LATIN AMERICAN +CARIBBEAN CYBER SECURITY

TRENDS

Published June, 2014

Organization of American States

Symantec

CONTENTS

Contributors

Organization of American States

Organization of
American States

Symantec

Symantec

AMERIPOL

Anti-Phishing Working Group

APWG

The Internet Corporation
for Assigned Names & Numbers

ICANN

Lacnic

lacnic

Microsoft

Microsoft

OAS Foreword

June 2014

A top priority for the Organization of American States (OAS) is to support our Member States' efforts and initiatives aimed at strengthening capacities for a more secure, stable, and productive cyber domain.

In 2004, OAS Member States formally recognized that combating cyber-crime and strengthening cyber resilience were imperative to economic and social development; democratic governance, and national and citizen security. Member States also recognized that in order to effectively confront evolving cyber threats and vulnerabilities, users, operators, and regulators of the Internet are in need of timely and accurate information. In response to this need, the OAS-Symantec report on *Latin American and Caribbean Cyber Security Trends* aims to continue the mapping-out process of the cyber ecosystem in Latin America and the Caribbean, a crucial step in implementing evidence-based cybersecurity capacity building.

Specifically, we at the OAS, at the request of Member States have promoted cooperation between the public and private sectors, as well as academia and end users to strengthen cyber resilience and protect critical infrastructure. Most recently, we sent a high-level delegation of international experts to Colombia in response to a request by President Juan Manuel Santos for a comprehensive cyber assessment. The mission resulted in a series of recommendations and actions to be taken on cybersecurity which are currently being considered by the Colombian government.

While there are many similar success stories, there are also significant challenges for our region. Where crimes or other illicit cyber incidents occur, Member States need to be equipped with the capacity to effectively prevent, mitigate, respond to, and where appropriate, investigate and prosecute any criminal misconduct. Moreover, in order to protect individual users – who in today's digital world are increasingly at risk, national authorities need to promote a culture and awareness of cybersecurity to equip individuals with the knowledge required to protect themselves and their information. As Member States have highlighted, building a culture of cybersecurity requires collaborative efforts and coordination among all national stakeholders.

Indeed, effective partnerships between the private sector and civil society entities are especially important in strengthening cybersecurity, as non-government entities manage and operate much of the critical infrastructure on which we rely; this not only refers to our internet infrastructure, but also that which controls transportation, health, banking, energy, and numerous other sectors. In Davos, Switzerland, for example, I met with business, government, and cybersecurity thought leaders for a discussion of the World Economic Forum's Risk and Responsibility in a Hyperconnected World initiative. This and many other events show the growing importance of cybersecurity as a key global issue.

Bearing this in mind, the report represents a multi-stakeholder effort, with contributions from Symantec, AMERIPOL, Microsoft, LACNIC, ICANN, and the Anti-Phishing Working Group. The report also provides a truly comprehensive landscape of cybersecurity in the Americas, with information submitted by 30 out of the 32 countries in Latin America and the Caribbean.[01] Together, the information has served to provide the clearest picture to date of where the region stands with regards to the cybersecurity. We acknowledge, however, that this is merely a snapshot in time of a dynamic landscape. As such, it is expected that this report will evolve to reflect the changes in this area, and will therefore be updated, should new and relevant information emerge. In this way, the report will serve as a basis for which to identify areas in need of improvement and develop evidence-based strategies in a time-sensitive manner. We hope that this information will be of assistance in guiding and strengthening all of our efforts going forward, particularly as we develop partnerships with others who are similarly engaged in the essential mission of building a safe, secure, and stable digital world.

Sincerely,

Amb. Adam Blackwell

Secretary for Multidimensional Security

Organization of American States

01 Bahamas contributed information to the report anonymously; it was integrated into the general summary and trends sections.

Symantec Foreword

June 2014

Symantec has a long and successful history of participating in public-priviate partnerships around the world. We believe that effective sharing of information on cyber threats, vulnerabilities, and incidents are an essential component of improving cybersecurity and combatting cybercrime. As such, we are pleased to partner with the Organization of American States (OAS) in developing this report, *Latin American and Caribbean Cyber Security Trends.*

In today's connected world, we rely on technology for virtually every aspect of our lives, from mobile banking to securing our most critical systems. As the use of technology increases so does the volume and sophistication of the threats. Criminals are constantly looking to exploit new vulnerabilities in order to steal money, intellectual property, and identities. Compounding the challenge, cyberspace is a domain without borders, where crimes are often committed at a great distance. In effect, every computer in the world is a potential entry point, making investigation and prosecution of cybercrimes a difficult task.

In 2013, we saw increases in data breaches, Banking Trojans, mobile malware and other online threats. Hacktivism also continued to be a challenge facing many governments in the region, although there are indications that for some countries, this trend may be diminishing. In this report, you will find an in-depth analysis of these trends along with precautions that users can take to protect themselves more effectively. In addition, the report details a number of other alarming new trends and vulnerabilities globally, as well as those specific to Latin America and the Caribbean.

Latin America and the Caribbean have one of the fastest-growing Internet populations in the world, giving rise to a number of significant cybersecurity challenges both today and in the future. This report is intended to provide readers with an informed overview of the threat landscape as well as some practical recommendations for improving cybersecurity to keep pace with the evolving threat. At Symantec, we are committed to improving information protection across the globe, and will continue working to partner with industry, governments and civil society on ways to do so.

Sincerely,

Cheri F. McGuire

Vice President,
Global Government Affairs
& Cybersecurity Policy

Symantec Corporation

Introduction

This report provides an overview of cybersecurity and cybercrime-related developments in Latin America and the Caribbean in 2013. It assesses the major trends in the region in terms of the threats to the cyber domain and those who depend on it, from government institutions to private enterprises to individual users. It also takes stock of the advances made by government authorities to better address the challenges they face in an increasingly connected and ICT-dependent world.

The research for and writing of this report was carried out jointly by the Organization of American States and Symantec, with additional input and support from AMERIPOL, Microsoft, the Latin American and Caribbean Network Information Center (LACNIC), the Internet Corporation for Assigned Names and Numbers (ICANN), and the Anti-Phishing Working Group (APWG). The OAS and AMERIPOL leveraged their network of official contacts with governments throughout the region, and in particular those national agencies or institutions leading cybersecurity and/or cybercrime related efforts.[01] Symantec gathered information through its global network, which is made up of more than 41.5 million sensors and records thousands of events per second. Spam, Phishing, and Malware data provided by Symantec is captured through a variety of sources including a system of more than 5 million decoy accounts, and a threat detection network processing over 8.4 billion email messages each month and more than 1.7 billion web requests each day across 14 data centers. Other partners contributed information according to their areas of expertise. For example, ICANN's research discusses the stability of the internet in the Americas; the APWG enumerates phishing and malware attacks in the region; and Microsoft highlights general cybersecurity trends, with a focus on malware. LACNIC's research centers on the security and resiliency implications of the internet's global routing system.

The information reported by government authorities and collected by Symantec and others yielded useful insights in terms of the trends observed in the region, the steps being taken to address them, and those areas where significant gaps or deficiencies remain.

01 Government authorities provided information voluntarily, and were able to indicate whether that information could be shared publically or referenced anonymously. All such preferences were respected in the writing of this report.

Executive Summary

2013 was another important year for cybersecurity and cybercrime-related activities in Latin America and the Caribbean. The digital divide continued to shrink as the region again experienced some of the world's highest rates of growth in connectivity. More users, more devices and systems, more networks, and more services all translated to more opportunities and benefits for more people. But it also meant increased threats and vulnerabilities, more victims, and higher costs, financial and otherwise.

The governments of the region strove to keep pace with the evolving landscape, and achieved some notable advances at both the regional and national levels. At the regional level, despite persistent obstacles and complications, responsible national authorities including national Computer Security Incident Response Teams (CSIRTs, also commonly referred to as CERTs or CIRTs) and law enforcement agencies shared more information and cooperated at a technical level more actively than ever before, often with positive results. For many countries cooperation in real-time in response to unfolding incidents or criminal activities became more commonplace, as well as more efficient and effective. Regional and international partners continued to play a key role in bringing officials together to build capacity, strengthen relationships, and share knowledge and experiences, as well as in providing tailored assistance to individual governments. And while initiatives to develop official regional standards have not borne fruit, there is no question that the bar has been raised in terms of what is expected of national authorities to secure the cyber domain.

Indeed, in 2013 many countries made important strides forward in developing their policy and legal frameworks and building their technical capacities. At least four governments, namely Guyana, Jamaica, Trinidad and Tobago, and Barbados, made significant headway in establishing or operationalizing a national cyber incident response team or capability. Other governments have initiated processes to do the same. While only one country in the Americas, Trinidad and Tobago, formally adopted a National Cyber Security Strategy, the OAS and partner institutions began working with three other countries towards the same end. Numerous laws were adopted during the course of the year, strengthening legal frameworks and enabling national authorities to better respond to, investigate, and prosecute nefarious cyber activities or crimes involving the use of ICTs.

Investments in training and capacity-building showed tangible results, as authorities responsible for incident management or the investigation of cybercrime responded more swiftly and effectively, mitigating the impacts of attacks and netting more perpetrators of crimes. Examples of this are highlighted in many of the individual country reports.

Recognizing that knowledge -- of the risks that come with using ICTs, and how to minimize and mitigate those risks -- is arguably the single most valuable tool that national authorities can develop and deploy to enhance cybersecurity and combat cybercrime, many countries stepped up their awareness raising activities in 2013. Innovative outreach efforts, awareness raising campaigns, and educational programs targeted the full range of stakeholders, including government personnel; business, banks and other private enterprises; students; and the public at large. The partnership campaign STOP.THINK.CONNECT continued to gain traction in the Americas, and now includes five participating government authorities and other stakeholders throughout the

region, with several other national authorities considering joining.

Despite the important advances, if the experience of 2013 demonstrated one most important thing, it is the need for all involved to double-down – on reforming laws and policies, building technical capacity, raising awareness, sharing information, and cooperating with other stakeholders.

A significant imbalance persists in terms of where States stand in their cyber-related development. Some have developed advanced and integrated technical and investigative capabilities, and have the requisite laws in place to utilize those capabilities to full effect. Others remain at or near the starting gate, grappling with the challenges inherent in determining what needs to be done, who needs to be involved, and how to best allocate limited financial human resources. The latter governments can benefit from the experience and expertise of their more advanced counterparts, and initiatives to encourage and facilitate this kind of horizontal cooperation and capacity-building must advance and increase. The OAS and other regional and international partners have a vital role to play here and must continue to tailor capacity building initiatives to countries' needs, exchange lessons learned and good practices in cybersecurity development, and continue to foster stronger partnerships for the benefit of states receiving assistance.

Even the most advanced countries in the region cannot afford to become complacent. Data provided by national authorities and collected by Symantec from the Americas and Caribbean clearly evidences significant increases in the volume of cybercrimes, attacks and other incidents in just about every country in the Hemisphere.

The most commonly reported incidents affecting individual users involved phishing, followed by misappropriation of a person's identity for financial fraud or through social networks. The latter seems to track with the expansion of social networks and their communities of users, now found in every OAS Member State in ever-growing numbers, and is reflected in increased reporting of incidents involving defamation, threats, and cyberbullying. The growth in the use of electronic banking services has brought about a parallel increase in efforts to defraud both banks and their clients, and has caused tremendous – although greatly underreported – financial losses. Unauthorized access to systems and the information they contain is another significant threat area where authorities noted a rise in the number of incidents, particularly involving private companies and small and medium sized enterprises (SMEs). Increasingly, in such situations a ransomware such as Cryptolocker is used in an effort to extort money in order to restore files. Many authorities also reported increases in the number of denial of services attacks against both government and private web sites. Interestingly, however, numerous countries reported a decrease in web defacements and other acts of 'hacktivism', which may reflect government efforts to identify perpetrators of previous incidents.

On the whole, as the volume of illicit activity has increased and the tools and techniques have become more sophisticated, it has raised the pressure on government authorities to keep up. Personnel responsible for detection, response and investigation have struggled to remain up to date with the latest technologies and exploits, and to develop and maintain proficiencies in specialized areas like forensics, intrusion detection, and malware and vulnerability analysis, among others.

For all the attention rightfully given to more sophisticated cyber attacks and exploitations using malware and hacking techniques, it cannot be overlooked that the prevalence of ICTs in every aspect of our lives has also translated to their increased use in many traditional crimes, both those carried out by individuals as well as organized criminal groups. Child pornography and other forms of exploitation of children and minors remains the largest such area of such on-line criminal activity, despite a host of national and international initiatives seeking to deter it.

Trafficking in arms, drugs and persons is also facilitated by ICTs and the Internet. This has necessitated that law enforcement and judicial authorities acquire the ability to investigate and prosecute crimes in a cyber ecosystem that is ever more complex, through the use of digital forensics, the preservation of digital evidence, and the presentation of that evidence in court. Developing these capabilities, however, requires financial and human resources that few law enforcement agencies have in abundance, if at all.

Recent experience also confirms that governments cannot do the job of securing the cyber domain alone. As the owners and operators of most of the critical infrastructures and systems in the region, and the purveyors of most online services, private sector entities are equally responsible for strengthening cyber resilience and combating cybercrime. Government authorities and key private sector stakeholders must do more to dialogue and share info, build trust, and identify and realize opportunities for collaboration. Developing the relationships and mechanisms for info-sharing and cooperation between national authorities and companies based outside the region, for example in the US, presents an especially urgent challenge.

In citing recent motivations for stepped up cybersecurity-related efforts, numerous national authorities highlighted leaks of government information throughout the hemisphere as a catalyst for action. Broad sectors of society have recognized the role cybersecurity plays in ensuring that privacy and individual freedoms are adequately protected in a rapidly-evolving digital age. While it is to be expected that national authorities seek to secure their assets and information from potential exploitation by other governments, it is vital that such activities do not undermine or otherwise distract countries from working in a more collaborative and open way.

Taken on the whole, the trajectory of cybersecurity and cybercrime-related efforts on the part of governments throughout the Americas and Caribbean was positive in 2013. Important progress and advances were made, as governments took concrete steps to bolster their capacity to better secure their cyber domain and deter and punish acts of cybercrime. Much more remains to be done however, in light of the clear rise in activities by those who would do harm by exploiting vulnerabilities in the cyber domain, and the growing costs of such activities for all of us.

CYBERSECURITY TRENDS IN LATIN AMERICA + THE CARIBBEAN

The Most Important Trends in 2013

Cyber-espionage, privacy concerns, and malicious insiders made headlines and shaped much of the cybersecurity discourse in 2013. Nevertheless, several large scale data breaches at the end of the year showed that cybercrime remains rampant and threats from cybercriminals continue to menace governments, businesses, and individual end users. Cybercrime continued to offer quick profits while the prospects for apprehending hackers and online fraudsters proved to be limited in all jurisdictions. These factors contributed to the high costs of global cybercrime in 2013, which, although inherently hard to measure, is widely estimated to be at least $113 billion – enough to buy an iPad for the entire populations of Mexico, Colombia, Chile and Peru.[01] In Brazil alone, cybercrime costs reached $8 billion, followed by $3 billion for Mexico, and $464 million for Colombia.[02] Globally, eight breaches each exposed 10 million identities or more, and the number of targeted attacks increased. At the same time, lax end-user attitudes towards social media and increased adoption of mobile devices led to an escalation in scams and provided greater opportunity for cybercriminals, as mobile-based social media use plays a greater role in our lives, particularly in Latin America and the Caribbean.

When combined as a region, Latin America and the Caribbean have the fastest growing Internet population in the world, with 147 million unique users in 2013, and growing each year.[03] Mobile devices are proliferating as a preferred method to access the Internet, and especially to use social media. Nearly 95 percent of Internet users in the region actively use social networking sites, and Latin American and Caribbean nations occupy five of the top ten spots for the most time spent on social networks.[04] While today, the Latin America and Caribbean region accounts for only a small percentage of global cybercrime, the rise in Internet use and corresponding cyber attacks emphasizes the need for development of effective cyber policies and defenses.

This report covers the wide-ranging threat landscape in Latin America and the Caribbean. It highlights several key trends and identifies specific threats that emerged from Symantec's analysis of its data and survey results provided by OAS Member States.

2013 Was the Year of the Mega Breach

In addition to a proliferation of financially motivated cyber breaches, hackers infiltrated dozens of companies and governments, including many in Latin America and the Caribbean, to gain access to sensitive information. Globally, there were 253 large-scale data breaches in 2013, a 62 percent rise from 2012.[05] And eight of these exposed more than 10 million identities each, imposing significant expenditures of time and financial resources for response, recovery and added protections on the part of retailers, financial companies, insurance companies, and individuals. By comparison, in 2012, only one breach exposed over 10 million identities.[06]

In 2013, Point of Sale (PoS) data breaches were used as a major vector of attack to steal customers' personally identifiable information (PII). The graphic on the following page walks through the architecture of a PoS breach as well as some of the methods that criminals use to break into corporate PoS systems.

In total, over 552 million identities around the world were exposed in 2013, putting consumer credit card information, birth dates, government ID numbers, home addresses, medical records, phone numbers, financial information, email addresses, logins, passwords, and other personal information into the criminal underground.[07] To put this in perspective, stolen credit cards can be sold for as high as $100 per card on the black market, making data breaches a low risk and simple, yet profitable activity for cybercriminals.[08]

Fig. 1

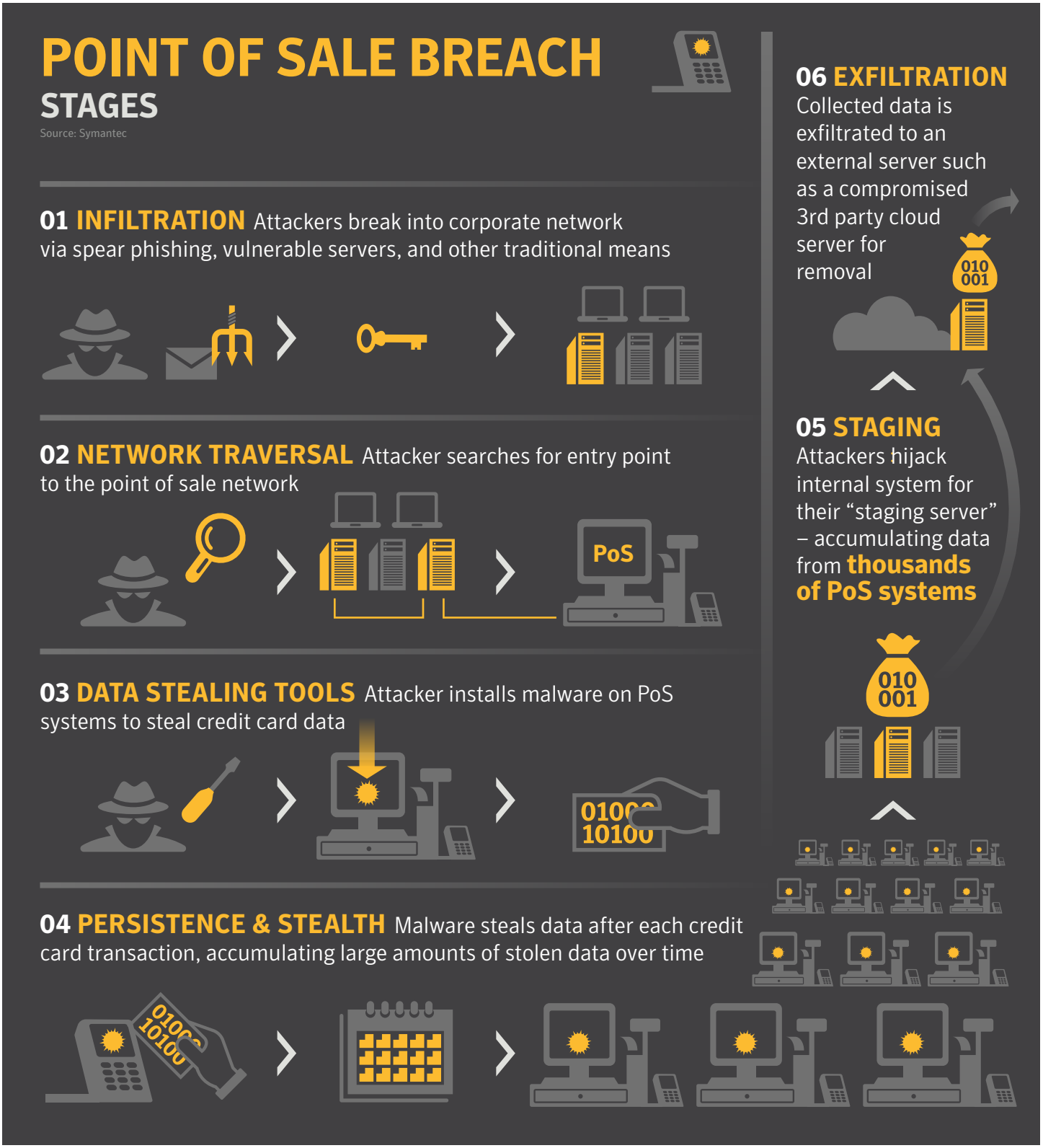

POINT OF SALE BREACH
STAGES
Source: Symantec
01 INFILTRATION Attackers break into corporate network via spear phishing, vulnerable servers, and other traditional means
02 NETWORK TRAVERSAL Attacker searches for entry point to the point of sale network
PoS
03 DATA STEALING TOOLS Attacker installs malware on PoS systems to steal credit card data
04 PERSISTENCE & STEALTH Malware steals data after each credit card transaction, accumulating large amounts of stolen data over time
05 STAGING
Attackers hijack internal system for their "staging server" – accumulating data from thousands of PoS systems
06 EXFILTRATION
Collected data is exfiltrated to an external server such as a compromised 3rd party cloud server for removal
010
001

Fig. 2

Analysis of Spear-Phishing Emails Used in Targeted Attacks (Global)

Source: Symantec

Executable type	2013	2012
.exe	31.3%	39%
.scr	18.4%	2%
.doc	7.9%	34%
.pdf	5.3%	11%
.class	4.7%	<1%
.jpg	3.8%	<1%
.dmp	2.7%	1%
.dll	1.8%	1%
.au3	1.7%	<1%
.xls	1.2%	5%

- *More than 50 percent of email attachments used in spear-phishing attacks contained executable files in 2013.*
- *Microsoft Word and PDF documents were both used regularly, making up 7.9 and 5.3 percent of attachments respectively. However, these percentages are both down from 2012.*
- *Java .class files also made up 4.7 percent of email attachments used in spear-phishing attacks.*

Targeted Attacks Grow and Evolve

The use of malware to steal sensitive or confidential information has been a prevalent attack method since the early 2000s. A targeted attack uses malware aimed at a specific user or group of users within a particular organization and may be delivered through a spear-phishing email or a form of drive-by download known as a "watering-hole" attack. Spear-phishing is an email crafted through social engineering to fool an individual or small group of people for the purpose of a targeted attack. Alternatively, a watering-hole attack requires attackers to infiltrate a legitimate site visited by their target, plant malicious code, and then lie in wait. While targeted attacks continue to rise in Latin America and the Caribbean region, they are evolving. Whereas spear-phishing once was the preferred method attackers used to install malware, watering-hole attacks are slowly supplanting the former in the region. This is not to say that spear-phishing attacks are dead. While the total number of both emails used and targets per spear-phishing campaign has decreased, the number of spear-phishing campaigns themselves saw a dramatic 91 percent rise in 2013.[09] This is to say that these efforts are growing, and also becoming more tailored to potential victims in Latin America and the Caribbean. Brazil, Colombia, and Argentina are the top three sources of phishing attacks in Latin America and the Caribbean. In fact, these three countries contribute 74 percent of all phishing attacks in Latin America and 3.2 percent worldwide.[10]

These "low and slow" approaches—campaigns also ran three times longer on average than those in 2012, increasing from 3 days to 8 days—are a sign that user awareness and protection technologies have driven spear phishers to focus their targeting and improve their social engineering methods. We have also observed the integration of virtual and physical attacks in social engineering schemes, which has been done successfully by cybercriminals.[11]

In 2013, more than 50 percent of email attachments used in spear-phishing attacks globally contained executable files. Executable files have the potential to be dangerous as they can contain malware, or small programs to infect a user's machine. PDF or Microsoft Word documents were both used regularly, making up 7.9 and 5.3 percent of attachments respectively.[12]

Fig.3

TARGETED ATTACK

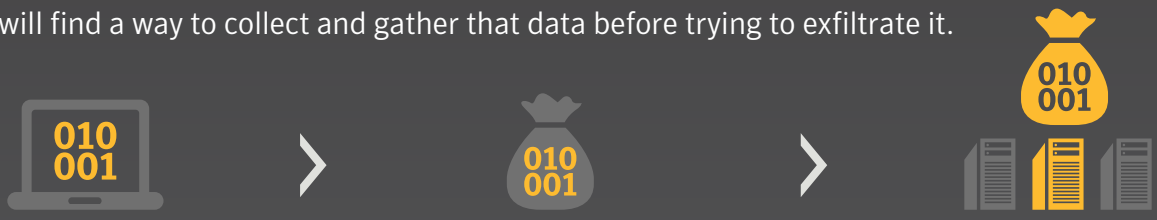
KEY STAGES

Source: Symantec

01 INCURSION The attacker gains entry to the targeted organization. This is often preceded by reconnaissance activities where the attacker is looking for a suitable social engineering tactic.

02 DISCOVERY Once the attacker has gained entry, they will seek to maintain that access as well as discover what data and other valuable resources they may wish to access.

03 CAPTURE Once the valuable data has been discovered and identified, the attacker will find a way to collect and gather that data before trying to exfiltrate it.



04 EXFILTRATION The attacker will find a mechanism to steal the data from the targeted organization. This may be by uploading it to a remote server or website the attackers have access to. More covert methods may involve encryption and steganography, to further obfuscate the exfiltration process, such as hiding data inside DNS request packets.

