Zyber Global

SEPTEMBER 2023 | ISSUE 38

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to Zyber Global Centre's monthly newsletter - September 2023, the 38th edition!

Hello, digital defenders! Unravel the insights in our September edition of our monthly newsletter!

August was quite the adventure for me. I ventured to Liverpool and Glasgow for the first time. In Liverpool, I snapped a picture with the iconic Fab 4. If you're wondering, it was a statue of the legendary Beatles: Paul, John, George, and Ringo!

While I've visited Edinburgh and Aberdeen in the past, Glasgow was a new experience. My timing was impeccable as Banksy's Exhibition was on at the Gallery of Modern Art. I even captured the quirky Duke of Wellington statue, famously adorned with a traffic cone, right outside the gallery.

However, August wasn't all about exploration. A U.S.-based friend reached out about someone she knew who had fallen victim to a crypto scam through a WhatsApp group, losing a staggering $200,000 USD. The priority became damage control, urging her to promptly report the incident to the FBI, FTC, and other relevant agencies, as swift action is crucial for any potential recovery.

Let us know If you are interested, and we will delve deeper into the topic of crypto scams in an upcoming newsletter. In the meantime, continue to be safe!

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

The Duke of Wellington Statue, Glasgow

Esther and the Beatles

"The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction and Resilience. Do remember: "Cybersecurity is much more than an IT topic"

Stephane Nappo
Global Head Information Security,
Société Générale International Banking

Zyber Focus Article

Cybercrime and Cybersecurity in Latin America and the Caribbean

by Arsha Gosine, Head of Research, ZGC

Cybercrime knows no borders and has no boundaries! In today's digitally interconnected world with approximately three billion internet users, cybercrime continues to demand a multifaceted approach – coordinated and cooperative.

In this article we take a look at the Cyjax White Paper - Strategic Intelligence Report: Latin America and the Caribbean 2023 (the Cyjax Report) and the "Cybersecurity: Risks, Progress, and the way forward in Latin America and the Caribbean" 2020 Report (the 2020 Report), to explore Latin America and the Caribbean to see how they are approaching the issue of cyber-risks/threats to their critical infrastructure, the challenges faced, what is being done and where are they, in terms of managing the burgeoning problem.

Latin America and the Caribbean (LAC) comprise of thirty-three countries, namely:

South America	Central America	The Caribbean
Brazil	Mexico	Haiti
Columbia	Guatemala	Dominican Republic
Argentina	Honduras	Cuba
Peru	Nicaragua	Jamaica
Venezuela	El Salvador	Trinidad and Tobago
Chile	Costa Rica	Bahamas
Ecuador	Panama	Barbados
Bolivia	Belize	St Lucia
Paraguay		Grenada
Uruguay		St Vincent and Grenadines
Guyana		Antigua and Barbuda
Suriname		Dominica
		St Kitts and Nevis

Around July 2020, the Organization of American States (OAS) and the Inter-American Development Bank (IDB) launched a joint study, the 2020 Report. This is the second edition of a report that initially assessed the state of cybersecurity readiness in the region (the first one "Cybersecurity: Are We Ready in Latin America and the Caribbean?" [2016 Report] was presented in 2016).

Where it started

The 2016 Report was the first of its kind produced jointly by the OAS and the IDB, while, the 2020 Report portrayed their continued commitment in supporting the LAC in their efforts to strengthening cybersecurity within the region.

Background and post 2016 in the LAC region

The purpose of the 2016 Report was to provide the LAC with a view on the state of cybercrime and cybersecurity throughout the region and possible next steps to improve and strengthen national cybersecurity capacities.

According to Miguel Porrúa Digital Government Principal Specialist, Data and Digital Government Cluster Coordinator, IDB and Belisario Contreras Manager, Cybersecurity Programme OAS, the region did not seem to realize the magnitude of the problem until the 2016 Report. Cyberattacks continued with LAC financial institutions being targeted. Like other countries worldwide the COVID-19 pandemic and the increase in digital activity generated in the region, further exposed the vulnerabilities of the digital space in LAC.

Given the increase in cyberattacks, the OAS and the IDB found it necessary to re-implement the Cybersecurity Capacity Maturity Model for Nations (CMM) to measure the growth and development of the capacities of the LAC member states to defend against the growing threats of cyberspace.

Sadie Creese Director, Global Cyber Security Capacity Centre, University of Oxford explains that the CMM was devised by the Global Cyber Security Capacity Centre (GCSCC, Oxford, England) in 2013 and is the basis for the OAS and Inter-American Development Bank (IDB) regional studies in 2016 and 2020. It follows a comprehensive approach that evaluates capacity in five dimensions:

- Cybersecurity Policy and Strategy;
- Cyberculture and Society;
- Cybersecurity Education, Training, and Skills;
- Legal and Regulatory Frameworks; and
- Standards, Organizations, and Technologies.

To reliably measure cybersecurity capacity, every aspect is further broken down into different levels with each level assessing capacity with progressive detail.

