Zyber Global

FEBRUARY 2024 | ISSUE 43

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the February edition of Zyber Global Newsletter.

In January we held our first Zyber Global webinar of 2024, I hope that you were able to attend. Our speaker was the esteemed Marina Jovanovska, Chief Investigator for Cybercrime at the Investigative Center within the Basic Public Prosecutor's Office in Macedonia. Marina's presentation on "***Navigating the Digital Underworld***" provided a highly informative and engaging exploration of online frauds and identity theft.

Her expert knowledge in cybercrime was clearly demonstrated through her impressive articulation of complex concepts and practical strategies, making the intricate subject matter accessible and enlightening to the audience. Her insights offered a deeper understanding of current digital threats, making the session both invaluable and inspiring. My thanks to Marina as she truly made it a memorable and enlightening experience

As we majored on online frauds and identity theft in January, we thought that this month, the Zyber spotlight would shine on a topic of immense significance and timeliness: "***The Impact of Telecom Regulations on National Security.***" In our increasingly interconnected world, the importance of telecommunications in national security is paramount.

This month's featured article by Graham Butler, Chairman of Bitek Global Limited, delves into the complex relationship between evolving telecom regulations and national security. It provides expert analysis on how recent telecom policy changes are influencing the cybersecurity and national defence landscape, highlighting the crucial balance between technological progress, regulatory frameworks, and safeguarding citizens and state interests in the digital domain. As the world becomes increasingly interconnected, the role of telecommunications in safeguarding national security has never been more critical.

Finally, in April I will be speaking at the Insig2 Data Focus 2024 conference. The conference will take place on the 9th of April in Zagreb, Croatia. This is a great conference to attend, registration will open soon. Do arrange to attend and let's meet up at the conference.

Here's to staying informed and vigilant in the ever-evolving world of cyber security.

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! In the meantime, continue to keep safe!

This Month's Features

Zyber Focus Article
The Impact of Telecom Regulations on National Security by Graham Butler, Chairman, Bitek Global Limited.

Zyber News
A roundup of the latest international cybercrime news.

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

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

Zyber Focus Article

The Impact of Telecom Regulations on National Security

A *Personal Introspection* by the Chairman of Bitek Global Limited, Graham Butler (https://bitek.com)

In the last five years much has changed in the Telecoms world from the transition of the traditional voice to the Data based encrypted services. Some of the changes are for good and other areas are now creating increased challenges to Security services. The volumes of fraud and scams have defiantly increased; but the area I would like to focus on today is 'Why it is getting harder to identify bad actors'.

Over the top services (data-based services) apply to many things from communication services to Gambling and financial services. Today it is not difficult to acquire an IP address in another country without supplying details such as owner address, and most important location information, can you imagine, being able to acquire a telephone number but provide nothing for example, your name and address, so you could hide in plain sight. Almost every country where we have worked, less than 15% of IP addresses are registered.

So, as we move into all Data based services under 5G where the future of Voice will just be an application within data how will things change. Regretfully there are no signs that telecom regulators have fully understood the dynamic shift change that is happening. If you can recall a few years ago when telecom operators fought hard against services like Zoom /skype and WhatsApp whereas today they embrace them as the new oil improving their income levels despite the loss of now over 75% of their original long distance traffic incomes. Telecom carriers understood this shift change many years ago and removed old expensive class 5 switches and replaced them all with new modern data-based systems, regretfully leaving Governments and telecom regulators behind the curve in understanding or altering the way taxes are paid in country, leading to major trust issues between the parties. Many regulators for example created income for Governments through the sale of new licenses but it is so easy to deploy operations in another country today using secure encrypted technology that virtually no one buys licenses anymore.

Carriers have reacted to this by over charging the cost of data in most countries. to compensate them for losses caused by illegal or unlicensed operators. We are seeing some countries with 90% of the population online as their average rate of data equals $0.04 cents per gig (and they still make a profit) against other carriers where its over $6 USD per gig and the countries are struggling to get more than 20% of the population online. The impact of overpriced data dramatically effects the GDP growth and technology jobs in these overpriced countries.