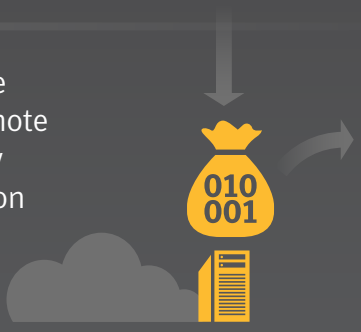
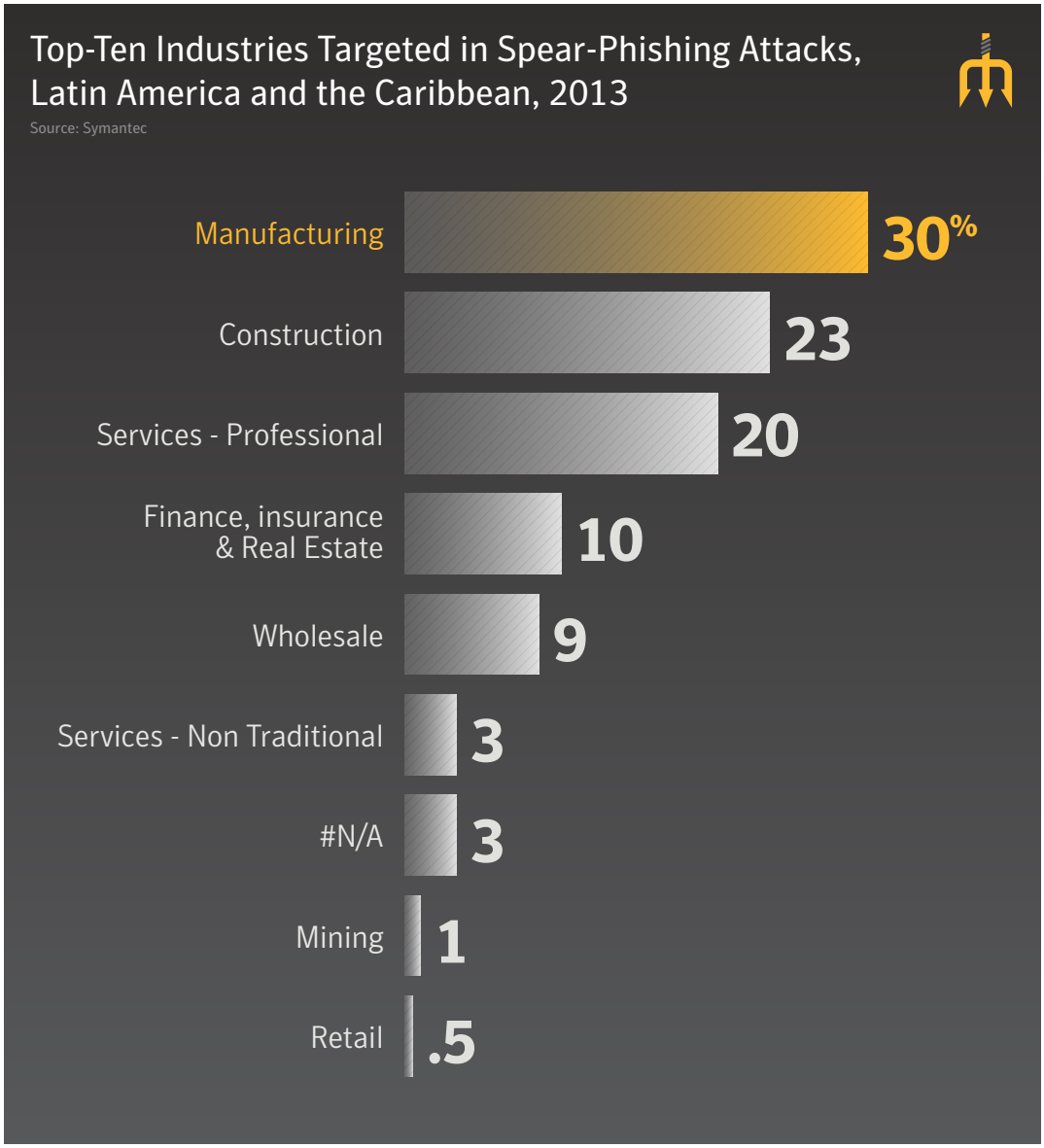


Fig. 4



- *Manufacturing topped the industries targeted in 2013, comprising 30 percent of all attacks in Latin America.*
- *The Professional category includes Engineering, Accounting, Legal, and Heath-related services.*
- *The Non-Traditional category includes Business, Amusement, and Repair-related services.*

Case Study: The Mask [13]

Background

Modern cyber-espionage campaigns are regularly defined by their level of sophistication and professionalism. The cyber-espionage group known as "The Mask," is no exception. Research into this group shows that The Mask has been in operation since 2007, using innovative tools and techniques to compromise, monitor, and exfiltrate data from infected targets. The group uses high-end exploits and carefully crafted emails to lure unsuspecting victims. The Mask has the tools to infiltrate all major operating systems including Windows, Linux, and Macintosh.

Interestingly, "The Mask" uses tools specifically designed to target the Spanish speaking world. For instance, the malware is designed to look for documents in Spanish pathnames such as "Archivos de Programas" instead of "Program Files." The intended targets appear to reside mainly in Europe and South America, and The Mask appears to be one of the first advanced persistent threats (APT) designed either by Spanish-speakers or for use in Latin America.[14]

The Longevity of the Operation

It has been active for seven years, the access to highly sophisticated tools, and the precise and targeted nature of the victims indicate this is a very professional, well organized team of attackers with substantial resources.

Targeting the Victim

The Mask typically infects the victim with a specifically crafted email. Using the lure of a CV (résumé) or political content, the attachments observed have been in the form of malicious PDF or Microsoft Word documents. The following is a sample of some of the attachment names used:

- Inspired By Iceland.doc
- DanielGarciaSuarez_cv_es.pdf
- cv-edward-horgan.pdf

Upon opening the document, the recipient is presented with what looks like a legitimate document, however a Remote Access Trojan (RAT) is also installed, allowing full remote access to the compromised computer. Once compromised, The Mask can then install additional tools for enhanced persistent and cyber-espionage activities.

Cyber-espionage – A Professional Suite

The Mask has a suite of tools at its disposal. One tool in particular distinguishes this group from typical cyber operations. Backdoor.Weevil.B, a sophisticated cyber-espionage tool that is modular in nature, utilizes a plug-in architecture and a myriad of configuration options.[15] This tool is reminiscent of those associated with other sophisticated campaigns such as Duqu,[16] Flamer,[17] and MiniDuke.[18] There is no evidence, however, that The Mask is associated with these campaigns. The default install boasts nearly 20 modules built for intercommunication, network sniffing, activity monitoring, exfiltration, and rootkit capabilities.

The plugin architecture allows for additional modules to be downloaded and loaded as needed. The Trojan can log activity in all the major browsers and has a comprehensive list of file extensions on which to gather information.

The types of documents targeted by the Trojan are:

01 Word, PDF, Excel

02 Encrypted files, PGP keys, encryption keys

03 Mobile backup files

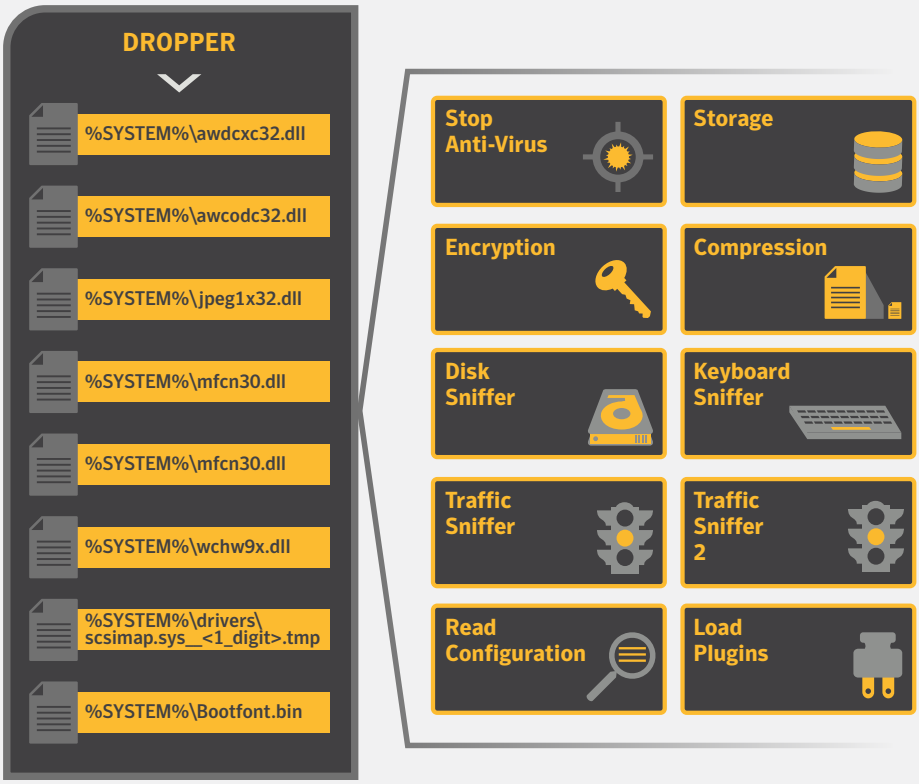
04 Email archives

The information can then be securely exfiltrated to attacker-controlled servers using the HTTPS protocol. The data-stealing component provides clues as to The Mask's targets. It searches for documents in Spanish-language pathnames, for example "archivos de programa", indicating that their targets are running Spanish-language operating systems.

Cyber-espionage campaigns conducted by professional teams are increasingly common. Numerous espionage operations spanning years have been highlighted over the last few years. Examples include Flamer, MiniDuke, and Hidden Lynx.[19] The Mask joins this notorious list but also shows how the targets of these sophisticated campaigns are becoming increasingly diverse. Coinciding with these campaigns has been the emergence of companies that develop tools for use in espionage campaigns. Companies such as Hacking Team and Gamma International provide remote access suites that offer sophisticated surveillance capabilities. All of this serves to highlight how the geographical and technical boundaries of cyber-espionage are expanding.

Fig. 5

Some of The Mask's Modules



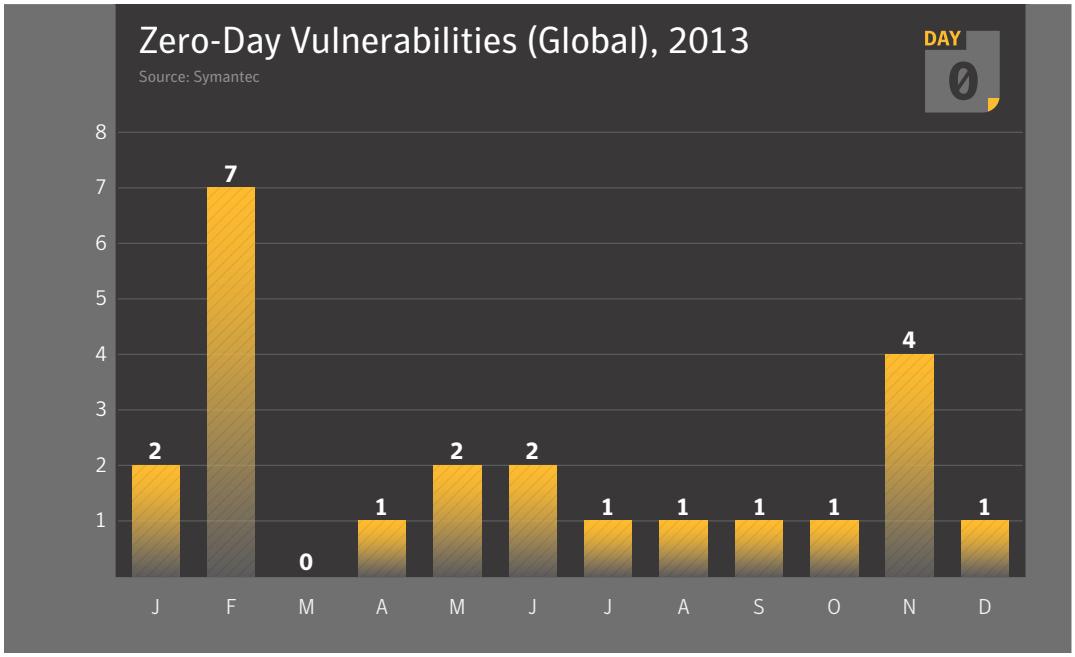
Zero-day Vulnerabilities and Unpatched Websites Facilitated Watering-Hole Attacks

Security researchers discovered more zero-day vulnerabilities in 2013 than in any other year since 2006. The 23 zero-day vulnerabilities discovered last year represent a 61 percent increase from 2012 and total more than the two previous years combined.[20]

A zero-day vulnerability is one that is reported to have been exploited in the wild before the vulnerability is public knowledge and prior to a patch being publicly available. The absence of a patch for a zero-day vulnerability presents a threat to organizations and consumers alike, because in many cases these threats can evade purely signature-based detection until a patch is released. In addition, zero-day vulnerabilities uniquely give attackers the means to infect their victim without having to use email attachments, links, or other methods which may raise undue suspicions. They simply apply these exploits in a watering-hole attack, greatly increasing the chances of evading detection. Unfortunately, legitimate web sites with poor patch management practices have facilitated the adoption of watering-hole attacks. Globally, 77 percent of websites had exploitable vulnerabilities and 1-in-8 of all websites had a critical vulnerability.[21] This gives attackers plenty of choices of websites in which to hide their malware and entrap their victims.

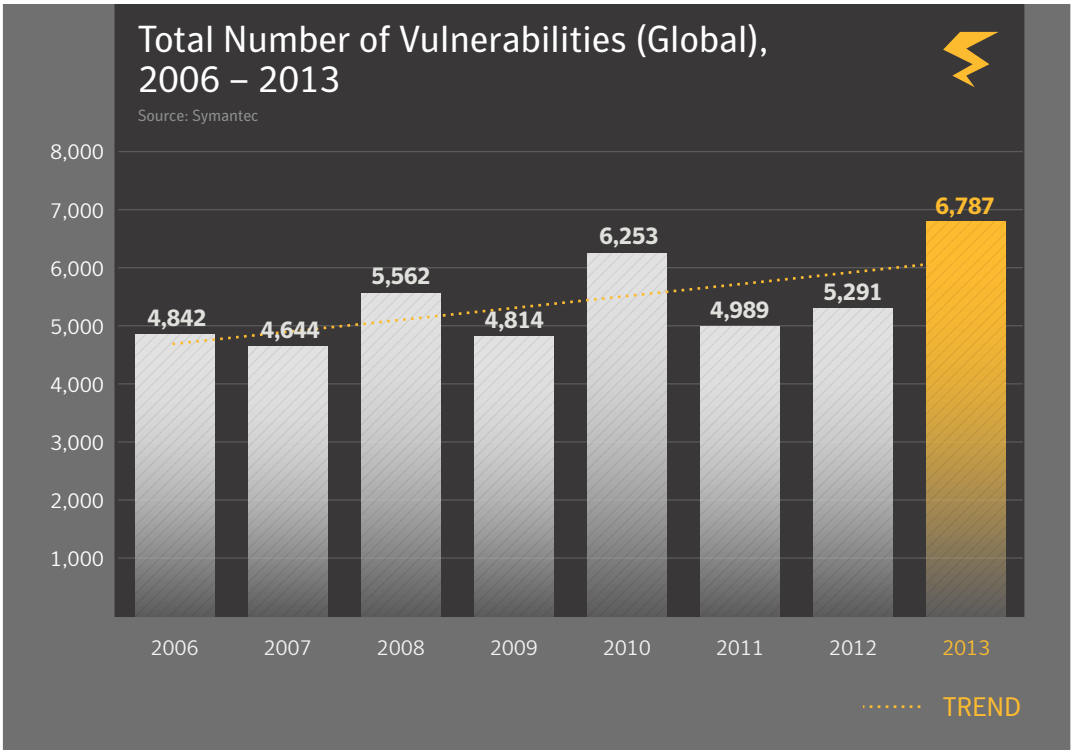
Cutting-edge attackers typically stop exploiting a zero-day vulnerability once it is made public and strive to employ an alternate vulnerability in order to remain undetected. But this does not bring an end to their use. Cybercriminals rapidly incorporate exploits for zero-day vulnerabilities into their toolkits to threaten all of us. Even though the five most prevalent zero-day vulnerabilities were patched on average within four days, in 2013 there were at least 174,651 attacks using these within the first 30 days after their publication and patching, as attackers understand that there is often a delay in patch application that provides a rich target environment.[22]

Fig. 6



- *A zero-day vulnerability is one that is reported to have been exploited in the wild before the vulnerability is public knowledge and prior to a patch being publicly available.*
- *The total number of zero-day vulnerabilities reported in 2013 was 23, compared with 14 in 2012.*
- *The peak number reported in one month for 2013 was 7 (in February), compared with a monthly peak of 3 (June) in 2012.*

Fig. 7



- *There were 6,787 vulnerabilities disclosed in 2013, compared with 5,291 in 2012.*
- *In 2013 there were 32 public SCADA (Supervisory Control and Data Acquisition) vulnerabilities, compared with 85 in 2012 and 129 in 2011.*

Ransomware Attacks Grew in the Region and Became More Sophisticated

Scammers continued to leverage profitable ransomware scams in 2013. Often, the attackers pretend to be local law enforcement, demanding a fake fine typically between $100 and $500 USD to unlock a computer that was ostensibly locked and used by authorities during an investigation. First appearing in 2012, these threats escalated in 2013, and grew by 500 percent globally over the course of the year.[23] Latin America and the Caribbean have indeed followed these global trends. In April 2014, the spread of ransomware prompted the Mexican Police Force to issue a formal public warning.[24]

Ransomware attacks are highly profitable and modified regularly to ensure their continued success. The next step in this evolution was Ransomcrypt, commonly known as Cryptolocker. Cryptolocker is the most prominent new type of ransomware, which, as opposed to posing as law enforcement, explicitly requests a ransom for a targeted users' files to be decrypted. Cryptolocker uses a high-grade RSA 2048 encryption which currently is not possible to break. Unless a user backed up their data prior to a Cryptolocker attack, their data will likely be rendered permanently inaccessible. This threat causes even more damage to businesses where files on shared or attached network drives are also impacted. Research indicates that on average, 3 percent of infected computer users pay the ransom, while the other 97 percent either lose their data, or revert to a backed up version.[25]

Holding encrypted files for ransom is not an entirely new concept, but getting the ransom paid has previously proven problematic for the crooks. With the appearance of online payment methods, Ransomcrypt is poised for growth in 2014. Small businesses and consumers are most at risk from losing data, files or memories. Prevention and backup are critical to protecting users from this type of attack.

Fig. 8 Ransomware example targeting users in Argentina

Fig. 9 Ransomware targeting users in Mexico

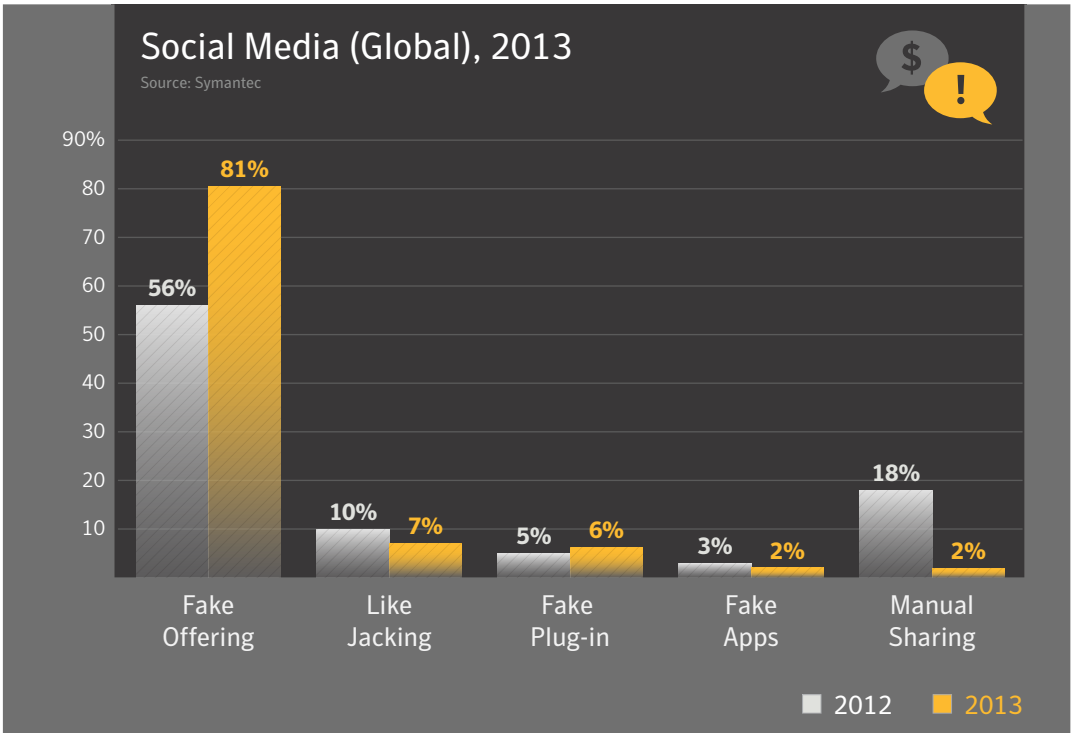
Social Media Scams and Malware Flourish on Mobile

While the prevalence of mobile malware globally is still low compared to that on laptop or desktop computers, 2013 demonstrated that the environment is ripe for marked growth in scams and malware targeting handheld devices. In 2013, a global survey of end-users showed that 38 percent of mobile users had already experienced mobile cybercrime in one form or another.[26] Lost or stolen devices often precipitate malicious mobile activity, but risky behavior of mobile users makes them susceptible to many types of potential attacks.

In particular, mobile users are exhibiting risky behavior by storing sensitive files online (52 percent), storing work and personal information in the same online storage accounts (24 percent) and sharing logins and passwords with families (21 percent) and friends (18 percent), putting their data and their employers' data at risk.[27]

Yet only 50 percent of these users take even the most basic of security precautions, with the other 50 percent foregoing the use of passwords or security software on their mobile devices.[28]

Fig. 10



Fake Offers These scams invite social network users to join a fake event or group with incentives such as free gift cards. Joining often requires the user to share credentials with the attacker or send a text to a premium rate number.

Manual Sharing Scams These rely on victims to actually do the work of sharing the scam by presenting them with intriguing videos, fake offers or messages that they share with their friends.

Likejacking Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.

Fake Plug-in Scams Users are tricked into downloading fake browser extensions on their machines. Rogue browser extensions can pose like legitimate extensions, but when installed steal sensitive information from the infected machine.

Fake App Users are invited to subscribe to an application that appears to be integrated for use with a social network, but is not as described and may be used to steal credentials or harvest other personal data.

- *Fake Offers accounted for the largest number of social media based attacks in 2013, with 81 percent, compared with 56 percent in 2012.*
- *Manual sharing scams have also decreased in 2013, from 18 percent in 2012 to 2 percent.*
- *Micro-blogging based scams accounted for one percent of total attacks detected for the social media category, for both 2012 and 2013.*

The number of new malware families created slowed as malware authors have turned their attention to perfecting existing malware. In 2012 each mobile malware family had an average of 38 variants. In 2013 each family had, on average, 58.[29] Further, events in 2013 indicated that mobile users are highly susceptible to scams through mobile applications. It appears that mobile malware has not yet exploded, in part because would be criminals have other means to achieve their goals.

Users continue to fall prey to scams on social media sites, often lured by a false sense of security conveyed by the presence of so many friends online. Fake offers, such as those purporting to give away free cell phone minutes accounted for the largest number of malicious incidents impacting Facebook users in 2013 – 81 percent in 2013 compared to 56 percent in 2012.[30] Although twelve percent of social media users say someone has hacked into their social network account and assumed their identity, one quarter continue to share their social media passwords, and one third connect with people they don't know.[31]

In Latin America and the Caribbean, nearly 95 percent of Internet users access social network sites. Latin American and Caribbean nations account for five of the top ten countries spending the most time on social networks.[32] As social media becomes increasingly accessed by mobile devices, any risky behavior is likely to have increasingly grave consequences for users and their data.

2014 FIFA World Cup: A Rich Target for Cybercriminals

The 2014 FIFA World Cup in Brazil is expected to be one of the largest sporting events of this century. While the world comes together to celebrate and compete in sport, cybercriminals have unfortunately identified vulnerabilities and may be plotting attacks against critical infrastructure.[33] In fact, members of international hacking groups such as Anonymous have recently made threats against official websites operated by FIFA, the Brazilian Government, and corporate sponsors of the games.

Several malware operations, phishing attacks, and email scams linked to the World Cup have already been discovered. One particular scheme involves a fraudulent CIELO Brazil promotion. It takes the form of a spear-phishing attack that targets users, leading them to a webpage where they are asked to input their username, date of birth, and Brazilian tax registration number (CPF).

Another type of World Cup related attack discovered by Symantec this year involves a sophisticated malware operation targeting financial institutions. Once a user clicks on the infected email to download a "free ticket" to the World Cup tournament, they are then prompted to download an infected file named "eTicket.rar," which to the unsuspecting user may appear to be harmless. Next, a file named "thanks.exe" (Infostealer.Bancos)[34] is dropped into the system and runs every time Windows starts.

The Trojan will continue to run in the background while evading security measures to steal confidential financial information, log the stolen data, and send it to a remote attacker at a later time.

Users in Latin America and the Caribbean should be on guard before and during the tournament for malware and phishing schemes like those cited here.[35] In addition to the threat posed by the World Cup, the 2016 Summer Olympics in Rio de Janeiro is likely to be a major target for cybercriminals employing malware, phishing, email scams, and attacks on banking infrastructure. Similar cyber trends emerged during the 2014 Winter Olympics in Sochi as well as the 2012 Summer Olympics in London, which suggests similar activity during the World Cup and other major sporting events.

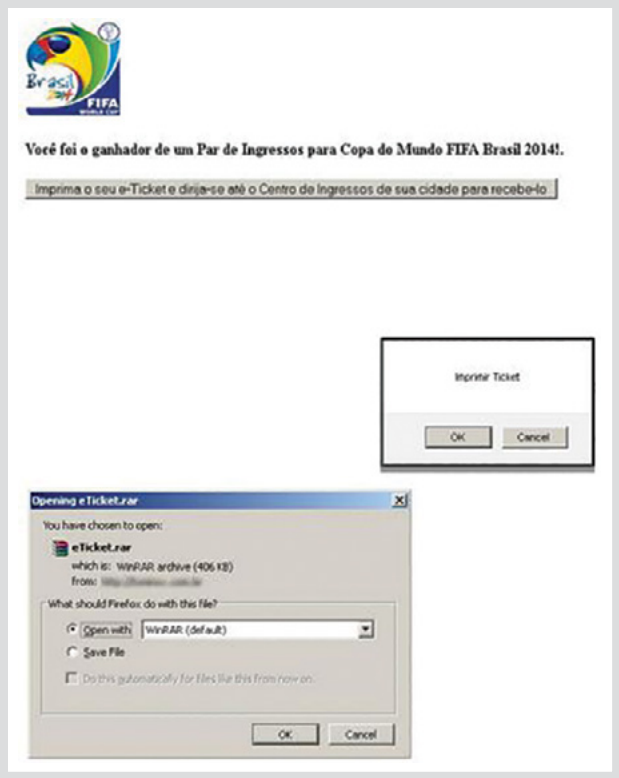


Fig. 11 Clicking the link leads to malicious download of Infostealer.Bancos malware.

Banking Trojans and Heists

Across Latin America and the Caribbean, incidents involving banking Trojans and heists have increased. Today's threats continue to focus on modifying banking sessions and injecting extra fields in the hope of either stealing sensitive banking details or hijacking the session. Some of the most common banking Trojans this year include Trojan.Tylon[36] and a variant of the Zbot botnet called Gameover Zeus.[37] Infostealer.Bancos is highly prevalent in Latin America and the Caribbean. Symantec's State of Financial Trojans 2013 whitepaper concluded that in the first three quarters of 2013, the number of banking Trojans tripled.[38] While more than half of these attacks were aimed at the top 15 financial institutions, more than 1,400 institutions have been targeted in 88 countries worldwide. Browser-based attacks are still common, but mobile threats are also used to circumvent authentication through Short Message Service (SMS) messages, where the attacker can intercept text messages from the victim's bank.

The most common form of attack continues to be financial Trojans which perform a Man-In-The-Browser (MITB) type of attack on the client's computer during an on-line banking session. In a MITB attack, malware resides in the web browser on an individual's device and gets between the user and the website, changing what is seen by the user and altering their account information and finances without their knowledge. Symantec analyzed 1,086 configuration files of 8 of the most common financial Trojans. The malware was configured to scan for URLs, or web addresses, belonging to 1,486 different organizations around the world.