Roll on 2023

Today, internet access continues to improve across Latin America and the Caribbean, however there are still marked differences across the region. According to Statista (a global data and business intelligence platform), 90% of people resident in Chile, Uruguay, The Bahamas and Antigua & Barbuda came online in 2023, with the populations of Costa Rica, Argentina, Barbados and the Dominican Republic in second place at 85%. This contrasts sharply with Nicaragua, Guyana and Haiti, where only around 50% of people have access to the internet. Due to sustained investment, mobile connectivity is helping to address the gap, though Venezuela and Ecuador are trailing in this regard.

Governments throughout the LAC region were generally slow in developing national cybersecurity strategies and cybercrime laws compared with some other parts of the world. Brazil, for example, did not publish its first national cybersecurity strategy until 2020.

There has been much improvement in cybersecurity throughout the LAC region within the last three years, since this 2020 Report was written.

We see that a joint, coordinated and informative approach continues to be required to face the challenges of the increasing complexity of cybersecurity which is now 'core business'. This will continue to be explored in the October Newsletter. Stay tuned!

Read more: https://zyberglobal.com/blog

Zyber News Roundup

Federal Court Case Uses Blockchain Tech to Fight Russian and North Korean Hackers

For years, cryptocurrencies such as Bitcoin (BTC) and Ether (ETH) have been the favoured methods of payment for cybercriminals.

Ransomware crime rings rely almost exclusively on Bitcoin payments to extract vast sums from major institutions, including hospitals and providers of critical infrastructure.

But in a landmark federal court case in Chicago, technology was used to lock cybercriminals out of their blockchain accounts, marking a significant shift in the battle against those who misuse cryptocurrencies for illicit activities.

The case targeted Russian and North Korean hackers, including major entities like Hydra Market and the Lazarus Group, both of which have been sanctioned by the U.S. Treasury Department. Using a unique judicial injunction, the court froze all accounts holding the cryptocurrency JTC, a coin that emerged from a Bitcoin software update.

This move allows victims who lost Bitcoin to claim their JTC either through the Jurat Wallet app or by pursuing legal action. The technology behind this enforcement was developed by Jurat Blockchains, a firm that specializes in legal tech for blockchains and smart contracts. Industry estimates of cryptocurrency crimes range above $20 billion annually

Read more:
https://dailyhodl.com/2023/08/28/federal-court-case-uses-blockchain-tech-to-fight-russian-and-north-korean-hackers/

US Releases Tornado Cash Founder on Bail After $1,000,000,000 Money Laundering Charge

One of the founders of crypto mixer Tornado Cash has been released on bail after being charged with laundering $1 billion by the U.S. Department of Justice (DOJ).
According to defense attorney Brian Klein, Roman Storm, one of the founders of the sanctioned crypto mixer, has been released on bail.

However, according to Klein, the implications of the prosecutors' case against his client are far-reaching and could impact all software developers as Storm is being charged with money laundering for helping develop Tornado Cash rather than for laundering money himself. According to a press release from the DOJ, Storm, alongside Roman Semenov, another Tornado Cash founder, was charged with conspiracy to help North Korean hacking group Lazarus launder money earlier this week.

Read more:
https://dailyhodl.com/2023/08/27/us-releases-tornado-cash-founder-on-bail-after-1000000000-money-laundering-charge/

UN Warns Hundreds of Thousands in Southeast Asia Roped into Online Scams

A new report sheds light on cybercrime scams that have become a major issue in Asia, with many workers trapped in virtual slavery.

The U.N. human rights office says criminal gangs have forced hundreds of thousands of people in Southeast Asia into participating in unlawful online scam operations, including false romantic ploys, bogus investment pitches, and illegal gambling schemes.

The Office of the U.N. High Commissioner for Human Rights, in a new report, cites "credible sources" that at least 120,000 people in strife-torn Myanmar and roughly 100,000 in Cambodia "may be held in situations where they are forced to carry out online scams."
The report sheds new light on cybercrime scams that have become a major issue in Asia, with many of the workers trapped in virtual slavery and forced to participate in scams targeting people over the internet.

Laos, the Philippines and Thailand were also cited among the main countries of destination or transit for tens of thousands of people. Criminal gangs have increasingly targeted migrants, and lure some victims by false recruitment — suggesting they are destined for real jobs.

Read more: https://www.securityweek.com/un-warns-hundreds-of-thousands-in-southeast-asia-roped-into-online-scams/

St Helens Council Warns of Phishing After Ransomware Breach

A UK local authority has warned citizens to watch out for follow-on scams after it was breached in a ransomware attack discovered in late August. St Helens Borough Council in the north-west of England said it first identified the attack and reached out immediately to a third-party security firm.

It claimed in a statement seen by Infosecurity that it is continuing to provide services through the council website, although some systems have been disrupted.
"Some internal systems to the council are currently being affected due to the actions we have put in place to prevent any further impact, and whilst a full investigation is undertaken," the statement noted. "While we work through this ongoing situation we would recommend that residents are mindful of how to keep themselves safe online and be alert to any communications they may have received from the council."

Local government authorities in the UK and US are a popular target for ransomware actors, as they're deemed to be less well-resourced than state or national peers.

