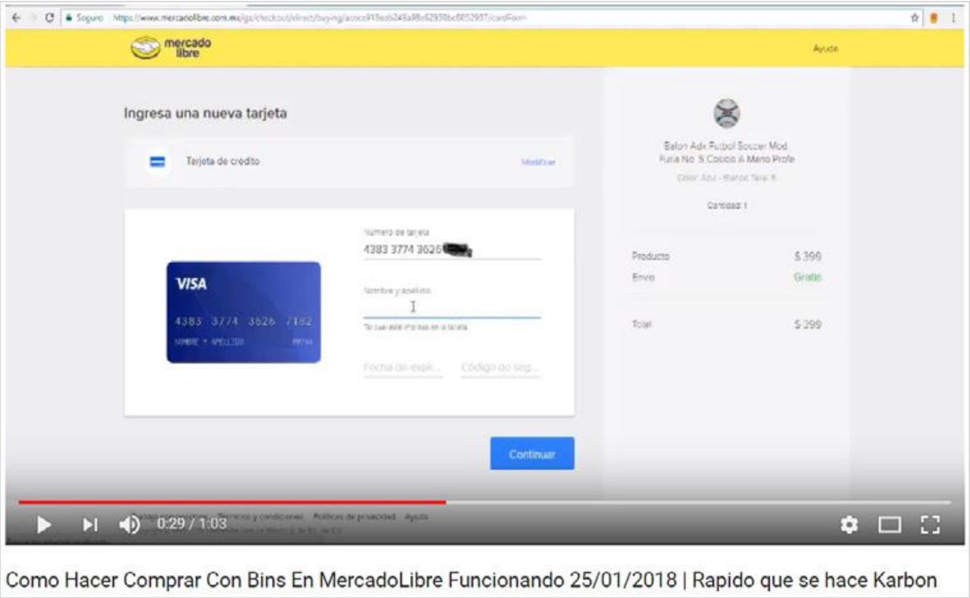
As North American and European companies become increasingly difficult to defraud, our analysts consider that refund fraud might become more commonplace in the Latin American underground. English-speaking refund fraud vendors may decide to sell or share their old methods that no longer work to cybercriminals in other linguistic communities. Similarly, experienced refund fraud vendors with knowledge of Spanish or Portuguese may move to capitalize on these markets.

Furthermore, e-commerce will become increasingly prevalent in Latin America as internet penetration increases along with the banked population. As more individuals use e-commerce platforms, fraudsters will continue to test how they can abuse them for personal gain.

7.1.2.3.Binero Fraud

'Binero' fraud is a peculiar and prevalent type of fraud discussed in the Latin American underground. Those interested in binero fraud endeavor to discover specific bank identification numbers (BINs) that are improperly validated by online payment processors. Once an improperly validated BIN and website combination has been discovered, the fraudster will fabricate the rest of the information necessary for making an online purchase – such as the remaining 10 digits of the card number and expiration date – and then conduct the 'purchase' using this invented card.

Fraudsters discuss binero fraud and swap vulnerable BINs and website combos in various spaces, including underground forums, crime-themed Telegram groups, and even on YouTube. The majority of this activity takes places in the Spanish-language underground, though discussions of binero fraud can likewise be found in the Portuguese-language underground.



Ingresa una nueva tarjeta

Tarjeta de credito

Numero de tarjeta: 4383 3774 3026[redacted]

Productos $ 399

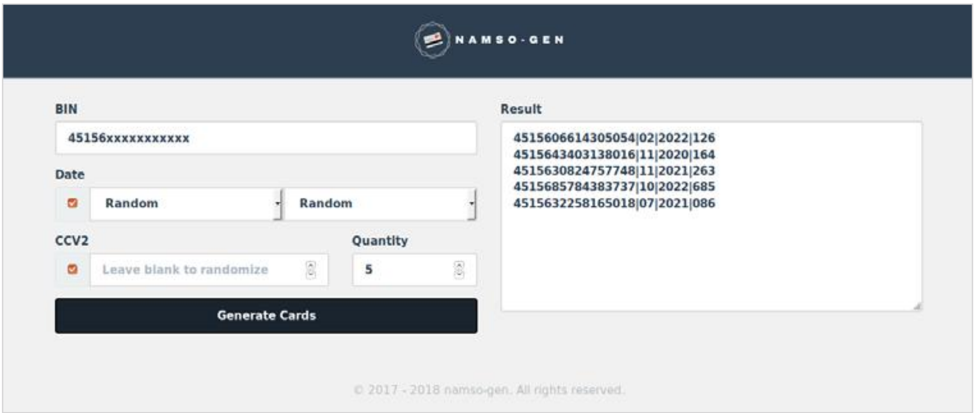
Envío Gratis

Total $ 399

Como Hacer Comprar Con Bins En MercadoLibre Funcionando 25/01/2018 | Rapido que se hace Karbon

Figure 9: A YouTuber shares a video showing a purchase being made on MercadoLibre Mexico using a fabricated card number using a BIN pattern to conduct a purchase. This video was uploaded January 25, 2018.

Our analysts assess that it is likely that fraudsters identify websites that improperly validate BINs through manual trial and error. Upon discovering a BIN (or card "pattern" as seen above), fraudsters typically rely on card generators to fill in the rest of the information in a realistic way. Card generators typically supply the user with realistic sixteen-digit card numbers, expiration dates, and CVV codes.



BIN: 45156xxxxxxxxxx

Date: ☑ Random | Random

CCV2: ☑ Leave blank to randomize

Quantity: 5

Result:

```
4515606614305054|02|2022|126
4515643403138016|11|2020|164
4515630824757748|11|2021|263
4515685784383737|10|2022|685
4515632258165018|07|2021|086
```

Figure 10: Namso generator produces results for the BIN 45156. Namso and other card number generators are typically free to use.

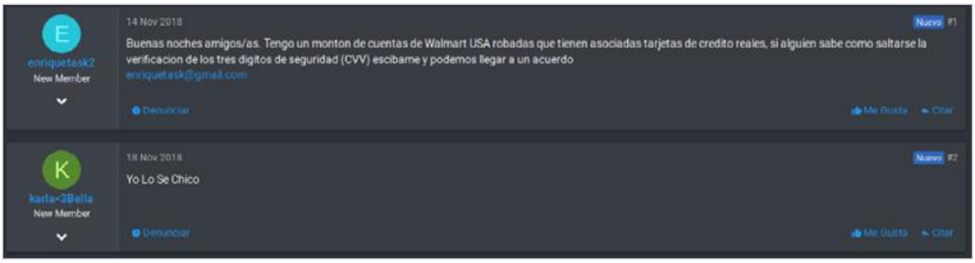
Individuals interested in binero fraud often share vulnerable BINs and website combos (as the vulnerable BIN is specific to a vulnerable website) freely, illustrating a lack of concern about burning methods, as well as the importance of reputation in this community.

Many cybercriminals interested in binero fraud utilize binero techniques to defraud online streaming services, such as Netflix of Spotify, and to a lesser extent e-commerce sites and online retailers.

Binero fraud has also gained the interest ofLatin American cybercriminals, with Spanish-language forums often hosting binero-specific subforums or regularly seeing individuals sharing binero fraud guides. For that reason, our analysts assess that binero fraud will likely continue to be of great interest to cybercriminals in the region.

