Organización de los Estados Americanos
Organização dos Estados Americanos
Organisation des États Américains
Organization of American States

Latin American and Caribbean Cybersecurity Trends and Government Responses

TREND MICRO LEGAL DISCLAIMER

ORGANIZATION OF AMERICAN STATES LEGAL DISCLAIMER

Contents

Introduction

In a connected world, a trade-off exists between enjoying the convenience that information technology (IT) offers and minimizing the opportunities its use presents to cybercriminals. Cybercriminals can, for instance, spread sophisticated threats by exploiting popular mobile devices and cloud applications to infiltrate high-value targets. They have made cyberspace a means to victimize the public.

Throughout 2012, global trends in illicit cyber activity showed how previously unknown threats evolved to become mainstream and a danger to all types of Internet users. Tools like the Blackhole Exploit Kit, automatic transfer systems (ATSs), and ransomware surged in use, employing better social engineering strategies, evasion techniques, and scare tactics.[1] The all-too-familiar story of new technology hijacked for nefarious aims reemerged in 2012, as the growth of mobile threats ballooned at a much faster pace than those affecting normal computers.[2] Pieces of Android malware rose from a thousand to more than 350,000 in the span of just one year.

Cyber incidents demonstrated the importance of staying up-to-date on global cybercrime trends, especially concerning the use of mobile and personal computing devices. Consequently, IT security specialists and cyberthreat analysts must render global averages into organization-, industry-, or region-specific statistics to determine how best to protect the sensitive information they keep. Failure to produce tailored threat analyses will skew critical data, keeping countries and businesses from designing and implementing effective cybersecurity policies and technical capabilities, thereby keeping citizens vulnerable.

Knowledge of the cyberthreat landscape and government responses in Latin America and the Caribbean is incomplete. Much of what is known about the region's cyberthreat landscape is based on uninformed news reports and innuendo. Some sources show that banking malware was the region's top cybercrime problem in 2011 while others judge that the biggest issue was multipurpose malware that compromised routers on a scale larger in Latin America than in any other part of the world.[3] These divergent views show that more specific data is needed to accurately diagnose the threat to our citizens.

1 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_blackhole-exploit-kit.pdf; http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_automating_online_banking_fraud.pdf; http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_police_trojan.pdf; http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-police-ransomware-update.pdf

2 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-evolved-threats-in-a-post-pc-world.pdf

3 http://blog.trendmicro.com/trendlabs-security-intelligence/latin-america-router-compromising-malware-found/

In collaboration with Trend Micro Incorporated, the Organization of American States (OAS) and its Secretariat for Multidimensional Security (SMS) would like to share this report to illustrate the cybersecurity and cybercrime trends in Latin America and the Caribbean. Information presented has been gathered through both quantitative and qualitative methods, drawing data from a survey of OAS member-state governments, as well as an in-depth analysis of global threat intelligence from honeypots and client-provided data collected by Trend Micro. Unless otherwise noted, graphs and tables use data that was collected by Trend Micro. The analysis and conclusions of this report only cover countries that responded to the OAS survey.

OAS Country Survey Results

The 32 OAS Member States from Latin America and the Caribbean were invited to voluntarily provide information on the types and extent of cybersecurity incidents their countries faced in 2012, as well as their responses to those incidents. Thirteen of the 18 Latin American Member States and seven of the 14 Caribbean Member States subsequently made contributions to this report. Qualitative data was provided by a mix of institutions, most prominently National Computer Security Incident Response Teams (CSIRTs), and to a lesser extent national police cybercrime units.

Much of the information gathered is presented here in aggregate form to maintain the confidentiality of certain sensitive findings. And as with any large-scale survey of cyber incidents and illicit cyber activity, this effort to collect and analyze such data for the Americas and Caribbean has inherent limitations. For one, no network administrator or national incident response team knows how many incidents succeed and go undetected. Network intrusions are routinely discovered months or even years after the original breach was perpetrated. Furthermore, discussions with participating Member States revealed that a lack of effective communication and information sharing within governments in reporting cyber incidents remains a key challenge. Whether due to interagency competition, concerns about projecting an image of ineffectiveness, or a simple lack of channels or mechanisms necessary for information sharing, failure to exchange information regarding cyber incidents or network security breaches remains a widespread reality that must be taken into account when analyzing data on cyber activity in the region.

This study is also limited by a lack of defined and harmonized terminology. Upon analyzing data, it became clear that the term “cyber incident” was not uniformly understood or applied across the region, and it was beyond the scope of this study to urge states to integrate their respective definitions. Some governments interpret a cyber incident as any report or complaint sent to a national response team, while others are more exacting in their classification. Some survey results included incidents levied against the public and private sector as well as end users and academia. Others only included information pertaining to government networks while others still only described cyber incidents involving one or two key ministries. Despite the shortcomings presented by nuances in taxonomy or classification, this report offers an opportunity for governments to present their experiences, both positive and negative, in the hope that they allow relevant stakeholders to gain a better understanding of what is happening in the region, and what remains to be done.

Trends Seen

General Trends

In 2012, governments generally noted an increase in the frequency of cyber incidents compared with 2011, even where definitive quantitative data was incomplete or unavailable. The minimum assessed increase in cyber incidents over the period 2011 to 2012 reported by a government was 8–12%, while on the high end, two others reported an increase of 40%. Most governments cited increases somewhere within this range, although, interestingly, several reported that overall, fewer incidents were detected.

In addition to highlighting the varied definitions of cybersecurity terms, interpreting and analyzing the data collected raised other important considerations. Several governments clarified that the numbers they provided did not necessarily reflect real changes in attack frequency, but rather improvements in network monitoring and better trained personnel, which allowed organizations to detect more system breaches and other illicit cyber activities. Interestingly, those countries with recently established national CSIRTs reported some of the most significant increases in managed incidents. These reinforced the notion that attacks had been occurring all along but had simply gone undiscovered or undocumented.

Also noteworthy is the fact that most states did not differentiate between the types or severity of the cyber incidents they reported. This presents a shortcoming in data analysis, given the range in potential consequences of different kinds of incidents or attacks—a large-scale and sophisticated attack on national critical infrastructure will likely have a greater impact than the defacement of a government website. Data that did specify attack types was usually aggregated, although in some places, we have been able to display frequencies of the types or severity of attack received. One nascent national CISRT, for example, indicated that it managed 45 incidents in 2012, and deemed only one a “priority” case.

Obviously, the cyber incidents about which OAS Member State governments reported represent only a fraction of the total number of incidents and other forms of cybercrime carried out in the region. But collecting data to enable a truly comprehensive and detailed picture of the extent of all such incidents and activities in the Americas and the Caribbean, or anywhere else, remains at this point simply impossible.

As stated before, information sharing within governments—even those with the most advanced cybersecurity capabilities—continues to come up short, largely due to the practical realities of multiple organizations having to simultaneously respond to an ever-evolving range of threats and targets. And many private companies and other nongovernmental entities continue to be hesitant to report attacks or breaches. Accounting for the number of incidents affecting individual citizens poses an even greater challenge, given the still higher percentage of these that go undetected and unreported. Finally, a general and persistent lack of collaboration among stakeholders at all levels further complicates the collection of reliable and actionable information on data breaches. The net consequence of all of these factors is a less than adequate awareness of the problem, and the continued vulnerability of critical networks and information systems (IS).

Hacktivism or politically motivated hacking received widespread media attention in 2012, and information provided by the Member States suggests that this form of cyber incident is indeed on the rise in the region. Two countries reported coordinated cyber-attack campaigns in response to legislative initiatives to strengthen copyright enforcement and reform tax codes. In both cases, as the bills neared ratification, hacker forums became saturated with plans to launch large-scale cyber attacks on governmental infrastructure unless the bills were vetoed. Both national CSIRTs received advanced warnings of the pending attacks and thus managed to keep the damage to a minimum. Investigations of both incidents were inconclusive; one did not yield actionable evidence while the other eventually stalled after early leads went cold.

