Zyber Global

AUGUST 2023 | ISSUE 37

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to Zyber Global Centre's monthly newsletter - August 2023, the 37th edition!

July was a whirlwind of exciting travels and engaging encounters, with cybersecurity insights gathered from every corner. My journey took me to the tech-savvy city of Copenhagen, Denmark, where I managed to steal a moment with the iconic Little Mermaid statue. Despite its petite size, the statue left a lasting impression, much like the subtle yet significant cybersecurity threats we often encounter. I have attached a photo for your viewing pleasure.

My travels also led me to Oslo, Norway, home to the stunning Opera House, a testament to unique architectural innovation, much like the innovative cybersecurity solutions we strive to develop.

Mark your calendars for the 21st of September, as we are hosting the Zyber Global Webinar titled "Cybercrime Uncovered: From Prosecution to Prevention".
This is an opportunity to delve into the world of cybercrime, understand its intricacies, and learn how to stay a step ahead.
Spaces are filling up fast, so make sure to register soon.
I am eagerly looking forward to your participation in this interesting and enlightening event.
For more information, see
https://www.subscribepage.com/zgcwebinar

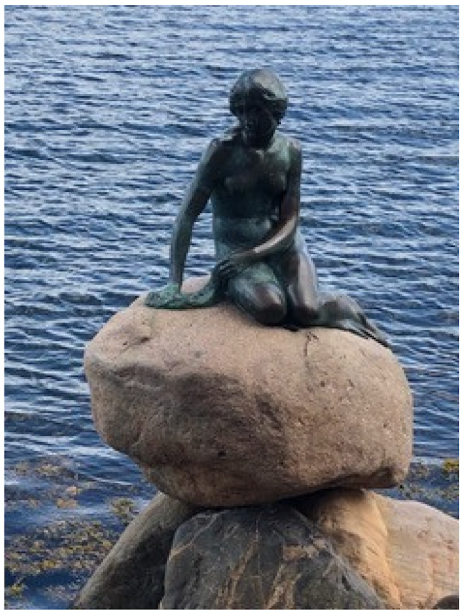
Have a fantastic summer!

Do continue to let us know what topics you would like to see discussed in the next newsletter and as always stay safe!

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features



"Most people are starting to realize that there are only two different types of companies in the world: those that have been breached and know it and those that have been breached and don't know it."

Ted Schlein,
Partner, Kleiner Perkins Caufield & Byers, USA

Zyber Focus Article

Ransomware in the Caribbean - A Focus on Trinidad and Tobago

by Arsha Gosine, Head of Research, ZGC

In my previous article, last month on ransomware [ZGC Newsletter 36th Edition], I focused on the much-needed transparency in reporting ransomware and looked at de-bunking some of the myths surrounding ransomware.

We see that ransomware continues to be a worldwide problem and the Caribbean is no exception. In the last few years, the region has 'become a new frontier for cyber-attacks and crime at an estimated cost of around US$90 billion per year' (see 2016 Cyber Security: Are we ready in Latin America and the Caribbean, Centre for Strategic Studies and McAfee).Pricewaterhouse Coopers (Caribbean Region) in 2017 also warned that Caribbean firms were 'not paying enough attention to cybersecurity risks'.

One of the major ransomware incidents was when Ansa McAl, one of the largest financial and insurance conglomerates in the Caribbean was hacked in 2020. The hackers, criminal cybergang REvil, said it had "numerous financial documentation, agreements, invoices, reports" – at least 17,000 documents that it threatened to release on a public server if a ransom was not paid". The incident started at its Barbados operations and migrated to Trinidad. According to technewstt.com, the hackers made good on that promise and released 12.9 gigabytes of Ansa's data "into the wild for public access," allegedly because the company refused to pay any ransom.

Since then, the problem has just gotten worse. In a Newsday article dated 9, February 2023, it was mentioned that during the first half of 2022, the Caribbean experienced 144 million cyberattack attempts, with ransomware being the most common breach.

Trinidad and Tobago (TT) was among the Caribbean countries that experienced such attacks. Last year, the TT Cybersecurity Incident Response Team (TT-CSIRT) of the Ministry of National Security reported a significant increase in cyber-attacks, especially ransomware. In April last year, the Massy Group, one of TT's largest suppliers of consumer goods and pharmaceuticals, (with 23 stores in TT and 61 stores throughout the Caribbean) was forced to close it stores in TT. It took approximately four days to get its systems running but at what cost? In a later press release Massy Group admitted that the data unlawfully accessed by the attackers was more extensive than the preliminary stages of the investigation had revealed.