An increase in hardware-supported attacks was also observed in 2013. In addition to the still popular skimming attacks throughout Latin America and the Caribbean, a new piece of malware was discovered named Backdoor.Ploutus which targeted Automated Teller Machines (ATMs).[39] Initially discovered in Mexico, the malware soon spread to other countries, with English versions emerging later.

Case Study: Criminals Hit the ATM Jackpot

First discovered being used by criminals in Mexico, Ploutus is a new way to steal money from individuals' bank accounts. ATMs have always been a common target of thieves, but the challenge there is actually getting the money out of the machine. While there are several ways to accomplish this, an increasingly popular method is ATM Skimming. Skimming is the process of recording the data on the magnetic strip of a credit or debit card so that it can be used later in a fraudulent way. It isn't the easiest way, but it produces the most viable data for fraudsters to sell.Criminals would like nothing more than to make an ATM spew out all of its cash just by pressing some buttons. Unfortunately for banks, it seems as though the criminal's dreams may have come true. In parallel investigations with other security firms, Symantec identified this sample on August 31, 2013, and a detection (Backdoor.Ploutus) has been in place since September 4, 2013.

Infection Methodology

According to external sources, the malware is transferred to the ATM by physically inserting a new boot disk into the CD-ROM drive located on the outside of the machine. The boot disk then transfers malware.

Impact

The criminals created an interface to interact with the software on a compromised ATM, and are able to withdraw all of the available money from the containers holding the cash, also known as cassettes. One interesting aspect to note is that the criminals are also able

to read all of the information typed by cardholders through the ATM keypad, enabling them to steal the sensitive information without using any external device.

Actions Performed by Backdoor.Ploutus

- Generate ATM ID:
  Randomly generated number assigned to the compromised ATM, based on current day and month at the time of infection.
- Activate ATM ID:
  Sets a timer to dispense money. The malware will dispense money only within the first 24 hours after it was activated.
- Dispense cash:
  Dispense money based on the amount requested by the criminals.
- Restart (Service):
  Reset the dispense time period.

The list of commands mentioned above must be executed in order, since the malware must use a non-expired activated ATM ID to dispense the cash.

The source code contains Spanish function names that suggest the malware may have been coded by Spanish speaking developers.

Dispense Process Compromised

It is clear that the criminals have reverse engineered the ATM software and produced an interface to allow them to interact with the machine. This assertion is based on code that Symantec's security experts have reviewed. What this discovery underlines is the increasing level of cooperation between traditional criminals who targeted physical assets and cybercriminals. With the ever-increasing use of technology in all aspects of security, traditional criminals are realizing that in order to carry out successful heists, they now require another set of skills that previously was not a necessity. Modern day bank robbers now need skilled IT practitioners on their team to help them carry out their heists.

And criminals have since started taking it up a notch. Shortly after Backdoor.Ploutus (above) was discovered, a similar variant of the malware was uncovered, Backdoor.Ploutus.B.[40] This variant of Ploutus was particularly interesting because it allowed cybercriminals to simply send an SMS text message to the compromised ATM, then walk up and collect the dispensed cash. It may seem incredible, but this technique is presently being used in a number of places around the world.

Conclusions

The current threat landscape in Latin America and the Caribbean shows that users are being impacted both by threats that are trending globally as well as others that are region-specific. Compounding the challenge, Latin America and the Caribbean has the fastest growing Internet population in the world, expanding 12 percent over the past year. This report has identified the major trends impacting the region:

01 **Data breaches are on the rise.**
Dubbed "The Year of the Mega Breach," over 552 million identities were exposed by data breaches in 2013, putting at risk consumer credit card, financial, medical, and other types of personal information. The source of this trend was led by cybercrime-driven breaches and acts of hacktivism, with hackers accounting for 32 percent of all breaches in 2013.

02 **Targeted attacks continue to grow.**
Attacks against specific individuals or organizations are evolving, with cybercriminals adapting spear-phishing campaigns to be stealthier and adding watering-hole attacks to their toolkits.

03 **Social media scams are on the rise.**
In 2013, cybercriminals sought to exploit the data we share online through social media, and as these sites become increasingly interconnected the security of our data and personal information online becomes more important than ever.

04 **Banking Trojans and heists.**
Across Latin America and the Caribbean, the number of incidents involving banking Trojans has increased significantly. Initially discovered in Mexico, malware targeting ATMs has spread to other countries throughout the Americas, especially in Spanish speaking countries.

05 **Major events provide rich targets.**
The upcoming World Cup in Brazil has already become a major vector for cybercriminals who have engaged in countless malware operations, phishing schemes, and email scams related to the tournament. Global events such as concerts and sporting events tend to be attractive for cybercriminals, and the 2014 World Cup will be no exception. In fact, during the 2014 Winter Olympics in Sochi and the 2012 Summer Olympics in London, numerous targeted email campaigns used Olympic themes to bait potential victims – with one piece linked to a dangerous malware campaign dubbed "Darkmoon."[41]

Footnotes

01 Symantec Corporation, 2013 Norton Cybercrime Report (October 2013), 8. Available at: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

02 Symantec Corporation, 2013 Norton Cybercrime Country-Specific Report (Colombia). Available at: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

03 Jason Kohn, "The Internet is Booming in Latin America, Especially Among Younger Users," Cisco Blogs, October 17, 2013. Available at: http://blogs.cisco.com/cle/the-internet-is-booming-in-latin-america-especially-among-younger-users/

04 Richard Simcott, "Social Media Fast Facts: Latin America," Social Media Today, April 3, 2014. Available at: http://socialmediatoday.com/richard-simcott/2317236/social-media-fast-facts-latin-america

05 Symantec Corporation, Internet Security Threat Report 19 (April 2014), 40. Available at: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf See also the Norton Cybercrime Index

06 Ibid. at 40.

07 Ibid. at 40.

08 Symantec Corporation, "Underground Economy Servers – Goods and Services Available for Sale," Symantec Security Response, 2010. Available at: http://www.symantec.com/threatreport/topic.jsp?id=fraud_activity_trends&aid=underground_economy_servers

09 Symantec Corporation, Internet Security Threat Report 19, 25.

10 ISTR 19, at 33.

11 Symantec Corporation, "Francophoned – A Sophisticated Social Engineering Attack," Symantec Security Response, August 28, 2013. Available at: http://www.symantec.com/connect/blogs/francophoned-sophisticated-social-engineering-attack

12 Symantec Corporation, Internet Security Threat Report Region Specific Data, (April 2014).

13 Stephen Doherty, "The Mask," Symantec Security Response Blog, February 10, 2014. Available at: http://www.symantec.com/connect/blogs/mask

14 Matthew Hilburn, "'Mask' Malware Called 'Most Advanced' Cyberespionage Operation," Voice of America, February 13, 2014. Available at: http://www.voanews.com/content/mask-careto-called-most-advanced-cyber-espionage-operation/1850889.html

15 See "Backdoor.Weevil.B," Symantec Security Response, February 10, 2014. Available at: http://www.symantec.com/security_response/writeup.jsp?docid=2014-021017-4904-99

16 See "W32.Duqu: The Precursor to the Next Stuxnet," Symantec Security Response, October 11, 2011. Available at: http://www.symantec.com/connect/http%3A/%252Fwww.symantec.com/connect/blogs/w32_duqu_precursor_next_stuxnet

17 See "Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East," Symantec Security Response, May 28, 2012. Available at: http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east

18 See "Backdoor.Miniduke," Symantec Security Response, February 27, 2013. Available at: http://www.symantec.com/security_response/writeup.jsp?docid=2013-030119-2820-99

19 Symantec Corporation, "Hidden Lynx – Professional Hackers for Hire," Symantec Security Response Blog, January 23, 2014. Available at: http://www.symantec.com/connect/blogs/hidden-lynx-professional-hackers-hire

20 Symantec Internet Security Threat Report 19, at 38.

21 Ibid. at 6.

22 Ibid. at 6.

23 Ibid. at 48.

24 "Mexican Police Issue 'Ransom Ware' Virus Warning," Associated Press, April 10, 2014. http://www.41nbc.com/story/d/story/mexican-police-issue-ransom-ware-virus-warning/39517/Zt2c0Ra-hkmr8YT_vK1Wcg

25 Brian Krebs, "Inside a 'Reveton' Ransomware Operation," KrebsOnSecurity, August 12, 2013. Available at: http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/

26 Symantec Corporation, 2013 Norton Cybercrime Report, (October 2013), 7. Available at: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

Footnotes

27 Symantec Internet Security Threat Report 19, at 6.

28 2013 Norton Cybercrime Report, at 8.

29 Ibid. at 6.

30 Ibid. at 6.

31 2013 Norton Cybercrime Report, at 8.

32 See Simcott, April 3, 2014.

33 Esteban Israel, "Hackers Target Brazil's World Cup for Cyber Attacks," Reuters, February 26, 2014. Available at: http://www.reuters.com/article/2014/02/26/us-worldcup-brazil-hackers-idUSBREA1P1DE20140226

34 See "Infostealer.Bancos," Symantec Security Response, July 17, 2003. Available at: http://www.symantec.com/security_response/writeup.jsp?docid=2003-071710-2826-99

35 See Sean Butler, "Fraudsters and Scammers Kick Off Their Campaigns for the 2014 FIFA World Cup," Symantec Security Response Blog, February 3, 2014. Available at: http://www.symantec.com/connect/blogs/fraudsters-and-scammers-kick-their-campaigns-2014-fifa-world-cup

36 Kevin Savage, "Trojan.Tylon Risk Assessment," Symantec Security Response Team, November 16, 2013. Available at: http://www.symantec.com/security_response/writeup.jsp?docid=2012-111612-5925-99.

37 See "Trojan.Zbot," Symantec Security Response, January 10, 2010. Available at: http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99

38 Symantec Corporation, "The State of Financial Trojans 2013," Symantec Security Response Team, December 17, 2013. Available at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_state_of_financial_trojans_2013.pdf

39 Daniel Regalado, "Criminals Hit the ATM Jackpot," Symantec Security Response Team, October 11, 2013. Available at: http://www.symantec.com/connect/blogs/criminals-hit-atm-jackpot

40 Daniel Regalado, "Texting ATMs for Cash Shows Cybercriminals' Increasing Sophistication," Symantec Security Response Blog, March 24, 2014. Available at: http://www.symantec.com/connect/blogs/texting-atms-cash-shows-cybercriminals-increasing-sophistication

41 Symantec Corporation, "Sochi Olympics Terrorism Fears Used as Bait for Targeted Darkmoon Campaigns," Symantec Security Response Blog, February 28, 2014. Available at: http://www.symantec.com/connect/blogs/sochi-olympics-terrorism-fears-used-bait-targeted-darkmoon-campaigns

BEST PRACTICE GUIDELINES FOR ENTERPRISES

Best Practice Guidelines for Enterprises

01
Employ defense-in-depth strategies

Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls as well as gateway antivirus, intrusion detection or protection systems (IPS), website vulnerability scanning with malware protection, and web security gateway solutions throughout the network.

02
Monitor for network incursion attempts, vulnerabilities, and brand abuse

Receive alerts for new vulnerabilities and threats across vendor platforms for proactive remediation. Track brand abuse via domain alerting and fictitious website reporting.

03
Antivirus on endpoints is not enough

On endpoints, it is important to have the latest versions of antivirus software installed. Deploy and use a comprehensive endpoint security product that includes additional layers of protection including:

- Endpoint intrusion prevention that protects unpatched vulnerabilities from being exploited, protects against social engineering attacks, and stops malware from reaching endpoints;
- Browser protection for avoiding obfuscated web-based attacks;
- File and web-based reputation solutions that provide a risk-and-reputation rating of any application and website to prevent rapidly mutating and polymorphic malware;
- Behavioral prevention capabilities that look at the behavior of applications and prevent malware;
- Application control settings that can prevent applications and browser plug-ins from downloading unauthorized malicious content;
- Device control settings that prevent and limit the types of USB devices to be used.

04
Secure your websites against Man In The Middle attacks and malware infection

Avoid compromising your trusted relationship with your customers by:

- Implementing Always On SSL (SSL protection on your website from logon to logoff);
- Scanning your website daily for malware;
- Setting the secure flag for all session cookies;
- Regularly assessing your website for any vulnerabilities (in 2013, 1 in 8 websites scanned by Symantec was found to have critical unpatched vulnerabilities);
- Choosing SSL Certificates with Extended Validation to display the green browser address bar to website users;
- Displaying recognized trust marks in highly visible locations on your website to show customers your commitment to their security.

05
Protect your private keys

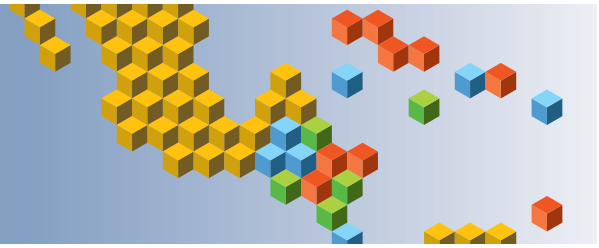
Make sure to get your digital certificates from an established, trustworthy certificate authority that demonstrates excellent security practices. It is recommended that organizations:

- Use separate Test Signing and Release Signing infrastructures;
- Secure keys in secure, tamper-proof, cryptographic hardware devices;
- Implement physical security to protect your assets from theft.

06
Use encryption to protect sensitive data

Implement and enforce a security policy whereby any sensitive data is encrypted. Access to sensitive information should be restricted. This should include a Data Loss Protection (DLP) solution. Ensure that customer data is encrypted as well. This not only serves to prevent data breaches, but can also help mitigate the damage of potential data leaks from within an organization. Use Data Loss Prevention to help prevent data breaches: Implement a DLP solution that can discover where sensitive data resides, monitor its use, and protect it from loss. Data loss prevention should be implemented to monitor the flow of information as it leaves the organization over the network, and monitor traffic to external devices or websites.

- DLP should be configured to identify and block suspicious copying or downloading of sensitive data;
- DLP should also be used to identify confidential or sensitive data assets on network file systems and computers.



Best Practice Guidelines for Enterprises

07
Ensure all devices allowed on company networks have adequate security protections

If a 'bring your own device' (BYOD) policy is in place, ensure a minimal security profile is established for any devices that are allowed access to the network.

08
Implement a removable media policy

Where practical, restrict unauthorized devices such as external portable hard-drives and other removable media. Such devices can both introduce malware and facilitate intellectual property breaches, whether intentional or unintentional. If external media devices are permitted, automatically scan them for viruses upon connection to the network and use a DLP solution to monitor and restrict copying confidential data to unencrypted external storage devices.

09
Be aggressive in your updating and patching

Update, patch, and migrate from outdated and insecure browsers, applications, and browser plug-ins. Keep virus and intrusion prevention definitions at the latest available versions using vendors' automatic update mechanisms. Most software vendors work diligently to patch exploited software vulnerabilities; however, such patches can only be effective if adopted in the field. Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organization.

10
Enforce an effective password policy

Ensure passwords are strong; at least 8-10 characters long and include a mixture of letters and numbers. Encourage users to avoid re-using the same passwords on multiple websites and sharing of passwords with others should be forbidden. Passwords should be changed regularly, at least every 90 days.

11
Ensure regular backups are available

Create and maintain regular backups of critical systems, as well as endpoints. In the event of a security or data emergency, backups should be easily accessible to minimize downtime of services and employee productivity.

12
Restrict email attachments

Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF, and .SCR files. Enterprises should investigate policies for .PDFs that are allowed to be included as email attachments. Ensure that mail servers are adequately protected by security software and that email is thoroughly scanned.

13
Ensure that you have infection and incident response procedures in place

- Keep your security vendor contact information handy, know who you will call, and what steps you will take if you have one or more infected systems;
- Ensure that a backup-and-restore solution is in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss;
- Make use of post-infection detection capabilities from web gateway, endpoint security solutions and firewalls to identify infected systems;
- Isolate infected computers to prevent the risk of further infection within the organization, and restore using trusted backup media;
- If network services are exploited by malicious code or some other threat, disable or block access to those services until a patch is applied.

14
Educate users on basic security protocols

- Do not open attachments unless they are expected and come from a known and trusted source, and do not execute software that is downloaded from the Internet (if such actions are permitted) unless the download has been scanned for viruses and malware;
- Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends;
- Deploy web browser URL reputation plug-in solutions that display the reputation of websites from searches;
- Only download software (if allowed) from corporate shares or directly from the vendor website;
- If Windows users see a warning indicating that they are "infected" after clicking on a URL or using a search engine (fake antivirus infections), educate users to close or quit the browser using Alt-F4, CTRL+W or the task manager.

OAS COUNTRY REPORTS

Antigua and Barbuda

★ St. John's

Population: **88,000**
Internet Penetration: **59%**
Fixed Broadband Subscribers: **4.6%**

Several government agencies play a leadership role in promoting cybersecurity and combating cyber-crime in Antigua and Barbuda. The Organization of National Drug Control Policy (ONDCP) serves as the National Point of Contact for engagement with international organizations such as the OAS and the Ministry of Information is designated as the lead government representative for cybersecurity matters in general. Additionally, the Regional Cyber Investigation Laboratory (RCIL), housed within the Antigua and Barbuda Police Force, is responsible both for processing digital evidence in criminal matters and investigating reported incidents of cybercrime issues in Antigua and Barbuda and the greater Caribbean region.

While the Government of Antigua and Barbuda has not formally established a national Computer Security Incident Response Team (CSIRT), consultative meetings with potential stakeholders have been held to discuss issues related to doing so, and these efforts are on-going. Similarly, while national authorities have taken steps towards developing a national cybersecurity strategy and policy, none have as yet been adopted. 2013 was, however, marked by significant improvement to the country's relevant legislative framework, with the passage of the Electronic Transactions Bill, the Electronic Evidence Act, the Electronic Crimes Act, and the Data Protection Act.

No formal cybersecurity awareness raising campaign has been undertaken as of yet, but the Ministry of Information, in partnership with the Connect Antigua Barbuda Initiative, is currently seeking to develop a campaign that would center around small courses to be delivered to civil servants on email security awareness. There are also plans to produce several public service announcements on cybersecurity-related issues.

Private sector entities are not required to report cybersecurity incidents to national authorities, nor are there in place the necessary frameworks or memorandums of understanding to facilitate such information-sharing or cooperation. The government has, however, endeavored to demonstrate its willingness to work with the private sector by seeking to engage the participation of key entities including telecommunications, financial, critical infrastructure, utilities, ISPs, and other such stakeholders – in numerous government-led meetings on cybersecurity. Cooperation with other countries has been somewhat more robust, as the RCIL actively works with a number of governments in the region. However, the lack of an official national incident response capability or lead agency for incident response has inhibited engagement with other countries on that front.

There are no cybersecurity specialized degree programs offered in the country, although the Antigua Barbuda International Institute of Technology, which specializes in information technology coursework, does cover security-related content in several of its courses.

Given that there is no official body tasked with responding to cyber incidents and most go unreported, national authorities are unable to assess any change in the frequency or type of incidents or

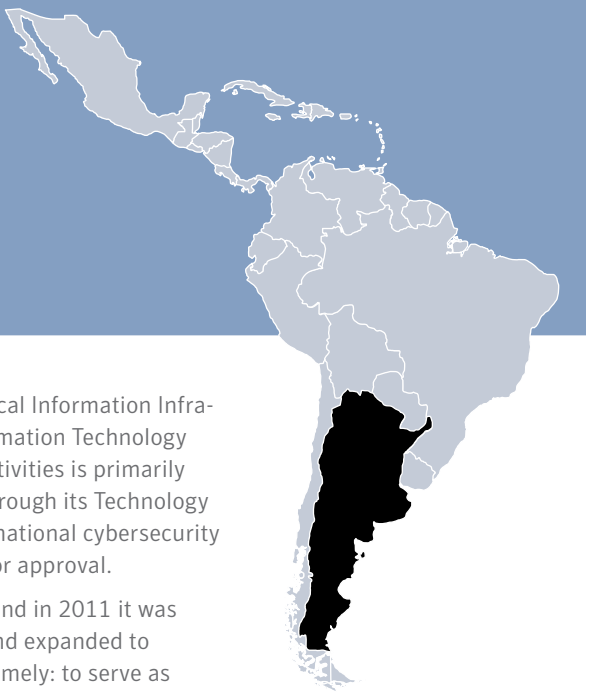
attacks affecting persons, companies or institutions within the country. In 2013, the RCIL received only a very small number of reports of hacked personal email accounts. In the one case that received press attention, several persons whose accounts were accessed were then extorted for money. However, due to the lack of reporting, especially by the private sector, national authorities cannot pinpoint any trends or significant cybersecurity incidents that may have taken place within the country.

Going forward, the success of current efforts to improve Antigua and Barbuda's national cybersecurity posture will in large part hinge on several key factors, including: the level of buy-in and support at the leadership and ministerial level, the degree of participation of the various national stakeholders in developing a cybersecurity policy, and the availability of financial resources for launching a national CSIRT.

Argentina

★ Buenos Aires

Population: **41,350,000**
Internet Penetration: **55.8%**
Fixed Broadband Subscribers: **10.9%**



The lead agency for cybersecurity in Argentina is the National Program for Critical Information Infrastructure and Cyber Security (ICIC), which is part of the National Office of Information Technology under the Cabinet of Ministers. The investigation of cybercrimes and related activities is primarily carried out by the Argentine National Gendarmerie (ANG), or national police, through its Technology Crimes Division. While the Government of Argentina does not presently have a national cybersecurity strategy or policy, authorities reported that one is currently being considered for approval.

Under the ICIC (www.icic.gov.ar) the first national CERT was founded in 1994, and in 2011 it was formally designated as part of the National Office of Information Technology, and expanded to provide additional services. ICIC-CERT currently has four primary objectives, namely: to serve as a repository for relevant information regarding cybersecurity incidents, tools and techniques; to promote coordination between network administrators for all national public institutions to prevent, detect, manage and recover from security incidents effecting their networks; to centralize reporting of incidents effecting government networks and facilitate information-sharing to more effectively address them; and to interact with other incident response teams in the country and region.

While the Technology Crimes Division of the ANG is the lead unit responsible for cyber-related investigations, other entities within the national police are also engaged as per the specific nature of the case.

Private sector entities are not legally required to report incident-related information to the national authorities. Nonetheless, authorities reported that there are established mechanisms in place to facilitate information-sharing on the part of private entities, such as ISPs or email service providers, when there is a clear legal and judicial basis for an investigation. The current cybercrime-related legislation was passed in 2008, and has enabled successful investigation and prosecution in several

important cases. Authorities stated, however, that their efforts to fully apply the law in combating cybercrime have been somewhat hampered by the challenges stemming from the inherent borderless and evolving nature of many cyber crimes.

In terms of maintaining the resiliency of their own institution, the ANG developed in 2007 an information security policy which outlines norms and procedures in the event of a security incident, as well as steps for raising awareness of threats and good practices among network users. Outside of their own institutional network, the ANG utilizes secure access systems such as site-to-site or client-to-site VPNs.

Government-led efforts at raising awareness regarding the range of cybersecurity-related issues and challenges have largely centered on discussion sessions and talks held in densely populated areas, and efforts to develop training centers and appropriately equipped operational units at the level of local authorities. The ICIC has also developed an initiative referred to as Internet Sano ("healthy" or "sound" Internet), which aims to promote responsible use of ICTs and the Internet. And a second awareness raising program called "With you on the web" has been developed by the National Directorate for the Protection of Personal Information, under the Ministry of Justice and Human Rights.

Several institutions of higher learning in Argentina currently offer certification and degree programs in a wide range of aspects of cybersecurity, including digital forensics. The National Institute for Public Administration (INAP) also reportedly offers training and coursework on cybersecurity-related topics.

Although detailed records and hard numbers are not available for public distribution, national authorities have observed over the past year an increase in certain cyber crimes and other malicious cyber activities, including: identity theft and fraud via social networks, email, or e-banking using social engineering or keylogger and other malware; web site defacements; and APTs. However, there is no available data indicating which sector of the population has been most targeted or impacted.

Government authorities identified three primary impediments to their on-going cybersecurity and cybercrime-related efforts, specifically: the persistent lack of awareness among stakeholders at all levels, issues and concerns regarding privacy, and insufficient funding.

Barbados

★ Bridgetown

Population: **276,000**
Internet Penetration: **73.3%**
Fixed Broadband Subscribers: **23.09%**

The past year has been marked by noteworthy advances on the cybersecurity front in Barbados and important initiatives continue in various stages of development. Within the Government of Barbados, two national authorities have taken a leadership role, namely the Telecommunications Unit within the Ministry of Energy and Telecommunications, which is in the process of creating a national CIRT, and the Cyber Crime Unit of the Royal Barbados Police Force.

Although not yet operational, the CIRT is presently in the implementation phase, which to date has included panel discussions to promote awareness of its future functions and training activities. The latter has entailed training of staff on both cybersecurity systems and theories. There is no official national cybersecurity policy or strategy currently in place, although it is reported that one is in the pipeline. The Government of Barbados is collaborating with other Caribbean governments as well as the Caribbean Telecommunication Union (CTU) and Commonwealth Telecommunications Organization (CTO) in the organization of a series of consultative discussions regarding the creation of a Commonwealth "cyber governance model", which would be adopted and implemented by the Commonwealth countries to create a shared standard. Since 2010, the Telecommunications Unit of the Prime Minister's Office has undertaken a public awareness effort aimed at protecting children in cyber space, culminating more recently in a partnership with a private sector company to promote the "Think Click Surf" campaign. Finally, appropriate government personnel are being encouraged to attend policy and practical level cybersecurity events as they take place.

While there is no legal requirement that private sector entities must report to the government regarding specific cyber incidents, this may change with the Privacy and Data Protection Act, currently in the draft phase. The act seeks to address issues on reporting security breaches and includes the establishment of timeframes for reporting incidents.

Government authorities report that increasing cooperation is a key priority, with officials participating in all relevant regional forums, and on-going efforts at the national level to engage private enterprise and academia (University of the West Indies) in awareness-raising and the development of strategies for managing cybersecurity in Barbados. The launching of the national CIRT sometime later this year is expected to result in the articulation of a more focused approached to strengthening cooperative mechanisms both nationwide and regionally. Cooperation with the ITU has been central to the process of creating the national CIRT to date, and is expected to remain a core partnership for the government.

There are no cybersecurity-related degree programs available in Barbados, although the local campus of the University of the West Indies does offer several courses on aspects of cybersecurity and various private enterprises conduct seminars and workshops on the subject.

Although no hard numbers are available yet, the government reports that the Telecommunications Unit is collecting data on cyber attacks and incidents across government departments, which will

soon enable a critical analysis of the types and frequency of attacks, as well as the kind and efficacy of mitigation techniques being employed. It was reported that a series of incidents in early 2014 affected numerous government offices and that these were brought to the attention of the Office of the Prime Minister, which arranged assistance in managing and mitigating the impact of the incidents on their targets.

A lack of funding was identified as the most significant impediment to Barbados' cybersecurity advancement.