Interestingly, in some cases such hacktivist campaigns brought important unforeseen benefits. In two of the countries that contributed to this report, unidentified groups threatened to launch attacks against multiple governmental institutions. For one of the countries threatened, it was the first instance of an explicit warning of politically motivated hacking. The threats motivated both governments to implement plans of action to mitigate and respond to potential attacks. Although the incidents in question never fully materialized, they did provoke increased collaboration among key stakeholders, including law enforcement agencies, Internet service providers (ISPs), and an infrastructure operator. The information provided by the Member States indicates that the capacity gained and lessons learned from planning for and, in some cases, proactively responding to such incidents have become a central driver for increasing countries' national cyber-resilience.

Other important cybersecurity trends were reported as well. Spyware was found on law enforcement servers in at least one country. Numerous states provided information suggesting that traditional organized crime syndicates have increasingly turned to the Internet to extort and launder funds—very much in keeping with observed global trends. One country reported that more than 80% of the crimes they investigated in 2012 involved some aspect of electronic crime or the illicit use of IT. And while information and communication technology (ICT) may not yet be the main vehicle for the majority of crimes, it certainly has become an integral part of all investigations, highlighting the need for appropriate legislative instruments, trained investigators and prosecutors, and increased international cooperation on cyber issues.

Despite better visibility, hacktivism did not supplant monetary gain as the primary motivation behind hacking and the illicit use of the Internet in the region. Hackers still went after personal and financial data, fueling online black markets worldwide. Yet accurately measuring in quantitative terms the economic impact and loss hacking caused in the Americas and the Caribbean in 2012 is impossible. The figure is extremely high, likely greater than the loss caused by any other form of crime, including drug trafficking.

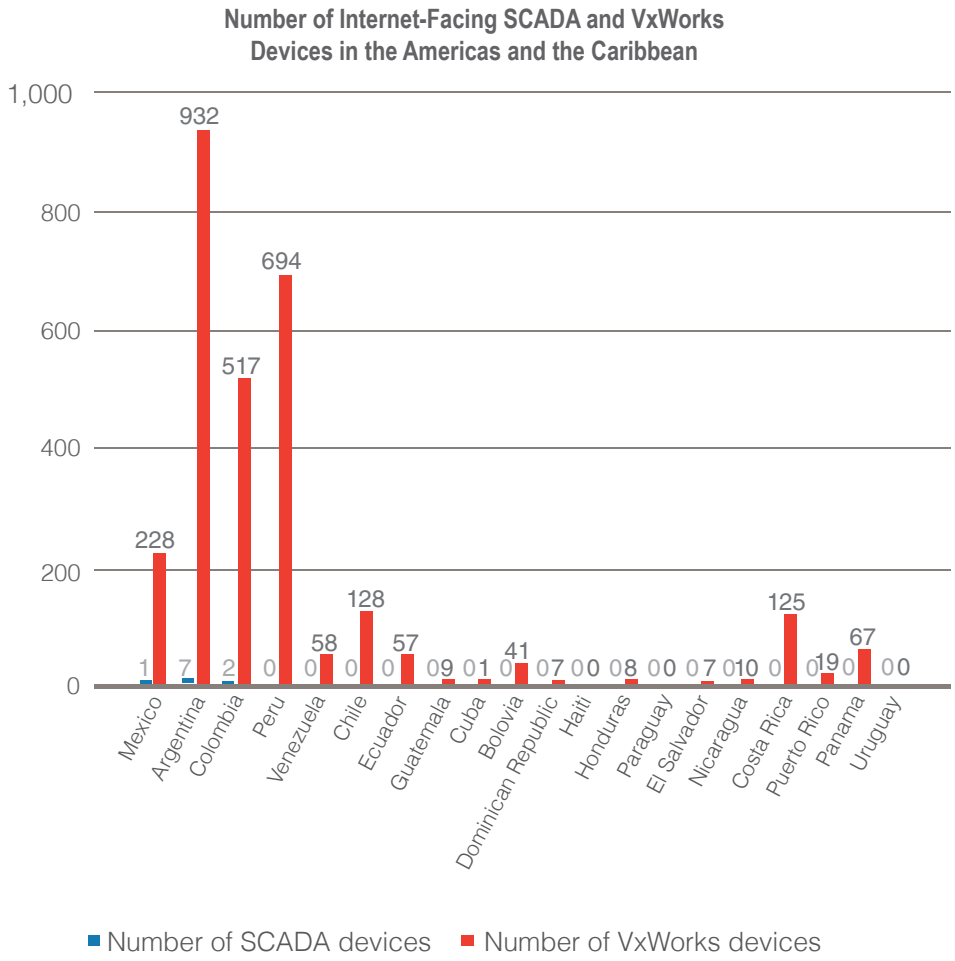
ICS Concerns

Both OAS and Trend Micro data indicated a rise in the number of attacks against critical infrastructure. Many critical infrastructures, including those that drive the financial, transportation, energy, and healthcare sectors, are dependent on industrial control systems (ICS). Many of these ICS, in turn, utilize the Internet, which allows critical infrastructures to efficiently and cheaply function. While it enables cheap and timely delivery of critical services, however, ICS connectivity also provides criminals and terrorists opportunities to strike countries where they will feel it most.

Numerous case studies over the last year illustrate the pressing nature of the aforementioned threats to ICS. A publicly operated national energy utility in one country experienced a spate of cyber attacks, although the national CSIRT was able to minimize damage caused by the breaches. Another government reported widespread attacks against financial institutions that formed the base of its special economic zone (SEZ). In this case, the attacks may have the potential to be especially damaging, considering that the SEZ accounts for a high percentage of the country's economic output and much of its foreign direct investment (FDI). One country's leading telecommunications service provider was also attacked, causing a brief but extensive disruption to cellular service. Unlike most attacks, the perpetrators of the latter incident were caught and convicted.

These incidents highlight the dangers that well-coordinated attacks on critical infrastructures pose to public well-being and economic development. While attacks involving critical infrastructures have not yet caused catastrophic losses or physical damage in the Americas and the Caribbean, they do highlight the need for vigilance and improved resilience, as many critical systems in the region remain exposed.

In 2012, 51 vendors in the ICS security community reported 171 vulnerabilities in various Internet-facing ICS, and the problem in the Americas is especially acute. Looking at the two most popular types of ICS used in the region, Trend Micro found that many of these devices were connected to the Internet.



Source: http://www.shodanhq.com/

Even though the use of Internet-facing ICS is not inherently dangerous, many of the systems shown in the figure above were not password protected or kept up-to-date with the latest security patches, needlessly exposing them to attacks. A Trend Micro study detailed that Internet-facing ICS suffer daily attacks. Data shows that over a period of 28 days, a total of 39 attacks from 14 different countries were recorded. Out of these 39 attacks, 12 were unique and could be classified as "targeted" while 13 were repeated by several of the same actors over a period of several days and could be considered "targeted" and/or "automated."[4]

Country Reports on Cybercrime

All of the information in this section came from reports submitted by OAS Member States.

Cybercrime Trends in Chile

In 2012, the number of cyber incidents that led to investigation and response in Chile decreased by 33%, as reported by the cybercrime unit of the Federal Police Department. The number of Internet-based wire fraud incidents, which often consisted of phishing and pharming attacks, decreased by 122% overall. Authorities attributed the decrease in this type of incident, which made up a large portion the country's criminal web traffic, to the dismantling of a notorious syndicate responsible for large-scale malware distribution often used in defrauding banks and individuals. Chile noted that many crimes now involve elements of Internet exploitation, as drug dealers and other criminals use the web to facilitate their activities. The prevalence of Internet-based crime there highlighted difficulties in international cooperation, which was cited in Chile as the biggest hindrance to cyber incident response, investigation, and deterrence.

Cybercrime Trends in Colombia

According to colCERT, which is Colombia's national CSIRT, the country recorded fewer cyber incidents in 2012 than in 2011, pairing it with Chile as one of the few Latin American countries with that distinction. It was unclear, however, whether this was due to a real decrease in the number of incidents, better security management on the part of government agencies that colCERT served, or the implementation of policies that changed the scope of assistance Colombia's response teams rendered.

In any case, fraud was the most prevalent type of cyber incident reported by colCERT in 2012. One notable contributor to this number was prolific cybercriminal, Jorge Maximilian "Pacho" Viola, who was captured in Colombia last year. Dubbed the "Tsar of Cloning," Viola had committed fraud in at least seven Latin American countries and was eventually arrested with over 8,000 cloned credit cards and US$9 million in his possession.[5]

Various types of hacking and website spoofing followed in Colombia's list of most prevalent cyber incidents. Hacktivist attacks, which most frequently targeted state and military entities and financial institutions, were widely reported by the country's response teams.