7.1.2.4. Additional Retail intelligence

While defrauding retailers is of interest to cybercriminals in Latin America, our analysts did not identify a strong interest in obtaining compromised retail accounts by Latin American cybercriminals. Retail-related checkers and bruteforcers are uncommon in Spanish and Portuguese-language undergrounds, and when they are offered they are typically English or Russian-language tools. Similarly, account shops are typically English-language and rarely, if ever, include compromised accounts from Latin American retailers. That said, our analysts did identify a handful of threat actors interested in compromised retail accounts.



14 Nov 2018

Buenas noches amigos/as. Tengo un monton de cuentas de Walmart USA robadas que tienen asociadas tarjetas de credito reales, si alguien sabe como saltarse la verificacion de los tres digitos de seguridad (CVV) escibame y podemos llegar a un acuerdo
enriquetask@gmail.com

18 Nov 2018

Yo Lo Se Chico

Figure 11: The threat actor operating under the alias "enriquetask2" seeks help using compromised Walmart accounts on Carding21.[12]

Our analysts did not identify discussions of large-scale gift card of prepaid card fraud in the Latin American underground. In other underground communities, gift cards and prepaid cards are often a popular method of cashing out compromised assets. The dearth of information about this type of fraud in the cybercriminal underground may indicate either that this type of fraud is not popular, or perhaps is organized and conducted off of underground forums.

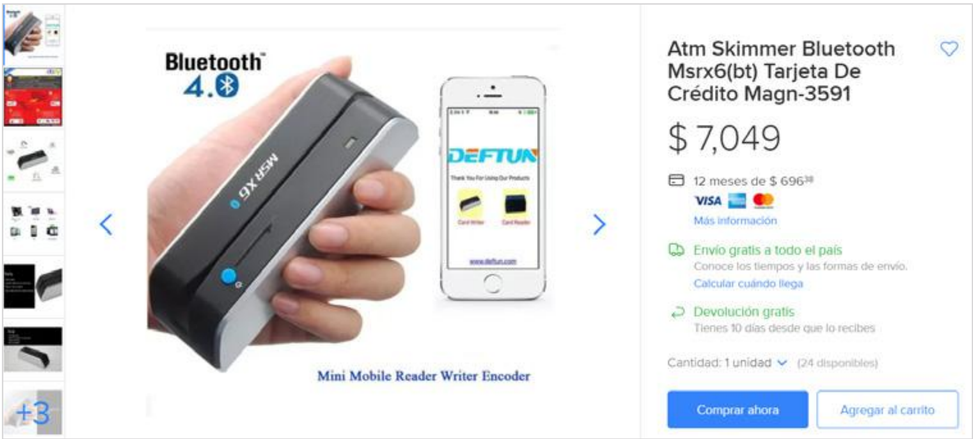
7.1.3. SKIMMING

Many Latin American financial institutions have been slow to adopt EMV security measures for payment cards, leaving the region particularly vulnerable to skimming. Skimming is when threat actors use devices, called "skimmers," to read, record, and thereby steal the track data encoded on the payment card's magnetic stripe.

Many Latin American financial institutions have been slow to adopt EMV security measures for payment cards.

Oftentimes fraudsters will insert skimmers into point-of-sale (POS) devices or ATMs in order to surreptitiously gather information from payment cards. Fraudsters working in the service industry who regularly come in contact with high-value cards (see "Insider Threats") may elect to use pocket-sized skimmers to collect data manually from clients.

Low barriers to entry into the world of skimming is one of the major draws of this type of fraud. At its most basic level, skimming requires little specialized knowledge, while skimmers can be easily found for sale online. Both legitimate e-commerce sites, such as MercadoLibre in Latin America, as well as deep and dark web forums and marketplaces carry and sell skimming devices.



Atm Skimmer Bluetooth Msrx6(bt) Tarjeta De Crédito Magn-3591

$ 7,049

12 meses de $ 696³⁸

Más información

Envío gratis a todo el país

Conoce los tiempos y las formas de envío.

Calcular cuándo llega

Devolución gratis

Tienes 10 días desde que lo recibes

Cantidad: 1 unidad (24 disponibles)

Figure 12: A skimmer for sale on MercadoLibre Mexico. There are legitimate businesses uses for skimmers, though cybercriminals can easily obtain these products and misuse them.

Fraudsters working in the service industry who regularly come in contact with high-value cards may elect to use pocket-sized skimmers to collect data manually from clients.

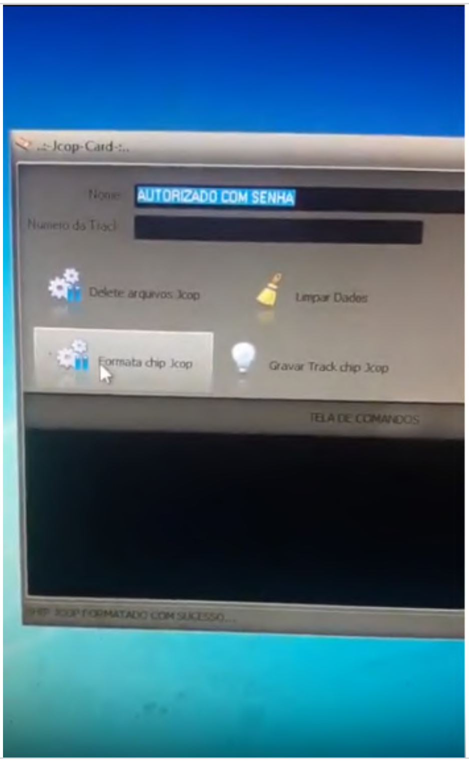
While purchasing skimmers from e-commerce sites is perhaps the most convenient option, OPSEC-minded cybercriminals may be more inclined to purchase these devices from dark web sources in order to better protect their privacy and mask their illicit activities from law enforcement. Dark web vendors may also offer skimmers in bundles, which include products such as card-writing software or instruction manuals on how to conduct payment card fraud.

Skimming packs a punch in the region at large, resulting in fraud and losses that impact consumers, retailers, and financial institutions. According to a January 2018 report released by the Mexican National Commission for the Protection and Defense of Financial Service Users (Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros; CONDUSEF), the country saw over 1.6 million fraud claims in relation to card compromise at POS devices from the period of January – September 2017.[13] Skimming accounted for the vast majority of those cases.

.the country saw over 1.6 million fraud claims in relation to card compromise at POS devices from the period of January – September 2017.

7.1.3.1.EMV Skimming

EMV security protections have been rolled out around the globe in an attempt to stem the tide of massive breaches of track data resulting from POS malware compromise. Unlike magnetic stripe data, which remains the same until the card's expiration and has few additional security protections, payment card information used in an EMV transaction is authenticated using encryption standards. Many EMV chip cards use static data authentication (SDA), wherein the card's encryption key signs static application data. This application data, as the name suggests, remains the same for the life of the card. Cards employing dynamic data authentication (DDA), however, sign dynamic application data with their card-specific encryption key, meaning each transaction is uniquely authenticated. This makes it extraordinarily difficult for cybercriminals to successfully steal and utilize compromised DDA information. The fixed nature of the authentication of SDA cards render these cards less secure than their DDA counterparts and opens them up to the possibility of replay attacks.[14]



.:-Jcop-Card-:.

