Zyber Global

JANUARY 2024 | ISSUE 42

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Happy New Year and welcome to Zyber Global Centre's monthly newsletter - January 2024, the 42nd edition! This is where we bring you exciting updates from the dynamic world of cybersecurity!

As we bid farewell to a dynamic and challenging 2023, it's time to reflect on our remarkable journey and set our sights on the promising horizon of 2024. Last year was a milestone in our collective quest for a safer digital world. Together, we navigated the complex landscape of cyber threats, adapted to emerging challenges, and strengthened our defences against the ever-evolving tactics of cybercriminals.

This year, we're not just continuing our mission; we're elevating it. We are thrilled to announce the launch of our monthly webinars, an initiative born from the vibrant community we established last year. Our first webinar will be held on the 31st of January 2024 15:00 - 16:00 GMT online.

Our speaker is Marina Jovanovska, the Chief Investigator for cybercrime at the Investigative Center within the Basic Public Prosecutor's Office, North Macedonia. Ms Jovanovska will be speaking on ***"Navigating the Digital Underworld: Strategies for Tackling Online Frauds and Identity Theft."***

These webinars are more than just meetings; they are a melting pot of ideas; a platform for sharing ground-breaking strategies; and a beacon for those seeking guidance in the vast expanse of cybercrime prevention and cyber security.

As we step into 2024, let's carry forward the spirit of collaboration and innovation that defines us. We look forward to achieving greater heights together, armed with knowledge, driven by passion, and united in our commitment to making the digital world a safer place for everyone.

Here's to a year of learning, growth, and continued success in our fight against cybercrime!

We look forward to seeing you at the webinar! https://www.subscribepage.com/zgcwebinar

Please continue to let us know what topics you would like to see discussed in future newsletters and remember to remain alert and cautious in the digital realm! Keep safe!

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Focus Article

2023: Navigating the Cyber Threatscape – A Year in Review

Zyber News

A roundup of the latest international cybercrime news.

Zyber Global Events Information

A focus on forums/conferences around the world.

Marina Jovanovska

Chief Investigator for cybercrime at the Investigative Center within the Basic Public Prosecutor's Office, North Macedonia.

Zyber Focus Article

2023: Navigating the Cyber Threatscape A Year in Review

Esther George, CEO, ZGC

In the ever-evolving digital age, 2023 has unfolded as a year marked by an unprecedented escalation in cybercrime threats, presenting formidable challenges to individuals, organizations, and governments worldwide.

With cybercriminals becoming more sophisticated and audacious in their methods, understanding the landscape of these threats is not just a matter of staying informed—it's a critical defence strategy for anyone navigating the digital world. From the menacing rise of Ransomware 2.0 to the insidious use of deepfake technology, the cybercrime threats of 2023 are not only diverse but also alarmingly innovative, exploiting every conceivable vulnerability in our interconnected systems.

This article lists some of the worst global cybercrime threats of the year, we see businesses crippled by ransomware, supply chains compromised, and personal data snatched from unsuspecting fingertips – these are not mere headlines; they are stark reminders of the ever-present dangers lurking in the digital shadows.

Buckle up for a whirlwind tour of some of 2023's notorious data breaches and hacks. From the enhanced menace of Ransomware 2.0 to the deceptive intricacies of supply chain breaches, we will explore the darkest nooks of the cyber underworld.

JANUARY:

Royal Mail Ransomware Attack: This was a ransomware attack which significantly disrupted the Royal Mail's international delivery services. The "Lockbit" ransomware attack primarily impacts systems for dispatching and tracking international posts, while domestic services remain unaffected amidst ongoing investigations and efforts to resolve the issue.

JD Sports Hack: The fashion retailer JD Sports said the personal and financial information of 10 million customers was potentially accessed by hackers in a cyber-attack.

FEBRUARY:

Reddit: Reddit experienced a cyberattack where hackers accessed internal systems via a phishing scam that targeted employees, leading to the theft of internal documents, source code, and some employee and advertiser data.

Águas e Energia do Porto: The LockBit ransomware group claimed responsibility for a cyberattack on Águas e Energia do Porto, a major water utility in Portugal, demanding a ransom and threatening to publish stolen data, although the attack did not affect the public water supply and sanitation.

MARCH:

New Zealand and Australia Driving licence hack: Consumer finance firm Latitude Financial reported a major cyberattack resulting in the theft of personal information, including driver license and passport numbers, of 7.9 million people in Australia and New Zealand, alongside another 6.1 million records with personal details dating back to 2005.

Capita Data Breach: In March, the largest UK outsourcing services company, Capita, was hit by a cyber-attack which caused widespread disruption. Subsequently, around 90 organisations filed data breach reports to the ICO (Information Commissioner's Office) with hundreds of thousands of people being notified their data has been breached.

OCTOBER:

The Indian Council of Medical Research (ICMR): The ICMR experienced a significant breach with the sensitive details of 81 million people being offered for sale on the dark web, originating from Covid-19 test data; this major incident is one of India's largest.