4 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf

5 http://latinamericacurrentevents.com/head-of-major-credit-card-cloning-ring-arrested-in-colombia/18040/

The Colombian government reported low levels of cybersecurity awareness, which precipitated unsafe online habits, causing vulnerable Internet users to be defrauded. In addition, insufficient police training on advanced attacks, difficulties in preserving and examining digital evidence, and lack of cooperation from ISPs and other private entities constituted major impediments to stopping cybercrime in Colombia.

Cybercrime Trends in Jamaica

The Jamaican government reported a 14% increase in the number of cyber incidents in 2012, which most often targeted public institutions. Nevertheless, financial institutions and a prominent critical infrastructure service provider were also the objects of high-profile hacking incidents. The survey revealed that, as in Chile, ICT was a component of many crimes in Jamaica in 2012. The growing frequency of cyber incidents in Jamaica is complicated by the lack of highly trained incident response and digital investigation personnel, inadequate domestic and international cooperation, and a lack of proactive measures to deter hackers and attackers.

Cybersecurity awareness in Jamaica generally remains low although the government has begun a large-scale awareness-raising campaign aimed at students.

Cybercrime Trends in Mexico

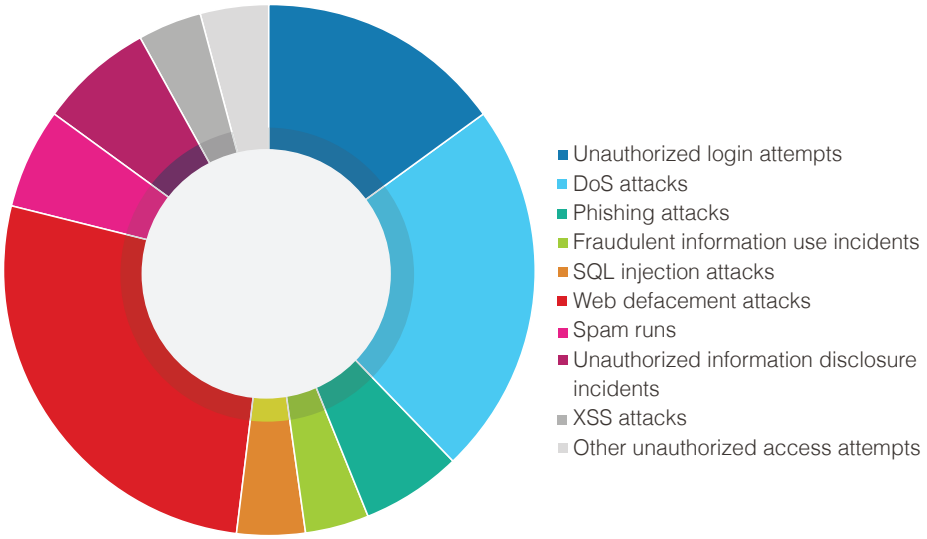
Mexican authorities registered a 40% increase in the number of cyber incidents in 2012, largely due to hacktivist attacks. Despite having several units tasked with responding to and analyzing cyber incidents, the country still cites a lack of legislative norms and public awareness as reasons for cyber insecurity.

The most serious attacks in 2012 targeted governmental infrastructures specifically created and employed to support the presidential elections in July. Hackers launched distributed denial-of-service (DDoS) attacks, defaced web pages, and carried out cross-site scripting (XSS) and SQL injection attacks. Cyber security technicians were well-equipped to deal with the attacks since they were similar to other hacktivist incidents that occurred throughout 2012.

Cybercrime Trends in Panama

Web defacement was the primary type of cyber incident reported in Panama, comprising 27% of all cases managed by CSIRT-PANAMA, the country's national incident response team. This was closely followed by DDoS attacks (23%), and unauthorized login attempts (15%).

Most Dominant Cyber-Incident Types Reported in Panama



Source: OAS Survey

Cases involving phishing (6%), fraudulent information use (4%), SQL injection (4%), spamming (6%), unauthorized information disclosure (7%), XSS use (4%), and other unauthorized access attempts (4%) completed the attack chart. The majority of incidents in Panama were reported in the third quarter of 2012. Authorities correlated this to the introduction of Law 510 in August, which sought to expand enforcement mechanisms on copyright violations and provoked a vocal and well-publicized hacktivist response.

The aforementioned cyber incidents were paired with reports from Panamanian authorities that customer service centers often had more access to clients' personal information than necessary, needlessly exposing individuals to insider threats. These service centers were frequently exposed to DDoS attacks, compounding risks to precariously stored sensitive information.

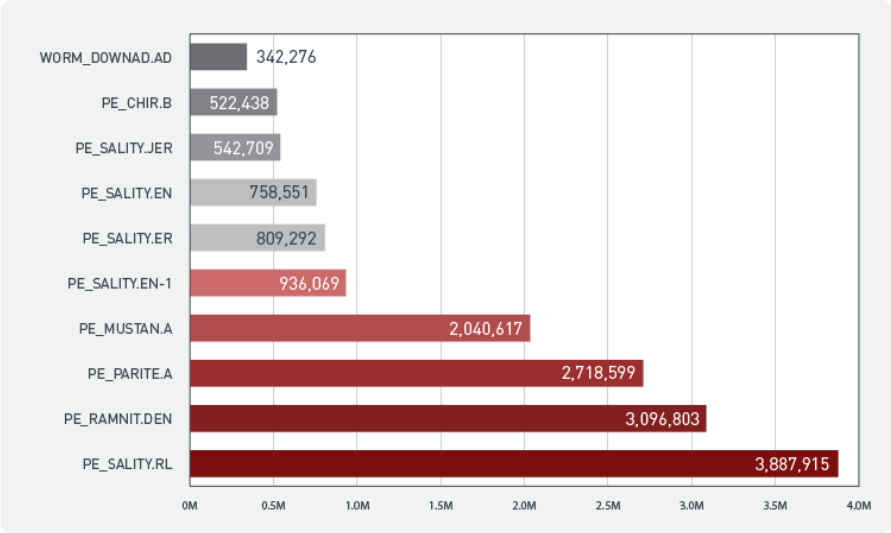
Panama cited a lack of qualified digital forensics and incident response specialists as the main roadblock to improving cybersecurity and fighting cybercrime. Authorities blamed many cyber incidents on a large-scale lack of awareness, including after investigation, as attacks were often found to have been preventable. This is due to the fact that Internet users were hesitant to learn about cybersecurity, thinking that safe computing habits were either too complex or too technical to master. Though several financial institutions disseminated educational materials, efforts were poorly coordinated and small awareness-raising campaigns failed to achieve the desired impact. To battle lax Internet security attitudes and promote secure Internet use, the government is currently planning to establish more awareness-raising initiatives in 2013.

Trend Micro Global Threat Intelligence Analysis

Malware

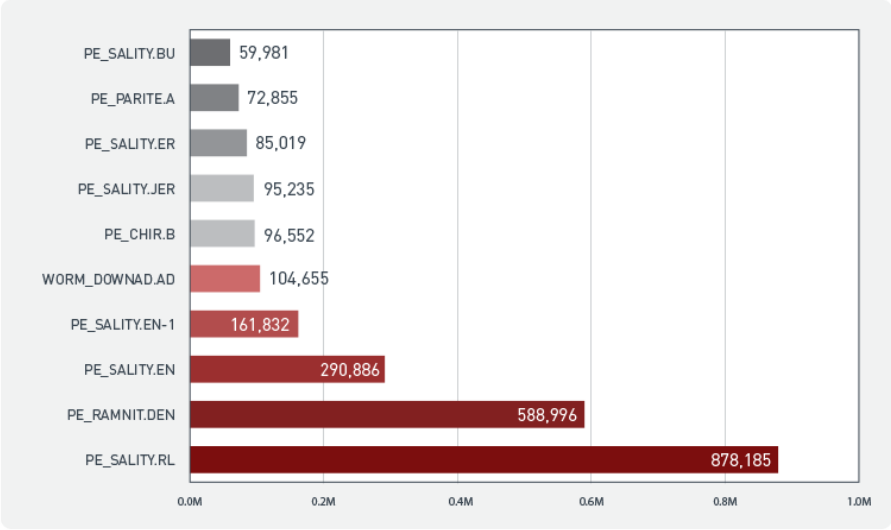
Latin America and the Caribbean were affected more by file infectors than any other type of malware in 2012 This often indicates the prevalence of insufficiently secured removable storage devices and unpatched operating systems (OSs) and/or applications.