Nome: AUTORIZADO COM SENHA

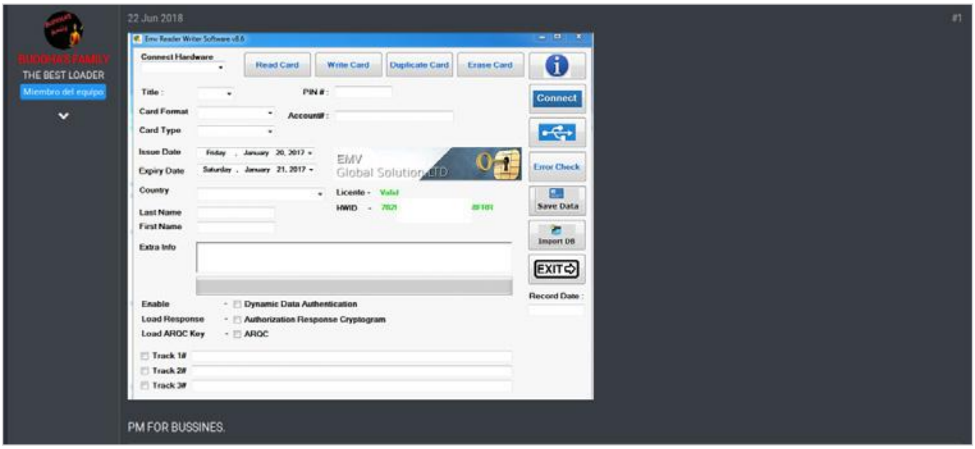
Numero da Track:

CHIP JCOP FORMATADO COM SUCESSO...

Figure 13: posts a Portuguese-language video on YouTube that appears to show the individual writing EMV chip data to a JCOP chip card.

Brazilians fraudsters in particular have proved adept at developing so-called 'EMV skimmers' and accompanying writing software.

Though Brazilian threat actors have proved themselves particularly skilled in this arena, Spanish-speaking cybercriminals also experiment with EMV skimming and chip-writing technology. Often Spanish-speakers utilize Brazilian or Russian technology in order to accomplish these objectives. A multitude of unverified EMV skimming and writing software exists on cybercriminal forums and marketplaces.



BUDDHA'S FAMILY
THE BEST LOADER
Miembro del equipo

22 Jun 2018 #1

Emv Reader Writer Software v8.6

Title :

PIN # :

Card Format

Account# :

Card Type

Issue Date Friday , January 20, 2017

Expiry Date Saturday , January 21, 2017

Country

Licente - Valid

HWID - 7821 8F101

Last Name

First Name

Extra Info

Enable - □ Dynamic Data Authentication

Load Response - □ Authorization Response Cryptogram

Load ARQC Key - □ ARQC

□ Track 1#

□ Track 2#

□ Track 3#

Record Date :

PM FOR BUSSINES.

Figure 21: "BUDDHA'S FAMILY," a member of the administration team of the Spanish-language carding forum Carding21, offers "EMV reader writer software" for sale. BUDDHA'S FAMILY did not develop this program themselves. Despite the checkbox for "Dynamic Data Authentication," analysts have yet to observe successful targeting of DDA cards.

7.2. PHISHING

Phishing remains a major problem across all sectors and regions. Though the attacker profiling performing many phishing attacks is usually less sophisticated than counterparts using malware or performing major fraud, it is still a persistent threat which all organizations should remain aware of.

In April 2017 over 50,000 Brazilians were impacted by a phishing message disseminated via WhatsApp in a period of just five days.

Phishing-related conversations and offerings are incredibly prevalent across the Latin American cybercriminals underground, specifically within Portuguese-speaking communities. Phishing can prove to be a lucrative enterprise for cybercriminal actors; low security awareness in Latin America leaves many people susceptible to even the most low-sophistication attacks. To illustrate this point, in April 2017 over 50,000 Brazilians were impacted by a phishing message disseminated via WhatsApp in a period of just five days.[15]

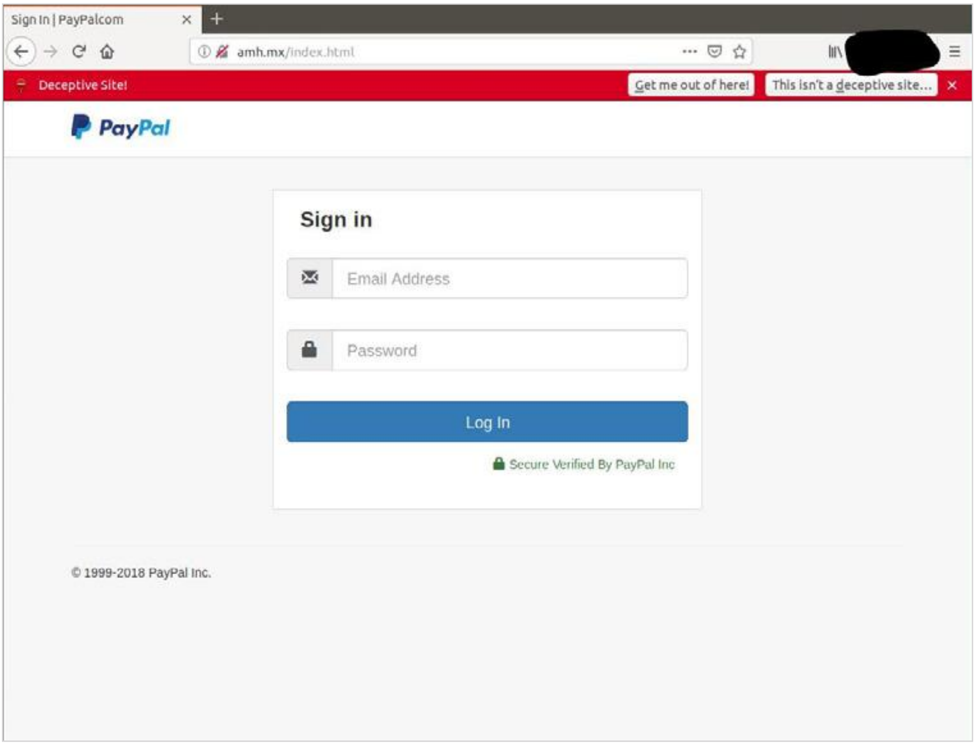


Figure 14: A phishing page imitating a Mexican organization "AMH" attempts to dupe victims into giving away PayPal credentials.

Brazil experiences the greatest number of phishing attacks in the world, with nearly a quarter of the population either being targeted by or falling victim to phishing schemes in the first half of 2018.[16] Argentina, Venezuela, and Bolivia also find themselves among the top ten countries most impacted by phishing, while many other Latin American countries have identified phishing attacks as being a rising problem within their borders.[17]

From December 1st 2017, to November 30th 2018, over 71% of the 1,800 crimeservers hosting pages with Mexican TLDs were phishing-related.

In November 2018, we detected 125 phishing-dedicated crimeservers hosting phishing pages with Mexican TLDs. From December 1st 2017, to November 30th 2018, over 71% of the 1,800 crimeservers hosting pages with Mexican TLDs were phishing-related.

