Zyber Global
INDEPENDENT CYBERCRIME, CYBERSECURITY, DIGITAL EVIDENCE, LEADERSHIP AND BUSINESS CONSULTANCY
www.zyberglobal.com

NOVEMBER 2024 | ISSUE 52

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the November edition of our newsletter – our 52nd issue, and we couldn't be more excited to share it with you!

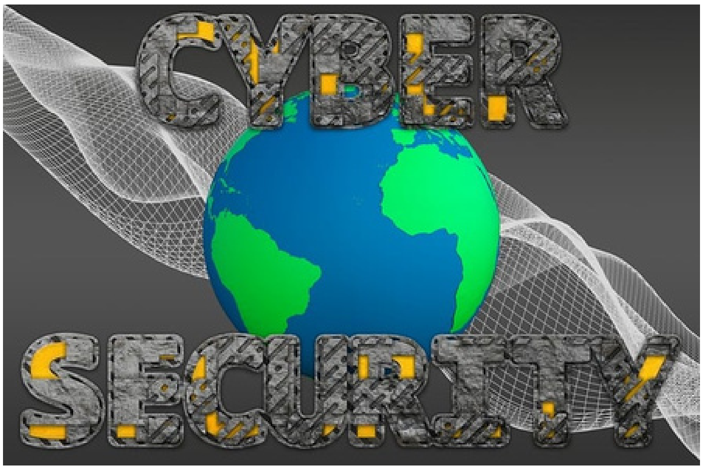
October in the UK was filled with reflection and awareness, marking both Black History Month and Cybersecurity Awareness Month—a reminder of the strength we draw from resilience, both in history and online security. With the clocks turned back and the darker, colder days settling in, it's a fitting time to strengthen our defences and keep our security awareness sharp.

We're also thrilled to announce our upcoming Wisdom of the Crowd webinar, "Cybersecurity in the Crossfire: The New Risks Facing Telecom Carriers and Digital Platforms," scheduled for 14 November at 3pm GMT. You'll find further details in this newsletter.

So, stay warm, stay vigilant, and let's dive into November's insights!

Stay safe and secure,

Esther George, CEO Zyber Global Centre



This Month's Features

1. **Wisdom of the Crowd**
"Cybersecurity in the Crossfire: The New Risks Facing Telecom Carriers and Digital Platforms"

2. **Zyber Focus Article**
Digital Shadows: Inside the High-Tech Crime Networks Operating Across Southeast Asia and Beyond

3. **Zyber News**
We have a roundup of the latest international cybercrime news.

4. **Zyber Global Events Information**
A focus on forums/conferences around the world.

🎉 Exciting Event Alert: Wisdom of the Crowd! 🎉

We’re thrilled to invite you to another meeting of the Zyber Global Community – “Wisdom of the Crowd!”

This 30-minute session, happening on 14th November at 3 PM GMT, is all about sharing knowledge and supporting each other.

We’ll kick off with a 15-minute presentation, by **Graham Butler (Chairman and Founder of Bitek Global Ltd)** followed by a 15-minute Q&A where our fantastic group members (that’s you!) can exchange insights, advice, and experiences.

Graham Butler will be speaking on the topic **“Cybersecurity in the Crossfire: The New Risks Facing Telecom Carriers and Digital Platforms"**.

In today’s interconnected digital world, telecom carriers and online platforms are facing unprecedented cyber threats, from data breaches to sophisticated DDoS attacks. This webinar delves into how these threats impact both sectors, examining shared vulnerabilities and how attackers exploit weaknesses across networks and platforms.

Join us as Graham shares cutting-edge strategies for securing infrastructures, mitigating risks, and fortifying defences in this evolving landscape. This session provides essential insights for staying resilient and ahead of cyber threats.

Graham Butler, the visionary Chairman and Founder of Bitek Global Ltd., is a pioneering expert in internet voice services, recognized for launching the world’s first international VOIP calling card service. With experience collaborating with over 60 telecom regulators and deploying anti-fraud systems globally, Graham brings unparalleled insight into the fight against telecom fraud and illegal SIM banks.