Top 10 Malware in the Americas and the Caribbean in 2012



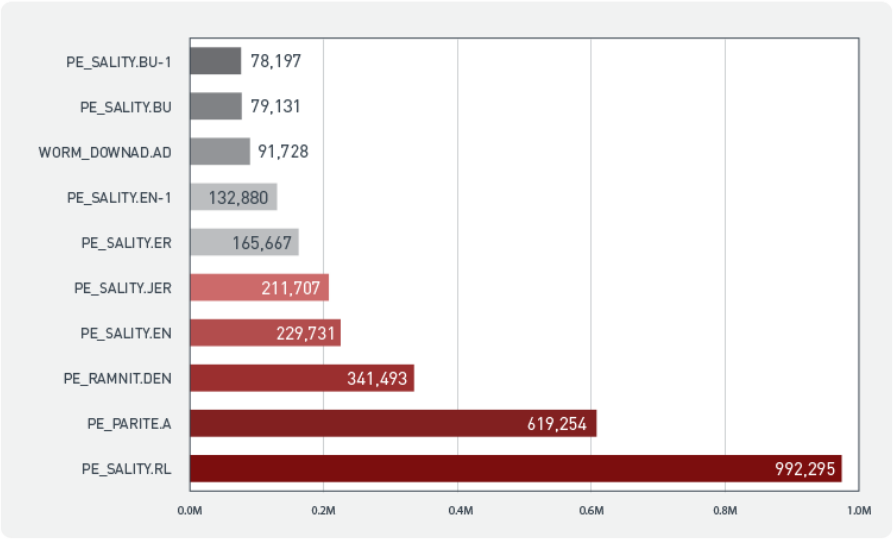
Source: Trend Micro™ Smart Protection Network™

Top 10 Malware in the Americas and the Caribbean in 1Q 2012



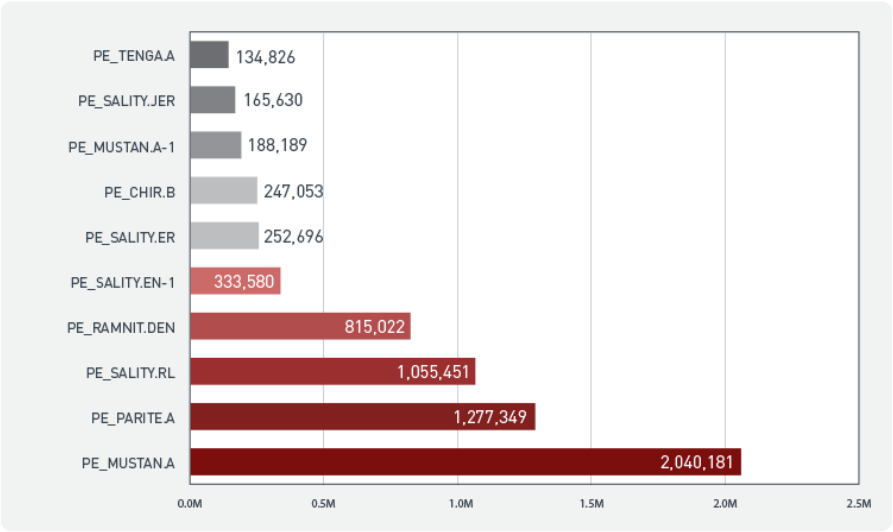
Source: Trend Micro Smart Protection Network

Top 10 Malware in the Americas and the Caribbean in 2Q 2012



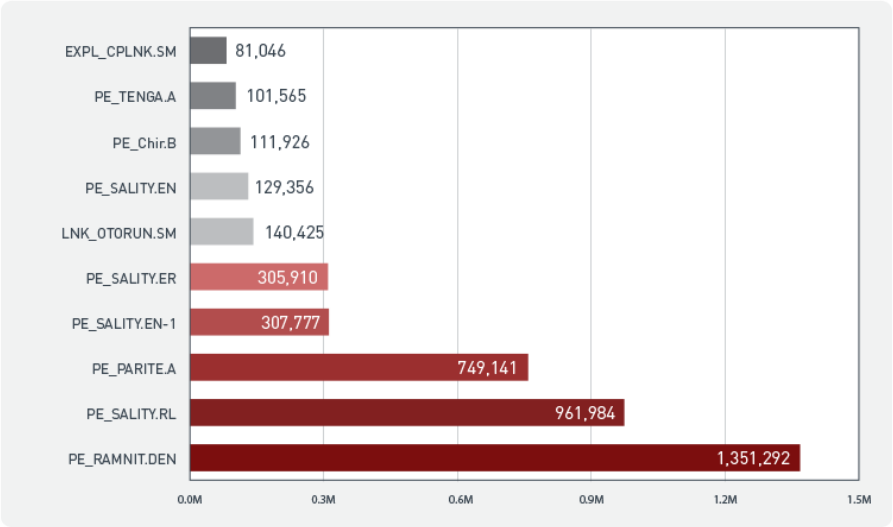
Source: Trend Micro Smart Protection Network

Top 10 Malware in the Americas and the Caribbean in 3Q 2012



Source: Trend Micro Smart Protection Network

Top 10 Malware in the Americas and the Caribbean in 4Q 2012



Source: Trend Micro Smart Protection Network

Spam

The global spam volume has been declining since 2011 due to huge botnet takedowns and other spam-related operations by law enforcement. However, the volume of spam has far from bottomed out. In 2012, among the Latin American and Caribbean countries covered in this report, the top spam-sending country was Mexico, followed by Argentina and Colombia.

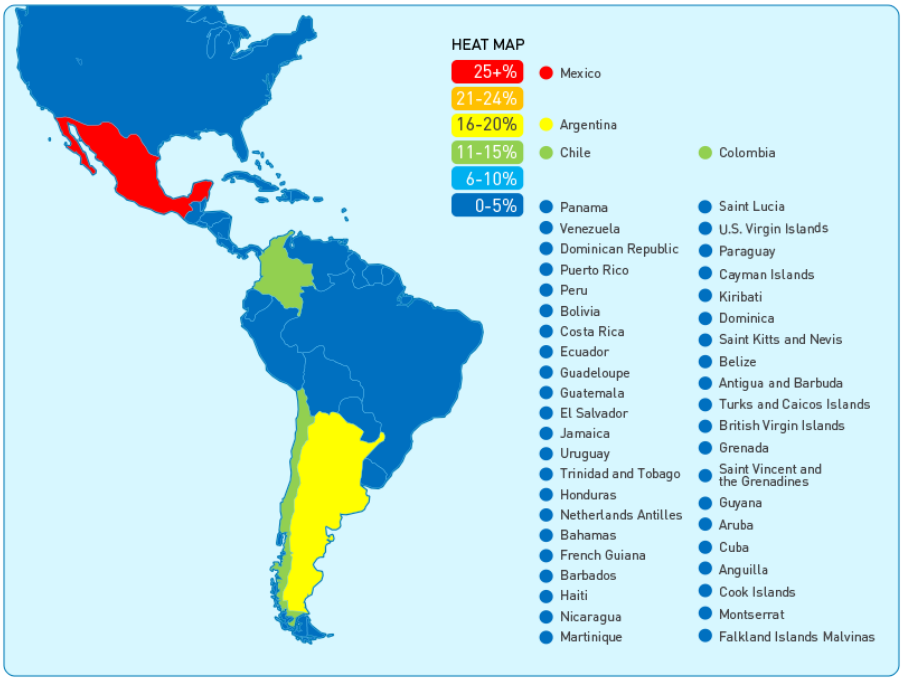
Latin American and Caribbean Spam-Sending Country (Excluding Brazil) Share Breakdown

Source: Trend Micro Smart Protection Network

Malicious URLs

Malicious website hosting was a serious problem in the Americas and the Caribbean. The top 2 spam-sending countries also topped the list of countries that hosted the greatest number of malicious URLs. Colombia, the country that ranked third in terms of spam sending, was replaced by Chile from the list of top malicious URL hosts.