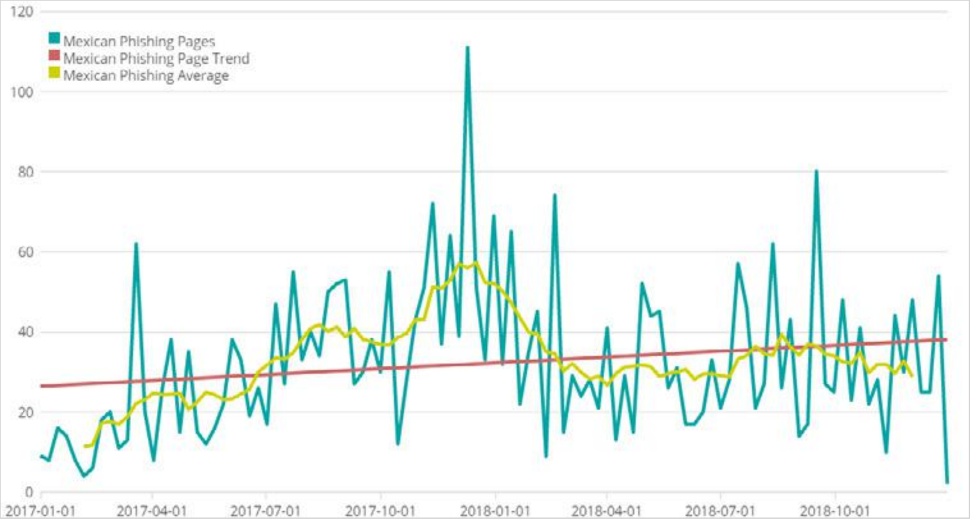
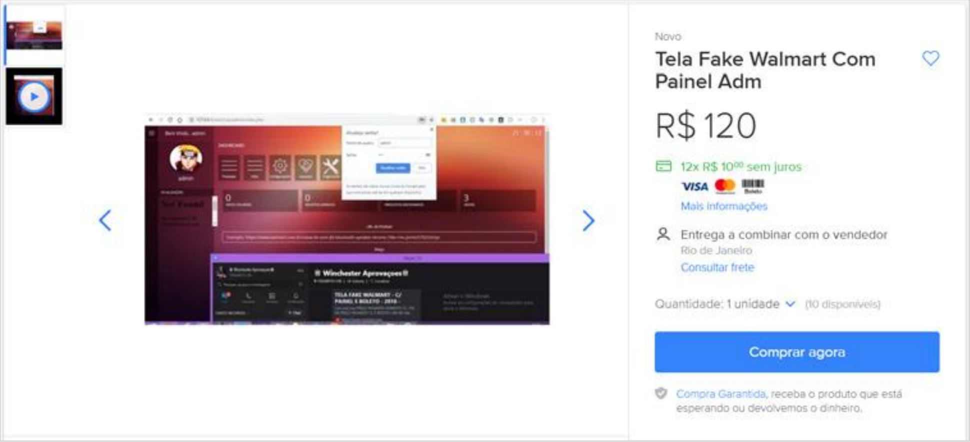


Figure 15: Data from our crimeserver dataset over 2017 and 2018 reveals an upward trend (in red) of more phishing-dedicated crimeservers hosting pages with Mexican TLDs.

7.2.1. PORTUGUESE-LANGUAGE

Cybercriminals create, sell, and swap phishing pages to turn a profit. The instability of Portuguese-language cybercriminal forums and marketplaces – which often experience long periods of downtime or simply disappear – has prompted many Brazilian cybercriminals to utilize legitimate platforms such as MercadoLibre (MercadoLivre in Portuguese) and YouTube to advertise and sell their products.


Novo

Tela Fake Walmart Com Painel Adm

R$ 120

12x R$ 10^{00} sem juros

VISA

Mais informações

Entrega a combinar com o vendedor

Rio de Janeiro

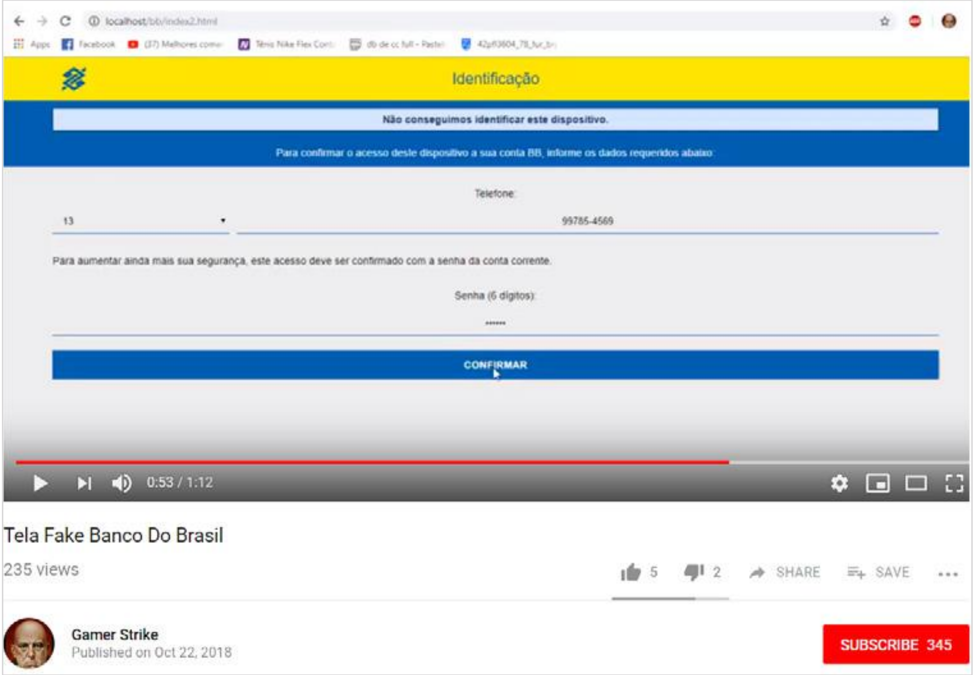
Consultar frete

Quantidade: 1 unidade (10 disponíveis)

Comprar agora

Compra Garantida, receba o produto que está esperando ou devolvemos o dinheiro.

Figure 16: A Walmart phishing page for sale on MercadoLivre.[18] *The page is for sale for R$120 ($31.71 USD)*



Identificação

Não conseguimos identificar este dispositivo.

Para confirmar o acesso deste dispositivo a sua conta BB, informe os dados requeridos abaixo:

Telefone:

13 ▾ 99785-4569

Para aumentar ainda mais sua segurança, este acesso deve ser confirmado com a senha da conta corrente.