Belize

★ Belmopan

Population: **340,000**
Internet Penetration: **25%**
Fixed Broadband Subscribers: **3.1%**

While the Government of Belize does not currently have an official policy or strategy for cybersecurity, two national authorities – the Ministry of National Security and the Belize Police Department (BPD) – share leadership for managing cybersecurity-related issues at the national level. The handling of cybercrimes or related matters is done on an ad hoc basis by the BPD, with the IT Unit (PITU) taking the lead with assistance as required from the Special Branch for Security and Intelligence (SB). When the investigation of a cybercrime or other incident necessitates cooperation or information-sharing with other regional or international security or intelligence organizations, such communications are handled by the SB. There is neither a national CIRT nor an established policy or procedure for responding to cyber incidents. The BPD's IT Unit does, however, undertake an annual countrywide "ICT Road Show" to promote increased awareness of Internet and cybersecurity-related issues among the general public.

The BPD's efforts to tackle cybercrime have yielded some successes, but remain hampered by the lack of an adequate national legal framework to allow for the prosecution of perpetrators, as well as the need for increased resources including personnel, training, equipment, software and office space.

The Ministry of National Security – specifically the focal point for CICTE-OAS – is presently working on establishing an ICT Steering Committee within the ministry, with the dual aims of developing a national cybersecurity strategy and reviewing and strengthening the legislative framework regarding cybercrime. Additionally, government authorities have recently begun working to develop a "National ICT Innovation Policy". While this policy will focus primarily on e-Governance issues, it will include a component dealing with cybersecurity and the protection of critical infrastructures.

Although private sector institutions are not legally required to report cyber incidents to national authorities, the BPD has worked to establish cooperative relationships with many private sector entities, and has provided support and assistance when it has been requested. Cooperation with other countries' national authorities has been limited. The BPD did, however, coordinate with other CARICOM members on cybersecurity matters in the run-up to the 2007 Cricket World Cup, and has

assisted US authorities by recovering data from computers used by criminals involved in human trafficking, as well as in the investigation of individuals with suspected links to terrorist and other criminal networks.

Although it does not presently maintain official statistics, the Government of Belize reported a notable increase in cybersecurity incidents over the past year and cites additional informal reporting from the private sector – including telecommunications companies and other owners and operators of critical infrastructure – which anecdotally confirm an increase in cyber attacks. Incidents involving financial institutions have not been reported as widely to national authorities, perhaps out of a desire to avoid drawing unwanted attention from their customers. Rather, such institutions presently prefer to handle cybersecurity matters internally.

National authorities express an awareness of both the trends and challenges relating to cybersecurity in Latin America and the Caribbean, and the vulnerabilities of their own industrial and financial sectors as well as critical infrastructures, such as telecommunications and public utilities. This awareness is driving current capacity-building and policy development efforts at the national level, including those focused on adopting a national strategy, reforming the legal system, and creating a national CIRT.

Bolivia

★ La Paz and Sucre

Population: **10,517,000**
Internet Penetration: **34.2%**
Fixed Broadband Subscribers: **1.05%**

Efforts on the part of the Government of Bolivia to develop its national cybersecurity regime are carried out primarily by two national authorities. The first of these is the Scientific Technical Research Institute of the Police University (IITCUP), which is the lead agency for the investigation of cybercrimes and is primarily focused on processing and analyzing digital evidence. This work is carried out by the staff of the Digital Forensics Division, who have been trained in the US, Argentina, and Peru, and regularly attend other courses and events domestically and abroad as both trainers and participants. Strengthening their capacity to conduct digital forensics has been a central priority for IITCUP in the past year.

The second lead national authority is the Agency for the Development of an Information Society in Bolivia (ADSIB), which is housed under the Vice Presidency of the State and the Presidency of the National Assembly. Among other things, ADSIB is working on implementation plans both for e-Government and the utilization of free software, both of which will address a range of important cybersecurity points. While there is not yet an official national Computer Incident Response Team (CIRT), ADSIB is in the process of creating a national incident response capability utilizing its existing team of trained and competent personnel. It is anticipated that this body will be operational in 2014. ADSIB has also organized a training seminar on protecting web sites from cyber attacks.

Government authorities took the lead in pushing for the creation of the first Internet Exchange Point (IXP) in Bolivia, reportedly motivated by the revelations that came with the Snowden leaks in the US.

While IITCUP maintains channels for requesting information and cooperation from private sector entities, it cites the continued lack of formal mechanisms for accessing such information in a timely fashion from social network and other operators as a principal obstacle to investigating and prosecuting cybercrimes. And given the relatively limited engagement between IITCUP and other national authorities and private sector entities, the latter tend to rely on themselves for their own security and incident management. Similarly, private sector entities are not required to report to ADSIB, and no information was provided by the latter regarding on-going collaboration or information-sharing between the two sides. Cooperation between ADSIB and counterpart entities in other countries has been more fruitful, however. One particular reported security incident resulted in direct coordination with the national CIRT of Argentina, ArCERT, in responding to and resolving a situation involving phishing and the targeting of an enterprise deemed critical to Bolivia's national interests. The successful management of this incident was considered a major success for the government.

Although IITCUP has its own robust internal information security protocol, it reports that there are no common protocols or procedures between other government agencies. And while in theory each institution should adopt its own protocols as required, many still do not have established information or network security procedures.

IITCUP reports that many universities in Bolivia offer cybersecurity-related coursework, including in digital forensics, and that appropriate personnel from IITCUP often utilize these courses for training. However, most of the coursework offered is general in scope and theory-based, and incorporates little in the way of hands-on practical training.

Both authorities report that very little has been done to date to raise cybersecurity awareness within government, the private sector, or society at large.

Although ADSIB does not have quantitative data regarding the frequency or types of cyber incidents in Bolivia, IITCUP has observed an exponential uptick in such incidents in the past several years, citing an increase of at least 60 percent in 2013 as compared to the year prior. The most affected groups, according to IITCUP, have been individual users, followed by the government. According to ADSIB's reporting, the significant incidents in the past year have also involved theft of data, civil unrest, and modifications to root users of key sites. IITCUP observed that the most common means of attack or exploitation were threats, extortion, and kidnapping of minors via social networks, and attacks and defacements against the web sites of government institutions. IITCUP reported opening roughly 150 cybercrime-related cases last year. In one noteworthy case, an individual was using Facebook to contact and falsely offer work opportunities to underage women. He would lure the women into face to face meetings, photograph them in comprised situations, and then extort them with threats of publishing the photographs. Authorities were able to apprehend the individual, collect and process evidence from various computers and electronic devices, and secure a successful conviction.

Going forward, both IITCUP and ADSIB cite the need for increased cooperation between agencies of the state, as well as further training and assistance to support their respective capacity-building efforts.

Brazil

★ Brasilia

Population: **201,033,000**
Internet Penetration: **49.8%**
Fixed Broadband Subscribers: **9.2%**

The Government of Brazil has developed advanced capabilities in cybersecurity and deterring cybercrime, with numerous state institutions and agencies playing active roles in this area. The Federal Police (DPF) is the lead agency for the investigation of all criminal offenses in the country, and as such is the primary authority for cybercrime-related matters, namely through its Office for the Suppression of Cybercrime (SRCC). It also maintains a second specialized group tasked with combating crimes involving child pornography on the internet, GECOP, although this will soon be integrated with the SRCC. Where the nature of a particular cyber-related crime merits it, appropriate persons from other DFP units as well as other institutions may also be involved. In the case of a crime committed against an individual, the Civil Police of the particular state where the crime took place will play an active role, providing evidence to the DPF the latter requires it for an international investigation.

No relevant information regarding cybersecurity policies or incident response was provided for the preparation of this report.

The DPF maintains a robust internal and external security regime to ensure the resiliency and integrity of its networked information systems, including a technical unit for investigating and resolving internal security breaches, the use of highly secure rooms, and a redundancy of connections and power supply for servers hosting the most important services and information. It follows guidelines laid out by the Brazilian Government's ICT Management Committee (CGTI).

SRCC personnel and other officials responsible for investigating cybercrimes are regularly provided training on specific aspects of computer forensics to remain current with and proficient in the use of relevant tools and techniques.

National authorities, primarily within the Department of Information Security and Communications (DSIC), of the Institutional Security Cabinet (GSI) of the Presidency, have developed and implemented awareness raising campaigns to encourage smart and responsible use of the Internet by individual citizens.

While there is no legal requirement that private sector entities provide incident-related information to national authorities, authorities reported that cooperation between the two sides is routine and robust. One example highlighted involves an agreement between the DPF and Microsoft, where Microsoft provides registration information for users of its services when requested by the DPF via en electronic form. Authorities also noted that Brazil has a large and productive sector of custom developed cybersecurity-related software for private entities, such as banks, as well as public institutions.

Authorities cited several trends observed in 2013, although hard numbers were not available. These included an increase in reporting to the DPF of cybercrimes and related activities, which

authorities speculate stemmed primarily from the recent entry into force of a law amending the Criminal Code to include cybercrimes. The most common form of cybercrime reported was electronic bank fraud targeting users and providers of Internet banking services. Authorities reported that the most impacted is the commercial sector, particularly companies selling products or service over the Internet, as well as the aforementioned banks and credit card companies. In 2013, authorities reported that 91 persons were arrested for cybercrime-related activities.

While authorities did not cite a particular significant incident for inclusion in the report, the significant increase in reports of electronic banking fraud was again highlighted as a major trend with potentially significant costs.

In terms of the impediments to enhancing cybersecurity and combating cybercrime, authorities cited the need to take further steps to criminalize certain offenses, and the lack of requirements for ISPs to store data about their users and provide that information to authorities in the event of an incident or investigation without a court order. However, it was reported that the national congress is now considering legislation to address the latter issue.

Chile

★ Santiago

Population: **16,841,000**
Internet Penetration: **61.4%**
Fixed Broadband Subscribers: **12.4%**

Several agencies within the Government of Chile share responsibilities related to promoting cybersecurity and combating cybercrime. On the cybersecurity front, the Ministry of the Interior and Public Safety, the General Secretariat of the Presidency, and the Sub-secretariat of Telecommunications all play key roles. For cybercrime-related matters the Carabineros, or national police, is the designated lead, through its Investigative Department for Criminal Organizations (OS9). Within the operational structure of OS9 is the High Complexity Section, which serves as the lead for investigations involving ICTs or the collection and analysis of digital evidence. The Department of Criminology of the Carabineros (LABOCAR) also maintains a computer laboratory dedicated to performing analysis of computers and devices seized during investigations of threats, grooming, phishing, and other illicit activities.

While there is no official national cybersecurity strategy or policy document, Chilean authorities have been working for a number of years to develop a strong national capacity for cyber incident response and management. Their approach to doing so has been somewhat unique, in that rather than focusing on the creation of a single national CSIRT or similar body, emphasis has been placed on developing standardized procedures and best practices for incident management and cybersecurity more broadly. These are outlined in Supreme Decree No. 1299, Program for the Improvement Information Security Systems Management. While a CSIRT has existed and functioned within the government since 2004, referred to as CSIRT-CL, it is not a formal institutional entity so much as an operational capacity and structure maintained by the Ministry of the Interior and Public Safety. Its aims are to provide cybersecurity-related support to the State Connectivity Network and other

entities of the central government, and promote national and international cooperation, awareness raising, and the strengthening of national laws and policies. CSIRT-CL has actively collaborated with other national CSIRTs around the region in responding to incidents, and has participated in initiatives to train personnel in other OAS Member States. In addition to the work of CSIRT-CL, private companies are able and encouraged by the government to also provide incident management-related services, both to other private enterprises as well as public institutions.

Personnel from OS9, LABOCAR and CSIRT-CL receive technical training in aspects of cyber investigations and incident management from experts in the field. Additional training often takes the form of instruction provided by the suppliers of a particular hardware or software being utilized, to ensure the proper management and use of the device or program. And when and where there is a need for more specific expertise than that possessed by the existing staff, for example if OS9 requires a person skilled in software engineering with a focus on cybercrime, one is hired on a contract basis. Cybersecurity and cybercrime-related bachelors and masters degrees are offered by the University of Chile and other top-level academic institutions.

To promote systems resiliency and data integrity within their own institution, the Carabineros employ both a disaster recovery plan and disaster recovery software, thus ensuring that operations can resume quickly in the event of a man-made or natural disaster. And the institution's own systems administrators and security managers regularly review the processes, policies and procedures related to recovery and IT infrastructure continuity. Security policies and procedures have been established to ensure that users within the institution contribute to secure information systems management. These include requiring users to change passwords periodically, and a prohibition against installing peer-to-peer (P2P) programs on work computers. Regular risk assessments and trainings for staff are also carried out. In addition, an internal Intranet system, including an internal web site, enables all users to communicate and access information within a secure and access-controlled environment, ensuring that any individual can only access databases relevant to their work responsibilities. The use of a secure VPN adds another layer of protection for users seeking to access the system remotely.

There is no law in Chile requiring that private enterprises share incident-related information with national authorities, unless that information is sought as part of an official criminal investigation. However, national authorities actively seek to develop and maintain channels with key private sector entities whose cooperation is essential for effective investigation or incident management. It was reported that these channels are often working-level and person-to-person, which, while they can help to facilitate and expedite the flow of information, do not benefit from the types of institutional framework or mechanisms which can facilitate, normalize and validate such exchanges.

To raise awareness and promote a culture of cybersecurity the Ministry of Education has developed and is implementing, in partnership with several private sector entities, a long-term campaign called Secure Internet," or "Internet Segura" in Spanish.

Authorities reported that they do not have sufficient information to provide a quantitative assessment of any increase or decrease in cyber incidents or cybercrimes in 2013. However, they did report that based on available data, the most common types of incidents alerted to national authorities in 2013 involved phishing, malware, and the hacking of government websites by hacktivists, the latter reportedly having increased 30 fold in 2013. Of these, however, phishing reportedly accounts for the highest percentage of cyber-related cases in the country. Other frequently reported incidents involved grooming and threats against persons. It has been observed by law enforcement authorities that for each type of cybercrime or illicit activity, a constant factor in that type of crime appears to be the age grouping of the victims. For example incidents of grooming, which is legally classified as "improper sexual abuse ", generally affects children between 6-15 years of age, independent of their socio-economic or academic position.

Authorities reported that there is no available record of the exact number of opened cybercrime cases in 2013, nor the number of persons convicted of such crimes. They did, however, highlight several significant cases in 2013. In one case referred to as Operation Minerva, persons affiliated with a hacktivist movement developed malware which they deployed through phishing in a successful effort to infect the computers of numerous government officials and gain unauthorized access to information. Authorities eventually detected the malicious activity, conducted a forensic analysis to determine the nature and source of the compromise, and identified the persons responsible for it. In a separate incident, death threats were made through Twitter against a senior government official with security-related responsibilities. An investigation by OS9 identified the responsible person and led to his arrest.

Chilean authorities cited two principal impediments to efforts to enhance cybersecurity and combat cybercrime. The first is the need to further raise awareness among senior decision-makers as to the urgency of both cyber threats and the steps that must be taken to address them. The second and related impediment is the lack of recognition about the extent of the costs of cybercrime and cyber vulnerabilities, for the public as well as private sector, and the importance of developing a strategic and integrated approach which outlines the roles and responsibilities of all stakeholders.

Colombia

★ Bogota

Population: **47,130,000**
Internet Penetration: **49%**
Fixed Broadband Subscribers: **8.2%**

Cybersecurity and cybercrime-related efforts by the Government of Colombia are primarily guided by the CONPES 3701, a national policy for cybersecurity and cyber defense which has been in place for several years. The policy defines guiding principles, delineates roles and responsibilities, and highlights priority areas for action and investment on the part of government authorities. It was based on this policy document that the specialized Police Cyber Center (CCP) was established within the National Police of Colombia, under the Directorate of Criminal Investigations and INTERPOL (DIJIN). The CCP is the lead designated unit in Colombia for investigating cybercrimes throughout the country, and its personnel have received training in cyber investigations and digital forensics from the US Department of State (DS/ATA) and the FBI, as well as from the governments of Spain and France. CONPES 3701 also provides the mandate for ColCERT, the national body responsible for cyber incident response and coordination among stakeholders at the national level. Numerous other ministries and agencies share a broad range of cyber-related responsibilities under the leadership of these two lead entities. Law 1273, passed in 2009, constitutes the centerpiece of the country's national legislative framework for cybersecurity and cybercrime.

To promote internal systems resiliency and information integrity, the National Police have developed their internal information security management systems in compliance with ISO standard 27001.

This included developing their own application for the management of their information assets and system information security, known as SINAI. Staff and other systems users are informed of

relevant policies and procedures via internal communications. Also, as added measures of security, the National Police maintains its own CIRT and has ordered the creation of an alternate site to host applications and databases deemed critical to their institution.

In terms of cooperation and information-sharing between the private sector and government authorities, specific rules are outlined in Decree 1704 (2012), which establish provisions to be met by providers of telecommunications networks and services to support in an effective and timely manner the work of national authorities. In addition, national authorities have sought to develop relationships with key private sector entities to further increase cooperation and information-sharing.

International cooperation has been robust, as national authorities have collaborated directly with counterpart agencies in other countries in the region in responding to cyber attacks or acts of cybercrime. One such example involved the active participation of Colombian authorities in a multinational initiative under the auspices of INTERPOL's Working Group for Latin America on IT Crime, aimed at identifying and arresting users of online forums exchanging and distributing material on sexual offenses against children and adolescents. Other collaborating countries included Argentina, Brazil, Chile, Costa Rica, Ecuador, Uruguay, Venezuela and Spain.

Notably, the government recently invited an International Commission of Experts to visit the country and conduct a thorough assessment of cybersecurity in Colombia. The team of experts was comprised of persons from Canada, Spain, the US, the UK, the Dominican Republic, Estonia, Israel, the Republic of South Korea, and Uruguay, as well as the OAS, the Council of Europe (COE), the World Economic Forum (WEF), INTERPOL, the United Nations (UN), the Organization for Economic Cooperation and Development (OECD), and the University of Oxford. Emphasis was placed on cybersecurity policies, incident response and management, international frameworks and cooperation, cybercrime legislation and investigation, and cyber defense. Experts met with officials and observed operations in numerous government institutions, and exchanging information and ideas with relevant actors engaged in national cybersecurity efforts. Following the visit, a comprehensive package of observations and recommendations was prepared and presented to senior Colombian authorities for their consideration and use.

Colombian universities and other educational institutions offer a wide range of academic and training programs on the full range of cybersecurity and cybercrime-related topics, including network security and digital forensics.

As the Colombian citizenry gains increased access to new information technologies and the cyber domain continues to expand, authorities have observed a parallel and systematic increase in the transition of criminal actions from the physical to the virtual world. In Colombia, this phenomenon has been most evident in the area of electronic fraud affecting users and entities of the Colombian banking system. Increasingly, reported incidents involve the use of keyloggers, spyware and other such malicious software. The same dynamic has been reflected in the area of identity theft, where perpetrators have increasingly turned to more sophisticated crimes such as virtual "kidnapping" using ransomware, and the use of Cryptolocker in targeting both the small and medium enterprise (SME) community as well as larger companies.

Data collated by the National Police yields some interesting statistics regarding the growth of ICT use and the accompanying rise in cyber incidents and crimes. The following numbers were reported for 2013: 448,983 followers on Twitter, 256,987 visitors to the website www.ccp.gov.com, 16,789 web pages locked for child pornography, 2,652 new alerts for cyber threats, 422 persons detained for cybercrimes, and a total of 4,290 complaints received by the National Police regarding ICT-related incidents (marking an increase of 1,194 complaints over the year before).

In 2013, the CCP responded to 1,647 cyber attacks or incidents, of which 62 percent involved individual citizens and 21 percent involved entities in the banking sector. The rest of the incidents

addressed involved an approximately equal mix of entities in the government, law enforcement, communications, energy, health, and education sectors.

Colombian authorities have identified three specific cybercrime trend areas. The first is the increased use of malicious code, phishing, and the theft of information affecting the users and institutions involved in the growing virtual banking sector. Authorities assert that this has been perpetuated by a weak culture of security and a corresponding lack of security awareness-raising for users by companies. The second trend area involves incidents affecting cybersecurity, including unauthorized access to or leakage of information, data interception, abusive access to systems, denial of service (DoS), and web defacement. The third observed trend area is in the increased use of the Internet, social networking, email and the Deep Web on the part of common criminals and organized crime. This has included the massive illegal collection of money (e.g. cyber pyramids), the use of virtual currency as a mechanism for money laundering, and the perpetration of illicit deals involving traf-ficking in arms, drugs, child pornography, etc.

The National Police reported a marked increase in the number of persons arrested for cybercrimes and other-related illegal acts in 2013, up to 422 as compared to 323 in 2012, and 252 in 2011. Also, the aforementioned Purity II Operation targeting distributors of child pornography and related offenses, carried out under the auspices of INTERPOL and in collaboration with law enforcement and other agencies from numerous other countries, was cited by Colombian authorities as a major success story in their on-going efforts to reduce cybercrime.

Authorities reported that the primary impediment to increasing the country's cybersecurity posture is the continuing absence of a culture of information and computer security among citizen users and businesses alike. They also highlighted the lack of usage policies for Internet-supported ICTs and their limited capacity to act in this sphere, given the fact that most Internet services providers and operators are based outside the national territory and cooperative relationships are limited.

Costa Rica

★ San Jose

Population: **4,667,000**
Internet Penetration: **47.5%**
Fixed Broadband Subscribers: **9.3%**

The principle authority for cybersecurity matters in Costa Rica is the Ministry of Science, Technology and Telecommunications (MICIT). However, numerous other agencies and institutions also share in this responsibility, including: Digital Government / Digital Secretariat, the Directorate for Digital Signatures, the Computer Crimes Section of the Judiciary, the Agency for Data Protection (Prodhab), the Central Bank, CSIRT-CR, and the Superintendency for Telecommunications.

The Computer Crime Section of the investigative branch of the Judiciary was created over a decade ago to oversee and assist in investigations of crimes involving the use of ICTs and digital evidence. In 2012, CSIRT-CR was established under the Ministry of Science, Technology and Telecommunications to respond to and mitigate the effects of cyber incidents affecting government institutions. CSIRT-CR

is also mandated to coordinate among entities of the State, autonomous institutions, companies and banks to identify threats, minimize risks, and improve cooperation and information-sharing on relevant cybersecurity-related matters.

A National Digital Strategy has been adopted by the government, however its primary focus is on defining a vision for the integrated use of technologies by the State, and it does not go much beyond identifying cybersecurity as a priority. There is presently no national cybersecurity strategy or policy guiding the related efforts of national authorities.

In terms of training and capacity-building, relevant personnel of the Computer Crime Section have received training in aspects of digital investigations and forensics from counterpart agencies in the United States and Canada, as well as other needed training from regional organizations including the OAS . In addition, CSIRT-CR personnel have received technical training from outside partners, including the OAS and incident response experts from other OAS Member States.

At the institutional level, certain measures are in place to enhance system resiliency and the integrity of information. Data is backed up from servers to SAN (Storage Area Network) units on a daily basis, and security systems are in place for computers on and databases within the network. Security policy dictates that only some designated host servers are able to connect to databases on the network.

Costa Rica's relevant legislative framework includes a law on digital signatures, which provides for policies on both the government's certification of registered certifiers and the official formats for digitally signed electronic documents. Another law (No. 8968) deals with protecting individual's personal information, defining how companies must handle any personal information they gather and restricting how such information can be used. More recently, Costa Rican authorities approved a new law on cybercrime (No. 9048) which includes important reforms to the penal code defining new cybercrimes. Although Costa Rica has been invited to accede to the Budapest Convention and despite ongoing efforts by some national authorities to move forward on that front, the country has not yet done so.

There is no legal obligation for private sector entities to share information with national authorities in the event of an incident and the links and mechanisms necessary for facilitating such cooperation are limited and informal. The creation of CSIRT-CR and its subsequent efforts to engage potential partners in both government and the private sector have achieved some progress on this front, but cooperation is inconsistent and generally lacking.

Costa Rican authorities have remained actively engaged with international partners on several fronts. In 2013 a Regional Symposium on Cyber Security was organized by the Ministry of Science, Technology and Telecommunications in conjunction with the OAS and the country's Network Information Center (NIC). The symposium brought together officials from throughout the region and representatives from academia and the private sector, to explore opportunities to further develop national cybersecurity capabilities. Technical training was delivered to personnel from CSIRT-CR, NIC Costa Rica, the Judiciary, the Central Bank, the Costa Rican Institute for Electricity (ICE), and numerous other owners and operators of critical infrastructure. A second, similar initiative was carried out in the spring of 2014, in conjunction with many of the same partner institutions and organizations, and involving the participation of officials from the US, Panama, Mexico, Peru, Honduras and Argentina. Discussions focused on topics such as network security, ethical hacking, international standards for combating cybercrime, and tools and techniques for digital forensics. In another demonstration of effective international partnership, the Government of Costa Rica reported receiving technical assistance from the Ministry of Science of the Government of South Korea, as well as the Institute for the Development of an Information Society in Korea (KISDI) and the Korea Internet and Security Agency (KISA). This assistance included recommendations for the revision and application of a Costa Rican national cybersecurity policy.

While numerous educational institutions in Costa Rica offer cybersecurity and cybercrime relevant courses, currently only two offer degrees or specializations. The Center for the Formation of ICTs (CENFOTEC) offers a specialization in Cyber Security: Engineering in ICT Security, while the Latin American Science and Technology University (ULACIT) offers a specialization in Information Security which includes coursework in ethical hacking, digital forensics and cryptography.

There is no official government cybersecurity or cybercrime awareness raising campaign. National authorities do organize talks and trainings on the subject for interested parties, but there is no initiative to inform the general public about the threats that exist in cyber space. Limited awareness raising is undertaken within government institutions, where each organization's Management Unit is responsible for informing all users of relevant policies, procedures and responsibilities, including account security and proper use of information contained within the systems.

In terms of observed trends national authorities report that although some information has been collected, the number of reported cases remains relatively limited, and hard data is lacking. Authorities cited several sporadic attacks against government web sites last year by hacktivist groups, although few of these were officially reported by the targeted institution. Nationwide last year, approximately 600 phishing, pharming or related incidents were reported to authorities, resulting in the opening of 300 cases by investigative bodies. Other incidents involved some form of violation of electronic communications, such as unauthorized access to a users' account. Based on the limited information available, authorities identified government institutions and commercial entities as the two most affected groups.

In July 2013, a major incident targeting a national institution, the telecommunications network of ICE (national electricity provider) was targeted by a denial of service (DNS) attack originating in Russia, entailing almost 25 million attempts to access the site in a period of 48 hours. The incident was detected by the institution's own in-house CSIRT (CSIRT-ICE), which notified CSIRT-CR, which then reached out to US-CERT and its partners in Europe. The resulting assistance enabled the incident to be fully mitigated some twelve hours after it was initially reported.

Government authorities have highlighted several key impediments to strengthening Costa Rica's cybersecurity posture going forward. The lack of a culture and awareness of cybersecurity, including an adherence by users to norms regarding good practices, was identified as perhaps the single greatest such impediment. Similarly, authorities cited the need to update existing technology-related norms in the context of their use and to better train the relevant authorities of the State (including in the Judiciary) to promote and uphold these new norms.

Authorities reported that within government, a fragmented approach to working on cybersecurity and cybercrime issues prevails, with individual institutions working as independent islands rather than in a coordinated fashion or in accordance with an overarching strategy. While some government institutions have created their own cybersecurity-related mechanisms and policies, these need to be more aligned and standardized throughout the government. Increasing demands on the Computer Crime Section necessitate a corresponding increase in financial and human resources to deal with the workload.