23andMe Data Leak: In early October 2023, genetic testing company 23andMe disclosed a data leak potentially affecting millions of customers, sourced through credential stuffing attacks and not a direct system intrusion; this exposed data, including names, sex, birth year, and some genetic history details, is being sold online.

NOVEMBER:

TransForm Shared Service Organisation: Daixin Team claimed responsibility for a ransomware attack on five Canadian hospitals serviced by TransForm Shared Service Organization, disrupting Wi-Fi, email, and patient systems.

Germany's the Südwestfalen-IT (SIT), and the 72 member municipalities: A ransomware attack on Südwestfalen IT in Germany disrupted local government services in over 70 municipalities, affecting online systems and internal and external communications.

DECEMBER:

Yakult Australia: Yakult Australia confirmed a "cyber incident" affecting its Australian and New Zealand IT systems in mid-December, with cybercrime actor DragonForce claiming responsibility and leaking 95 GB of data including business documents, employee records, and identity documents.

Trinidad and Tobago Social Security Agency: Trinidad and Tobago's National Insurance Board (NIBTT), a key agency running the nation's social security system, announced a ransomware attack on December 26, leading to a closure of all offices and limited operations for the rest of the year, affecting over 630,000 people.

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

Zyber News Roundup

Unveiling the '*Pig Butchering*' Romance Scam A Modern Cybercrime Threat

The 'Pig Butchering' romance scam represents a significant and growing threat in the cybercrime landscape, exploiting unsuspecting individuals through social media platforms. This scam involves a scammer, often pretending to be a successful executive, who gradually builds a romantic relationship with the victim.

As trust develops, the victim is lured into investing in fake cryptocurrency or foreign currency trading platforms, showing unreal profits. The scam reaches its climax when victims, deeply entrapped both emotionally and financially, either run out of funds or try to withdraw their profits, only to find their accounts closed, additional payments demanded, and the scammer disappearing.

This scam is not only emotionally damaging but also financially devastating, with victims losing substantial amounts of money, often unrecoverable. The operations behind these scams are sophisticated and often based in Southeast Asia, making it challenging for law enforcement to tackle them effectively.

The US alone reported over $3.31 billion in losses from investment scams last year, but the actual numbers could be higher due to underreporting.

Law enforcement agencies recognize the seriousness of these scams but face limitations in addressing them due to their complex, transnational nature.

Read more:
https://bnnbreaking.com/breaking-news/crime/unveiling-the-pig-butchering-romance-scam-a-modern-cybercrime-threat/

African Organizations Aim to Fix Cybersecurity in 2024

African nations, recognizing their vulnerability to cyber threats and acknowledging a skills gap in cybersecurity, are increasingly investing in training programs to develop local expertise. Initiatives like the Cyber Hub in Nigeria, launched by the University of Lagos and other partners, aim to cultivate home-grown cybersecurity solutions and skilled professionals. These efforts are part of a broader strategy across the continent to close the cybersecurity skills gap, with emphasis on collaborations, such as the Biden-Harris administration's partnership with the Cybersafe Foundation.

Read more :
https://www.darkreading.com/cybersecurity-operations/african-organizations-aim-to-fix-cybersecurity-in-2024#

Canada: Good Samaritan who helped thwart attempted Facebook Marketplace robbery urges public to be careful

One of two Good Samaritans who intervened in an attempted robbery stemming from a Facebook Marketplace sale on Boxing Day is speaking out, urging people to be careful when they meet up to buy or sell goods.

Meraj Ahmed, an international student from Bangladesh who works part time for a food delivery service, recounted the incident that resulted in a sliced tendon in his hand.

Ahmed says he was leaving a building in Olympic Village on Tuesday after completing a delivery when he saw a man who appeared to have been pepper-sprayed calling for help. He said he saw a second person carrying what he described as a "computer device" trying to escape by getting in a vehicle. "He could do the same thing again so I thought that we need to stop him," he said.

Ahmed said he and another bystander — also a delivery driver — tried to trap the man. The man stabbed both Ahmed and the other bystander and was arrested by the police.

Sgt. Steve Addison with the Vancouver Police Department (VPD) is warning the public to use caution when completing online transactions in person.

Read more:
https://www.cbc.ca/news/canada/british-columbia/good-samaritan-who-helped-thwart-attempted-facebook-marketplace-robbery-urges-public-to-be-careful-1.7072037

Cyber-hackers target UK nuclear waste company RWM

Radioactive Waste Management (RWM), the company involved in the £50bn Geological Disposal Facility (GDF) project in the UK, experienced attempted cyberattacks via LinkedIn.

These attacks targeted RWM after its merger into Nuclear Waste Services (NWS), which consolidated several nuclear entities. Despite these efforts, RWM's chief executive, Corhyn Parr, assured that the cyber incidents did not materially impact the organization, highlighting the effectiveness of their robust cyber defenses.