Senha (6 dígitos):

••••••

CONFIRMAR

Tela Fake Banco Do Brasil

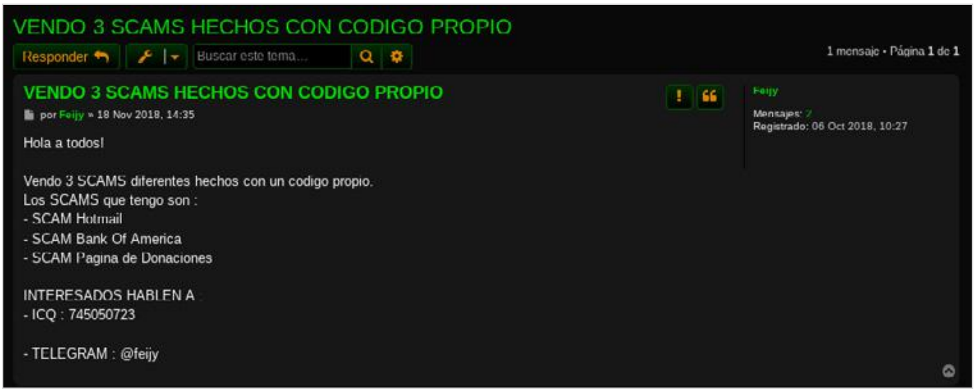
235 views

Gamer Strike
Published on Oct 22, 2018

Figure 17: A user operating under the alias "Gamer Strike" shares a YouTube video advertising a phishing page targeting Banco do Brasil.[19] *The individual urged interested parties to contact them on Facebook.*

7.2.2.SPANISH-LANGUAGE

Conversely, Spanish-language cybercrime-oriented forums are relatively more stable than their Portuguese counterparts, allowing for a trade in phishing pages to occur within these spaces.



VENDO 3 SCAMS HECHOS CON CODIGO PROPIO

VENDO 3 SCAMS HECHOS CON CODIGO PROPIO
por Feijy » 18 Nov 2018, 14:35

Feijy
Mensajes: 2
Registrado: 06 Oct 2018, 10:27

Hola a todos!

Vendo 3 SCAMS diferentes hechos con un codigo propio.
Los SCAMS que tengo son :
- SCAM Hotmail
- SCAM Bank Of America
- SCAM Pagina de Donaciones

INTERESADOS HABLEN A
- ICQ : 745050723

- TELEGRAM : @feijy

Figure 18: The actor operating under the alias "Feijy" advertises several phishing pages for sale on the Spanish-language carding forum Libertor.

In addition to selling pre-fabricated phishing pages, several threat actors operating in the Spanish-language cybercriminal underground have posted detailed tutorials instructing readers on how to create their own phishing pages. For instance, the threat actor 'DarkSide', the admin of the Spanish-language dark web forum Libertor, authored two popular guides on the forum detailing how to create Facebook and Twitter phishing pages.[20],[21] Though created in May and June 2017, both threads have continued to generate interest in the year since.

7.2.3. CRIMEWARE-AS-A-SERVICE

Various phishing-related Crimeware-as-a-Service (CaaS) offerings exist within the Latin American – particularly Portuguese-language – underground. These services are typically advertised on WordPress blogs, where the various offerings and pricing options are advertised. Our analysts identified one such service dubbed "Dr. InfoDNS." Dr. InfoDNS allows interested parties to rent hosting infrastructure and helps these threat actors identify and target potential victims.[22] Dr. InfoDNS's cheapest plan, costing R$1,000 ($266.25 USD) a week, includes the following (translated from the original Portuguese):

> *Consists of 3 servers 1, 1 for [hosting phishing] pages and 2 for DNS systems (redirection)*
>
> *In this module, you pay PER PHISHING PAGE ONLINE and the process of infecting victims is my responsibility*
>
> *Here you don't have to worry about the technical parts, just [let us know] an email to receive the [stolen] information.*

Both novice and seasoned cybercriminals are attracted to services such as those offered by Dr. InfoDNS. These services allow newbies to cut their teeth in the world of cybercrime while paying for the help they need, while veteran cybercriminals can use these services to outsource elements of their fraud schemes.

These services allow newbies to cut their teeth in the world of cybercrime while paying for the help they need.

In addition to stealing payment card information, phishing pages are employed by cybercriminals in hopes of compromising credentials, PII, or other monetizable information.

Phishing pages are employed by cybercriminals in hopes of compromising credentials, PII, or other monetizable information.

Phishing kits are another Crimeware-as-a-Service offering which have been widespread for many years, and attackers using them tend not to be highly skilled, or 'juniors' starting out in cybercrime. Kits can be bought in cybercrime forums but some of them have become publicly available and been reused for years. It is not uncommon to see currently active phishing kits showing 2012 in their copyright line. The criminals simply use the same phishing kit, modify some files and upload it to compromised sites. As a result, it is quite usual to see the reuse of files and code snippets among different phishing kits.

7.3. MALWARE

This section contains an overview of significant malware types found in Latin America, with a special focus on RATs and POS malware. It concludes with a case-study of Emotet, which has recently been very active, targeting Mexican email addresses in particular.

7.3.1. REMOTE ACCESS TROJANS: THE PREFERRED MALWARE IN LATIN AMERICA

Using our datasets, analysts have determined that Mexico, Colombia, Brazil, Argentina, and Peru are the top five Latin American countries most impacted by malware distribution. Most of the malware families found in the TOP5 in

Mexico, Colombia, Brazil, Argentina, and Peru are the top five Latin American countries most impacted by malware distribution.

those countries are Remote Access Trojans (RATs), being njRAT, DarkComet and XtremeRAT the most popular ones.

7.3.1.1.DARKCOMET

Name	DarkComet
First Seen	2008
Last Seen	Currently active
Sale Platform	Freely available on a number of black markets
Author/Actor	Jean-Pierre Lesueur aka DarkCoderSc
Price	Free
Actors using it	Syrian Government: In 2012, opponents of the Syrian regime claimed that the government was using a Trojan to monitor and disrupt the protestors' network. SynBots: A 2012 campaign that appeared to be aimed at Runescape users or other gaming communities. Iranian hackers from Ashiyane forum: Less than a week after the January 7 2015 Paris attacks, DarkComet malware was found in the wild specifically targeting French systems and being spread using the #JeSuisCharlie hashtag.
Description	DarkComet is a freeware RAT developed by Jean-Pierre Lesueur in 2008. It started proliferating in 2012. The latest version is 5.3.1 and can be found on the internet for free. Some features of this RAT include: process, registry, window, files and network shares management, remote shell, password stealer, webcam, keylogger, IP scanner, DDoS, and more.

Less than a week after the January 7 2015 Paris attacks, DarkComet malware was found in the wild specifically targeting French systems and being spread using the #JeSuisCharlie hashtag.

Since the service was designed specifically for gamers, the majority of targets were within the gaming community.

7.3.1.2. NJRAT

Name	njRAT
First Seen	2012
Last Seen	Currently active
Sale Platform	Cracked versions can be found on the internet
Author/Actor	Njq8
Price	Free
Actors using it	Skayzzen and AllyzzCorp: Versino v0.7 was built by these two threat actors in 2013. Saudi Arabia Hackers: In 2015, an njRAT campaign originating from Saudi Arabia was observed using old FakeAV tactics. Discord VoIP chat servers: In 2016, attackers used Discord VoIP chat servers to host njRAT. Since the service was designed specifically for gamers, the majority of targets were within the gaming community.
Description	njRAT is a general-purpose RAT written in .NET, with the following features: • Remote desktop • Network / File / Registry / Window / Process management • Infected machine information (IP, full computer name, full username, OS, install date, country) • Download and execute a file from disk or URL • Remote shell • Webcam capture • Audio capture • Keylogger • Browsers and other applications passwords stealing After njRAT source code was leaked, a worm variant appeared based on this source code (njworm or h-worm). Due to this, the most distributed version is 0.7d.