"*These cyberattackers take advantage of system vulnerabilities and in many cases not only affect data centers or databases, but also any system or equipment connected to an internet connection network or cloud*," said Jaime Reinoso, South English Caribbean territory manager at Schneider Electric.

Meanwhile, Ronald Walcott, managing director of Precison Cybertechnologies and Digital Solutions Ltd, TT said attacks on business systems could come from anywhere.
"*The reality is there is no hard and fast rule when it comes from cyberattacks. They are generally organised and use artificial intelligence. They can come from anywhere – Russia, China, the US, or it could come from right here.*"

While, Anish Bachu, a cybersecurity analyst with TTCSIRT, noted that the top hacking group targeting Caribbean systems is Lockbit, and said that many attacks are coming through improperly configured firewalls, unpatched vulnerabilities in software and compromised user credentials.

On July 8 2023, it was reported in the Trinidad Guardian that there had been a cyber-attack on the Attorney General's network system. The Ministry of Digital Transformation was reported to have said, "*This unauthorised and illegal access has negatively impacted operations at the Ministry of Attorney General and Legal Affairs (AGLA) and certain associated Divisions. Having taken actions to minimise the threat, an investigation, in partnership with leading industry cybersecurity experts is ongoing*". There were services such as the electronic service of court documents that were severely disrupted and practical measures were put in place to ensure 'business as usual'.

The TT-CSIRT continues to publish regular advisory notices on the significant increase in ransomware attacks targeting Caribbean organizations.
The advisory notices ask that local firms be diligent and aware of the threat level. The notices also explain how and where to report an incident; the different levels of incidents; and the confidentiality and privacy measure that is in place so that there is a reassurance in reporting these incidents.

The TT-CSIRT also explains a number of key preventative measures against the main vectors used to target Caribbean firms, namely:

- Exploiting system vulnerabilities (particularly outdated firewall devices and exposed remote desktop protocol)
- Phishing emails with infected attachments or links
- Compromising user credentials

All three of these vectors are well known methods used to infect corporate networks with ransomware. Phishing, for example, is still the main way that malware ends up on a device. Phishing causes 90% of data breaches and 1 in 3 employees have been found to click the malicious link in a phishing email. Phishing is behind credential theft and malware infection with credential loss due to phishing increasing by over 280% since 2016.

The local companies need to act on these advisory notices and put these measures in place and ensure that their security systems are regularly updated.

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

Zyber News Roundup

Emails with link to pay fines a phishing scam, warn Dubai Police

The Dubai Police have issued an urgent warning to the public about a rampant phishing scam that is currently ongoing. The alert comes after many people complained of receiving suspicious emails purportedly from the Dubai Police, urging recipients to click on a link to pay fines and service fees.

In a statement, Dubai Police warned residents and citizens to remain vigilant, to exercise caution when dealing with such messages, and to verify the authenticity of any email claiming to be from the Dubai Police.

The phishing scam typically involves an email, seemingly from the Dubai Police, alerting the recipient that they have outstanding fines or service fees that need to be paid immediately. A link is included in the email, which leads the user to a fraudulent website designed to steal personal and financial information.

Read more:
https://gulfnews.com/uae/crime/emails-with-link-to-pay-fines-a-phishing-scam-warn-dubai-police-1.97133234

Downtown Los Angeles 'SIM Swapper' Pleads Guilty to Hacking into Instagram Users' Accounts to Fraudulently Obtain Money

Amir Hossein Golshan, a 24-year-old man from Los Angeles, has pleaded guilty to three felony charges related to cybercrime, including unauthorized access to a protected computer to obtain information, wire fraud, and accessing a computer to defraud and obtain value. Golshan's scheme, which involved "SIM swapping" to hijack social media accounts and defraud victims, caused approximately $740,000 in losses to hundreds of victims over several years. His tactics included social media account takeovers, Zelle payment fraud, and impersonating Apple support.