In this can’t-miss session, Graham will dive into pressing topics like cybercrime, large-scale fraud, botnets, and national security, offering unique perspectives on today’s top security challenges

We’d love for you to join us and be part of this enriching experience.
Joinhere: https://us02web.zoom.us/j/82661003308?pwd=nfCkOJbafCumv5Ra7vNfZbZsvFrY0K.1
Meeting ID: 826 6100 3308
Passcode: 614324

Looking forward to seeing you there!

Best regards,
Esther George
Zyber Global Community Team

Zyber Focus Article

Digital Shadows: Inside the High-Tech Crime Networks Operating Across Southeast Asia and Beyond

by Esther George and the Zyber Global Research Team

The recent UNODC report, Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking, and Technological Innovation: A Shifting Threat Landscape, sheds light on the rapid expansion of transnational organized crime (TOC) originating in Southeast Asia which has evolved into a sophisticated web of cyber-enabled fraud, underground banking, and technological innovation, making it increasingly challenging for law enforcement to counteract. Leveraging tools like artificial intelligence (AI), deepfake technology, and cryptocurrency, TOC groups are expanding their reach globally, affecting regions including South America, the Middle East, Europe, and Africa. The convergence of these elements has transformed Southeast Asia into a hub for global cybercrime, where digital infrastructure weaknesses and minimal regulatory oversight have allowed these criminal networks to flourish and expand operations across borders.

One of the main drivers of this TOC ecosystem is cyber-enabled fraud, which caused an estimated $18-$37 billion in losses across East and Southeast Asia in 2023, according to the United Nations Office on Drugs and Crime (UNODC). These criminal syndicates exploit unregulated online gambling platforms and cryptocurrency exchanges, along with underground banking channels, to launder illicit funds and bypass traditional financial monitoring systems. High-risk virtual asset service providers (VASPs) in areas like the Golden Triangle—a tri-border region between Thailand, Myanmar, and Laos—are particularly vulnerable due to limited oversight, enabling TOC groups to operate with little interference. Using these channels, TOC networks move funds globally, circumventing conventional financial systems and authorities, thereby complicating law enforcement efforts. The integration of cryptocurrencies in these activities presents an additional challenge, as it allows instant, anonymous transactions that are nearly impossible to trace.

TOC networks are also quick to adopt the latest technological innovations, from AI to deepfake technology, which they use to make their schemes more convincing and evade detection. The proliferation of encrypted messaging platforms, darknet marketplaces, and other privacy tools allows these criminals to operate invisibly, conducting international scams under the radar. AI-powered tools are now being used to automate social engineering tactics, generating personalized scripts for victims in multiple languages to increase success rates in phishing and fraud schemes. Generative AI and deepfake technology allow criminals to create hyper-realistic images or videos of non-existent people, which they use in scams like "pig butchering"—a scheme that builds intimate relationships with victims before soliciting investments.

According to UNODC, these advancements have lowered the technical barriers for cybercrime, enabling a broader range of criminal actors to engage in these lucrative schemes without needing deep technical expertise. The result is an informal yet thriving "criminal service economy" that is well beyond the reach of conventional law enforcement methods.

The UNODC's report emphasizes the global spread of Southeast Asian TOC activities, noting their increasing impact on South America, the Middle East, Europe, and Africa.

In South America, for instance, drug cartels are integrating cyber-enabled fraud and underground banking into their revenue streams. The Middle East, where traditional underground banking is already entrenched, has also seen an uptick in cybercrime linked to TOC networks. Europe and Africa are not immune, with cyber-enabled fraud schemes taking advantage of jurisdictional gaps and differing regulations across the continent...