7.3.1.3.XTREMERAT

Name	XtremeRAT
First Seen	2010
Last Seen	Currently available
Sale Platform	Freely available on a number of cyber black markets
Author/Actor	XtremeCoder
Price	Free. The author was charging 350 EUR for the source code, before it was leaked online.
Actors using it	Molerats: In 2012, XtremeRAT was used against a variety of governments as well as Israeli and Palestinian targets in what was known as Operation Molerats. PackRat: In 2013 and 2014, Packrat seems to have adopted XtremeRAT as well. Colombian groups: In 2015, At least four groups are using malicious email attachments to deliver the W32. Extrat remote access Trojan to Colombian financial employees. Malspam: In 2017, Malspam activity was noted on August 1st 2017 delivering an Xtreme RAT variant.
Description	XtremeRat is a freely available general-purpose RAT. It has been seen distributed in different campaigns around the world, and still used nowadays. The newer version found is 3.9. Once a machine is infected, bots connect to the C2 to receive commands. The following features are available: file, process, window, service, registry, clipboard and device list management, desktop, webcam and audio capture, chat, keylogger, download and execute, etc. The RAT keeps its configuration into a file on disk, encrypted with RC4 and a fixed key. The most distributed versions are 2.9 and 3.6 Private.

7.3.2. POINT OF SALE (POS)

The heavy reliance on magnetic stripe transactions in Latin America.make this region particularly vulnerable to massive breaches resulting from POS malware.

POS malware is endemic to all regions of the globe. The heavy reliance on magnetic stripe transactions in Latin America, however, make this region particularly vulnerable to massive breaches resulting from POS malware.

Despite this, malware is rarely discussed within the Latin American underground outside of simple RATs. Our analysts consider that Latin American threat actors may not be as interested in malware offerings due to the relative ease at which cybercrime can be committed in the region using simpler attack vectors, such as phishing pages. More malware-focused and technically sophisticated Latin American cybercriminals have often maintained profiles on both Spanish or Portuguese-language as well as more malware-heavy Russian or English-language forums, signaling that a robust cybercriminal economy around the sale of malware likely does not exist in Latin America.

While it may not be offered for sale in the cybercriminal underground, POS malware certainly exists and is disruptive in Latin America. Our analysts assess that campaigns using POS malware in Latin America are likely carried out by highly-vetted groups of Latin American cybercriminals, perhaps working in collaboration with threat actors from other linguistic communities.

In March 2018, the emergence of the first confirmed chip and PIN stealing malware being used in the wild, dubbed Prilex, was reported.

Evolving EMV standards have inspired cybercriminals to get creative and innovate with their approaches to ATM malware. In March 2018, the emergence of the first confirmed chip and PIN stealing malware being used in the wild, dubbed Prilex, was reported.[23] Prilex is attributed to Brazilian cybercriminals, though reports indicate that it is being deployed in other Latin American countries, including Mexico.[24] Our analysts think that Prilex is likely only capable of compromising data from SDA EMV cards; the original report referred ambiguously to "bad implementation of [EMV] technology."

Our analysts assess that the development and utilization of POS malware in Latin America will likely increase, especially as more Latin Americans become banked.

Indeed, Latin American users are opening more and more banks accounts and using debit cards more often. Many of these cards either have weak (static data authentication instead of dynamic data authentication) or nonexistent EMV chip technology.

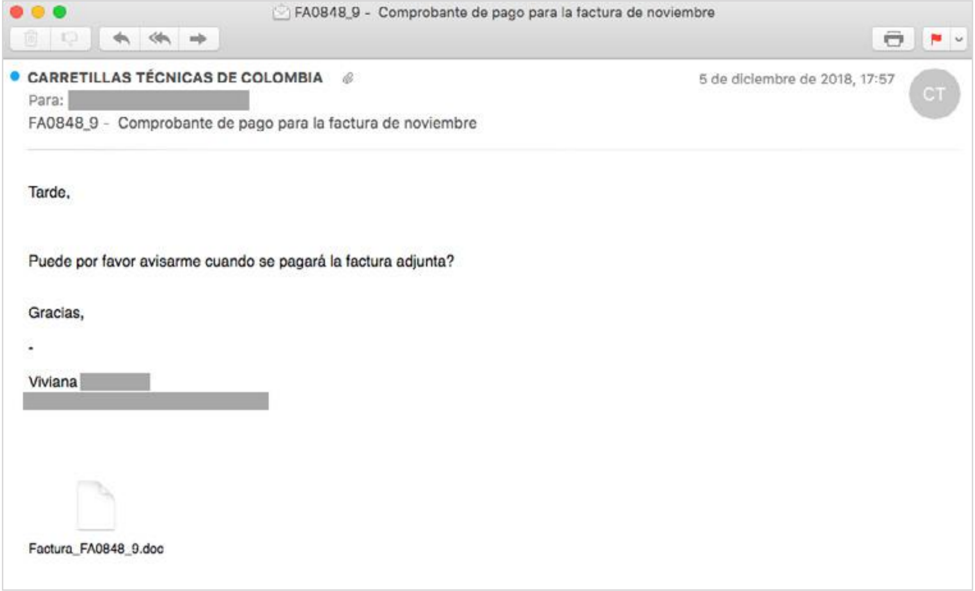
The Emotet spam botnet targeted over 40,000 email addresses with Mexican TLDs (.mx).

7.3.3. EMOTET ACTIVITY IN LATIN AMERICA

As mentioned before in this report, Emotet re-emerged in December 2016 as a spambot to spread additional malware.This latest version is known as Emotet v4. Its spambot module allows it to spread both itself and additional malware families. It makes use of email templates, attachments, recipient email addresses and email credentials that it downloads from its C2. The email credentials are stolen and collected from infected computers using a different module.

Blueliv analysts looked into Emotet for approximately one month in November 2018 to summarize its activity for this report. The Emotet spam botnet targeted over 40,000 email addresses with Mexican TLDs (.mx).

The following image shows a real example of the emails used during the spam campaign, where Mexican compromised accounts were used to target Colombian businesses:



FA0848_9 - Comprobante de pago para la factura de noviembre

CARRETILLAS TÉCNICAS DE COLOMBIA

5 de diciembre de 2018, 17:57

Para: [redacted]

FA0848_9 - Comprobante de pago para la factura de noviembre

Tarde,

Puede por favor avisarme cuando se pagará la factura adjunta?

Gracias,

-

Viviana [redacted]

[redacted]

Factura_FA0848_9.doc

Figure 19: Emotet spam campaign targeting Colombian businesses

Throughout November 2018, Emotet was dispatching approximately 185,000 spam message a day, using over 50,000 different sender emails. These sender emails represent 15,000 unique domains, of which ~8% have Latin American TLDs. The recipients of this latest campaign are largely corporate email addresses, representing 1,200,000 million different domains.

The recipients of this latest campaign are largely corporate email addresses, representing 1,200,000 million different domains.