Regarding the private sector, authorities reported that the lack of laws or clear standards regarding ISPs retention of records unnecessarily complicates their ability to acquire information needed for an investigation. In addition, it was asserted that private sector entities should do more – including investing more resources – to enhance security in the delivery of online services and systems, including through better authentication data protection measures.

Dominica

★ Roseau

Population: **71,000**
Internet Penetration: **55.2%**
Fixed Broadband Subscribers: **11.9%**

Efforts to develop Dominica's national cybersecurity regime have been stepped up in the past year, stemming from an on-going collaboration between the Ministry of National Security, Immigration and Labour and the Ministry of Information, Telecommunications and Constituency Empowerment. The government has embraced a model for cybersecurity development in which it guides and facilitates efforts but seeks to employ a holistic, multistakeholder approach. While the country does not yet have an official national policy or strategy for cybersecurity, it has begun working with the OAS, the Commonwealth Cybercrime Initiative (CCI), and the Council of Europe (CoE) to develop an overarching national policy and to strengthen cybercrime legislation. The two aforementioned ministries have assumed a leadership role in developing the government's capabilities, including work towards the creation of a national CIRT and a unit equipped to investigate crimes using information technologies.

Presently, all reports of cyber crimes or related activities are handled by the Criminal Investigations Department of the Commonwealth of Dominica Police Force, which is housed within the Ministry of National Security, Immigration and Labour. Although the Police Force does not maintain computer forensic infrastructure, there is a range of cybercrime legislation, including an extensive Electronic Crimes Bill, pending adoption which will align Dominican legal statutes with international norms.

Awareness raising has not yet been undertaken by the government in any systematic manner, although financial institutions have circulated sporadic advisories in the wake of phishing and other attacks. As there is not an entity in place to track or manage cyber incidents, data on the type, number or impact of such incidents at the government or national level is not available. Private sector entities are not required to report cyber incidents to national authorities and largely deal with these without government involvement.

Efforts to develop regional and international partnerships have accelerated in 2013 and 2014. While formal partnerships are yet to be finalized, Dominica has hosted events sponsored by the OAS, the CCI, the CoE, the Caribbean Telecommunications Union (CTU), and the Caribbean Network Operators Group (CaribNOG). There are no cybersecurity-related academic or training programs offered in the country, although it is not uncommon for Dominicans to attain degrees in information security from universities abroad, including around the Caribbean, Europe, or in the United States. However, after receiving degrees, many of these trained technicians look for employment outside of Dominica, reflecting a trend in many Caribbean countries. Dominica has stated as a priority establishing a retention program for skilled IT professionals.

National authorities reported that the lack of a national policy and strategic framework, as well as the absence of capacity-building and awareness raising initiatives, constituted the greatest impediments to cybersecurity advancement in Dominica. It was also reported that the need for increased

capacity-building efforts at home was highlighted by the leaking of sensitive information from the US government last year.

Going forward, the Government of Dominica will continue to collaborate with regional and international partners to further develop the country's cybersecurity capabilities. Assistance will be sought from the OAS and other international partners for capacity-building relating to the creation and development of a national incident response capability, and for developing the country's external partnerships for cooperation and information-sharing. Authorities are also working towards accession to the Budapest Cybercrime Convention and establishing international linkages to better combat cybercrime. Finally, Dominica is exploring the possibility of establishing a Cyber Security Centre to be housed at the Dominica State College, in partnership with international agencies like the OAS, COMSEC, COE, World Bank, IDB, and ITU. The facility would serve as a regional hub for training and capacity-building.

Dominican Republic

★ Santo Domingo

Population: **9,745,000**
Internet Penetration: **45%**
Fixed Broadband Subscribers: **4.3%**

Efforts by the Government of the Dominican Republic to enhance cybersecurity involve multiple agencies working in a coordinated fashion through the Inter-Institutional Commission for High-Technology Crimes. This Commission performs five core functions. First, it ensures coordination and cooperation among all national police, military, judicial and other responsible agencies engaged in responding to, investigating and prosecuting cyber crimes. Second, it coordinates and cooperates with other national governments, international institutions, and other stakeholders to prevent and reduce the frequency of illicit cyber activities in the Dominican Republic and worldwide. Third, it defines policies, establishes directives, and develops cybersecurity strategies and plans for submission to the Executive branch. Fourth, it promotes the adoption and implementation of relevant international treaties and conventions. And finally, it works to ensure that the government is represented by the appropriate institution and persons in all international organizations involved in combating cybercrime and promoting cybersecurity.

In terms of cybercrime investigations, two specific entities have been created: the Department for the Investigation of Cyber and High Technology Crimes (DICAT) in the National Police, and the Cybercrime Investigations Division (DIDI), in the National Department of Investigations (DNI). Underpinning the work of these agencies is Law 53-07, which criminalizes a range of cyber activities and provides a framework for the government to prevent and respond to them. However, there is no official overarching national strategy or policy for cybersecurity, nor is there an established CIRT similar incident response capability.

Since its inception, the DICAT has undertaken a cyber risk prevention campaign consisting of a series of talks delivered at educational institutions and for private and public sector entities. It has also carried out an awareness-raising campaign via social networks aimed at preventing cyber

delinquency. Other state institutions have also worked to inform the public on cyber risks and good practices, including the Dominican Telecommunications Institute (INDOTEL), which has a program titled "Healthy Internet" (http://www.internetsano.do/). To address a deficiency in cybersecurity related coursework at universities in the country, government authorities are presently working in partnership with the Technological Institute of Santo Domingo (INTEC) to develop relevant coursework and certification programs.

The private sector is not obligated to report cyber incidents to national authorities. However, there are established judicial mechanisms for officially requesting such information from entities based within the country. Information-sharing has been further enhanced through the development of collaborative partnerships between the government and private sector that have emerged as a result of the former's extensive efforts to raise awareness and reach out to potential private sector partners.

Cooperation with other countries has increased significantly as well. Joint investigations have been carried out with authorities from the Governments of Spain and Colombia, and officials have actively participated in several successful multi-lateral operations. As a member of the Budapest Convention and the various 24/7 networks of the G8, INTERPOL and the OAS, the Dominican Republic has advanced significantly in developing the mechanisms to cooperate effectively with authorities from other countries. Indeed, Dominican officials assert that the country's accession to the Budapest Convention and the substantial capacity-building assistance it has received from international partners like the OAS has greatly strengthened the country's cybersecurity posture. Nonetheless, the government reports that the single greatest obstacle to increasing cybersecurity and successfully investigating cybercrimes is the difficulty encountered in obtaining needed information from other countries, principally from ISPs social network operators based in the United States.

National authorities report that as the number of Internet users in the Dominica Republic has steadily increased, so has the number of victims of attacks and exploitation. Available statistics indicate an increase in cyber incidents in the country of approximately seven to ten percent (7-10 percent) per year over the past three years. Victims range from individual users to businesses to the government. The most common incidents reported include: credit card cloning, defamation through email and social networks, digital identity theft, phishing, and telephone-related scams. There were also numerous attacks against and defacements of government websites, largely by carried hacktivist groups.

Authorities reported having opened 654 cybercrime related cases in 2013, resulting in 300 submissions for prosecution. They also reported having successfully dismantled hacktivist groups within the country, after a six month joint investigation between the National Police, the Public Ministry, INTERPOL, and authorities from four other countries which led to the arrest of six persons affiliated with Anonymous RD, an Anonymous offshoot based in the Dominican Republic.

Investigators and officials responsible for digital forensics within DICAT routinely receive training to maintain and improve their capabilities. Government authorities assert that increasing such training and capacity-building opportunities for their personnel is a key priority going forward.

Ecuador

★ Quito

Population: **15,779,000**
Internet Penetration: **35.1%**
Fixed Broadband Subscribers: **5.3%**

While no one ministry or agency is designated as the lead for cybersecurity in Ecuador, numerous national authorities and organizations share responsibility for promoting cybersecurity and combating cybercrime. The National Secretariat of Public Administration, through its Directorate for Technological Architecture and Information Security, promotes the use and implementation of an e-Government platform and oversees management of the security of information through the promulgation of regulations, decrees and ministerial-level agreements. The Ministry of Intelligence, through its Counter-intelligence and Info-communications Section and its Strategic Technological Operations Center, implement security measures within the central government entities, and are responsible for the formation of a national incident response capability. The Superintendency of Telecommunications is also responsible for the formation and eventual operation of a national CSIRT, tentatively called EcuCERT, through its National Information Technology Directorate. Primary responsibility for the investigation of cybercrimes and criminal activities involving ICTs lies with the Technological Crimes Investigations Unit of the National Directorate of the Judicial and Investigative Police, within the National Police. In some instances, the Cyber Investigations Unit of the Attorney General's office is also involved in investigations.

Although a national CSIRT has not been established, policies and procedures for cybersecurity and incident response have been developed and are in place. For example, Decree 166 of the National Secretariat of Public Administration establishes that all entities of the Central Public Administration must comply with technical standards for information security. Additionally, the organization has implemented the use of digital signatures, and formed 47 departments, each with a dedicated IT officer.

Despite past and current government-led efforts to engage other national CSIRTs and organizations active in the Americas, as well as Ecuador's participation in the Latin American Working Group on Cybercrime of INTERPOL, bolstering international partnerships remains an area for improvement.

The Technological Crimes Investigations Unit has begun to create spaces for increased inter-institutional cooperation between public and private sector entities, both within the country as well as at the international level. Emphasis has been placed on promoting the exchange of information and cooperation, particularly in the investigation of electronic fraud and child pornography.

Other key initiatives include: participation within the National Assembly to identify necessary reforms to the new Organic Comprehensive Criminal Code to define and typify cybercrimes in Ecuador; development and administration of a page on Facebook (www.facebook.com/CibercrimenPJ.EC) to promote awareness raising and prevention of cybercrimes through publication of complaints, security alerts, information campaigns, technical assistance, and cybersecurity tips for citizens; participation in the Security Committee of the Association of Ecuadoran Banks to share experiences

and coordinate investigations; and the organization of conferences and discussions at universities, high schools and schools about cybercrime and citizen cybersecurity.

On the awareness raising front, the Ministry of Intelligence has also created a project called "Promoting a culture of intelligence", which aims to do precisely that through democratization and more robust citizen participation.

While there are presently no courses offered that specifically deal with digital forensics and other aspects of investigation crimes involving the ICTS, the National Police are designing a curriculum to provide training through the various national police training centers to investigative agents and detectives within the Judicial Police. The Technological Crimes Investigations Unit does already receive other relevant technical training from higher education institutions within the country, as well as international organizations. Although national authorities have not designed any security-related software or tools, there are presently numerous proposals by academic and private sector actors to do so.

Two principle impediments to reducing cybercrime activities in Ecuador were identified. The first is the lack of adequate cybercrime legislation criminalizing specific activities and defining punishments. The second is the persistent lack of awareness among and educational resources for citizen users, regarding both the responsible use of the Internet and ICTs, and the proper utilization of security measures offered by social networks, email providers, microblogging sites, etc.

New legislation presently being considered would, if adopted into law, address a range of key issues, including: electronic commerce, and illicit access and attacks against data and systems integrity; illegal interception of data; falsification of information; electronic and computer fraud; child pornography and sexual exploitation; protection of intellectual property; and international cooperation, among others.

2013 was marked by an exponential rise in the number of computer-related complaints citizens logged with national authorities. Available data from the Automated System of Judicial Proceedings of Ecuador (SATJE) indicates that 93 percent of reported incidents were directed to national prosecutor's office, with the remaining 4 percent of reports going to units of the National Police and 3 percent via a "1-800 crime" number within the Interior Ministry. Cases logged by citizens included unlawful interception attacks on data integrity, system abuse devices, cyber forgery, computer fraud, child pornography, and offenses against intellectual property. The number of cases filed and accumulated in the period from 2008-2013, moreover, increased 203 percent and 458 percent, respectively.

Among the processes registered by the Crime Investigation Unit Technology of the National Police in 2013, the majority of cases (almost 80 percent) were by misappropriation through techniques such as skimming, phishing and exploitation of online payment systems. The National Police reports that in the second half of 2013 the country experienced significant increases in the number of such incidents of electronic fraud, with the single most effected group being the general public, accounting for 58.94 percent of all incidents reported. Citizens also fell victim to a range of other activities and crimes involving the use of ICTs, including murder, pyramid schemes, extortion, threats, interception of communications, and unauthorized access to information systems. Entities in the banking sector account for another large percentage of incidents recorded to the National Police, at 38.48 percent, as well including large numbers of reports of fraud perpetrated through phishing and skimming. And 2.58 percent of reported incidents targeted children and minors, such as pornography, grooming, sexual harassment and cyber bullying.

In late 2013, national authorities were alerted to a possible threat of a massive attack, or "hackathon", targeting the Ministry of Intelligence. Although the attack never materialized, the Ministry of Intelligence informed other national stakeholders and, in a show of cooperation, coordinated steps were taken to shore up potential vulnerabilities. While no other specific incident was

cited as having a major impact, a number of child pornography and electronic fraud cases were resolved positively, despite surprising authorities with the sophistication of the techniques used. Although the perpetrators were convicted and sentenced for crimes involving electronic fraud and child pornography, the present lack of adequate cybercrime legislation has prevented authorities from trying any persons for cybercrimes.

El Salvador

★ San Salvador

Population: **6,635,000**
Internet Penetration: **25.5%**
Fixed Broadband Subscribers: **3.8%**

Two ministries share responsibility for cybersecurity and cybercrime in El Salvador. The Ministry of Justice and Public Security is the designated lead for cybersecurity matters, while responsibility for the investigation of cybercrime rests primarily with the Computer Crime Investigations Group of the National Civil Police. The latter is presently in the process of transitioning into a new Cybercrime Unit.

A national CIRT has been established, with the acronym SALCERT and is operational. Although there is not yet an established national strategy or policy for cybersecurity, one is presently being developed.

The National Civil Police are currently formalizing a partnership with the United Nations Office on Drugs and Crime (UNODC) to receive cybercrime related training to bolster its existing capabilities, most of which have been developed in an ad hoc manner through self-training using online courses and informal interaction with counterpart authorities in the region.

There are established legal mechanisms in place which enable the National Civil Police to request the cooperation of private enterprises where information is required for combating cybercrime. In some instances, however, the law requires that these requests must be made by the Attorney General's Office, which has the constitutional mandate for carrying out criminal investigations. A new piece of proposed legislation entitled the Special Law against Cybercrime is currently being considered by the Presidency.

The government employs a strategy for data recovery and operational continuity within its own institutions based on the use of two remote storage sites in real time for information contained in network databases, a primary and a secondary site. When data is stored on a user's computer and not one of the two remote storage sites, forensics software is used for recovery. Within individual institutions, firewalls are employed for filtering out malicious packets of information, backed up by Oracle's Advance Security system for database security. External access through a VPN is password protected. The government adds that additional security measures, un-described here, are rigorously employed throughout its institutions. Individual users are provided a cybersecurity policy manual which provides explicit instructions about authorized and responsible use of government-run information systems.

Authorities cite a range of impediments to enhancing cybersecurity and combating cyber crime in El Salvador. Chief among these are budget constraints and the lack of support from ISPs in providing relevant information regarding users who are suspected of having committed a cybercrime. Similarly, the government does not maintain cooperative ties with companies based outside of El Salvador that provide relevant Internet services, such as email providers, social networks or website owners. The lack of a comprehensive legislative framework for combating cybercrime and the need for more training for investigators and prosecutors are other major deficiencies identified, as well as the need to increase opportunities for members of the emerging Cybercrime Unit to participate in regional and international capacity-building forums. Finally, authorities highlighted the lack of educational or awareness raising initiatives to better inform Internet and ICT users of risks and good practices to reduce their vulnerability.

A range of illicit activities have been reported to the National Police in recent years. Authorities reported that 72 cybercrime cases were opened in 2013, leading to 5 convictions. In addition, since the Computer Crime Division's inception in 2011, another 51 cases of child pornography, 26 cases involving threats or intimidation, 23 cases involving the illegal dissemination of information, and 15 cases of sexual harassment were reported.

And while current laws don't criminalize hacking as a crime per say (although it is considered in some cases a form communications fraud or a violation of security measures), hacking techniques are being employed for gaining unauthorized access to email accounts and social networks, which has provided a basis for committing other illicit activities such as extortion, illegal dissemination of information, etc. However, since the techniques used in the perpetration of the latter crimes are not themselves criminalized, there are no statistics available to asses any increase in their use.

In one noteworthy case, a sexual predator was contacting young victims through social networks, gaining their trust, and then inducing them into making and sharing sexually explicit videos and photographs. The National Police were alerted, an investigation was performed which led to the discovery of evidence on the perpetrator's computer. The individual was subsequently prosecuted and convicted for sexual predation of minors, a first for El Salvador.

Going forward, government authorities will emphasize passage of the more comprehensive Special Laws against Cybercrime, the development of a national strategy and policy for cybersecurity, further developing the capacity of personnel responsibility for incident management and investigation of cybercrimes, awareness raising, and strengthening international partnerships.

Grenada

★ St. George's

Population: **103,000**
Internet Penetration: **42%**
Fixed Broadband Subscribers: **13.7%**

The lead agency for cybersecurity and cybercrime in Grenada is the Royal Grenada Police Force, and specifically its Information and Communications Technology Department (ICT). While the government does not have a national cybersecurity strategy and has not created a national CIRT or other framework for managing cyber incidents, it is in the process of considering undertaking a national awareness raising campaign, through the Telecommunications Regulatory Commission. And in 2013 the legislature passed Electronic Crimes Act #23, which increases the government's ability to prosecute cyber criminals.

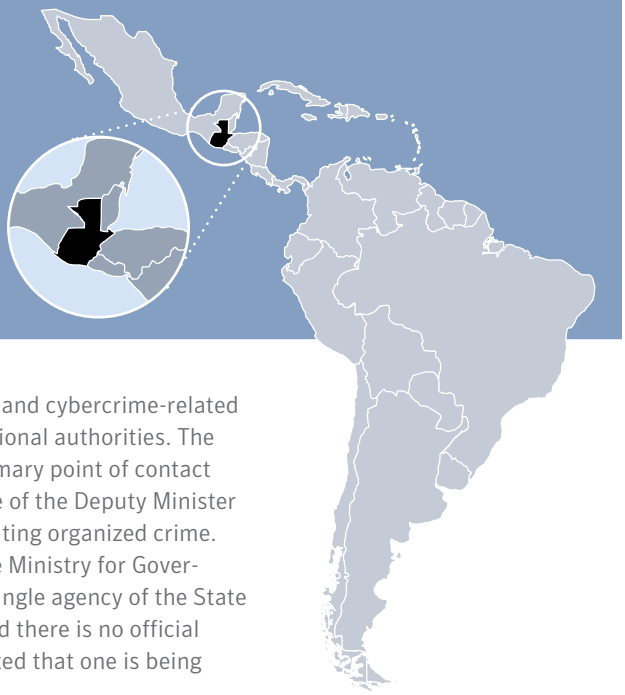
Private sector entities are not required to report information regarding cyber incidents to national authorities, and the government does not actively work with private sector entities on matters of cybersecurity. National authorities reported that collaboration with other countries is fruitful, although it is done in an unofficial manner. A partnership between the government and the ITU and IMPACT included an assessment of the country's cybersecurity posture and yielded recommendations for steps the government can take going forward. There are presently no cybersecurity-related degree programs or other course work on offer within the country's academic institutions.

National authorities report not having observed an increase in the number of cyber incidents or other illicit cyber activity in the past year, and have no record of any significant cyber incidents having taken place. The lack of a national CIRT was identified by government authorities as the major impediment to advancing cybersecurity in Grenada.

Guatemala

★ Guatemala City

Population: **15,440,000**
Internet Penetration: **16%**
Fixed Broadband Subscribers: **1.8%**



To the degree that it is officially designated, responsibility for cybersecurity and cybercrime-related efforts within the Government of Guatemala is shared between multiple national authorities. The national incident response capability, CSIRT-gt, effectively serves as the primary point of contact and national coordination body for cybersecurity-related matters. The office of the Deputy Minister of the Interior is responsible for increasing the country's capacity for combating organized crime. In addition, the Directorate for IT, under the Vice Ministry for ICTs within the Ministry for Governance, also performs certain cybersecurity related functions. However, no single agency of the State is designated as the lead for cybercrime investigations or related efforts, and there is no official national strategy or policy for cybersecurity as of yet, although it was reported that one is being developed.

Notably, while CSIRT-gt (www.csirt.gt) has been created in practical terms, it is not officially established by law, and is essentially operating as a pro-bono service being offered by its public sector constituency. One other CSIRT—CERT-Cyberseg—was recently established in the country and is in now operation. However, it is a private sector entity and does not have national level responsibility.

The existing legislative framework for cybersecurity and cybercrime was established in 2009, when the national Congress passed a Law on Computer Crimes which aimed to provide a basis for preventing and punishing cybercrimes and protecting the confidentially, integrity and availability of data and information technologies. Current efforts are underway to update the legislative framework, as well as to promote legal and regulatory modifications to enable the official creation and operation of the national CSIRT under the Ministry of the Interior.

Private sector entities are not legally obligated to share information regarding specific incidents with national authorities, and there are presently no formal agreements between the two sides regarding such cooperation. The one exception is financial institutions under the supervision of the Super Quartermaster of Banks (SIB), which are required to report when they have been affected by a cybersecurity incident. Authorities acknowledged that the general lack of cooperation with the private sector largely owes to the lack of a national strategy for cybersecurity as well as the lack of a legal framework for prosecuting most activities that might be deemed "cybercrimes". When government authorities require such information they request it directly from the private sector entity in question, however information was not provided as to the rates of compliance with these requests.

Cooperation between Guatemalan authorities and their counterparts outside of the country is limited and generally occurs in an informal and ad hoc fashion, between persons or offices where contacts have been made through participation in regional workshops or other activities. Such engagement is limited primarily to entities in Central America and the Caribbean.

Authorities reported that there are cybersecurity-related programs and courses on offer at universities and academic institutions in Guatemala, including a graduate-level program in computer security at one particular university. No additional information was provided however.

The Government of Guatemala presently does not maintain any official or organized cybersecurity awareness raising initiative. However, individual personnel working on aspects of cybersecurity do undertake their own efforts to raise awareness and promote more of a culture of security, for example through blogs and interviews given to local newspapers.

National authorities reported having observed several important trends over the past year. These include the following approximate increases in the frequency of the specified activities: skimming – 100 percent; credit / debit card cloning – 50 percent; various forms of online/email fraud (e.g. Nigerian scam, "sweepstakes offers", etc) – 100 percent; spam – 200 percent (likely owing to the absence of a law restricting its use); and unauthorized access to information systems – 100 percent. In addition, authorities have observed an increase in DDoS attacks, which is supported by data provided by the private CSIRT (CERT-Cyberseg). However it is unclear whether there is indeed an upward trend, or more such incidents are simply being detected by CERT-Cyberseg's sensors. Authorities also acknowledged that the reported numbers regarding incidents of credit / debit card cloning may be low, as they suspect banks are reluctant to share complete information for fear of adversely impacting their reputation and market share. At least one incident was reported where a bank was known to have suffered significant losses as a result of such an illicit operation, but no exact numbers or other specifics were made public.

While no particular investigations or convictions were reported, authorities highlight as a success over the past year the progress achieved with the development of CSIRT-gt as a resource for public and private sector institutions, and focal point for outreach to and assistance from regional and international partners. Similarly, some authorities see the creation of CERT-Cyberseg, the first private CERT in the country, as another success story, citing that it has on some occasions coordinated with the CSIRT-gt in responding to incidents involving online scams, spam, attempted infiltrations, and small-scale DDoS attacks.

Guatemalan authorities highlighted numerous impediments to promoting increased cybersecurity in their country. The first of these is the previously mentioned lack of a national policy or strategy for cybersecurity, the result of which is that the entities of the State continue to work in an ad hoc and fragmented fashion. Equally important is the lack of a legal framework to criminalize certain activities as cybercrimes and provide a basis for investigation and prosecuting them. Authorities also emphasized the absence of a culture of cybersecurity and the lack of awareness at all levels, which makes individual users more vulnerable, and inhibits the government from taking the requisite steps to securing the country's critical and information infrastructures. Finally, it was again cited that updates to the legal and regulatory regimes must be made to enable the official formation of the national CSIRT, and provide it the human and financial resources that will allow it to develop into an effective national incident response capability.

Guyana

★ Georgetown

Population: **798,000**
Internet Penetration: **33%**
Fixed Broadband Subscribers: **3.7%**

The Government of Guyana has made several noteworthy advances on the cybersecurity front over the past year. Chief among these was the creation of the Guyana National Computer Incident Response Team, or GNCIRT (www.cirt.gy) in August 2013. Although GNCIRT is still working to develop its policies, procedures and capabilities, it is operational and has been designated as the authority responsible for managing cyber incidents at the national level. The investigation of cybercrimes remains the responsibility of the Criminal Investigations Department of the Guyana Police Force. Presently the Government of Guyana does not have an overall guiding policy or strategy for cyber-security. Under the leadership of the four person GNCIRT, however, it is planning to develop this year a national cybersecurity awareness raising initiative, potentially based on the STOPTHINK-CONNECT campaign. Furthermore, national authorities report that they are working to create a policy framework for addressing cybersecurity in a more strategic, comprehensive, and pro-active manner.

There is no legal requirement for private sector entities to report cyber incidents to the government, although national authorities consider it a high priority to work in partnership with the private sector to support improvements in cybersecurity. However, mandatory reporting by government agencies is currently under consideration as a means to promote more effective cybersecurity administration and the gathering of accurate and detailed statistics on cyber incidents.

Collaboration with counterpart authorities in other countries has increased somewhat, mainly through the membership of GNCIRT in the OAS-CICTE network and the strengthening of contacts with other national CIRT personnel in the Americas through participation in OAS-CICTE training and conferences. Organizational level, CIRT to CIRT collaboration and partnership remains to be strengthened, however. There are presently no cybersecurity degree programs or relevant coursework on offer within the country's academic institutions.

Since GNCIRT's creation in August 2013, the country has experienced numerous cybersecurity incidents ranging from the defacement of government websites to credit card fraud to the defrauding of a prominent businessman. Although authorities do not have hard data indicating a quanti-tative increase or decrease in the number of incidents, there has been a clear rise in the number of incidents reported by the public. The aforementioned defrauding of a businessman received particular attention in the press, after the individual, whose identity remains unknown, was tricked into depositing payments into fraudulent bank accounts. In February 2013, there was another high profile incident in which ten websites, including seven websites of the Government of Guyana, were defaced by international hackers who later touted their exploits on their Facebook pages and on hacker websites. In the case of the second incident, GNCIRT was able to coordinate with and support the other affected government agencies as well as the local private hosting company, and provided daily situational analysis to the government minister with responsibility for national security.

According to government reporting, the major challenges facing Guyana's cybersecurity advancement going forward include the lack of personnel with the requisite cybersecurity skill sets, inadequate training opportunities to build cybersecurity capacity, and the fact that while cybersecurity is among national priorities, it still is not viewed as a first level security imperative.