Latin American and Caribbean Malicious-URL-Hosting Country (Excluding Brazil) Share Breakdown



Source: Trend Micro Smart Protection Network

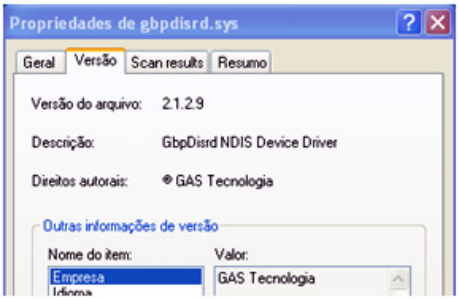
Underground Activity

Online Banking Theft and Crimeware Use

Online banking theft has been widely reported in Latin America. This activity has distinctive features, depending on the target country or bank and the nature of the authentication and security measures protecting financial data.

Cybercriminals have consistently found ways to undermine online banking security measures the moment they are improved or updated, which makes securing financial networks a continuously evolving and especially difficult task. If a bank uses a simple authentication scheme involving only a user name and a password, keyloggers are used to gain access. Banks that use one-time password (OTP) systems are injected with ATS scripts that hide illegal transactions. Like ATSs, Browser Helper Objects (BHOs) are also used against complex systems that implement two- or three-factor authentication. These techniques show the ingenuity of cybercriminals, who match every advance in online bank security with an equally innovative means to evade it.

Most sophisticated crimeware kits use popular online banking Trojans that are offshoots of the BANCOS family of crime kits. BANCOS malware often function like rootkits by removing security components in target computers used to access bank accounts. Although these kits have been prevalent for years, they were only considered a significant threat in the Americas and the Caribbean because of unpatched security systems and low levels of awareness.[6]



TSPY_QHOST.AFG pretends to be a component of a legitimate banking site plug-in to get into victims' computers.

TSPY_QHOST.AFG is an example of a BANCOS Trojan.[7] Unlike most strains it does not only change an infected computer's HOSTS file, it also employs uniquely advanced functions to evade anti-malware detection.

Address	Length	Type	String
.rdata:00010D80	00000054	unicode	_BB_F=_ZLQGRZV_v|vwhp65_gulyhuv_hwf_krvwv
.rdata:00010DD8	0000004C	unicode	_BB_F=_surjudp#ilohv_jesoxjlq_lvj1jsf
.rdata:00010E28	0000005C	unicode	_BB_F=_dutxlyrv#gh#surjudpdv_jesoxjlq_lvj1jsf
.rdata:00010E88	00000056	unicode	_BB_F=_surjudp#ilohv_jesoxjlq_jelhklvj1goo
.rdata:00010EE0	00000066	unicode	_BB_F=_dutxlyrv#gh#surjudpdv_jesoxjlq_jelhklvj1goo
.rdata:00010F48	00000070	unicode	_BB_F=_ZLQGRZV_Grzqordghg#Surjudp#Ilohv_JeSoxjlqlvj1lqi
.rdata:00010FB8	0000005C	unicode	_BB_F=_zlqgrzv_v|vwhp65_gulyhuv_jesqglvug1v|v
.rdata:00011018	0000006A	unicode	_BB_F=_zlqgrzv_Grzqordghg#Surjudp#Ilohv_vfsvvvk51lqi
.rdata:00011088	0000004A	unicode	_BB_F=_zlqgrzv_v|vwhp65_vfsYlvwd1h{h
.rdata:000110D8	0000004A	unicode	_BB_F=_zlqgrzv_v|vwhp65_vfsvvvk51goo
.rdata:00011128	00000046	unicode	_BB_F=_zlqgrzv_v|vwhp65_vfsOLE1goo
.rdata:00011170	00000046	unicode	_BB_F=_zlqgrzv_v|vwhp65_vfsPLE1goo
.rdata:000111B8	00000050	unicode	_BB_F=_surjudp#ilohv_Vfsdg_vfsvvvk51goo
.rdata:00011208	0000004C	unicode	_BB_F=_surjudp#ilohv_Vfsdg_vfsOLE1goo

TSPY_QHOST.AFG encrypts strings to evade detection and complicate analysis.

Cybercriminals in the Americas and the Caribbean also use Domain Name System (DNS) changers and remote access Trojans (RATs). They change proxy configurations and/or add information to the HOSTS file to breach online banking systems.

The previously discussed tools are most frequently delivered by embedding malicious links in spam or convincing phishing websites.

6 http://blog.trendmicro.com/trendlabs-security-intelligence/new-crimeware-in-bancos-paradise/
7 http://about-threats.trendmicro.com/malware.aspx?language=au&name=TSPY_QHOST.AFG

Cybercriminal Underground

Large botnet takedowns worldwide in the last few years, including that of Esthost in 2011, have forced cybercriminals to alter their tactics. They now endeavor to configure their own servers in data centers worldwide instead of using hijacked servers to host their command-and-control (C&C) infrastructures, spam tools, and other operational components. They avoid registering host names or domains for their servers and only use Internet Protocol (IP) addresses to avoid being indexed by search engines like Google.

In contrast to the preference for paid and proxy servers manifested by criminals in Eastern Europe, those in Latin America prefer using free hosting services.[8] Malware, C&C servers, phishing pages, and other malicious content used by the cybercriminals in Latin America are often hosted on Dot TK or other free web-hosting sites based in Eastern Europe. Cybercriminals take advantage of free trial services to register malicious domains and steal user information. Doing so allows access that lasts for a week at the longest, but may also be beneficial in obscuring evidence and covering up one's digital footprint. Crimeware kits and the data they steal are commonly traded and shared on social networking sites. Orkut, more than Facebook, is the leading marketplace in Latin America.

Orkut posts offering various cybercrime wares are a common sight in Latin America.

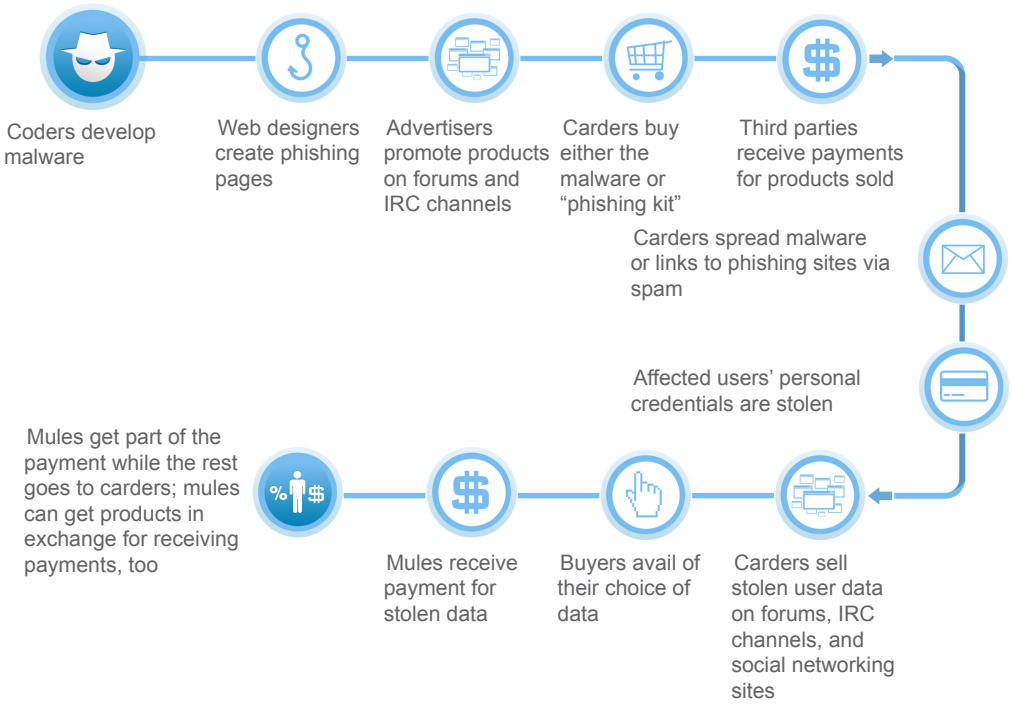
8 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

As in many regions, Internet Relay Chat (IRC) servers, hacker forums, and other channels are used to buy and/or sell credit card information, crimeware kits, and other personally identifiable information (PII).