8.2019 TRENDS

8.1.CYBERSECURITY CAPTURING THE ATTENTION OF THE BOARD

Cybersecurity has morphed rapidly from the domain of a handful of employees, to a concern of the entire organization – including the boardroom. As security incidents become bigger, more frequent, and more widely reported – and with GDPR upping the ante – the threat of both reputational and financial damage from neglecting to take security seriously has begun to change attitudes. It is critical that organizations start to examine their own security posture seriously and transparently. As organizations begin to recognize the intersection between cybersecurity and business strategy, leaders will be prompted to reach across departments in order to collaborate on, educate about, and integrate good practices.

8.2.STABILIZATION OF CYBERCRIMINAL UNDERGROUND MEANS LOWER BARRIERS TO ENTRY FOR HACKERS AND FRAUDSTERS

The barrier to entry for cybercriminals is lower than ever.

The barrier to entry for cybercriminals is lower than ever. Long gone are the days where these crimes were the domain of only veteran hackers; now, the cybercriminal underground is crowded with threat actors advertising and selling bulletproof hosting services, exploit kits, credential stealers, compromised accounts, and all manner of other tools for cybercrime.

Underground communities facilitate the exchange of good sand services among cybercriminals, allowing for many threat actors to specialize in providing specific illicit offerings that in turn lower the barrier to entry for other threat actors. These offerings allow novice cybercriminals easy access to the illicit world of cybercrime while allowing seasoned threat actors to scale their operations through outsourcing. Stable underground communities are necessary to facilitate this environment.

The year 2018 saw the stabilization of English-language darknet marketplaces following a prolonged period of volatility, kicked off by the law enforcement takedowns of the AlphaBay and Hansa marketplaces in summer 2017.

The year 2018 saw the stabilization of English-language darknet marketplaces following a prolonged period of volatility, kicked off by the law enforcement takedowns of the AlphaBay and Hansa marketplaces in summer 2017. After weathering the storm of untrustworthy new marketplaces, a handful of exit scams, the exposure of bugs on major marketplaces, and a deep and persistent paranoia regarding the possibility of law enforcement infiltration, it appears that many of the English-language darknet markets that currently exist, such as DreamMarket, Empire Market, and Wall Street Market, have established their credentials and have begun to win back users.

The Spanish-language underground also saw a major development in 2018, with the return of the storied forum Cebolla Chan 3.0 after over a year long hiatus. The return of Cebolla Chan 3.0 is largely symbolic; the forum has for a long time functioned as the central watering hole of the Spanish-language cybercriminal community. It's likely that the resurrection of this forum will have a knock-on effect, driving participation on other Spanish-language forums as well.

With these stabilizations helping to lubricate the wheels of illicit commerce on both the English-language and Spanish-language undergrounds – coupled with the relative stability of other major underground communities – 2019 will likely herald further increased access to malicious products and services for cybercriminals of all stripes.

8.3. RANSOMWARE... MORE LIKE RANSOM? WHERE?

A decline in ransomware in 2018 has been recorded by many researchers, after experiencing two years of attention and near hysteria.

The significant decline in ransomware incidents is likely due in part to the exodus of less advanced threat actors moving away from this once-trendy cybercrime in favor of other types of crime – such as cryptomining – that allow them to monetize quickly with little time and money invested.

More advanced attackers, however, will surely continue to deploy ransomware in deliberate and thought-out schemes, typically using private ransomware versions to attack big organizations in hopes of lucrative returns. Evidence of this can be seen in the actions of the Dridex Gang, which have reportedly been using their proprietary ransomware BitPaymer (alternatively known as Friedex) to hold entities hostage, such as an Alaskan municipal government and even the PGA.

A similar example to this situation can be observed when evaluating the banking Trojan landscape of the late aughts: the banking malware scene became popularized, drawing in experienced threat actors who could easily access and buy banking Trojans and put them to use. As years passed, however, less experienced cybercriminal lost interest in the banking Trojan scene and moved onwards to ransomware, leaving the space to be dominated by big players such as the Dridex and Dyre gangs. These gangs continued to make money in a more advanced way and using more sophisticated resources, a marked distinction from the capabilities of the lesser advanced attackers.

In 2019, we will likely see the continued privatized use of ransomware among sophisticated cybercriminal gangs, resulting in less frequent but more devastating attacks.

8.4. CRYPTOJACKING DOMINATES THE MALWARE SCENE

As ransomware has fallen in popularity, cryptojacking has risen to take its vacated throne. Despite the fall in the prices of cryptocurrencies this year, the number of cryptojacking attacks quintupled in 2018.

A number of factors contribute to the rise of cryptojacking. Simply, the growing number of device online broadens the attack surface. From a cybercriminal perspective, these crimes can be conducted with relative ease – there are open source miners and miners available for sale on the darkweb – as well as a low risk of getting caught.

8.5. EXTORTION, OLD AND NEW

In addition to cryptojacking, less sophisticated cybercriminals have chosen to abandon the ransomware game in favour of other extortion tactics. The DDoS extortion schemes of the past – such as those by the Armada Collective – have given way to clever SEO attacks that threaten to tank an organization's reputation on social media and popular review sites through the use of bots coded to leave negative reviews. One such case occurred in August 2018, in which a group calling itself "STD Company" threatened a small airline company with a negative SEO attack if their ransom was not paid.

A group calling itself "STD Company" threatened a small airline company with a negative SEO attack if their ransom was not paid.

A more ham-fisted – though lucrative – approach to extortion is the batch sending of threatening emails claiming to have compromising photos or videos of the subject; the attacker threatens to disseminate the non-existent material unless the victim pays a ransom of several hundred dollars in Bitcoin.

During 2019 we will see new creative scams, using social engineering to make companies and individuals pay certain amount of money.

8.6. TELEGRAM

Researchers continue to observe an increasing use of Telegram as a cybercriminal communications platform. Various cybercrime and fraud-centric groups exist on the messaging app, facilitating the exchange of illicit techniques, the sharing of advertisements for cybercriminal offerings, and the dissemination of cybercrime news. For instance, many Brazilian cybercriminals have turned to Telegram as an easy way to widely share HTTP injectors – a tool used for fraudulently obtaining free mobile internet.

Elsewhere, Eastern European and Iranian cybercriminal have begun to experiment with using Telegram as a friendlier and more intuitive interface for bots and no-distribute anti-virus scanners. By building off of familiar app that many already have installed on their phones, these innovative threat actors help pave the way towards a simpler introduction into the word of cybercrime for the uninitiated.

Eastern European and Iranian cybercriminal have begun to experiment with using Telegram as a friendlier and more intuitive interface for bots and no-distribute anti-virus scanners.

Still yet, Telegram is being used for 1-on-1 business dealings between cybercriminals. Wariness about the stability of online forums and marketplaces – especially following the summer 2017 law enforcement takedowns of major darknet marketplaces – have driven cybercriminals to look towards the use of other communication platforms for their dealings such as Telegram and Wickr.

As Telegram continues to rise in popularity among legitimate users around the globe, illegitimate users are sure to flock to the platform as well. In 2019 we will likely see the continued and expanded uses of Telegram as a platform not only for cybercriminal communication, but also for cybercriminal innovation.

9.CONCLUSIONS

This year, the cyber threat landscape has revealed itself to be increasingly complex and the potential attack surface is growing faster than ever. Business and consumers are acquiring more smart devices which increases exponentially the risk of sufferingfrom cyber incidents. A growing number of new malware categories are performing new attacks putting at risk companies data, infrastructure, and reputation.