Haiti

★ Port-au-Prince

Population: **10,671,000**
Internet Penetration: **9.8%**
Fixed Broadband Subscribers: **N/A**

The Government of Haiti has identified cybersecurity as a priority and is actively taking steps to enhance its national capacity for managing cyber threats and combating cybercrime, yet much work remains to be done. There is no official national policy or strategy for cybersecurity, and no agency within the Haitian government is officially tasked with responding to cyber attacks or cybercrime. However, an e-Governance unit established within the Prime Minister's cabinet (Primature) has been assigned responsibility for working with other government agencies and stakeholders to develop a national cybersecurity framework and capability. This unit recently created a working group in partnership with the national telecommunications authority (CONATEL), the national police, and the Secretariat of National Security, with the aim of advancing the national cybersecurity agenda.

Today, a number of agencies are engaged on a case-by-case basis, often with the support of cooperating foreign authorities. The Central Directorate of the Judicial Police (Direction Centrale de la Police Judiciaire - DCPJ), for example, has taken the lead on investigating identified cyber attacks. In conjunction with the national e-Governance Coordinator, CONATEL has undertaken an awareness raising campaign consisting of a series of events to inform decision-makers and other national stakeholders and assess opportunities to combat cyber and IT related vulnerabilities and crime. And a key focus in early 2014 has been the development of the multi-stakeholder task force, which has several objectives, including: devising a national strategy, working with members of parliament to draft and pass requisite laws, creating and building a national CIRT, working with the DCPJ on the investigation of cybercrime and attacks, and strengthening partnership with the private sector and international community. Government authorities have actively sought to benefit from available training and technical support offered by regional and international partners, including the OAS, ITU, and entities within the European and the Caribbean communities. Also, in line with the objective of harmonizing relevant national legislation with that of other countries in the Caribbean, proposed new laws are presently under consideration regarding electronic signatures, online public services, and e-commerce. To improve response capabilities and inter-agency cooperation, CONATEL and numerous private sector actors have recommended that a national CIRT be created as soon as possible.

While the private sector is not required to report cyber incidents to national authorities, and no official links or liaisons between the government and private sector exist, there is some degree of informal and unofficial cooperation. A survey conducted last year by CONATEL suggested that banks

and telecommunication operators are generally well informed on the issue of cybersecurity, and most large enterprises have internal security teams. Those entities which reported cybersecurity as a low priority attributed this to either a lack of resources or a lack of concern about the likely costs of cyber threats. The aforementioned national task force will seek to engage key private sector stakeholders and will have increased cooperation and information-sharing as a core objective.

In terms of capacity-building, while some Haitian academic institutions offer course work in cybersecurity or related topics, most do not, and there are no formal cybersecurity degree programs in the country. Most Haitian cybersecurity experts have been educated abroad, many of them in France, and now work in areas ranging from information security to cyber law and information warfare, albeit in the absence of a community of peers or the underlying technical support structure that exists in other countries.

Haitian authorities report that the single biggest impediment to cybersecurity advancement is a lack of financial resources, and assert that despite their willingness to adopt the policies, plans and procedures required to become more cyber secure, present budget levels make doing so difficult to impossible. Nonetheless, some progress is being made. Operations carried out in early 2014 led to the capture of 69 criminals, 11 of whom have subsequently been convicted of cybercrimes.

Government authorities report a marked increase in the number of known cyber incidents, most of which involve social networks and the theft and/or misuse of users' identities and information. One such incident that received public attention involved the unauthorized access and misuse of the email account of a member of parliament.

Recognizing that the lack of a national cybersecurity framework makes Haiti vulnerable to cyber attacks and crime, as well as a potential haven for cyber criminals, authorities express a strong commitment going forward to working both internally and in collaboration with all interested partners to develop the country's cybersecurity capabilities. The timing is perfect for the creation a cybersecurity policy. From the government to the private sector, key players are emphasizing the necessity of a response team.

Jamaica

★ Kingston

Population: **2,715,000**
Internet Penetration: **46.5%**
Fixed Broadband Subscribers: **4.3%**

The lead agency for cybersecurity related matters in Jamaica is the Ministry of Science, Technology, Energy and Mining (MSTEM). The investigation of cybercrime falls under the purview of the Communication Forensic and Cybercrime Unit (CFCU) of the Jamaica Constabulary Force (JCF). The Ministry of National Security and the Office of the Director of Prosecution also play an influential role in on-going efforts to build a national cybersecurity regime.

Notably, the Government has established a National Cyber Security Task Force (NCSTF) comprising a broad cross-section of stakeholder representatives from the public and private sector, as well as academia and civil society. The NCSTF is charged with several core tasks. These include: assisting in creating a framework to build confidence in the use of cyberspace and the protection and security of related assets; promoting greater collaboration amongst all stakeholders; establishing a public education and awareness program; and formulating a strategy to develop, grow and retain high quality cyber talent for the national workforce.

Although the government has not yet adopted a national policy or strategy for cybersecurity, under the leadership of MSTEM and with assistance from the OAS the aforementioned NCSTF has begun a process to develop one. A first draft of a strategy was produced and is being reviewed by the relevant authorities and is expected to be finalized by the end of the first half of 2014.

The government is also in the process of establishing a national CSIRT to assist in the protection of Jamaica's online cyber infrastructure by coordinating efforts to prevent and respond to cyber threats. An assessment report and CSIRT User Requirement Specifications have been prepared with assistance from the International Telecommunication Union-International Multilateral Partnership against Cyber Threats (ITU-IMPACT). Government authorities hope that the CSIRT will become operational sometime in 2014.

Jamaica does not currently have a national cybersecurity awareness raising campaign, however the creation and implementation of one is a key strategic objective of the current draft cybersecurity strategy. Additionally, there are existing initiatives led by entities in the private and public sector, for example financial institutions and the JCF respectively, which seek to build awareness about specific areas of cybersecurity.

In response to the rising incidence of cybercrime, an eleven member Joint Select Committee of the Houses of Parliament was established in January 2013 to consider and report on the operation of the Cybercrimes Act. The recommendations made by the Committee for amendments to the Act were adopted by the Houses of Parliament, and efforts are currently under way to implement them. These include increasing the penalties for offences defined under the Act and the criminalization of actions prejudicing investigations and activities such as computer related fraud, forgery and malicious communication.

In May 2014, the High Court heard a case which resulted in a successful cybercrime prosecution, and there are presently at least three other cases being prosecuted in the courts with charges under the Cybercrimes Act.

Training and capacity-building for key government personnel is on-going, with police and prosecutors receiving training in key aspects of cybersecurity and cybercrime, and Management Information System Officers from throughout the government receiving training in network security.

Presently, private entities are not required to report information related to hacking or cyber attacks to government authorities. However, there is cooperation between the police and private entities where the former is engaged to investigate an incident or breach affecting the latter. The draft national strategy identifies defining measures and mechanisms for increasing public private sector cooperation and information-sharing as a core objective.

Although, to date, no significant incident or detected threat has necessitated collaboration with other countries, recognizing the eventuality of such an incident has spurred the creation of a national CSIRT and other steps contemplated under the draft strategy.

In terms of the availability of academic training in cybersecurity, Jamaica is in a relatively better position than most of its neighbors in the Caribbean region. Two of the major universities (Northern Caribbean University and the University of the West Indies) offer degrees in computer science with some degree of specialization in information security and network security, as well as more advanced coursework in cryptography. Other institutions (University of Technology and University College of the Caribbean) require students seeking a computer science degree to complete coursework on computer and IT security.

In terms of trends observed, national authorities report a 15 percent increase in cyber incidents in 2013 as compared to the year prior. The most prevalent activities reported included third party transaction online fraud, cyber defamation and cyber extortion. Despite increased reporting of such incidents to government authorities, only about 5 percent of the perpetrators were found, due mainly to the minimal level of support received from entities in other jurisdictions.

National authorities have identified several key challenges facing Jamaica in the area of cybersecurity, including: the lack of a official cybersecurity strategy to ensure a cohesive framework; the lack of a national CSIRT/CERT; insufficient personnel in the CFCU to investigate cybercrime incidents in a timely manner; and a deficiency in the level of awareness of cybersecurity imperatives and the effects of cybercrimes. As the above information reflects, however, steps are actively being taken to address each of these challenges in the short to mid-term, and improvements are expected.

Mexico

★ Mexico City

Population: **118,419,000**
Internet Penetration: **38.4%**
Fixed Broadband Subscribers: **10.5%**

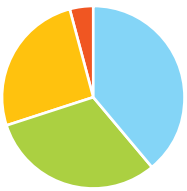
The Federal Police of Mexico serve as the lead operational authority for cybersecurity and cyber-crime-related efforts in Mexico, although numerous other government institutions also play an active role. Within the Federal Police the Scientific Division maintains a unit responsible for coordinating activities to investigate, prevent and prosecute all conduct considered criminal and which utilizes electronic and cyber means. In addition to developing a wide range of IT, information and communications security-related activities at the national level, this unit also employs special investigative techniques like monitoring public Internet activity, use of simulated user figures, and undercover operations. The Scientific Division is also where the lead CSIRT with national-level responsibility, CERT-MX, is housed. Although CERT-MX does not maintain its own website, its contact details can be found on the website of the Forum of Incident Response and Security Teams (FIRST).

Additionally, to engage all key stakeholders in advancing the country's cybersecurity agenda, the Specialized Information Security Committee (CESI) was created to develop a National Strategy for Information Security (ENSI), which guides all actions to be undertaken by entities of the federal government to prevent, identify, neutralize or counteract risks and threats to information security. The ENSI was created based on a recognition of the need for clearly articulated, coordinated and concrete actions to strengthen the capabilities of the State in the areas of information security , cybersecurity, cybercrime , cyber defense and the protection of critical infrastructures. Through CESI, authorities have also developed a Collaboration Protocol between CERT-MX and the various dependencies of the Mexican central government, to address and respond to cyber incidents that could potentially jeopardize the country's critical infrastructures.

Personnel at the Scientific Division have received and continue to participate in specialized training from the Police Development System of Mexico (SIDEPOL), as well as from numerous other security and law enforcement organizations in countries including Colombia, the US, Holland and Japan. Emphasis is placed on securing instruction to ensure that personnel are trained in accordance with their specific responsibilities, and that their knowledge and skills are as up-to-date as possible. Training relating to digital investigations and forensics has focused on chain of custody, identification and confiscation of digital evidence, telephony analytics, digital forensics and forensics of cellular devices. Additionally, some personnel have received training from non-governmental organizations such as both the National and International Centers for Exploited and Disappeared Children (NCMEC and ICMEC, respectively).

Entities Affected by Cyber Crimes

Source: Government of Mexico



39% Academia
31% Government
26% Private Sector
4% Other

To ensure continuity of operations and data assurance at the institution level, information is backed up and data recovery techniques are applied to individual devices as required. Also, compliance with ISO standard 207001's requirements for an information security management system is required of all key government institutions.

Requests for cooperation with private sector entities are generally filed through the Public Ministry's Social Representation division. CERT-MX also communicates and cooperates directly with private financial institutions. The ENSI has as one of its primary aims further increasing and institutionalizing cooperation and information-sharing between all sectors of society – public and private – in a more integrated fashion.

CERT-MX has made significant advances in promoting the establishment of organization-level CSIRTs in many federal institutions, and is encouraging that similar capabilities be created within key industries in the private sector to facilitate more effective and coordinated response to cyber incidents.

Mexican authorities have developed active collaborative relationships with other governments and international organizations, working both with national law enforcement entities and CSIRTs, as well as through International organizations like FIRST and the Organization of American States (OAS/CICTE).

Government-led efforts to promote increased cybersecurity awareness have included the organization of various conferences for both government institutions and educational institutions (elementary to university levels), as well as outreach to citizens and other public and private entities.

Government authorities cited numerous impediments to reducing cybercrime and enhancing cybersecurity in Mexico. Among these is the continued lack of legislation enabling law enforcement to take immediate action for addressing cybersecurity threats and incidents of cybercrime. The limited capacity of law enforcement to act in many instances undermines investigations, perpetuates a sense of impunity among organized criminal groups, and enables the latter to deploy the latest technologies and techniques to commit crimes. The other major impediment identified is the continuing lack of awareness of cybersecurity, including risks and good practices, among the general population.

According to data maintained by the Scientific Division of the Federal Police, there was a 113 percent increase in cybersecurity incidents in 2013 compared to the previous year. Also, preliminary data so far for 2014 suggests an even more pronounced increase in detected incidents, up as much as 300 percent over 2013. It should be noted that the marked increase in the present year is largely attributed to improvements in the processes for identifying incidents nationally and across the generation of new attack vectors.

Of the incidents reported to the Mexican Federal Police, and excluding incidents involving individual citizens, approximately 31 percent targeted government institutions, 26 percent targeted private sector entities, 39 percent targeted academia, and 4 percent targeted other entities. Incidents of unauthorized logical access have increased by approximately 260 percent, malware infections have increased by 323 percent, and incidents involving phishing have increased by 409 percent, while denial of service attacks have *decreased* by 16 percent.[01]

Significant increases were also observed in incidents involving Advanced Persistent Threats (APTs) targeting mid-sized companies and the use of malicious code to hijack users' information as a basis for subsequent efforts at extortion. The latter has also prompted a rise in the use of malware that uses complex security encryptions to attack the servers of Small and Medium-sized Enterprises (SMEs), thus increasingly impacting the productive sector.

01 The source of this information is the Government of Mexico. These statistics only cover cases where an official cybercrime investigation was initiated, at the request of the affected entity.

The most commonly reported cybersecurity incidents included the use of malware, phishing, hacking and defacement, and systems intrusions. The most frequently reported incidents of fraud and extortion included e-commerce fraud, Nigerian scams, e-banking fraud and extortion. In addition, reports of individual grievances included defamation, threats, password theft, identity theft, and harassment.

One particularly noteworthy case involved the use of a Ransomware disguised as "Anti-Child Porn Spam Protection 2.0." The perpetrator gained access to his targets' computers, installed the malware, encrypted their contents, blocked the owners' access, and demanded three thousand US dollars to recover the files. Since this case, however, authorities say that they have been limited to only some lines of investigation given their lack of information regarding the latest techniques of intrusion and malicious coding.

Given the fact that each State within the Mexican Federation independently prosecutes individuals for crimes committed, there are no available numbers regarding the total number of prosecutions nationwide for cyber-related crimes.

Nicaragua

★ Managua

Population: **6,216,000**
Internet Penetration: **13.5%**
Fixed Broadband Subscribers: **1.7%**

Within the Government of Nicaragua responsibility for cybersecurity and cybercrime related matters is shared between several agencies and institutions. The two primary entities for these matters are the Nicaraguan Committee on Science and Technology (CONICYT - www.conicyt.gob.ni), and the Commission on Electronic Government in Nicaragua (GOBENIC - http://www.gobenic.gob.ni), attached to the Vice Presidency.

The Government of Nicaragua has no official cybersecurity strategy or policy. Presently, both CONICYT and GOBENIC address the use and exploitation of ICTs affecting information systems, the public's information, and e-commerce, with relatively little emphasis on the security of information systems themselves. It is intended that the two authorities will soon propose new legislation on cybercrime as well as new governmental information security policies to prevent and respond to incidents targeting information systems.

To date the Government of Nicaragua has not established a formal CSIRT or mechanism, procedure or policy for responding to cyber incidents. As such there is no national level capacity for providing an immediate response to a critical security incident.

Similarly, there is no officially designated office, division, unit, etc tasked with preventing or investigating cybercrimes. However, the National Police has carried out investigations involving computers and/or digital evidence, mainly relating to credit card cloning, and conducted forensic analysis and the retrieval of digital information for presentation as evidence in criminal trials involving organized crime and money laundering, among other felonies. These efforts have involved the work of several

branches of the National Police, including: the Special Crimes Division, the Directorate of Economic Investigations, the Directorate of Police Intelligence, the Directorate of Legal Aid, and the Central Crime Laboratory. And the Central Crime Laboratory increasingly provides support to other institutions of the State when an incident requires digital forensic analysis.

Notably, the Directorate of Economic Investigations has proposed the creation of a Department of Computer Forensics (DAFI), to serve as a technical body to specialize in and coordinate the work of the different law enforcement and judicial entities combating organized crime and other complex crimes where the use of ICTs is commonly involved. Additionally, the Central Crime Laboratory has created a department specialized in the analysis and verification of audio visual evidence in digital formats to support relevant criminal investigations. Officials working on these matters within the National Police receive training from experts from numerous other countries including Mexico, Guatemala, El Salvador, the US, and Spain.

While there have been no new pieces of legislation passed recently, Nicaragua does have in place a legislative framework that enables government authorities to investigate and prosecute certain activities involving ICTs, and otherwise take steps to enhance the country's cybersecurity posture. The relevant laws currently in place include: Article 197 on prohibited records (Title III, Chapter I), Art 198 on access and unauthorized use of information (Title III, Chapter I), Art 229 on IT scams (Title VI, Chapter V), Art 245 on the destruction of computer records (Title VI, Chapter VIII), Art 246 on use of destructive programs (Title VI, Chapter VIII), Art 250 on the protection of software (Title VI, Chapter IX), and Art 275 on the seizure of company secrets (Title VI, Chapter VIII).

It was reported that at present a majority of lawmakers in Nicaragua believe that the use of ICTs and the Internet are primarily a means to the commission of other common crimes – such as fraud, money laundering, child pornography, forgery, intellectual property theft, corruption of minors, extortion, threats, terrorism, etc – rather than an area of activities that are potentially crimes unto themselves. As such, the current consensus in the legislature is that there is no compelling need for a new and separate law on cybercrime.

While Nicaragua's Criminal Code requires that any person with information regarding a crime under investigation share that with the investigating authorities, there is no other legal obligation for private companies to report to the government on cyber attacks or other incidents causing damage or loss of data. In general to obtain information relating to a specific incident investigating authorities must make a formal request to the relevant ISP or other operator. Authorities reported that private sector entities in Nicaragua, including the regulatory body for telecommunications, tend to underutilize their data backup systems, and there are no supervisory or control procedures regarding the use of proxy servers or data retention such as would support the investigation of cybersecurity incidents.

International cooperation between Nicaraguan authorities and their counterparts in other countries has been limited. Authorities cited one instance of collaboration where INTERPOL in Nicaragua cooperated with Spanish authorities in an international investigation of a pedophilia ring involved in producing and publishing child pornography on the web from Spain.

Numerous academic institutions including the National University of Engineering, Central University, and National University of Managua offer coursework and specialized training in information security-related topics and computer forensics.

The government has not developed a national campaign for cybersecurity awareness. According to authorities, only private financial institutions are actively engaged in cyber awareness-raising. However, a national television and radio campaign has sought to inform parents about how to protect their children from exploitation and trafficking, including against threats online and involving the use of ICTs.

National authorities reported not having hard data or quantitative statistics concerning changes in the incidence of cyber incidents or acts of cybercrime in 2013. However, based on available information, the commercial sector was the most adversely affected in the past year. In one incident deemed particularly significant, persons gained unauthorized access to a web server and carried out a massive denial of service attack on several service sites assigned to various companies, causing damage to subscribers sites. The perpetrators worked for one of the companies in question and were identified through analysis of IP addresses and logs obtained from the affected servers, and service was restored. Several other success stories entailed investigations that received the support of ISPs that agreed to identify the source of malicious electronic communications, fraud, scams, extortion, threats or the like. That information was then utilized as evidence in judicial proceedings which culminated in successful convictions.

Going forward, national authorities cited several key challenges or impediments that will need to be overcome to enhance Nicaragua's cybersecurity regime. First, the political will of legislators will need to be won over through efforts at raising their awareness of the need for new cybercrime legislation, as well as for a new specialized unit responsible for identifying, investigating and prosecuting the perpetrators of these crimes.

Similarly, efforts must be undertaken to increase political will at the highest levels of the government to participate in forums sponsored by regional and international forums and initiatives. Existing and new laws should also be reviewed, strengthened and harmonized, and rules regarding criminal procedures should be clarified to ensure that competent national authorities have the ability to investigate and prosecute cybercrimes. A Technologies Crime Unit should be formally established within the structure of the National Police, to serve as a specialized technical body for research, analysis and coordination in response to the needs of law enforcement and judicial authorities.

It was further recommended that an official national CSIRT be formed to lead efforts to prevent, respond to and mitigate the effects of cyber incidents, and to coordinate between government and other possible stakeholders in the event of a cyber attack or major act of cybercrime. A more dynamic and effective international cooperation regime should be pursued, to improve information sharing and increase training opportunities for relevant personnel regarding the latest threats, technologies and techniques.

Finally, authorities stressed the need to develop an integrated national approach to cybersecurity under the leadership of CONICYT and GOBENIC, with the aim of reducing Nicaragua's cyber vulnerabilities.

Panama

★ Panama City

Population: **3,605,000**
Internet Penetration: **45.2%**
Fixed Broadband Subscribers: **7.8%**

Within the Government of Panama, the institution responsible for the supervision and leadership of cybersecurity-related matters is the National Authority for Government Innovation (AIG), which operates through the national cybersecurity incident response center, CSIRT Panama. The Special Prosecutor for Crimes against Intellectual Property and Information Security, which is part of the Public Ministry, and the Directorate of Judicial Investigation, serve as the lead agencies for the investigation and prosecution of cybercrimes.

In early 2013 the Government of Panama approved the National Strategy for Cyber Security and Critical Infrastructure Protection (ENSC+IC), which guides and coordinates all national efforts to advance the country's cybersecurity posture. The ENSC+IC has a number of core objectives, including: combating the use of ICTs for criminal or terrorist purposes; protecting minors; increasing the resilience of critical infrastructure to cyber incidents or attacks; cybersecurity education and awareness raising, including regarding good practices and prevention; strengthening partnerships with private sector, civil society, academic and other stakeholders; increased national and international collaboration; and fostering a culture of cybersecurity. The ENSC+IC is currently being implemented by various institutions of the state, and official estimates are that it will take no less than 3 years to achieve full implementation.

PANAMA-CSIRT is the National Cyber Incident Response of Panama, operated by the National Authority for Government Innovation and designated by Executive Decree No.709 (2011). PANAMA-CSIRT coordinates all activities to prevent and respond to cyber attacks targeting government information systems and infrastructures deemed critical to the State, and serves as the focal point for engagement with national CSIRTs in other countries. It also fosters on-going collaboration and advises stakeholders regarding measures to increase security; serves as a repository for information about incidents, tools, and techniques for cyber protection and defense; and researches and disseminates information on new technologies and tools in the field of cybersecurity.

An investigative unit for computer crimes was created within the Directorate of Judicial Investigation, and is being developed and trained to perform investigations and digital forensics. Initial training for personnel includes instruction from technical staff from the Office of Information Security, which will eventually be supplemented with an internship in the Office and the Institute of Legal Medicine in Forensic Computing. Authorities reported that the scope of the training will eventually be expanded to strengthen trainees' investigative capabilities to conduct confiscation, collection and management of digital evidence.

To date, Panama has countered illicit cyber activities with various instruments, most of which have been relatively recently adopted. These include the National Strategy for Cyber Security and Critical Infrastructure Protection (2013); the Country Position Paper On Resilience of Critical Infrastructure, Protection of Minors on the Internet, and Cyber Security (2013); Law 79 – Adoption of the Budapest

Convention (2013); and official accession to the Budapest Convention (2014). There is also presently an initiative before the National Assembly to amend the Criminal Code on the subject of computer crime.

Panama 's access to the Budapest Convention marks a significant step forward in the government's agenda to combat cybercrime. To be in compliance with the instrument, the country's Penal Code will be amended to include new behaviors as acts of cybercrime and laws concerning digital evidence collection and the protection of personal data will be developed.

Private sector entities in Panama are not required to report information related to cyber attacks, regardless of whether data may be compromised. However, government authorities have endeavored to strengthen their relationships with the private sector in different aspects of cybersecurity, especially where private entities own or operate infrastructure or provide services deemed critical to the State. For example, despite the absence of regulations requiring reporting or information-sharing, national authorities maintain open and active lines of collaboration with key private enterprises in the banking and hydroelectric sectors. However, there is an established legal mandate dictating that private companies are obliged to cooperate with the police and the Attorney General when an investigation is on-going, including by providing assistance or information as required.

CSIRT Panama has collaborated with various other national CSIRTs in the region and globally, including those of Brazil, Germany, Mexico, and Venezuela, to name but a few. And the country's recent accession to the Budapest Convention provides a framework for potential on-going collaboration in the form of investigations, mutual legal assistance, and extraditions with a number of countries inside and outside the Americas.

National authorities reported that both public and private universities offer Master's degrees in computer security, computer engineering, controls and auditing. In addition, both the National Authority for Government Innovation, through its Technology and Innovation Institute, and the National Institute for Human Development, provide specialized courses in topics related to cybersecurity and cybecrime.

In 2013, Panama formally joined the messaging movement STOPTHINKCONNECT to leverage and implement throughout the country an awareness raising campaign to foster a culture of cybersecurity and combat cybercrime. Moreover, CSIRT-Panama offers open seminars and workshops focused on administrative and technical aspects of information security for ICT staff of public institutions as well as interested persons from civil society.

Panamanian authorities reported that the number of recorded cyber incidents increased by 30 percent from 2012 to 2013. A particularly significant increase was observed in the percentage of incidents involving phishing, which increased from 7 percent in 2012 to 47 percent in 2013. A similarly large increase was noted for malware-type incidents, which rose from 3 percent to 21 percent of all of the incidents attended to by CSIRT-Panama, thus becoming the most commonly reported type of it handled last year. Other increasingly common incidents included: web defacement, unauthorized access to systems and accounts, and DoS attacks. The most frequently reported cybercrime-related activities included: child pornography, cyber bullying, intellectual property theft, identity theft, fraud and financial crimes, and attacks on social networks.

In terms of the processes or assets that are most exposed and vulnerable unauthorized access and data breaches, authorities identified banks web pages, government web portals, individual email accounts, commercial accounts, institutional postal accounts, and trading processes. This assessment does appear to align with the available data on cybercrime cases that were initiated in 2013. Authorities reported that a total of two hundred sixty-two (262) cases were opened last year, including: 118 cases of financial crime, 85 cases involving a violation of computer security, 30 cases of child pornography, and 1 case of terrorism, among others.

As an example of a major incident reported, authorities highlighted a case involving a person gaining unauthorized access to the social network Twitter. The attack was carried out from a server in Panama, and after an investigation the perpetrator was identified and apprehended. Incidentally, investigators have encountered some difficulty in collecting the necessary evidence from the server because the latter is programmed in LINUX, with which the investigators were not familiar.

Given the many advances made by government authorities in 2013, it is not difficult to identify examples of successful efforts undertaken. Authorities cited the country's accession to the Budapest Convention on Cyber Crime as perhaps the biggest achievement to date.

Government authorities emphasized that the present position of the Panamanian state is a clear reflection of the country's commitment to free access to information, the resilience of critical infrastructure, and the protection of government systems and personal data of citizens. Nonetheless, authorities acknowledged more must be done. The main obstacle to the further development of cybersecurity in Panama was reported to be due to the lack of knowledge of the dependence of critical infrastructures on computer systems. This lack of knowledge makes it difficult to raise awareness on the subject as well as gain budget approvals for technical projects. Other impediments cited include the need for more training, the fluid and evolving nature of technology, the need to equip a computer forensics lab, the lack of a cybercrime research unit, and the tendency for victims not to report cybercrimes. The emerging National Strategy and Action Plan and other on-going initiatives should seek to address each of these in the short to midterm.