Golshan's crimes ranged from duping friends of social media influencers into sending him money, to demanding ransom for the return of hijacked accounts, and even threatening to post personal videos online. He also fraudulently advertised non-existent Instagram services, impersonated Apple Support personnel to steal NFTs and cryptocurrency, and sold a stolen NFT for $130,000 in cryptocurrency on an NFT marketplace. Golshan, who has been in federal custody since last month for violating the terms of his pretrial release, is set to face a statutory maximum sentence of 20 years in federal prison for the wire fraud count, and up to five years in federal prison for each of the computer access counts at his sentencing hearing scheduled for November 27.
Read more: https://www.justice.gov/usao-cdca/pr/downtown-los-angeles-sim-swapper-pleads-guilty-hacking-instagram-users-accounts

Maritime Cyber Attack Database launched

Researchers at NHL Stenden University of Applied Sciences in the Netherlands have developed the Maritime Cyber Attack Database (MCAD), a comprehensive record of over 160 cyber incidents impacting the global maritime sector. The database, which includes incidents such as location spoofing of NATO ships in the Black Sea in 2021, aims to increase awareness of cyber threats in the maritime industry and provide data for further research. The database covers not only incidents affecting vessels, but also ports and other maritime facilities worldwide.

The MCAD, now publicly accessible online, will be used to create realistic maritime cyber incident simulations to help companies, organizations, ports, and harbours prepare for potential attacks. The research group also plans to use the database to generate reports and research papers that highlight trends and provide detailed analysis of the data. The database will be regularly updated and augmented, with the team currently developing AI to automate the identification of new incidents and provide further details on known incidents.

Read more:
https://smartmaritimenetwork.com/2023/07/16/maritime-cyber-attack-database-launched/

Unmasking Cybercriminals: How Deception Technology is Revolutionizing Cybersecurity

Deception technology, a new cybersecurity strategy, uses decoys or traps to mislead cybercriminals, luring them into a controlled environment where their methods can be studied. This proactive approach not only identifies attackers but also provides insights into their modus operandi, enabling the development of more robust defense mechanisms. The technology turns the tables on cybercriminals, creating a landscape filled with traps and decoys that confuse and expose the attackers, and involves creating a simulated network with realistic data and behaviour to convince cybercriminals they've breached a real network.

However, deception technology has its challenges, including the risk of false positives and the complexity of managing and maintaining the decoy systems. Despite these, the potential benefits of deception technology are significant, providing a proactive and effective way to unmask and study cybercriminals, thereby strengthening defenses and contributing to a broader understanding of cybercrime. As the cybersecurity landscape continues to evolve, deception technology is set to play an increasingly important role in combating cybercrime and protecting digital assets.

Read more: https://fagenwasanni.com/news/unmasking-cybercriminals-how-deception-technology-is-revolutionizing-cybersecurity/50086/

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

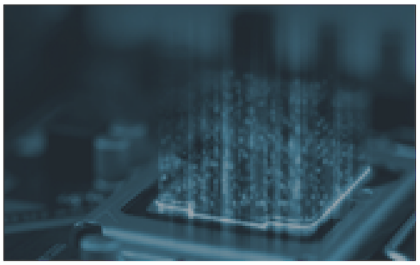
Black Hat USA **Mandala Bay Convention Center, Las Vegas, USA** **5-10 August 2023,**	**DEF CON 31** **Caesars Forum, Las Vegas, USA** **10 – 13 August 2023,**	**International Conference on Legal, Security and Privacy Issues** **London, England** **17- 18 August 2023**
Black Hat USA is a large conference that focuses on hacking and security vulnerability research. It takes place annually in Las Vegas and features keynote speeches from industry leaders, as well as hands-on training and workshops. The conference provides a unique opportunity for attendees to learn about the latest trends and developments in the field of hacking and security, and to gain insights into emerging technologies and techniques. The Black Hat cybersecurity conference is known for its high-quality presentations and engaging discussions, and has become a must-attend event for anyone interested in the field of hacking and security.	The DEF CON Conference is one of the oldest and largest cybersecurity conferences in the world, with a focus on hacking. It takes place in Las Vegas and offers a variety of talks and events, such as social engineering contests and lockpicking competitions. DEF CON provides a unique opportunity for attendees to learn about the latest trends and developments in the field of hacking, and to network with other professionals and experts in the industry. DEF CON is known for its lively atmosphere and engaging activities.	The International Conference on Legal, Security and Privacy Issues aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Legal, Security and Privacy Issues. It also provides a premier interdisciplinary platform for researchers, practitioners and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in the fields of Legal, Security and Privacy Issues.
For further information **https://www.blackhat.com/upcoming.html**	**For further information** **https://defcon.org**	**For further information** **https://waset.org/legal-security-and-privacy-issues-conference-in-august-2023-in-london utm_source=conferenceindex&utm_medium=referral&utm_campaign=listing**

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