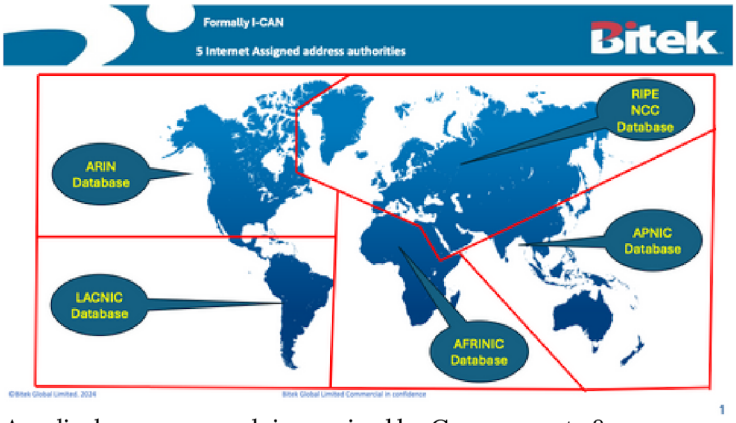
The solutions are easy, but major change is required; first a sweep of the entire country networks is required to identify who is operating unlicensed traffic or selling services in their country without paying taxes. So far, we have always found multiple illegals in every test we have undertaken, for example in a small Caribbean country we identified 373 Unlicensed operators, so border controls are now extremely critical.

The removal of old redundant voice taxes and replacing these with Data Taxes means each government can start to rebuild trust, while generating substantial new income through data Billing.

The problems are significantly worse with virtually all telecom operators using NATing through DNS servers where they strip out the IP address and replace this with their own IP address range That is like removing the telephone ID in a call so you cannot identify who is making the call, effectively providing total immunity to the sender as most of these operators are unable to advise what IP address initiated the fraud or scam. What is required, is the ability to define the Private IP address from the public one and in reverse Public back to private. Bitek has a solution for this: for regulators and/or security services.

In addition, there is no data on who owns a particular IP address (many do not have to verify name address and location of each IP address) some names if they are registered are false.

The system of registering IP addresses around the world is identified by ICAN and various other entities see chart below.



A radical new approach is required by Governments & Regulators to expand their understanding of data in their country review; clean up security and re-define the rules on licensing and make changes in the IP address control, and all this before more 5G becomes deployed.

Creating an IP address database for each country would substantially help not only the security services but also help to protect the carriers' income.

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

Zyber News Roundup

Deepfake Phishing: The Dangerous New Face of Cybercrime

Phishing, a decades-old hacking method, has evolved with technology, now employing deepfake phishing, which experts consider the most dangerous AI-fuelled cybercrime. This new tactic uses synthetic images, videos, or audio generated through deep learning to manipulate victims via sophisticated social engineering. Attackers utilize deepfakes in various forms, such as personalized emails, video calls, and voice messages.

Attackers now employ deepfakes in various formats, including personalized emails, video calls, and voice messages. These tactics, more advanced than traditional phishing, can convincingly impersonate CEOs on LinkedIn, use video deepfake on platforms like Zoom to extract confidential information, or clone voices for deceptive communication.

The threat of deepfake phishing is growing rapidly, with instances surging by 3,000% in 2023. AI's ability to mimic writing styles, clone voices accurately, and create lifelike AI-generated faces renders these phishing attacks hard to identify. As a result, deepfake phishing represents a significant and fast-evolving threat to organizations.

To combat this, organizations should focus on increasing employee awareness of synthetic content, training them to recognize and report deepfakes, and deploying robust authentication methods. Ultimately, fostering a culture of skepticism and intuition among employees is crucial to effectively counter this evolving cyber threat.

Read more:
https://www.forbes.com/sites/forbestechcouncil/2024/01/23/deepfake-phishing-the-dangerous-new-face-of-cybercrime/

$1.7 Billion Stolen in Cryptocurrency Hacks in 2023: Analysis

In 2023, cryptocurrency platform hacks led to the theft of $1.7 billion, a decrease from $3.7 billion in 2022 and $3.3 billion in 2021, despite an increase in incidents from 219 to 231, according to a Chainalysis report. The decrease in stolen funds is attributed to fewer successful attacks on decentralized financial systems (DeFi), with only $1.1 billion taken from DeFi protocols compared to $3.1 billion in 2022. Significant hacks in 2023 include Euler Finance, Mixin Network, and Poloniex Exchange, among others, while North Korea-linked hackers stole over $1 billion, less than in the previous year, despite an increase in their attack frequency.