Forum posts related to cybercriminal activity are also common.

In contrast to global norms, cybercriminals in Latin America use common money transfer services to pay for cybercriminal goods and services. Since this can lead to identification by authorities, cybercriminals hire mules to conduct transactions. In addition, systems like Webmoney are becoming much more widely used, as evidenced by expanding international collaboration between cybercriminals operating in Latin America and Eastern Europe.

Cybercriminal Business Model in Latin America

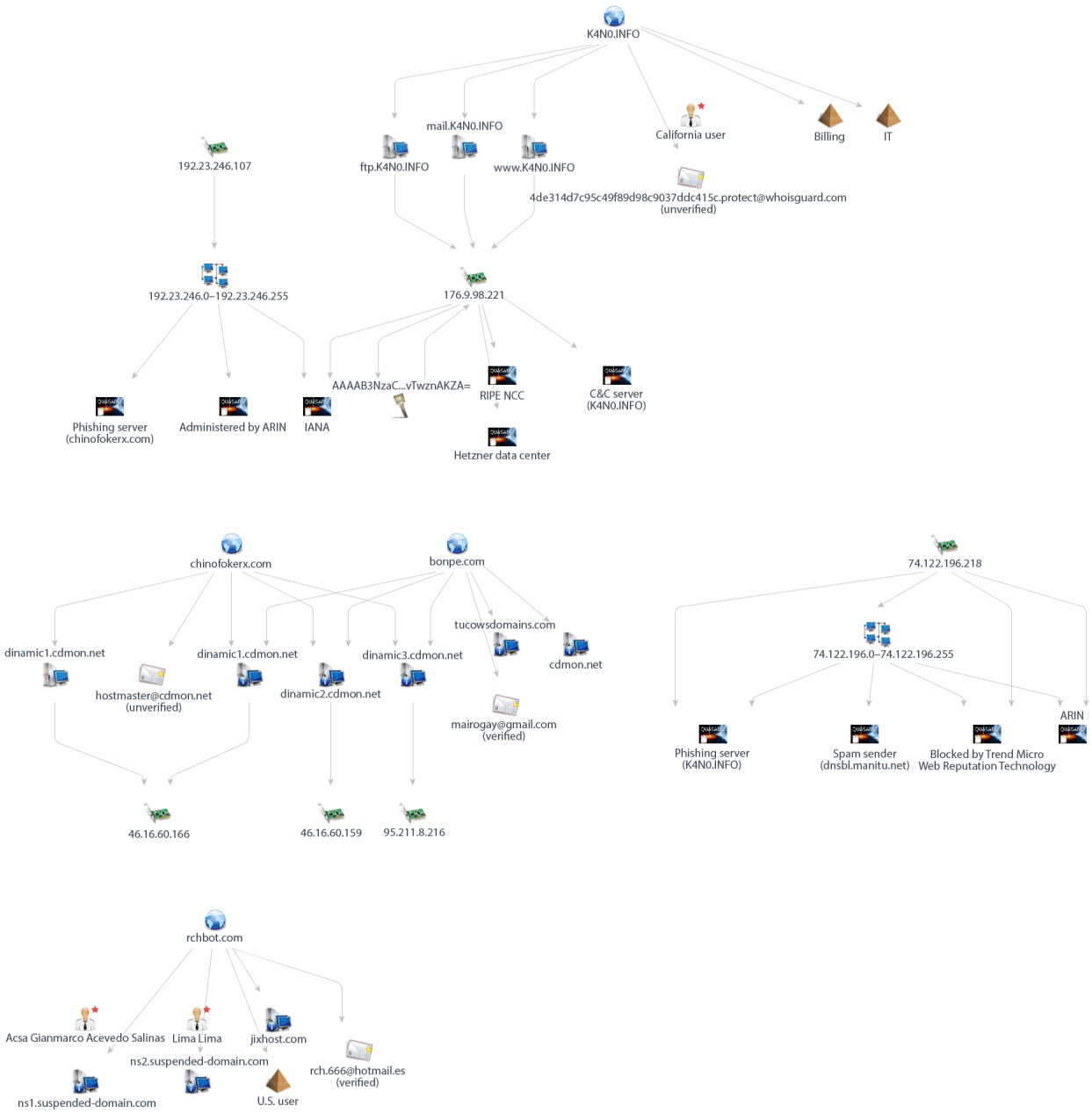


Source: Trend Micro

PiceBOT

Cybercriminals in OAS Member States are increasingly succeeding in custom designing and building their own crimeware kits. In December 2012, PiceBOT, a new crimeware kit that costs US$140, was introduced in Latin America. The malware associated with PiceBOT steals financial information from unsuspecting users and was developed in the region. PiceBOT has heralded a new era of sophistication in cyberthreats in the Americas and the Caribbean. More and more, malware will be homegrown and used against governments, the private sector, and citizens. The increased prevalence of crimeware kits that employ new malicious codes means that more than ever, security systems need to remain updated, administrators need to identify and patch vulnerabilities, and in general increased efforts need to be made to maintain parity with cybercriminals.

PiceBOT's Botnet Structure



Source: Trend Micro

State of Cybersecurity in the Americas

Each country approaches cybersecurity differently, depending on its prevailing economic, political, and cultural landscape. Some countries primarily see cybersecurity as a national security and defense issue. Others see it as having a greater impact on economic development or international competitiveness. Still others view it as an enabler of education, social interaction, and citizen-centric governance, although many countries are wisely trying to incorporate all of these considerations into their cybersecurity regimes. Despite varied approaches, case studies are emerging that will help all countries more efficiently enhance their cybersecurity policies.

Many governments are confronting rapid technological advances with bureaucracies that are slow to adapt, providing hackers and illicit organizations avenues to operate with little worry of prosecution or capture. One of the main impediments to curbing illicit cyber activity in 2012 was the lack of adequate legislation and robust cybersecurity policies. Paired with inexperienced cybercrime investigators and the shortage of prosecutors who specialize in technology-related offenses, many countries are facing difficulties deterring and prosecuting hackers and other cybercriminals.

In surveys submitted to the OAS, countries consistently discussed a need for highly skilled professionals who can secure networks, diagnose intrusions, and effectively manage cyber incidents as they unfold. This problem is manifested in the region by low enrollment in technical-degree programs. Given the time it takes to acquire cybersecurity skills and expertise, this low enrollment may have a noticeable impact in the coming years.

Compounding difficulties facing incident responders, investigators, prosecutors, and network administrators is the persistently low level of cybersecurity awareness among Internet users. Governments believed that public interest in cybersecurity remained fleeting and inconsistent, and most have yet to implement effective, large-scale awareness-raising campaigns.

In any case, the increased frequency of attacks and the associated publicity they received gave rise to changing attitudes and concrete improvements in cybersecurity in the region. While Internet users continue to be largely disengaged from the risks cyberthreats pose, governments are being roused to action and achieving positive results for their efforts. Several countries have adopted comprehensive cybercrime frameworks, taking into account both substantive and procedural laws. Others have expressed interest in adopting such frameworks and have begun to marshal resources and political will to the same end. Even countries with robust legal frameworks, however, continue to face difficulties in implementing and institutionalizing new norms, underlining the crippling effect of low levels of expertise in information security.

* Note that the information in this section came from the OAS country surveys.

Government Cybersecurity Policies

Many OAS Member States began their cybersecurity efforts by establishing CSIRTs. In fact, most countries, save some Caribbean states, now have national-level incident response capabilities. These CSIRTs represent the full spectrum of development. Some provide varied incident response and prevention services, while others are still facing difficulties protecting their networks. Problems facing the latter group are complicated by difficulties securing human and financial resources, precluding improved operations. Even the Caribbean states that have not yet established a national CSIRT have acknowledged the important role cybersecurity plays in economic and social development. Some maintain cyberforensic labs or will shortly launch CSIRTs. Still, significant barriers remain, including those particular to small island states. Even where operating a CSIRT may not make sense, Caribbean countries are taking other practical measures to mitigate cybersecurity risks, including raising awareness and strengthening police cybercrime units, although most governments agree that more needs to be done.[9]

Incident response only represents one area of cybersecurity in which Latin American and Caribbean states have made significant progress. Many are following the recent trend set by countries like Canada, Estonia, Germany, Japan, the United Kingdom, and the United States, and beginning to draft comprehensive national cybersecurity policies and strategies. With the support of the OAS, Colombia became the first Latin American country to adopt a comprehensive national cybersecurity and cyberdefense strategy. Countries like Chile, Peru, Mexico, Trinidad and Tobago, Uruguay, and others are endeavoring to do the same. Emulating those adopted by North American and European governments, Latin American and Caribbean strategies identify key stakeholders, delineate roles and responsibilities, establish coordination and information-sharing mechanisms, and prepare strategic action plans for national cybersecurity efforts.