Read more here: https://zyberglobal.com/blog?blogcategory=Article

Zyber News Roundup

Dutch cops pwn the Redline and Meta infostealers, leak 'VIP' aliases

Dutch police have announced the takedown of servers supporting the Redline and Meta info-stealers, two malware strains frequently used by cybercriminals to steal credentials and other sensitive data from compromised devices. Dubbed Operation Magnus, the international effort not only disrupted the malware's infrastructure but also enabled law enforcement to access critical data, such as usernames, passwords, IP addresses, and the source code of both malware strains, which could lead to further action against their users.

Read more:
https://www.theregister.com/2024/10/28/dutch_cops_pwn_the_redline/

Nationwide Telecommunications Provider and its CEO Plead Guilty to Massively Defrauding Federal Government Programs Meant to Aid the Needy

Issa Asad, CEO of Q Link Wireless, and his company pleaded guilty to defrauding federal programs by illegally claiming over $100 million from the FCC's Lifeline program, which provides discounted phone services to low-income consumers, and misusing Paycheck Protection Program (PPP) funds meant for COVID-19 relief. Asad admitted to tactics that misrepresented the number of active Q Link users, coerced customers into retaining unwanted services, and fabricated cellphone usage data to fraudulently claim government reimbursements...

Read more:
https://docs.fcc.gov/public/attachments/DOC-406639A1.pdf

How Interpol is adapting to the ever-evolving cybercrime landscape

Interpol, celebrating its centennial, continues its global mission of fighting crime in 196 countries, now increasingly focused on addressing cybercrime as technology and online threats evolve. Neal Jetton, head of Interpol's cybercrime unit, highlighted at the Global Cybersecurity Forum that cybercrime's transnational nature makes collaboration essential, as criminals exploit technological advances like AI and quantum computing to stay ahead. Interpol's approach includes building partnerships across sectors and focusing on regional operations, allowing tailored responses that improve global cybersecurity.

Read more:
https://www.csoonline.com/article/3587228/how-interpol-is-adapting-to-the-ever-evolving-cybercrime-landscape.html

Employees can become a cyber risk for companies

According to an international survey conducted by insurer Hiscox, cyberattacks on companies have continued to increase, with over two-thirds of 2,150 cybersecurity managers reporting a rise in incidents over the past year. Cyberattacks include tactics ranging from phishing emails and ransomware to fraudulent fund transfers, with the most common entry points being vulnerabilities in cloud server access. Alarmingly, nearly half (42%) of respondents view internal risks—such as employees, subcontractors, and business partners—as a major source of cyber threats, with incidents often fueled by "social engineering" techniques that manipulate employees into compromising company data.

Read more:
https://www.bluewin.ch/en/news/employees-can-become-a-cyber-risk-for-companies-2418832.html

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

SEE MORE >

The Security 500 Conference 2024 | November 18, 2024 | Washington D.C, United States

This event is designed to provide security executives, government officials and leaders of industry with vital information on how to elevate their programs while allowing attendees to share their strategies and solutions with other security industry executives.

The 17th annual SECURITY 500 Conference will unite high-level security executives and their direct reports. This one-day leadership conference is free to attend, and attendees are limited to security executives, senior management and their direct reports in both private and public sectors.

SEE MORE >

Global Cyber Conference 2024 (GCC) | November 26-27, 2024 | Zurich, Switzerland

The Global Cyber Conference (GCC) is a prominent international event in cybersecurity and privacy, uniting senior cybersecurity stakeholders, decision-makers, public authorities, and academia.

It serves as a vital networking and educational platform for influential leaders, allowing them to foster a collective comprehension of the measures necessary for enhancing cyber resilience.

SEE MORE >

Black Hat Middle East & Africa | November 26-28, 2024 | Riyadh, Saudi Arabia

Black Hat Middle East and Africa is a leading cybersecurity conference and exhibition held in Riyadh, KSA. The event brings together cybersecurity professionals, cutting-edge technologies, solution providers, and decision-makers from around the world, condensing several months of networking into just three days.

Zyber Global Online Events

Our Online Courses with INsig2
Sign up now at https://insig2-and-zyberglobal.learnworlds.com/

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

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.

CLICK HERE

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.

CLICK HERE