The attacks on RWM represent a growing trend where hackers utilize social media platforms to infiltrate organizations. By creating fake accounts or sending deceptive messages, hackers aim to steal credentials or sensitive information. This method, known as social engineering, is becoming a common tactic for cybercriminals to bypass traditional security measures and gain unauthorized access to valuable data.

Read more:

https://www.theguardian.com/business/2023/dec/31/cyber-hackers-target-uk-nuclear-waste-company-rwm

ZYBER GLOBAL CENTRE

31 JANUARY 2024 | 15 : 00 - 16 : 00 GMT, ONLINE

ZYBER GLOBAL CENTRE MONTHLY WEBINARS

"NAVIGATING THE DIGITAL UNDERWORLD : STRATEGIES FOR TACKLING ONLINE FRAUDS AND IDENTITY THEFT"

LIMITED SLOT!
REGISTER NOW

MARINA JOVANOVSKA

CHIEF INVESTIGATOR FOR CYBERCRIME AT THE INVESTIGATIVE CENTER WITHIN THE BASIC PUBLIC PROSECUTOR'S OFFICE

TOPIC: "NAVIGATING THE DIGITAL UNDERWORLD: STRATEGIES FOR TACKLING ONLINE FRAUDS AND IDENTITY THEFT"

WELCOME TO THE INAUGURAL 2024 SESSION OF ZYBER GLOBAL CENTRE'S MONTHLY WEBINAR SERIES! IN THIS VIBRANT AND ENGAGING PLATFORM, WE'RE EXCITED TO SHINE A SPOTLIGHT ON THE DIVERSE AND DYNAMIC MEMBERS OF THE ZYBER GLOBAL COMMUNITY. JOIN US AS WE CONNECT WITH INDIVIDUALS FROM AROUND THE WORLD, DELVE INTO RICH DISCUSSIONS, AND EXCHANGE UNIQUE PERSPECTIVES AND EXPERIENCES. TOGETHER, WE'LL EXPLORE BEST PRACTICES AND INNOVATIVE STRATEGIES, FOSTERING AN ENVIRONMENT OF MUTUAL LEARNING AND GROWTH. GET READY TO BE A PART OF A GLOBAL CONVERSATION THAT SHAPES THE FUTURE OF OUR COMMUNITY!

DURATION AND LANGUAGE: 1 HR | ENGLISH ONLY

AUDIENCE: THE EVENT IS OPEN TO CRIMINAL JUSTICE AUTHORITIES AND OTHER GOVERNMENT OFFICIALS FROM ALL COUNTRIES.

https://www.facebook.com/ZyberGlobal

https://www.linkedin.com/in/esther-george/

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

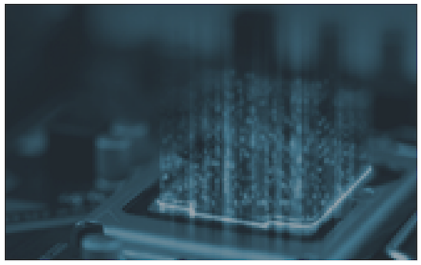
FutureCon Eastern Conference **Online** **12 January 2024**	**International Conference on Cybersecurity and Machine Intelligence 2024** **Odisha, India** **16 - 17 January 2024**	**SANS Cyber Threat Intelligence Summit & Training 2024** **Washington, D.C & Online** **29 January - 5 February 2024**
The FutureCon Eastern event brings together security professionals from across several eastern U.S. states to conduct cybersecurity training and network with their peers. "*Cybersecurity is no longer just an IT problem*". Gain the latest knowledge you need to enable applications while keeping your computing environment secure from advanced Cyber Threats. Demo the newest technology and interact with the world's security leaders and gain other pressing topics of interest to the information security community. Attendees can earn up to 12 CPE credits.	The International Conference on Cybersecurity and Machine Intelligence (ICCMI) aims to address the growing threat of cyber-attacks by bringing together experts in the field of cybersecurity and machine intelligence. Over the past few decades, cyber threats have increased significantly, and attacks usually occur in a series of stages, including reconnaissance, gaining access, and cover-up. These attacks can take many forms, including wireless, malicious code, and phishing attacks. Large-scale attacks such as viruses, worms, and spam are not targeted, so implementing risk management strategies to protect computing systems from vulnerabilities and cyber-attacks is crucial.	Join us in Washington, DC or Live Online and walk away from the Cyber Threat Intelligence Summit with new perspectives! Learn from case studies that challenge CTI assumptions and as a result experience a shift in your understanding. No matter your background or skill level, you'll have the chance to learn, connect, and share with thousands of cybersecurity professionals in attendance from around the globe. This is the summit for anyone involved in cyber threat intelligence (CTI).
For further information **https://futureconevents.com/events/eastern-january-2023/**	**For further information** **https://iimt.ac.in/ICMI/**	**For further information** **https://www.sans.org/cyber-security-training-events/cyber-threat-intelligence-summit-2024/**

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