Within this context, Blueliv foresees the following trends happening and/ or continue raising in 2019:

9.1.THREE MAJOR TRENDS

9.1.1.MALWARE TRENDS ARE SHIFTING:

Cybercriminal interest in ransomware appears to now largely be limited to highly skilled threat actors targeting more lucrative targets. Lesser sophisticated cybercriminals have embraced cryptojacking, a scheme that will likely continue to attract at least moderate cybercriminal interest in 2019.

9.1.2.LATIN AMERICA:

Latin America is home to growing cybercriminal communities. This region will both emulate new successful fraud schemes from elsewhere while also concocting their own that are more specific to their environment.

9.1.3.STABILIZATION OF UNDERGROUND:

The stabilization of English-language darknet markets means that cybercriminal enterprises are back up and running. This stability breeds specialization, partnerships, and knowledge sharing among cybercriminals in a manner that's been difficult for cybercriminals to duplicate ad hoc. Despite this stabilization, cybercriminal reliance on third party apps for communication – such as Telegram and Wickr – will likely continue as a knock-on effect of post AlphaBay paranoia

Allegedly state-sponsored threat actors such as the Lazarus Group are likely to continue their targeting, motivated by pure espionage as well as money.

High profile APTs will continue activity in 2019. Allegedly state-sponsored threat actors such as the Lazarus Group are likely to continue their targeting, motivated by pure espionage as well as money. The activity of cybercriminal gangs also shows no signs of abating. While the arrest of several members likely muted the activities of the Cobalt Group for a bit, this decreased activity likely won't last long, as already seen in the gang's distribution of a malware dubbed "Spicy Omlette."

9.2.HOW TO PROTECT YOUR ORGANIZATION

In this overall context, are expecting to continue to raise more sophisticated defense mechanism.

77% of businesses believe that Threat Intelligence is important to organization overall security posture, but they also expect to significantly improve the effective of their threat Intelligence infrastructure.

According to the Cyber security Insider Threat Intelligence report, 77% of businesses believe that Threat Intelligence is important to organization overall security posture, but they also expect to significantly improve the effective of their threat Intelligence infrastructure.

Blueliv real time, modular, scalable threat intelligence from Blueliv helps hundreds of businesses to address the growing range of cyber threats in a dynamic and proactive way. We scour the open, deep and dark web to deliver fresh, automated and actionable threat intelligence to organizations, helping to protect their networks from the outside in.

Our scalable cloud-based platform – Threat Compass – turns global threat data into sophisticated and relevant intelligence, enabling organizations to reduce their risk, save time and maximize resource by improving their incident response performance. Our solution is bespoke to each customer, highly modular and has the fastest deployment on the market.

Threat Compass delivers threat intelligence through ten targeted modules with more to be added in 2019.

Join us in the fight against cybercrime !

10.ENDNOTES

[1] https://www.statista.com/topics/2045/internet-usage-in-brazil/

[2] https://www.zdnet.com/article/more-than-half-of-connected-brazilians-suffered-cyberattacks/

[3] https://www.businesswire.com/news/home/20180816005244/en/Cybersecurity-Market-Latin-America---Outlook-2023

[4] https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html

[5] https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/

[6] https://thewire.in/tech/trai-rs-sharma-aadhaar

[7] https://publications.iadb.org/handle/11319/7449

[8] hxxps://carding21[.]cc/threads/compras-al-35-amazon-mercado-libre-linio-ebay-walmart-cualquier-sitio-web[.]19709/#post-76189

[9] hxxp://7pta37j2kgxquq6w[.]onion/foro/viewtopic[.]php?f=9&t=359&hilit=compras&sid=d15b44345a0d7ea9eed2098b7e8d08e6

[10] hxxps://www[.]mpgh[.]net/forum/showthread[.]php?t=1265792

[11] hxxps://carding21[.]cc/threads/servicio-de-reembolsos-en-amazon[.]12023/

[12] hxxps://carding21[.]cc/threads/bypass-walmart-cvv[.]20083/

[13] https://www.gob.mx/condusef/prensa/se-registran-4-8-millones-de-reclamaciones-por-posible-fraude-en-tc-y-td?idiom=es

[14] https://www.youtube.com/watch?v=5N3rmVafLHg

[15] https://www.tecmundo.com.br/whatsapp/115523-golpe-whatsapp-atinge-50-mil-brasileiros-rouba-dados.htm

[16] https://www.kaspersky.com.br/blog/phishing-klsec-brasil-assolini/10642/?utm_source=newsletter&utm_medium=Email&utm_campaign=kd%20weekly%20digest

[17] https://www.statista.com/statistics/266362/phishing-attacks-country/

[18] https://produto.mercadolivre.com.br/MLB-1136515696-tela-fake-walmart-com-painel-adm-_JM?quantity=1

[19] https://www.youtube.com/watch?v=nrWQapT4Rt8

[20] hxxp://7pta37j2kgxquq6w[.]onion/foro/viewtopic[.]php?f=6&t=192&sid=926f6855976e391abc9280c49dec60f3

[21] hxxp://7pta37j2kgxquq6w[.]onion/foro/viewtopic[.]php?f=6&t=353&p=4110&hilit=twitter&sid=926f6855976e391abc9280c49dec60f3#p4110

[22] hxxps://drinfodns[.]wordpress[.]com/kl-dns/

[23] https://latam.kaspersky.com/blog/prilex-malware-brasileno-para-puntos-de-venta-evoluciona-hacia-el-robo-de-datos-de-tarjetas-protegidas-por-chip-y-pin/12593/

[24] https://www.gob.mx/condusef/prensa/alerta-condusef-ante-nuevos-mecanismos-de-fraudes-en-terminales-puntos-de-venta?idiom=es

About Blueliv

Blueliv is a leading cyberthreat intelligence provider,headquartered from Barcelona, Spain. We scour the open, deep and dark web to deliver fresh, automated and actionable threat intelligence to organizations, helping protect their networks from the outside in. We enable organizations to save time and resources by accelerating incident response performance, providing user-friendly evidence accessible to all levels within cybersecurity operations teamswith our pay-as-you-need solution. We do not believe in a one-size-fits-all approach, and work together to configure a modular solution tailored to customer needs using separate intelligence modules, all backed up by our world-class in-house analyst team. Blueliv was named Enterprise Security and Enterprise Threat Detection 2018 category winners by Computing.co.uk, 'Threat Intelligence Company of the Year2018' by Cybersecurity Breakthrough, a Gartner 'Cool Vendor,' andGo-Ignite winner, in addition to holding affiliate membership of FS-ISAC for several years.

blueliv.com

info@blueliv.com

twitter.com/blueliv

linkedin.com/company/blueliv

computing
Security
Excellence
Awards
2018
Winner
Enterprise Threat
Detection Award

computing
Security
Excellence
Awards
2018
Winner
Enterprise Security Award

CYBERSECURITY
BREAKTHROUGH
AWARD
2018

Blueliv ® is a registred trademark of Leap inValue S.L. in the United States and other countries.All brand names, product names or trademarks belong to their respective owners.
© LEAP INVALUE S.L.ALL RIGHTS RESERVED