Recent acknowledgment of vulnerabilities in critical infrastructures has spurred several OAS Member States to adopt initiatives seeking to strengthen their ICS security. Argentina, for instance, will host the “2013 Meridian Conference” on critical infrastructure protection, the first Latin American country to do so.[10] Panama’s development of a national strategy also stressed the importance of protecting important ICS, especially those whose compromise would negatively affect businesses on a global scale. Mexico similarly acknowledged the acute risks that threats to ICS pose and supported specialized training for many of its incident response technicians. These three countries are just a few of those working to secure the increasingly important yet still vulnerable ICS in the region. Many others are studying technical- or policy-based measures for securing their most important infrastructures.

9 Agreements have been reached during the August 2012 Cybersecurity and Cybercrime Workshop for the Caribbean and during the 2013 OAS Permanent Council Meeting of the Committee on Hemispheric Security on “Special Security Concerns of Small Island States of the Caribbean.”

10 https://www.meridian2012.org/pages/the-conference

Inter-American Cybersecurity Efforts

Overall, OAS Member States have shown unity on cybersecurity issues. While the European Union (EU) adopted a Cybersecurity Strategy in February 2013, OAS Member States unanimously adopted the Comprehensive Inter-American Cybersecurity Strategy nine years earlier in 2004. As the threat landscape and government efforts evolved, they also approved a declaration on "Strengthening Cybersecurity in the Americas" in March 2012. Adopting these documents proves that while much work still needs to be done and states espouse differing opinions on how to best achieve cybersecurity, strong political consensus exists in the Western Hemisphere, which helps facilitate regional cooperation and information sharing. Working with and through the OAS, Member States have been able to reach an agreement on a difficult topic. OAS resolutions and declarations have engendered a collaborative atmosphere, allowing the General Secretariat of the OAS to provide technical assistance and improve member states' cybersecurity on many levels.

Case Studies

Argentina

The Argentinean government established the National Office of Information Technology (ONTI) to assess and implement a system of modernization and efficiently use digital resources. Through this office, the Argentine Computer Emergency Response Team (ArCERT) was created in 2005, making Argentina one of the first countries in Latin America to operate a national CSIRT. Early on, efforts focused on digital inclusion, universal access provision, and raising cybersecurity awareness.

To mitigate emerging threats to ICS, in 2012 Argentina created the ICIC, or National Program of Critical Information Infrastructure and Cybersecurity, which is specifically tasked with protecting the country's critical infrastructure.

The ONTI is currently working on the second draft of the National Cyber Security and Critical Infrastructure Protection Plan 2013–2015. This Plan is based on four pillars: awareness raising, securing digital assets, promoting judicial and academic understanding of information security and critical information infrastructure, and promoting lasting security partnerships between the government, businesses, and civil society organizations.

Colombia

In mid-February 2012, Colombia led "Operation Unmask," a multinational operation aimed to take down a ring of transnational cybercriminals and hacktivists that was launched in response to persistent attacks on critical infrastructures in Chile and Colombia. The operation was notable since it depended on collaboration between incident response teams and law enforcement bodies from Argentina, Chile, Colombia, and Spain. Indeed, raids were simultaneously carried out at 40 sites in 15 different cities. In total, Operation Unmask led to the arrest of 25 criminals and the capture of 250 computing devices, along with numerous stolen credit cards and cash.[11]

11 http://www.interpol.int/News-and-media/News-media-releases/2012/PR014

In 2011, Colombia adopted a comprehensive cybersecurity and cyberdefense strategy known as "CONPES 3701." The technical cybersecurity and cyberdefense aspects of CONPES are managed by three entities:

- **Centro Cibernético Policial (CCP) or the Police Cyber Center:** Responsible for ensuring the integrity of police and civil society networks; maintains robust investigative capability.
- **Comando Conjunto Cibernético (CCOC) or the Joint Cyber Command:** Military unit responding to attacks against the nation's military assets.
- **colCERT:** National-level coordinating entity that overseas all aspects of cybersecurity and cyberdefense.

Colombia recently requested accession to the Council of Europe Cybercrime Convention and hopes to join the treaty in 2013, complementing its policy and technical advances with a robust suite of cybercrime legislation.

Jamaica

In 2012, Jamaica revised its cybercrime legislation, expanded the capabilities of the Communication Forensic and Cybercrime Unit (CFCU) of the Jamaica Constabulary Force, and took steps to formally establish a CSIRT. Showing its increasing technical and investigative capabilities, the CFCU was responsible for the investigation and arrest of a high-profile hacker who had levied successful attacks against the country's critical infrastructure. To maintain parity with emerging threats, the unit maintains a robust digital forensic laboratory that is continuously audited and updated.

The Jamaican Ministry of Science, Technology, Energy, and Mining has been leading government efforts to improve its cybersecurity strategy and policy. In 2012, the ministry oversaw the creation of the National Cybersecurity Task Force that comprises all relevant government agencies and other stakeholders.

Mexico

The Mexican government initially only had one unit in the Secretariat of Public Security tasked to respond to cyberthreats. Increased frequency of cyber incidents impelled the creation of a new Coordination Center for the Prevention of Electronic Crimes. The center is responsible for managing cyber incident response, investigating electronic crimes, analyzing digital evidence, protecting critical infrastructures, and responding to digital threats that would affect the integrity of critical networks.

In addition, the National Specialized Cyber Incident Response Team was created to augment government capabilities. Technicians for this team are highly qualified and continuously trained to ensure knowledge of emerging hacking tools and techniques. This group monitors and secures the federal government's digital assets.

Panama

In March 2013, Panama officially adopted its National Strategy for Cybersecurity and Protection of Critical Infrastructures, joining Colombia as the only Latin American country with a comprehensive cybersecurity plan. The strategy is founded on six pillars:

1. Ensuring privacy and confidence in the use of ICT
2. Eliminating the illicit use of ICT
3. Ensuring continuity of critical infrastructures
4. Developing industry-friendly cybersecurity norms
5. Promoting a culture of cybersecurity
6. Protecting state-owned networks

The strategy will be implemented piecemeal through 43 specific tasks or processes, which include developing a large-scale national awareness-raising campaign and creating sector-specific CSIRTs.

Panama has also submitted a formal request to join the Budapest Convention to the Council of Europe.

Conclusion

We are currently living through a watershed period in cybersecurity. News of large-scale cyber incidents fill daily reports and are increasingly becoming the object of political deliberation and doomsday scenarios. Our greatest fear—of cyber attacks crippling infrastructures or creating chaos and economic depression—has luckily not yet come to pass. But to keep pace with those seeking to exploit digital vulnerabilities, more needs to be done. In the Americas and the Caribbean, individuals need to take note of how they use the Internet and ensure that they take any and all precautions to protect their data and devices from abuse. The Internet is a shared asset and cybersecurity is a shared responsibility, meaning individuals need to take ownership of and practice safe habits online. Dependence on ICT will likely continue to grow unabated. Accordingly, governments need to take appropriate measures to protect and secure their critical infrastructures by continuing or beginning to promote cybersecurity planning and legislation; increasing international cooperation; and engaging all relevant stakeholders, including the private sector.

Data gathered by the OAS and Trend Micro has led to conclusions in five major areas:

- State of government response to cybercrime
- State of Internet use
- State of the threat landscape

- State of the attack landscape
- State of the cybercriminal underground

State of Government Response to Cybercrime

Member State responses to cybercrime remain uneven. Many governments began taking serious steps to strengthen cybersecurity following the adoption of the 2004 OAS Cybersecurity Strategy. On the whole, political leaders are aware of the dangers that hackers and cybercriminals pose to development and public safety. Political will, however, does not always lead to changes in the status quo. In Latin America, efforts are most often hamstrung by two things—lack of resources dedicated to building cybersecurity capacity and shortage of specialized knowledge and expertise to implement technical policies or capabilities.