Read more :
https://www.securityweek.com/1-7-billion-stolen-in-cryptocurrency-hacks-in-2023-report/

Global ransomware threat expected to rise with AI, NCSC warns

A new report by the National Cyber Security Centre (NCSC) warns that artificial intelligence (AI) will likely increase the volume and impact of cyber attacks, including ransomware, in the next two years. AI is expected to lower the entry barrier for novice cyber criminals, enhancing their capabilities in conducting more effective attacks and ransomware threats. To counter this, the UK government has invested in improving cyber resilience, with a focus on AI's role in cyber security and the implementation of protective measures.

The report also highlights the emergence of 'GenAI-as-a-service', increasing the accessibility of advanced cyber crime tools, and emphasizes the importance of effective preparation and cyber hygiene to prevent ransomware attacks.
The NCSC's report details how AI will influence various aspects of cyber operations, such as social engineering and malware, in the coming years.

Securing future technology against AI-enhanced cyber threats is a key focus for the NCSC, underscored by initiatives like the Bletchley Declaration for responsible AI development and the upcoming CYBERUK 2024 conference. The report and these initiatives emphasize the urgent need for organizations and individuals to strengthen their cyber defenses in an increasingly AI-driven threat landscape.

Read more:
https://www.ncsc.gov.uk/news/global-ransomware-threat-expected-to-rise-with-ai

'VexTrio' TDS: The Biggest Cybercrime Operation on the Web?

A traffic distribution system (TDS) operator named VexTrio, controlling over 70,000 domains, plays a crucial role in cybercrime by connecting threat actors with vulnerable websites to spread scams, phishing, and malware. While not directly conducting malicious campaigns, VexTrio's network is instrumental in redirecting internet traffic to compromised or malicious sites, often targeting specific profiles based on browser data. Infoblox's report identifies VexTrio as a significant and pervasive cyber threat, affecting more than half of the organizations monitored in the past two years, demonstrating its widespread impact on internet security.
VexTrio's operations are sophisticated and elusive, employing techniques like domain generation algorithms and multi-staged redirection chains to avoid detection, making it challenging for security companies to target them directly.

Read more:
https://www.darkreading.com/threat-intelligence/vextrio-tds-biggest-cybercrime-operation-web

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

Munich Cyber Security Conference **Chamber of Commerce Munich, Germany** **15 - 16 February 2024**	**Common Good Cyber Workshop** **National Press Club,** **Washington DC, USA** **27 – 28 February 2024**	**10th Annual Rail Cybersecurity UK & Europe Conference** **Copthorne Tara, Scarsdale Pl, London, UK** **27 – 28 February 2024**
Addressing top level managers and executives from the private and public sectors, the Munich Cyber Security Conference (MCSC) offers a unique space for exchanging and discussing solutions to the manifold challenges in information and cyber security. Focusing on the role and responsibility of decision-makers, the conference emphasizes effective strategies and agile management concepts to deal with the current threat landscape and also provides insight into the future evolution of cyber security policies. The Cyber Security Conference Series of the Security Network Munich attracts decision-makers from the private and public sector as well as influencers and policy makers from around the globe.	The workshop aims to initiate a crucial project focused on understanding and addressing a specific challenge, targeting immediate actions and long-term solutions like innovative funding models, by analyzing past approaches and prioritizing impactful strategies. It seeks to unite a diverse group of experts, stakeholders, and representatives from various sectors to foster collaboration, drive meaningful change, and secure a safer Internet for the future.	Protecting modern railway infrastructure from cyberattacks is imperative and in many cases overlooked or neglected in the push for digital transformation. To remain competitive organisations must adopt new technologies, processes and business models, all of which can deliver significant shareholder value, but are not without their share of cyber risk. The increase in supply chain and ransomware attacks across critical infrastructure and manufacturing industries has highlighted just how vulnerable our interconnected systems are and the transportation sector is no exception. How can we innovate securely? The 10th annual Cyber Senate Rail Cybersecurity UK and Europe conference will provide cyber security experts, product manufacturers and asset owners a unique forum to better define how we collaborate, harden security controls, share best practice and define our maturity in acting on intelligence.
For further information **https://mcsc.io/mcsc-2424/**	**For further information** **https://commongoodcyber.org/events/**	**For further information** **https://events.eventzilla.net/e/10th-annual-rail-cybersecurity-uk--europe-conference-2138616012**

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