Read more: https://www.infosecurity-magazine.com/news/st-helens-council-warns-of-phishing/

OBJECTIVES

This is the first of a series of thematic webinars on cybercrime; the purpose of which is to:

- **Increase awareness and understanding of cybercrime trends and emerging threats;**
- **To exchange views and experiences; and**
- **To share good practice; and**
- **To collaborate with others globally.**

EXPECTED OUTCOMES

An increased awareness of emerging cyber threats: where participants will receive up-to-date information on the latest trends and tactics used by cybercriminals.

This will assist participants to stay ahead of the curve when it comes to detecting and responding to cybercrime.

A better collaboration between jurisdictions where participants from different countries, are able to foster and engender greater collaboration through networking and sharing good practice

The widespread use of Information Communication Technology has led to an increase in illegal activities committed against computer systems, highlighting the need for the retrieval of evidence in criminal investigations.

Cybercrime has become accessible to a wider range of individuals due to the availability of ready-made malicious software and online cybercrime-for-hire services, leading to the exploitation of new technologies for unlawful purposes.

Cybercrime affects individuals through scams, online child sexual exploitation, and cyberbullying, while organizations face threats to financial institutions and the theft of sensitive information. New measures are required to keep pace with these threats, including technical solutions to deal with encryption technologies and the complexities of transnational criminal activities in cyberspace, so register now to attend and learn more.

REGISTER HERE: **https://www.subscribepage.com/zgcwebinar**

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

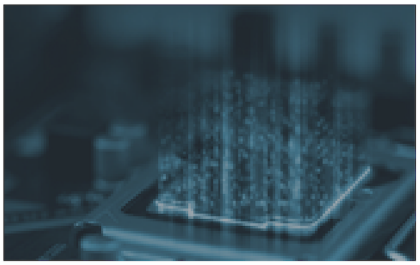
Global Cyber Conference Zürich, Switzerland **14 - 15 September 2023,**	**National Cyber Summit Huntsville, USA** **20 – 21 September 2023**	**Africa Internet Governance Forum** **Abuja, Nigeria** **19- 21 September 2023**
The Global Cyber Conference (GCC) is a leading international cyber security and privacy event gathering an audience of senior cyber security stakeholders, decision-makers, public authorities, and academia. It provides key decision-makers a networking and learning platform to gain a shared understanding of what needs to be done to strengthen cyber resilience.	The National Cyber Summit is the nation's most innovative cyber security-technology event, offering unique educational, collaborative and workforce development opportunities for industry visionaries and rising leaders. NCS offers more value than similar cyber conferences with diverse focus-areas, premier speakers, and unmatched accessibility. Our core focus is on three things: education, collaboration and innovation.	The 2023 Africa Internet Governance Forum (IGF) will bring together stakeholders from various sectors, including government, civil society, private sector, technical communities, and academia. The forum will serve as a platform for dialogue, collaboration, and exchanging ideas on crucial Internet Governance issues in the African region. Under the theme of "Transforming Africa's Digital Landscape: Empowering Inclusion, Security, and Innovation," the Africa IGF aims to address the challenges and opportunities presented by the rapidly evolving digital landscape. It focuses on empowering inclusivity, ensuring robust cybersecurity measures, and promoting innovation across the continent.
For further information **https://globalcyberconference.com**	**For further information** **https://www.nationalcybersummit.com**	**For further information** **https://igf.africa/2023-overview/**

Zyber Global Online Events

Our Online Courses with INsig2
Sign up now at https://insig2-and-zyberglobal.learnworlds.com/
Special discount: 15% Use Code: zyber

Courses per sectors

Legal Entities
Customized courses for legal entities: judges, lawyers and public prosecutors.
Explore deeper aspects of digital forensics and the forensic value of evidence while collecting, processing, and presenting digital evidence in criminal and administrative proceedings.



Law Enforcement
Customized courses for law enforcement officials: First responders, forensic investigators and analysts.
Delve into procedures, techniques, and tools used in digital forensic analysis and how to apply them in forensic investigations.

Private Sector Corporations and Small Businesses.
Customized courses for industry professionals working in the private sector; to help them understand the value and the need for digital forensic, and its implications in a corporate environment.

Course Structure

***FULL-TEXT REVISION**

***QUIZ AFTER EACH CHAPTER**

***CASE-STUDY AFTER FINAL EXAM**

c

At the end of each course, you will be issued a completion e-certificate which is immediately printable for your records. The number of **CPD** (Continuing Professional Development), **CPE** (Continuing Professional Education), and/or **CLE** (Continuing Legal Education) points will depend on the course.

DISCOUNTS

Special discount for groups of 10+ participants on all courses. The bigger the group, the bigger the discount.

BUNDLES

Stay on your forensic digital learning path and get the most from your e-learning experience by using course bundles.
https://bit.ly/31NRYsj

FREE COURSE ON PASSWORD MANAGEMENT

This covers different lock security methods, guidelines on securely storing your passwords, various password managers and how to use them.
https://bit.ly/3eMu7ED

Zyber Global – Tel: 07426719579 **Privacy Policy** **Register**
To unsubscribe contact us at office@zyberglobal.com