Latin America still faces budgetary constraints, and spending plans do not often contemplate large expenditures on things like IT security. Funds are more often spent on hard security, although this will likely change as cyber-risks increasingly pose threats to physical and economic well-being and government stability. In any case, it is important to note that despite constrained budgets, countries can still make great strides in cybersecurity. Uruguay, for instance, has developed a robust CSIRT and overall cybersecurity capability with minimal financial resources. Other countries have studied and implemented cost-effective awareness-raising programs to educate citizens. The amount of free cybersecurity software to which countries have access is astounding, although countries are not always able capitalize on opportunities.

The shortage of specialized knowledge and expertise needed to implement technical initiatives could be attributed to low enrollment in technical-degree programs. The lack of qualified experts in the Americas means that countries are virtually drowning in an unusable sea of open source cybersecurity software and educational materials. Some countries experience this shortage more than others, but the problem can be aided by international cooperation. The OAS will continue to promote networking and facilitate the exchange of best practices and professional knowledge within and between Member States. By ensuring the flow of information, countries can continue to add value to trainings and lessons learned.

In the context of the two aforementioned shortcomings, countries are struggling to raise awareness among their citizens and experiencing difficulties to maintain momentum in implementing technical and policy-based solutions to cybersecurity problems. Some governments do not have a central repository for information on cyber incidents. Some do not have the capability to respond to incidents. Even those that have taken certain steps experience problems with sharing information across ministries and departments. This reality was reflected again and again in the OAS government surveys.

But countries are moving in the right direction. The aforementioned success stories highlighted just a few initiatives that Member States have adopted. Awareness of cybersecurity issues is increasing every day and governments are striving to improve their policy instruments. Much work still needs to be done, however, to keep pace with those seeking to corrupt critical networks and abuse personal information.

State of Internet Use

Internet use in Latin America is increasing at one of the highest rates worldwide. Unfortunately, the number of digital citizens has not been accompanied by a proportional increase in protocols and infrastructures to keep people safe online. Responses to the OAS survey and Trend Micro data show that unsafe cyberhabits fed the high levels of cybercrime. The number of computer infections indicates that users are not keeping their anti-malware solutions up-to-date and continue to use storage devices while paying little attention to security concerns. Technical data was confirmed by government opinions that citizens, by and large, remained unconcerned and unaware of the dangers that cybercrime and hacking present.

For all these shortcomings, there are encouraging signs. Numerous nongovernmental organizations like USUARIA and STOP. THINK. CONNECT.[12] are active in the region. They have partnered with the OAS and with Member States to design and disseminate large-scale awareness-raising campaigns. Amid a plethora of vulnerable cybercitizens, a growing body of experts and organizations concerned with improving the resilience of networks by educating Internet users is emerging. The OAS actively promotes partnerships between governments and nongovernmental organizations like USUARIA and STOP. THINK. CONNECT., and is evidenced by positive results.

State of the Threat Landscape

Data from OAS Member States and the Trend Micro Smart Protection Network showed that cybercriminals launched a mix of politically and financially motivated attacks in 2012. Organized crime groups are becoming cybercapable and hacker syndicates are growing in number and sophistication. As such, governments need to continue strengthening coordination and information-sharing mechanisms with law enforcement agencies, ISPs, and the private sector to dismantle forums, bulletproof hosts, and implement alternatives to the payment channels that cybercriminals currently use.

New techniques and malware enable attackers to target ICS and other critical infrastructures. Indeed, the number of attacks against utilities, banks, water-purification plants, and other purveyors of essential services is on the rise. Scans have found that many ICS are connected to the Internet and vulnerable to cyber attack. Critical infrastructure operators need to implement norms and policies that contemplate cybersecurity, given the role that their services play in the society. Securing ICS presents particular problems since public-private partnerships (PPP) are inextricably linked with critical infrastructures. Again, this reinforces the need for all sectors and key stakeholders to remain engaged and collaborate on cybersecurity issues. Cybercriminals have no problem sharing information and collaborating across languages and borders; in this respect, we need to strive to be like them.

12 http://stopthinkconnect.org/

State of the Attack Landscape

One of the most surprising data points Trend Micro uncovered is that file infectors plagued the most citizens' computers. This often indicates the prevalence of insufficiently secured removable storage devices and unpatched OSs and/or applications. The continued viability of file infectors reflects the difficulties the region has been experiencing to protect itself from malware, which again is evidence of a lack of user awareness.

State of the Cybercriminal Underground

The cybercriminal underground in Latin America heavily relies on banking Trojans compared with other regions that use other malware like ransomware and ATSs.

Threat actors in the region learn from the mistakes of their criminal colleagues in other regions, notably in Eastern Europe. They recognized that the use of hijacked servers contributed to successful law enforcement operations, and have consequently shifted to using free hosting services to carry out malicious activities. Law enforcement agencies need to take note of this region-specific tactic and adjust their policing and investigation tactics accordingly.

Threat actors and their illicit economic operations heavily relied on Orkut and IRC services, which served as underground bazaars for the exchange of money and criminal goods and services. These processes were often facilitated by mules effecting payments to mask the identities of those organizing the schemes.

Recommendations

Based on the observations of OAS Member States and the data Trend Micro collected, three recommendations can be made:

1. Raise awareness of safe cyberhabits and general cybersecurity awareness among end users, critical infrastructure operators, and government employees. This will make it more difficult for cybercriminals to perpetrate attacks that were so common against the three aforementioned groups. Raising awareness can be one of the cheapest and most effective ways to minimize cybersecurity risks and close security gaps that remain wide open.

2. Invest in and promote enrollment in technical-degree programs. Securing government-owned and private networks requires technical know-how that is difficult to acquire in the short term. Along with awareness-raising campaigns in schools, academic institutions need to do more to attract students to computer science and information security degree tracks. This will ensure that there remains an ample pool of qualified candidates from which to draw professionals who will be needed to fill the increasing number of information security careers.

3. Continue to strengthen policy mechanisms to assign governmental roles and responsibilities related to cybersecurity and to codify information-sharing and cooperation mechanisms. This work has already begun but it is time for all states to strategically think about how they will develop their cybersecurity regimes, where they will focus their efforts, and how they will make their visions a reality.

References

- http://about-threats.trendmicro.com/malware.aspx?language=au&name=TSPY_QHOST.AFG
- http://blog.trendmicro.com/trendlabs-security-intelligence/esthost-taken-down-biggest-cybercriminal-takedown-in-history/
- http://blog.trendmicro.com/trendlabs-security-intelligence/latin-america-router-compromising-malware-found/
- http://blog.trendmicro.com/trendlabs-security-intelligence/new-crimeware-in-bancos-paradise/
- http://latinamericacurrentevents.com/head-of-major-credit-card-cloning-ring-arrested-in-colombia/18040/
- http://stopthinkconnect.org/
- http://www.interpol.int/News-and-media/News-media-releases/2012/PR014
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-evolved-threats-in-a-post-pc-world.pdf
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_automating_online_banking_fraud.pdf
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_blackhole-exploit-kit.pdf
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-police-ransomware-update.pdf
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_police_trojan.pdf
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf
- https://www.meridian2012.org/pages/the-conference

May 2013 / Mayo de 2013

1889 F Street, N.W.,
Washington, D.C., 20006
United States of America

www.oas.org/cyber/

Organization of
American States

Secretary General
José Miguel Insulza

Assistant Secretary General
Albert R. Ramdin

Secretary for Multidimensional Security
Adam Blackwell

Latin American and Caribbean Cybersecurity Trends and Government Responses

Tendencias en la Seguridad Cibernética en América Latina y el Caribe y Respuestas de los Gobiernos

Executive Secretary of the
Inter-American Committee against Terrorism
CICTE
Neil Klopfenstein

Editors
Brian Dito
Belisario Contreras
Tom Kellermann

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

TREND MICRO INCORPORATED

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003

www.trendmicro.com

Securing Your Journey to the Cloud