Paraguay

★ Asuncion

Population: **6,849,000**
Internet Penetration: **27%**
Fixed Broadband Subscribers: **1.2%**

The national Cyber Emergency Response Team (CERT-py), within the National Secretariat for Information and Communication Technologies (SENATICs), is the designated lead authority for cybersecurity in Paraguay, while the Specialized Unit for Computer Crime, within the Office of the National Prosecutor, is the lead agency responsible for investigating and prosecuting cybercrimes.

CERT-py was formed in late 2012 with the aim of facilitating and coordinating the protection of the computer and information systems supporting the government and national infrastructure and ensuring timely and effective response to cyber incidents. Presently, its operational capacity is limited to offering guidance and real-time support for unfolding incidents, although this enables it to understand and review the internal policies of the organizations that it assists. Based on this accumulated experience, CERT-py is devising policies, procedures and mechanisms for responding to cyber incidents and aims to continue to position itself as a national reference and resource for both proactive as well as reactive guidance.

Government authorities are currently working on the development of a National Plan for Cyber Security that will address a wide range of priorities regarding cybersecurity and the fight against cybercrime.

Training and capacity-building for personnel of both CERT-py and the Specialized Unit from Computer Crime has been a key priority, and assistance has been received from numerous partners including the OAS, the US Department of State (DS/ATA), and other competent national authorities in the region. Additional training delivered to government personnel and representatives of other sectors of society has aimed at preventing cybercrimes and cyber incidents by raising awareness about risks and good practices. Along these same lines, the government has undertaken a campaign called "Connect Yourself Safe PY [Paraguay]", the principle objective of which is to increase the public's consciousness about the dangers of posting sensitive personal information on social networking sites. SENATIC adopted a complementary initiative, STOPTHINKCONNECT, or PARAPIENSACONECTATE in Spanish, in 2013 which is in the implementation phase.

The government currently works with key private sector entities to develop shared norms for information security, including cooperation and information sharing. At the moment, the Office of the National Prosecutor is the only government authority capable of requesting information from international service providers (Facebook, Google, Twitter, etc.) when such information is required for an investigation. However, Paraguayan penal code (Law No. 1286/98) provides that any person with knowledge pertaining to an act punishable by the State is required to share that information with the Public Ministry or the National Police.

As previously mentioned, responsible authorities within the Government of Paraguay have received training from various partners in the region. Cooperation has also increasingly taken the form of working with counterpart authorities in other countries to respond to cyber incidents and, where necessary, take down sites involved in exposing vulnerable information. In this regard, CERT-py has been actively developing its cooperative ties with other national CSIRTs in the region, which it reported has enabled it to stay better informed of evolving cyber threats and techniques.

Government authorities reported that some universities in Paraguay are beginning to offer modules and courses specialized in cybersecurity, however, no additional information is available.

Concerning recent trends, national authorities have noted a reduction in attacks by hacktivist groups, while observing an increase in denial of service attacks (Dos and DDos), including incidents targeting the web portals of the Ministry of Finance, Presidency, and Vice Presidency of the Republic. Hacking has comprised the largest number of cyber incidents, including one reported incident still under investigation where a perpetrator modified data in a domain by breaching the user and password of the administration system domain register. The bulk of cybercrimes have entailed fraud through the use of counterfeit credit cards and the exploitation of other electronic payment mechanisms, as well as child pornography. However, all of these observations are anecdotal and inconclusive, as authorities have only limited access to data from ISPs, banks and other financial institutions.

One successful case highlighted by authorities involved the rapid response of a DoS attack against a government web site, where CERT-py detected the incident, took immediate corrective measures, and alerted other national CSIRTs in the region so that they might implement the necessary measures to prevent such an attack against their own assets. In another case, four Bulgarian citizens were caught using cloned credit cards at stores and ATMs. The individuals were identified as being involved with a broader international criminal organization and were tried and convicted for their crimes. One was extradited to the US for similar crimes committed there.

According to reporting authorities, the most effected sectors have been government institutions (particularly those with security-related roles), financial institutions and banking institutions. The

Specialized Unit for Computer Crime reported processing twelve cases last year, and apprehending twenty five persons for illicit activities.

Authorities cite a range of impediments to enhancing cybersecurity and reducing cybercrime in Paraguay. Among these are a lack of awareness among the public and individual users as to cyber threats and good practices for mitigating these, and a general lack of interest and awareness on the part of public sector entities and businesses. The latter point corresponds with a deficiency in investments to improve cybersecurity, particular in investments in infrastructure, equipment, and tools. And authorities responsible for investigating and prosecuting cybercrimes cited the need for more specialized training regarding threats, techniques for combating them, and the proper use of available tools.

Peru

★ Lima

Population: **30,476,000**
Internet Penetration: **38.2%**
Fixed Broadband Subscribers: **4.7%**

Two agencies serve as the primary leads for cybersecurity and cybercrime-related efforts in Peru. The national CSIRT, PeCERT, was founded in 2009 and is the lead entity responsible for cybersecurity-related matters in Peru, including incident prevention and management. The investigation of cybercrime and corresponding responsibilities falls primarily with the Division of High Technology Crimes (DIVINDAT), within the Directorate of Criminal Investigations (DIRINCRI) of the National Police of Peru (PNP).

While PeCERT is an operational CSIRT with national level responsibility, it is currently working to revise and update its mechanisms, procedures and policies for incident response.

Peru does not have an official national strategy or policy for cybersecurity, although one is under development.

Both DIVINDAT and PeCERT actively train their personnel to maintain and develop their capacity to perform their core functions. DIVINDAT, for example, reports regularly conducting workshops to update its staff's knowledge of and ability to effectively utilize digital forensics tools. While it was reported that academic institutions in Peru do offer degree programs with specializations in cybersecurity and cybercrime, no information was provided to indicate whether government officials benefit from the availability of those educational opportunities.

On the legislative front, the recent passage of three new laws – Incorporating Computer Crimes in the Criminal Code (Law 27309), Protection of Personal Data (Law 29733), and Computer Crimes Act (Law 30096) – has strengthened the country's legal framework for promoting cybersecurity and combating cybercrime. Additional modification of other existing legislation is currently under consideration.

Private sector entities are not obligated to report incidents to relevant national authorities. However, PeCERT has initiated a dialogue to increase collaboration with the private sector, particularly ISPs

and banks. This effort is in part based on the recognition that private enterprises generally have a greater ability to detect unusual traffic and attacks, as well as more mature security management systems, and, as such, are invaluable partners in securing the nation's critical infrastructures.

Collaboration and information-sharing with other governments' competent national authorities has been somewhat limited and was cited as an area where additional steps must be taken in the future.

Both PeCERT and DIVINDAT reported that they actively work to enhance the security of their constituencies and increase their resiliency and recovery capacity. These efforts have consisted of a combination of preventative and reactive measures.

On the preventative side, internal and external awareness raising and education have constituted a high priority. Internal awareness raising initiatives within their own institutions have entailed a full range of activities to ensure users' understanding of concepts not always associated with but key to cybersecurity such as physical security, security logic, and human security. External awareness raising activities have included media campaigns, and outreach and education for private sector entities including banks, payment processors, and other business and commercial interests. Awareness raising campaigns have also targeted citizens at large, emphasizing basic good practices for reducing vulnerability and protecting one's identity and information while using the Internet and ICTs.

DIVINDAT actively seeks assistance from foreign entities where and when appropriate. It also maintains active partnerships with and supports the efforts of national and international NGOs working to combat cyber and other crimes that have utilized ICTs (human trafficking, prostitution, pornography, organ trafficking, etc).

Both authorities reported a number of impediments that must be addressed in order to enhance the country's cybersecurity posture and improve its ability to combat cybercrime. Challenges regarding access to information received particular attention, including the difficulty of getting information from ISPs or other service providers in a timely fashion. Insufficient resources and a lack of willingness to share information and cooperate on the part of other government and private institutions were also highlighted as key impediments.

Government data shows an increase in 2013 of approximately 30 percent in the number of cyber incidents reported to national authorities and identifies the business sector, academia, telecommunications entities, the police, and other public sector institutions as the most affected sectors of the population.

A wide range of crimes were reported to authorities in 2013, the most common were: credit card cloning, identity theft, email threats, intrusion by hacking or cracking, unauthorized access to databases, Internet extortion, sexual blackmail, fraudulent financial operations, child pornography, and software piracy. The techniques used to perpetrate these activities varied just as widely and included: point of sale (PoS) intrusions, social engineering, pharming, phishing, and malware.

DIVINDAT reported that there were several relatively high impact incidents in 2013 to which they were able to respond effectively, ultimately identifying, locating and apprehending the perpetrators and presenting them to the appropriate judicial authorities. In one instance, the president of a government institution was receiving threatening and defamatory e-mails. Using forensic techniques DIVINDAT personnel were able to determine the source of the emails and identify the sender, at which point they notified their colleagues in the National Police in order to initiate criminal proceedings against the offender. PeCERT, in another incident, responded successfully to an attack against (defacement of) the web portal of the Presidency, accessing and analyzing the relevant information and taking the necessary steps to restore its integrity.

St. Kitts and Nevis

★ Basseterre

Population: **55,000**
Internet Penetration: **79.4%**
Fixed Broadband Subscribers: **27.3%**

The Cyber Crime Unit of the Royal St Christopher and Nevis Police Force is the primary agency responsible for cybersecurity-related matters in St. Kitts and Nevis, although when necessary it receives support from technicians in the Ministry of Technology or other ministries as required. There is no national CIRT or similar capability, and the government has not devised a national cybersecurity policy or strategy. However, efforts have been undertaken to raise awareness, principally in the form of a national conference hosted by the Ministry of Technology, which brought together representatives from both the public and private sector to exchange views regarding how the country can best move forward on the issue of cybersecurity. Additionally, numerous government officials from various agencies with legal, law enforcement, and technology-related responsibilities have participated in OAS-led technical training and policy-development workshops.

There is no established law, agreement or protocol that governs the reporting of cyber attacks by the private sector and government authorities report that it is difficult to assess the response of the private sector to such incidents because they have not received reports of any attacks against private institutions. Indeed, the national authorities report no observed increase in cyber incidents of any kind over the past year, nor any particular incident of noteworthy nature or consequence.

In terms of international cooperation, the Government of St Kitts and Nevis has not formalized any official memorandums of understanding with other governments regarding cybersecurity. Where requests are received for addressing known or suspected cybersecurity threats, however, it maintains the requisite mechanisms and capacity to respond and provide support. In addition, competent cybersecurity professionals working within the government maintain informal but daily communications with their counterparts in other countries in the region.

Going forward, the Government of St Kitts and Nevis identifies several challenges that will need to be addressed in order to enhance its national cybersecurity posture. Chief among these are the need to develop a national CIRT as well as the requisite legislative framework to investigate and prosecute cybercrimes. Authorities assert that the country has benefited from the participation of select officials in various training courses and workshop in recent years, and has taken some steps to reduce the risk that cyber incidents pose to the country's critical infrastructure. However, the absence of a national CIRT and legal framework, as well as insufficient awareness and cooperation among key private and public sector entities, means that the risk remains high. While at present the government has the capacity to effectively respond to an incident of small to medium scale, authorities do not believe the government is equipped to deal with a large scale attack.

St. Vincent & the Grenadines

★ Kingstown

Population: **97,000**
Internet Penetration: **47.5%**
Fixed Broadband Subscribers: **12.5%**

The lead agency for cybersecurity in St. Vincent and the Grenadines is the SVG Police Force, which has created an Information Technology Unit to oversee and support the investigation of all cyber-crime and information security-related matters. While the office of the Prime Minister has also played a guiding and facilitating role in examining cybersecurity policy, there is not an established national cybersecurity strategy or plan, nor has Saint Vincent and the Grenadines established a designated national CSIRT. However, authorities reported that a national incident management capability is currently under development. There is no national cybersecurity awareness campaign, and authorities reported that there is presently no effort underway to develop such an initiative.

Authorities from the SVG Police Force reported that the major observed increase in cyber incidents has related to social network in schools, as Internet and computers have become more accessible to students through the government's 'one laptop per child' initiative. However the rise in the incidence of these types of incidents, largely involving character defamation and threats through social networks like Facebook, has not precipitated any specific measures on the part of the State as of yet.

In those instances where incidents involving defamation or threats were reported, authorities were able to identify source IP addresses which they then passed to ISPs. It is unclear what actions, if any, were taken in response to these situations.

Authorities reported that cooperation and information-sharing between the SVG Police Force and private sector companies does take place, although no specific information was provided as to the form or frequency of such interactions, or whether there is a legal basis for them.

International cooperation has centered largely on solicitation of support when needed from the experts of the Cyber Forensic Laboratory in Antigua and Barbuda. Personnel from the government's Technology Unit have also participated in cybersecurity and cybercrime related training offered by regional and international partners including the OAS, US Department of State (DS/ATA), CTU, and INTERPOL, among others. There are no university level cybersecurity-related degree or certification programs within St. Vincent and the Grenadines, although as with other Caribbean States, it is common for interested students to pursue such coursework at other universities in the region, or in the US or Europe.

Authorities cited the recent linkages established between States in the Caribbean for the Automated Fingerprint Identification System (AFIS) as an example of the country's cybersecurity advancement in 2013.

Suriname

★ Paramaribo

Population: **539,000**
Internet Penetration: **34.7%**
Fixed Broadband Subscribers: **5.5%**

The Government of Suriname is currently in the process of reinvigorating and expanding its national cybersecurity regime and is taking steps to do so on multiple fronts. The Central Intelligence and Security Agency (CIVD) is the acting lead for cybersecurity-related matters, although a Cyber Crime Unit is being created within the National Police. Additionally, the defunct national CIRT (SurCSIRT) is in the process of being reactivated, and will soon have a new website. Negotiations among stakeholders are ongoing regarding the creation of a national cybersecurity policy and strategy; personnel from the national defense force are currently participating in a course on cybersecurity.

Private sector entities are not required to report cyber incidents to government authorities, however CIVD is in negotiations with major financial institutions and other key stakeholders regarding how best to share information and cooperate. Cooperation between CIVD or other national authorities and their counterparts in other countries has not occurred to any significant extent.

However, national authorities reported that the participation of Surinamese government officials in OAS-led cybersecurity capacity-building activities, including the June 2013 Crisis Management Exercise in Washington, DC and November 2013 Cyber Security Symposium in Uruguay were instrumental in spurring the reactivation of SurCSIRT. In terms of capacity-building resources available within the country, as of May 2014 the University of Suriname will offer a course on cybersecurity, although it is not clear whether government officials will directly benefit from this development.

The Government of Suriname does not maintain a centralized system or mechanism for the reporting of cybercrimes or security-related incidents, thus no official record of incidents or corresponding data is available. Authorities assert that in general cybercrime is not especially common in Suriname, although they do report having observed over the past year an increase in incidents involving skimming and bank fraud. As official records are nonexistent and reporting by the private sector is minimal, there are no known cases where an incident was successfully resolved.

Looking to the future, authorities have identified several key impediments which must be addressed in order to advance cybersecurity in Suriname. These include the present lack of trust among stakeholders which inhibits the sharing of sensitive data, a related absence of collaboration among stakeholders, insufficient funding for cybersecurity and cybercrime related initiatives, a lack of adequately trained personnel, and the absence of national legislative framework to underpin the development and effective operation of the national CIRT, SurCSirt.

Trinidad and Tobago

★ Port of Spain

Population: **1,344,000**
Internet Penetration: **59.5%**
Fixed Broadband Subscribers: **13.8%**

To date, two national agencies have taken the lead on cybersecurity and cybercrime efforts in Trinidad and Tobago, namely the Ministry of National Security and the Cybercrime Unit of the Trinidad and Tobago Police Service. Information security has been handled largely on an individual institution basis, such that each organization employs a network security officer responsible for its own system and information security. Some cybersecurity awareness raising efforts have been undertaken, mostly in the form of sensitization workshops conducted by the Ministry of National Security, the Police Service, and the Ministry of Science and Technology.

2013 was an active year on the cybersecurity front in Trinidad and Tobago and marks a turning point in the country's national cybersecurity regime. In 2011 an Inter-Ministerial Committee (IMC) for cybersecurity was created under the chairmanship of the Ministry of National Security, and included representatives from key ministries and agencies, as well as the private sector. The IMC was established with a two year mandate, and tasked with: developing a cybersecurity strategy and action plan, updating the country's legislative framework, creating a national CIRT, developing an implementation and regulatory regime, and creating framework and mechanism for assessing cyber risk to the nation's critical infrastructure. Working internally through an inter-agency, sub-committee process, and with technical and capacity-building support from international organizations, the IMC labored for the two years and has achieved significant progress towards the fulfillment of its mandates.

In December 2012 the Government approved a National Cyber Security Strategy to guide all operations and initiatives related to cybersecurity in Trinidad and Tobago. It is based on the government's Medium Term Policy Framework, 2011-2014, which underscores the role of information and communication technology (ICT) in advancing national development. The strategy is based on the five (5) pillars of governance, incident management, collaboration, culture, and legislation, and has thus far been helpful in serving as a guide for on-going cybersecurity-related efforts.

A cybercrime bill has been drafted and is under consideration by parliament. In general terms, the bill aims to: criminalize offences related to computer crime and cybercrime, institutionalize investigative mechanisms, enable the use of electronic evidence in prosecution, and define the obligations and restricts the liability of ISPs. In addition, training for law enforcement, prosecutors and the judiciary is expected to take place in the coming months, to build capacity to enforce the new legislation.

A Trinidad and Tobago Cyber Security Agency (TTCSA) will soon be created, under the purview of the Ministry of National Security, and will serve as the main entity responsible for coordinating and managing all cybersecurity activities. Specific responsibilities will include: implementing and advising on the national cybersecurity strategy; providing situational awareness information, and

collecting and analyzing cybersecurity-related data; promoting efficient network and information security management; and raising awareness and promoting local and international cooperation.

The government is also currently in the process of establishing a national CIRT (TT-CSIRT), housed within the Ministry of National Security, which will: provide warning of potential threats, incidents, and attacks; facilitate information-sharing and coordination among the TT-CSIRT constituency; analyze cyber vulnerabilities, incidents, and attack methodologies; provide technical assistance to government and other stakeholders; conduct investigations and forensics analysis; defend against attacks on critical information infrastructure; and lead national-level recovery efforts in the event of a cyber-incident.

Pillar 4 ("culture") of the national strategy addresses the need for public awareness through the adoption of a multi-disciplinary and multi-stakeholder approach, which includes embedding cyber-security in the wider aspects of policy formulation and educating all users of ICT and the Internet on their respective roles in cyberspace. The Ministry of National Security is in the process of launching a public awareness campaign targeting the general population, which will consist of video shorts on different types of cybercrime, and press articles and public service announcements providing basic information on cybersecurity. The Ministry is also working with local NGOs in the creation of a website that would provide information on cybersecurity.

While presently the private sector is not obligated to report incidents to the government authorities, the latter continues to work closely with private enterprises, particularly in the banking sector, on a number of cybersecurity issues. These include in the drafting of the National Cybercrime Policy approved in February 2013, and on-going joint efforts to define areas for partnership and collaboration in the future.

Cooperation with other countries is currently based on informal working relationships, with the sole exception of the Central Authority Unit of the Ministry of the Attorney General, which is responsible for mutual legal assistance. The establishment of the TTCSA, however, will enable the formation of formal bilateral relationships with other nations in the area of cybersecurity. In addition, excellent working relationships have already been established with international organizations such as the Organization of American States, the International Telecommunication Union and the Commonwealth Secretariat.

Currently, while ethical hacking courses are offered at some academic institutions, there are no cybersecurity degree or certification programs within the country. However, the Government intends to partner with local tertiary level institutions to develop such certification and degree programs.

Although this should soon be rectified by the cybercrime bill now before parliament, national authorities reported that the lack of such cybercrime legislation, as well as a lagging awareness of cybercrime and cybersecurity, have constituted the major impediments the country's cybersecurity to date. Another significant impediment to the country's cybersecurity advancement has been a lack of financial and human resources to effectively implement the national strategy.

In terms of observed trends in 2013, the fact that cyber incidents are rarely reported to national authorities makes it difficult for the government to assert with certainty any increase or decrease in illicit activity. In 2013 eighty five (85) cybercrime-related cases were opened by the police, although none resulted in convictions. Other anecdotal information indicates that most reported incidents are associated with impersonation of identity using Facebook or social networks or the exploitation of email for identity theft and fraud. One case that received particular attention and is still under investigation involved misuse of the email accounts of several high-ranking officials. Limited reporting further suggests that of the key sectors of society, the country's banking sector has been the most affected.

Uruguay

★ Montevideo

Population: **3,297,000**
Internet Penetration: **55.1%**
Fixed Broadband Subscribers: **16.6%**

The lead authority for cybersecurity issues within the Government of Uruguay is the Agency for e-Government and an Information and Knowledge Society (AGESIC), which also houses the national cybersecurity incident response center, CERTuy. The Computer Crime Unit of the National Police has primary responsibility for the investigation of cybercrimes and related activities, and receives technical support from CERTuy as needed.

While Uruguay does not have a specific cybersecurity strategy or policy document, relevant guidelines have been defined and incorporated into related initiatives such as the government's Digital Agenda. In addition, a series of official decrees established a clear framework for cybersecurity efforts at the national level. For example, Decree 452 (2009) states that central government agencies should have a policy of information security, while Decree 92 (2014) calls for the consolidation of all critical national public service organizations under a common criteria for the classification of web sites (i.e. ".gub.uy " and ".mil.uy ") and elevated security standards regarding the central administration's datacenter, emails and domain names.

Personnel from the Computer Crime Unit of the National Police have received technical training from outside partners including the OAS, primarily focused on improving their capacity for investigations and forensics. Personnel from CERTuy have attended numerous technical and policy-oriented workshops and seminars both as participants and expert instructors.

There is no legal compulsion for private sector entities to report information related to cyber attacks or compromised information to national authorities. Public institutions and agencies are, however, required to report such information to CERTuy. And in cases where a potentially high impact incident is impacting or could impact the target community or the State, regardless of what sector is being effected (public or private) CERTuy plays an active role in responding to and mitigating the incident.

Uruguayan authorities, and especially personnel from AGESIC and CERTuy, cooperate regularly and substantively with counterpart authorities in other countries, including in responding to incidents occurring both in Uruguay and in other countries. Authorities reported that to date all such cooperative activities have yielded positive results. In addition, CERTuy partners with various international organizations working to foster increased collaboration and communication between response centers, including OAS/CICTE, LACNIC, FIRST, and ITU, among others.

Authorities reported that both public and private universities in Uruguay offer relevant coursework and degree or certification programs in aspects of cybersecurity and combating cybercrime. No further information was provided.

Since November 2013, CERTuy has undertaken the "Connect Yourself Securely" campaign, which is aimed at the public and seeks to generate awareness of the problems that can arise with the use of ICTs. CERTuy is seeking the cooperation of other organizations and partners to assist in promoting

the campaign more widely going forward, and has also officially adopted the STOPTHINKCONNECT awareness raising campaign.

Data collected by CERTuy through monitoring and incident reporting suggests that the number of cyber incidents has increased significantly (although CERTuy personnel note that their monitoring and data collection techniques have evolved in that period). The incident that has been observed to have most increased in frequency is phishing.

Uruguay authorities noted that managing cybersecurity threats and risks is by its very nature an evolving and global challenge, as there are no defined geographical boundaries. As has been done since Uruguay first began to tackle the problems of cybersecurity and cybercrime in 2007, Uruguayan authorities will continue to strive to consider and integrate cybersecurity in all projects and initiatives where there is a need and opportunity to do so.

This will require addressing three primary impediments which continue to challenge national cybersecurity and cybercrime-related efforts, namely, lagging cybersecurity awareness within other government institutions, insufficient financial and material resources to carry out needed initiatives, and a lack of trained personnel.

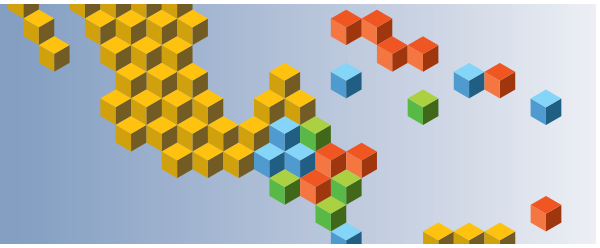
Venezuela

★ Caracas

Population: **29,760,000**
Internet Penetration: **44.1%**
Fixed Broadband Subscribers: **6.7%**

The lead agency responsible for cybersecurity in Venezuela, including cyber incident prevention and response, is the National System for Cyber Telematic Incident Management (known colloquially as VenCERT). Lead responsibilities for investigating and prosecuting cybercrime rests with the Center for Scientific, Penal and Criminal Investigations (CICPC) and its Cybercrime Division, and the National Center for Digital Forensics (CENIF) of the Superintendency of Electronic Certification Services (SUSCERTE).

While there is no national cybersecurity strategy or policy, there is a relatively longstanding legislative framework for the government's cyber-related efforts. This framework is comprised of three laws in particular, namely Law No. 1204 on Data Messages and Electronic Signatures (2001), the Special Law against Computer Crime (2001), and the Interoperability Act (2012). The most recent piece of legislation considered, the Info-Government Act (2013), provides additional relevant legal context for national cybersecurity-related efforts. It has as its main objective the establishment of principles, rules and guidelines governing the use of ICTs in the public sphere, and establishes legal value for the electronic signature, data messaging and all intelligible information in electronic form. Moreover, it establishes foundations and principles governing access to and the electronic exchange of data, information and documents between agencies of the state, in order to ensure adherence to a common standard for interoperability. Overall, authorities hope that the law will improve and



increase the transparency of public management, facilitate access on the part of citizens to information, and promote national development in a way that ensures technological sovereignty.

National authorities routinely undertake to build the capacity of personnel responsible for cybersecurity and cybercrime, for example through the participation of technical staff from various public institutions in courses on information security, incident management, social networking, computer forensics, and ethical hacking.

Existing legislation does not compel the private sector to report incidents to national authorities; however, a law currently being drafted on data protection will address this matter in some fashion. In addition, discussions have been initiated with the private sector and, in particular, enterprises with a science or technology orientation, with the aim of identifying and developing opportunities to strengthening information security in Venezuelan society.

While the Government of Venezuela does not maintain officially established lines of cooperation with other countries, authorities have managed to effectively and successfully coordinate efforts with other CSIRTs around the world in response to specific incidents. Similarly, a working group of cybersecurity experts within Mercosur has been established to promote increased information-sharing within that region.

Government-led awareness raising efforts in Venezuela have largely centered on a campaign called “Information security begins with you”, which has been in place since November 2009 and is currently focused on educating the staff of government institutions and organized communities.

Although information reported on the matter of educational and training opportunities within Venezuela was limited, it was indicated that there are cybersecurity and cybercrime related courses and degree offerings available up to the fourth level of study (diploma, specialization, and Master’s degree).

Available 2013 data indicates clear increases in the frequency of a wide range of cyber incidents. Web defacements increased by roughly 50 percent, for example, while Distributed Denial of Service (DDoS) attacks rose by 40 percent. One of the most significant incidents entailed the defacement of the web portals of several state institutions by various national and international hacktivist groups. Authorities were able to successfully identify the perpetrators through an analysis of historical records in the relevant servers.

According to national authorities, the main drawback for the development of cybersecurity in Venezuela has been the increase in the frequency of cyber attacks relative to the limited operational capacity of VenCERT. Despite a small increase in the size of the staff dedicated to managing the large volume of cyber incidents, this increase has reduced the already limited amount of time that personnel can devote to research, analysis and testing of new tools and techniques in the field of information security. The latter is important since the diversification of tools used to carry out attacks and their availability on the web necessitates that authorities stay current in their own capabilities.

CONTRIBUTIONS

Reflecting ongoing efforts to engage and collaborate with like-minded partners from a range of business, government, academic, and other non-governmental organizations, the OAS and Symantec asked institutions with whom we regularly work to contribute to this report. Each of these entities—Microsoft, LACNIC, ICANN, and the APWG—provided information related to their mission or specialty.

Anti-Phishing Working Group

Twice a year, the Anti-Phishing Working Group publishes its Global Phishing Survey, authored by Greg Aaron and Rod Rasmussen. This report seeks to quantify and understand the global phishing problem. It examines the number of phishing attacks observed, what top-level domains (TLDs) that phishing occurred in, provides other metrics, and explains the latest criminal techniques. The latest report, "Global Phishing Survey: Trends and Domain Name Use in 2H2013," is available at: http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2013.pdf

The report analyzed the phishing domains and attacks to see how they were distributed among top-level domains (TLDs). The majority of phishing world-wide continues to be concentrated in just a few namespaces. Most phishing takes place on compromised domain names, where the phisher has broken into the web server where the domain is hosted.

There were at least 115,565 unique phishing attacks worldwide in 2013. Of those, 8,865 of the attacks occurred on domain names within the country-code domains in the Americas. These attacks occurred overwhelmingly on hacked web servers, indicative of regular security breaches at hosting providers within the region and indeed across the world.

The complete statistics are presented in report, and below are the statistics for the top-level country code domains (ccTLDs) in the mericas.

- The median phishing-domains-per-10,000 score worldwide was 4.9.
- .COM, the world's largest and most ubiquitous TLD, had a domains-per-10,000 score of 3.7. .COM contained 46 percent of the phishing domains in thedata set, and 42 percent of the domains in the world.
- The authors therefore suggested that domains-per-10,000 scores between 3.7 and 4.9 occupy the middle ground, with scores above 4.9 indicating TLDs with increasingly prevalent phishing.

Top-level Country Code Domains (ccTLDs) in the Americas.

Source: APWG

TLD	TLD Location	# Unique Phishing Attacks 2H2013	Unique Domain Names Used for Phishing 2H2013	Domains in Registry, Nov. 2013	Score: Phishing Domains Per 10,000 Domains 2H2013	Score: Attacks Per 10,000 Domains 2H2013	Average Uptime 2H2013 hh:mm	Median Uptime 2H2013 hh:mm	# Total Malicious Domains Registered 2H2013	Malicious Registrations Score/ 10,000 Domains in Registry
ag	Antigua and Barbuda	3	3	19,766	1.5	1.5	22:56	25:15	2	
ai	Anguilla	7	4	3,800	10.5	18.4	13:05	11:54		
an	Netherlands Antilles	16	2	800	25.0	200.0	36:05	42:03		
ar	Argentina	829	658	2,800,000	2.4	3.0	36:29	8:51	7	0.0
aw	Aruba	0		625						
bm	Bermuda	1	1	8,100	1.2	1.2	25:46	25:46		
bo	Bolivia	12	11	8,500	12.9	14.1	9:42	4:40		
br	Brazil	3,674	3,023	3,322,000	9.1	11.1	33:16	9:43	29	0.1
bs	Bahamas	0		2,400						
bz	Belize	28	20	44,845	4.5	6.2	60:15	9:37	1	
ca	Canada	671	527	2,195,000	2.4	3.1	54:17	9:51	3	0.0
cl	Chile	1,010	807	443,251	18.2	22.8	38:52	10:40	3	0.1
co	Colombia	406	274	1,576,833	1.7	2.6	15:12	5:35	23	0.1
com	generic TLD	53,592	42,086	114,076,050	3.7	4.7	35:18	9:19	12,347	1.1
cr	Costa Rica	10	8	15,161	5.3	6.6	41:54	9:03		
cu	Cuba	0		2,351						
dm	Dominica	0		14,000						
do	Dominican Republic	18	18				19:30	0:26		
ec	Ecuador	35	31	30,500	10.2	11.5	37:58	9:13		
gd	Grenada	11	3	4,400	6.8	25.0	9:20	10:37		
gp	Guadeloupe	29	17	1,500	113.3	193.3	34:50	11:30		
gt	Guatemala	11	10	13,256	7.5	8.3	15:11	14:15		
gy	Guyana	13	3				7:14	8:49		
hn	Honduras	2	2				102:34	149:35		
ht	Haiti	428	5	2,200	22.7	1,945.5	16:19	11:17		
jm	Jamaica	2	2	6,300	3.2	3.2	0:17	0:17		
kn	Saint Kitts And Nevis	0								
ky	Cayman Islands	3	3				1:00	1:07		
lc	St. Lucia	15	12	3,950	30.4	38.0	12:19	10:36	1	
ms	Montserrat	23	8	9,500	8.4	24.2	90:16	54:24	1	1.1
mx	Mexico	486	335	687,155	4.9	7.1	24:38	7:02		
ni	Nicaragua	4	4	6,650	6.0	6.0	13:08	6:14		
pa	Panama	4	4				11:32	13:36		
pe	Peru	112	100	75,116	13.3	14.9	44:52	8:17		
py	Paraguay	37	33	15,000	22.0	24.7	79:46	8:02	1	0.7
tc	Turks and Caicos	8	7				5:36	4:08	1	
tt	Trinidad and Tobago	0		2,500						
us	United States	420	338	1,795,000	1.9	2.3	33:27	8:25	46	0.3
uy	Uruguay	50	42	68,381	6.1	7.3	51:11	11:50		
vc	St. Vincent and Grenadines	281	8	9,051	8.8	310.5	19:57	10:59	1	1.1
ve	Venezuela (estimated)	196	150	215,000	7.0	9.1	37:58	11:54		
vg	British Virgin Islands	1	1	8,600	1.2	1.2				
vi	Virgin Islands	0		17,500						

Top 10 Phishing TLDs by Domain Score, 2H2013*

Source: APWG

	TLD	TLD Location	# Unique Phishing Attacks 2H2013	Unique Domain Names Used for Phishing 2H2013	Domains in Registry, Nov 2013	Score: Phishing Domains Per 10,000 Domains 2H2013
1	.np	Nepal	105	88	32,500	27.1
2	.pw	Palau	1,007	924	350,000	26.4
3	.th	Thailand	215	155	64,990	23.8
4	.cl	Chile	1,010	807	443,251	18.2
5	.pe	Peru	112	100	75,116	13.3
6	.gr	Greece	463	407	377,000 (est.)	10.8
7	.id	Indonesia	126	104	101,892	10.2
8	.ec	Ecuador	35	31	30,500	10.2
9	.br	Brazil	3,674	3,023	3,322,000	9.1
10	.ma	Morocco	44	33	43,325	7.6

* Minimum 25 phishing domains and 30,000 domain names in registry

Malware Infection

In the fourth quarter of 2013, APWG member PandaLabs analyzed computers worldwide as part of an ongoing measurement study of malware infections. Pandalabs found that 28.39 percent of computers worldwide appeared to be infected with malware. That global infection rate was one of the lowest that PandaLabs has ever recorded. China had the highest infection rate by far -- 53.85 percent of all computers analyzed there were infected. Latin America and Asia were the regions with the highest number of computer infections. Eight of the ten least-infected countries were in Europe.

Highest Rank	Country	Infection Rate
1	China	53.85%
2	Taiwan	39.57%
3	Turkey	37.50%
4	Poland	36.65%
5	Peru	35.63%
6	Russia	34.55%
7	Argentina	34.42%
8	Canada	34.31%
9	Colombia	33.33%
10	Brazil	32.25%

Lowest Rank	Country	Infection Rate
45	Sweden	16.18%
44	United Kingdom	18.18%
43	Portugal	18.55%
42	Switzerland	19.23%
41	Germany	20.69%
40	France	21.02%
39	Netherlands	21.07%
38	Venezuela	23.13%
37	United States	23.85%
36	Spain	26.82%

The Internet Corporation
for Assigned Names & Numbers

Security, Stability and Resiliency of the Internet Identifier Systems: ICANN in the Americas

ICANN's Security, Stability and Resiliency Team (SSR Team) works across the globe with the Internet community pursuing the corporate goal of preserving and enhancing the stability, reliability and security of the Internet's identifier systems, as set forth in the ICANN Bylaws. The SSR Team does so by engaging and collaborating with those responsible for the security or the operation of Internet infrastructure, ranging from domain name registries and registrars, to Regional Internet Registries (RIRs), Internet exchange points and Internet service providers (ISPs), to research and security companies, universities, volunteers and law enforcement agencies.

To achieve these goals, the SSR Team engages in activities that include threat awareness and preparedness, measurement and analysis of identifier system behaviors or performance, and cooperative outreach that emphasizes coordination, capability building and knowledge transfer.

But, what does this all mean? Below we will briefly remember a success case that exemplifies what it means to address a threat against an Internet identifier system, then we will discuss about capability building and we will lastly focus on what this all means for the Americas.

Success Case: The Conficker Working Group

An excellent example of successful cooperative outreach and coordination performed by ICANN's SSR Team is the role it played in the coordinated response that led to the initial disruption of the Conficker worm back in 2009 and the ongoing containment efforts since. As the 'Conficker Summary and Review' report so clearly states, both Conficker and the operational response to contain it were landmark cases: Internet security researchers, operating system and antivirus software vendors that discovered the worm in late 2008, along with law enforcement agencies and ICANN staff, "formed an ad hoc effort with ICANN, Top Level Domain registries and domain name registrars around the world to contain the threat by preventing the malware writers from using tens of thousands of domain names algorithmically-generated by the Conficker infection".

The malware used domain names under more than 100 Top-Level Domains, including both generic and country-specific, instead of IP addresses to make its botnet resilient against detection and takedown. The operational response disrupted botnet command and control communications and led to the malware writers changing their behavior, mitigating a serious threat against the Domain Name System (DNS).

Needless to say, after the Conficker Working Group ICANN's SSR Team has continued to successfully address different threats collaborating with the relevant stakeholders in the community.

Capability Building and Knowledge Transfer

In many regions of the world, including Latin America and the Caribbean, law enforcement agencies lack personnel with high levels of knowledge, expertise and understanding of the online threat landscape. Yes, some countries have made efforts to create anti-cybercrime units, however these units often focused on digital forensic investigations (how to find the needle the in the haystack), digital evidence (discovery, preservation, administration and presentation) and copyright anti-piracy.

This means that there are regions of the world in which the authorities that should take or coordinate the actions to disrupt, mitigate, prevent and deter online threats, may be

unprepared or under-equipped. In these regions, risks against the Internet identifier systems can become actual threats and criminals know that online impunity is very high, as high as their profits. Countries in Latin America and the Caribbean, as well as those in mostly every other region, should continue to prepare and equip themselves to make sure that they are not in this situation.

ICANN's SSR Team continuously provides training to different regional and local members of the community all around the globe that, in one way or another, operate Internet infrastructure or can help make it more secure, stable and resilient. Over the course of many years, ccTLD operators, law enforcement personnel, ISPs and others, from all five continents, have received training -from the basics to very advanced- on matters related to the operation of the DNS, DNS abuse and misuse, as well as DNSSEC and IPv6. Also, through its participation in the Commonwealth Cybercrime Initiative, ICANN's SSR Team offers these capability-building programs to prosecutors and jurists to requesting Commonwealth states.

ICANN and the SSR Team in the Americas

As part of our Globalization efforts, ICANN opened in 2013 an engagement office in the Casa de Internet de Latinoamérica y el Caribe in Montevideo. With dedicated senior engagement and communications staff in Montevideo, Brazil, Mexico and St. Lucia, ICANN has been developing, along with members of the community, a Latin America and the Caribbean Strategy which includes projects related to capability building and strengthening the security, stability and resiliency of the DNS in the region.

Also, ICANN's SSR Team is present throughout the Americas actively seeking to strengthen its relationships with regional organizations such as the Organization of American States, LACNIC, LACTLD, ccTLD administrators and ISPs, national law enforcement agencies, Ameripol and Interpol's Buenos Aires regional headquarters, as well as security companies that have a focus on the Latin online threat landscape.

Depending on the countries involved, addressing threats to the Internet identifier systems in the Americas means in many cases, among other things:

- Language differences, which can make it difficult for researchers and investigators in the region to use many tools that they could otherwise use to detect, disrupt, mitigate and prevent threats.
- Differences between case law and civil law countries, which sometimes cause investigators from one country to make wrong assumptions regarding matters in another country as diverse as legal definitions (entrapment is always a good example), legal requirements of the chain of custody, privacy rights and others.
- Not all countries are parties to mutual legal assistance treaties (MLATs) or participate in networks that allow their law enforcement agencies to share information with their international peers. Knowing that significant threats can be deployed in minutes if not seconds, a request for information sent by a law enforcement agency from one country to its peer in a neighboring country can easily be responded to in nine months, without guarantee that the requested information will even be provided.

ICANN's SSR Team is familiar with issues of these kinds and is thus in an excellent position to bring its knowledge, expertise and collaboration to the relevant regional stakeholders. This is always done in ways that can help the entire community address threats related to the DNS.

ICANN is committed to strengthening its engagement in Latin America and the Caribbean, for example by providing content and training in Spanish, while maintaining the focus on its mandate of preserving and enhancing the security, stability and resiliency of the Internet identifier systems.

Lacnic

Executive Summary

Routing is one of the main functions that keeps the Internet running. This routing system is based on technologies that have remained essentially unchanged for over 15 years. We have gotten to know weaknesses in this system, which will be described here. This paper also highlights work being done to strengthen the routing function and how new techniques are being deployed in the Americas. In particular, the Resource Public Key Infrastructure will be described, showing its potential to mitigate the risks associated with said weaknesses. The global routing system's scope is such that events happening in one region can have huge impacts in another, highlighting the need to inter-regional cooperation.

Internet Numbering Resources Management

In order to achieve goals of conservation of IP addresses, internet routability, and a public registration of addresses, the Internet Registry structure was created. This is Registry is implemented by a hierarchy of several levels consisting of the following levels viewed from top to bottom:

01 **The Internet Assigned Numbers Authority (IANA)** manages all number spaces used on the Internet, including but not limited to IP addresses and Autonomous System Numbers.

02 **The Regional Internet Registries (RIRs)** are organizations that operate in large geographical areas. Currently five of these RIRs exists: ARIN, for the US, Canada and parts of the Caribbean; RIPE NCC for Europe, the Middle East and parts of Central Asia; APNIC, serving Asia-Pacific; LACNIC, serving Latin America and parts of the Caribbean and AfriNIC, serving Africa. RIRs manage IP address space allocated to them by the IANA and establish policies and procedures that allow striking the adequate compromises among the different goals established by RFC 2050.

03 **Local Internet Registries** serve country-sized areas and are established under the authority and recognition of the RIRs and IANA. They manage IP addresses allocated to them by the RIRs and their duties are similar to those of the RIRs as well.

The constraints outlined by documents that outline IP address allocation can prove conflicting, particularly regarding conservation and routability. If conservation alone had priority over other constraints, then IP addresses would be assigned in small blocks to organizations covering only short-term needs. However this would lead to a large increase in the number of entries in the global routing table, an undesirable side-effect leading to increased costs for providers and slower response times for the whole Internet.

Since the whole Internet Registry system started operating particular care has been put into establishing policy development processes that are open to all and working in a bottom-up manner highlighting compromise and balance among conflicting goals.

The Global Routing System – A Brief Description

Given its global scope and size, the Internet has been naturally partitioned into smaller administrative domains. This scheme has been one of the critical factors that enabled the Internet to grow exponentially for long periods of time and even during economic depression or uncertainty. These administrative domains are called Autonomous Systems (AS) and are identified by numbers called Autonomous System Numbers (ASNs). AS are operated by different organizations that agree to exchange routing information. This routing information is essentially a huge index which contains the information needed for Internet Protocol packets to traverse the Internet and connect any pair of end points. During each exchange of information (known as an **"update"**) neighboring AS tell each other how to reach different portions of the Internet. Each update contains a list of reachable networks (known as **"prefixes"**), and each prefix entry contains a set of attributes that helps control how this routing information is propagated and used.

Prefixes are said to **originate** in one autonomous system. This origin AS is the first AS that announces a certain prefix to its neighbors. The origin AS is an attribute of each prefix. Until today it is implicitly assumed that the organization managing the origin AS for a prefix has **authority** over the use of the number resource being announced.

Weaknesses in the Global Routing System

It is implicitly assumed that the organizations originating prefixes from their AS have the authority to do so. Regional and local Internet registries maintain authoritative databases binding organizations and number resources and thus are the ultimate source of resource usage authority. Internet Service Providers exchanging routing information with other AS are encouraged to check whether the prefixes they receive from neighbors are being originated by the rightful assignees. Unfortunately ISPs do not always implement these checks or do so inattentively. To make things worse, there is no single information repository an ISP can query to confirm the right to use of a resource.

While some databases do exist, for example the different existing Internet Routing Registries (IRRs), where an organization can register its resources and the routing policies, their use is not mandatory and many organizations do not make use of IRRs. The checks implemented by the service providers are in usually performed off-line, meaning that if authority checks are performed at all they are not implemented in the routing equipment itself but in information systems external to the network devices, leading to long delays in applying any accept/reject decision over a prefix announcement.

These loopholes open the global routing system to manipulation and to operational mistakes that could affect large portions of the Internet. An attacker could, for example, announce prefixes corresponding to the network of a large bank or financial organization to its upstream ISP, and if successful, part or all of the traffic destined to the target organization could be redirected to the attacker's network, potentially exposing transaction data, login credentials, emails and other types of sensitive information. Such an attack could also create large Denial of Service situations, where rightful service users cannot access resources due to their traffic being redirected to different location. This scenario is one example of what is commonly called "Route Hijacking" in the literature. While there have been no records of malicious attacks of this nature there have been some cases of operational mistakes during the past two years.

The INDOSAT incident, 2014

On April 2, 2014 Indonesian Internet service provider INDOSAT claimed ownership of over 320,000 prefixes, accounting for approximately 60 percent of all valid Internet routes. Many networks in the Americas were affected, including LACNIC's services, as well as other major operators

in the hemisphere. Luckily, visibility of these bogus announcements was limited and the denial-of-service situations were mostly limited to operators neighboring Indonesia.

Route Hijacking Incidents in the Americas

There is evidence of local route hijacking events occurring within the region, although no official reports have been made public. In 2012 an ISP in Chile mistakenly announced in the Internet prefixes belonging to a cable operator in Argentina, causing a moderate denial-of-service situation for the latter company. In the same year an autonomous system in Argentina announced a large amount of prefixes corresponding to an ISP in Venezuela again causing service disruptions for these users. Evidence periodically surfaces in mailing lists and operator forums pointing to the ongoing occurrence of such events.

Strengthening the Global Routing System

RPKI: Asserting Authority over the Use of a Number Resource

The Resource Public Key Infrastructure (RPKI) is a security framework that will allow the verification of the association between rightful resource holders and the Internet number resources assigned to them. Any RIR will be able to issue a **resource certificate** for any Internet number resources they assign as long as the RIR can verify the legitimacy of original allocations and the rights of the holders. Resource holders will also be able to establish their own **Certificate Authorities**, which means they will be able to issue resource certificates to their own downstream customers. A resource certificate is an electronic document that states that a specific resource has been registered by the certifying RIR. It contains several data-holding fields, including:

- Public key (critical part of the RPKI, allowing digital signature verification);
- Resources covered by the certificate; and
- Digital signature of the issuing registry (in this case the issuing RIR).

Resource certificates are conceptually equivalent to well-known certificates used for encryption by many websites. However, resource certificates will not contain personal identity information, as the legitimacy of the certificate will be verified by checking the digital signatures. It is assumed that anyone able to sign objects with the private key associated with a resource certificate is the legitimate owner of the resources listed in that certificate. Resource certificates will not be used to check a user's identity but rather to improve the technical reliability of the global routing system.

The key benefit provided by Resource PKI is the ability to **validate**. Once a certificate has been issued for a specific resource, the legitimacy of that resource's can be checked. This validation can also be **automated**, paving the way for implementing such validation in the routing infrastructure itself without the need to rely on human intervention.

RPKI Deployment in LACNIC's Service Region

Network operators in LACNIC's service region are embracing RPKI as a measure to mitigate the impact of route hijacks. Currently Latin America and the Caribbean have the second highest deployment of RPKI and associated technologies, only behind Europe. Besides adoption by operators, in 2013 LACNIC, the Internet Society, NAP.ec and Cisco Systems partnered to implement RPKI and origin validation in routers in NAP.ec. The organization groups most Internet-connected providers in Ecuador and by deploying RPKI in NAP.ec's network, Ecuador became the first country to be almost 100 percent covered by RPKI.

Microsoft

LATAM Security Trends, H2, 2013

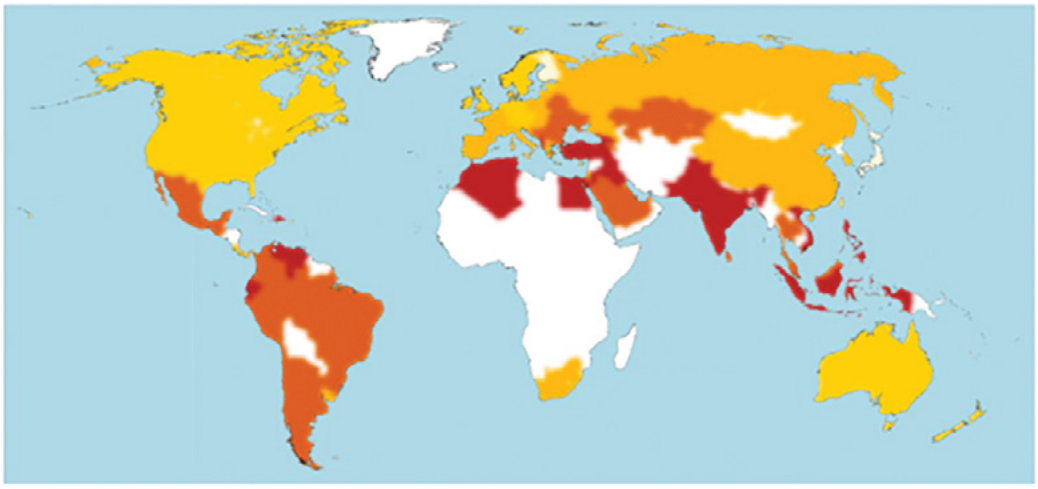
Continuing recent trends, researchers in 2013 focused on finding vulnerabilities in applications, instead on trying to find them in operating systems, operating system applications, or web browsers. Interestingly and despite shifting research priorities, the number of OS vulnerabilities found has actually increased. Below are some statistics highlighting global vulnerabilities and malware trends from 2013.

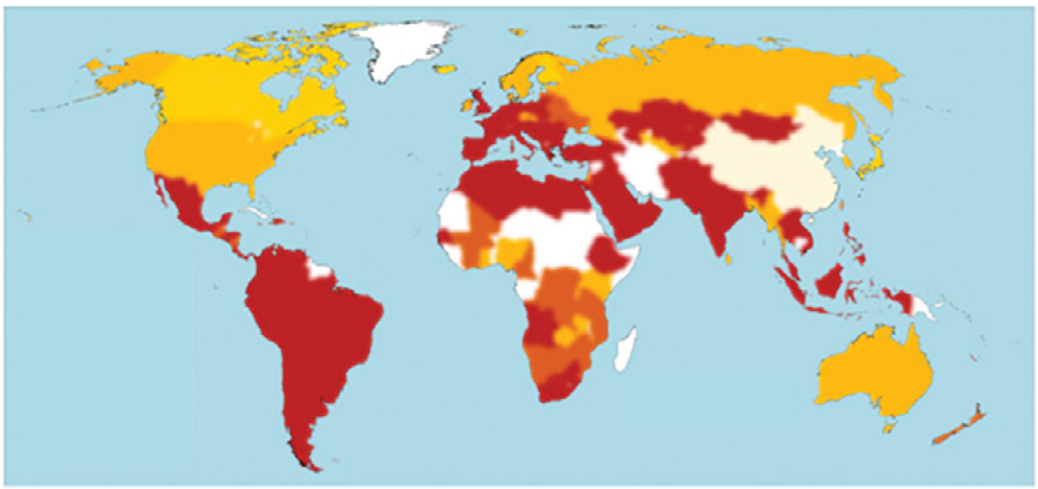
- Vulnerabilities in applications (excluding web browsers and operating system applications) increased 34.4 percent in the second half of 2013 and accounted for 58.1 percent of total number reported for the period.
- Operating system vulnerabilities increased 48.1 percent in the same period, going from least to most commonly found vulnerability. Overall, operating system vulnerabilities accounted for 17.6 percent of total number reported for that period.
- After reaching a high point in the first half of 2013, operating system application vulnerabilities decreased 46.3 percent in 2013, and accounted for 14.7 percent of total disclosures for the period.
- Browser vulnerability disclosures decreased 28.1 percent in the last sixth months of 2013 and accounted for 9.6 percent of total disclosures for the period
- Exploits against Java and HTML/Javascript were the most prevalent in 2013; attacks against the OS, Adobe Flash and Document formats are also significant.
- Despite decreasing each quarter, Java exploits were the most commonly encountered type of exploits in the second half of 2013.
- Encounters with web-based (HTML/JavaScript) threats decreased by more than half in the first six months of 2013 to become the second most commonly encountered type of exploits.
- Detections of operating system, Adobe Flash, and document exploits remained mostly stable during the second half of the year.
- Java is targeted by a significant amount of malware families.
- On average, about 21.2 percent of reporting computers worldwide encountered malware each quarter in 2013. At the same time, malware was removed from about 11.7 out of every 1,000 computers that Microsoft anti-virus worked on.
- Latin America remains a critical region, with high levels of detections in several of the largest countries—among them Mexico, Brazil, Colombia, Argentina, Peru, and Chile, although high levels of infections prevail in most of the region.

- Threats are mostly trojans, Trojan downloaders and droppers and worms. This is tied to the increased activity in credential theft and botnets in Latin America. Brazil saw consistently higher rates of this activity than most other countries in the region.
- The malicious site activity in the region tends to be predominantly concentrated on malware distribution hosting sites, probably due to the incremental malware development activities in some of the countries.
- Brazil is very active in malware development and distribution
- Drive by download hosting activity is seen predominantly in Brazil and Colombia.

Encounter Rates (top) and Infection Rates (Bottom) by Country/Region in 4Q13

Source: Microsoft Security Intelligence Report – http://www.microsoft.com/sir





Organization of
American States

Latin American and Caribbean Cybersecurity Trends

Tendencias de Seguridad Cybernética en América Latina y el Caribe

Secretary General
José Miguel Insulza

Assistant Secretary General
Albert R. Ramdin

Secretary for Multidimensional Security
Adam Blackwell

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

Lead Author
Brian Sullivan

Editors
Brian Dito
Belisario Contreras

Vice President,
Global Government Affairs
& Cybersecurity Policy
Cheri McGuire

Director
William Wright

Contributing Editors
Andrew Barris
Paul Wood

Data Analyst
Kavitha Chandrasekar

Graphics & Design
Scott Wallace

June 2014 / Junio de 2014

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

www.oas.org/cyber/

04/14