Zyber Global

JUNE 2024 | ISSUE 47

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the June edition of Zyber Global Newsletter, the 47th edition! Stay Ahead with June's Most Exciting Cybersecurity Developments and Trends!"

I love the summer months in London, long days (its light to 9pm now) and short nights; if only the sun would shine more often, I would do staycations here rather than holidays abroad!

Recently, I received an intriguing email that appeared to be from the "China Intellectual Property Office." The message claimed they were managing Chinese brand and domain names and wanted to verify if I had authorised a company named "Megaa International Ltd" to register "zyberglobal" as their Chinese brand name. They urged me to either confirm this authorization or raise a dispute if it was unauthorized. The email was quite convincing, using official-sounding language and presenting a seemingly legitimate query.

However, I was already aware of this particular scam. The real objective of these scammers is to trick recipients into paying them to register domain names. This tactic is designed to create a sense of urgency and legitimacy, pushing you to act quickly without fully considering the request's authenticity. Fortunately, as I had prior knowledge about this scam, I did not fall for their ploy. This is a stark reminder that such scams continue, only because they occasionally find success, from preying on those unfamiliar with their tactics.

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Focus Article

PART 1- *Crisis management: Damage control during cybersecurity incidents in large business systems* by Damir Delija, Senior Lecturer, Digital Forensics and Cybersecurity, TVZ.

Zyber News

A roundup of the latest international cybercrime news.

Zyber Global Events Information

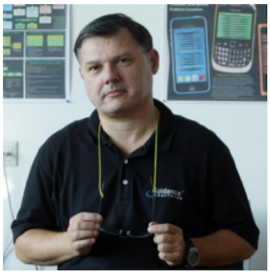
A focus on forums/conferences around the world.

This experience reinforces the importance of staying informed and vigilant, particularly when dealing with unsolicited requests related to intellectual property and domain registration.
Always verify the authenticity of such emails and consider seeking professional advice if you're unsure.

Remember to stay alert in cyber matters which means staying ahead of the threats and continuing to be informed about the latest trends in our ongoing cybersecurity adventures.

Zyber Focus Article

PART 1- Crisis management: Damage control during cybersecurity incidents in large business systems



by Damir Delija
Senior Lecturer, Digital Forensics and Cybersecurity, TVZ.

In a modern, digitally connected world, cybersecurity is key to protecting vital business operations. Effective management of cybersecurity incidents is essential not only to reduce immediate losses, but also to protect reputation and ensure the long-term sustainability of the enterprise. In order to control damage during cyber incidents, organizations need to focus on preparedness, rapid response and recovery strategies, taking into account complex contractual relationships and different legal regulations.

As cybersecurity refers to the practice of protecting systems, networks, and programs from digital attacks, we have to remember origins of the term, from a science of cybernetics, to understand its full meaning. Cybernetics is the interdisciplinary study of the structure, functions, and regulation of complex systems. It involves the understanding and application of feedback and control mechanisms in both biological and artificial systems. The term was coined by Norbert Wiener in the 1940s, deriving from the Greek word "*kybernetes*," which means "*steersman*" or "*governor*."

Creating a specialized incident response team, involving members from different departments with clearly defined roles and responsibilities, is critical to effective action. During a cyberattack, panic and miscalculations can cause adverse consequences, including overemphasized decisions and misfocusing resources, which can result in operational interruptions and a potential escalation of the incident. In this text, we try to put on paper some thoughts about the state of affairs in the light of recent wars, incidents and trends in the industry.

This text explores key crisis management strategies, highlighting the importance of an integrated approach that includes preparation, coordinated response and in-depth post-incident analysis. The necessity of specialized teams, the importance of clear communication channels and how legal and international regulatory frameworks affect incident management processes are considered. Also based on recent cases and industry trends, an insight into possible best-practice methods is provided.

The complexity of contractual relationships

Large corporations often depend on a range of external suppliers and partners, including those providing IT services, maintenance and security solutions. In the context of cybersecurity, contracts must clearly define the responsibilities and obligations of each party in the event of a security incident. The inclusion of clauses on safety standards, incident response protocols and mechanisms for mitigating harm is essential to reduce legal and operational risks. One of the inheretic but hardly visible problems is the meaning of clauses on maintenance and application in incident situations. Very often contracts do not recognize an incident but a malfunction that can significantly set back the resolution of the incident. It is important to understand that in such a situation, the technician who eliminates the "*malfunction*" acts in accordance with the Service Level Agreement (SLA), which aims to perform basic functions rather than identifying and controlling the incident, which can mean the destruction of digital artifacts and evidence.

Jurisdictional differences and international regulations

For international organizations, cyber incidents can simultaneously affect operations in multiple countries, each with its own data protection and cybersecurity laws. Managing these challenges requires an understanding of local legal frameworks and compliance with international standards such as General data Protection Regulation (GDPR) in Europe or California Consumer Privacy Act (CCPA) in California. Organizations need to develop strategies that are flexible and adaptable to different legal requirements. In such complex relationships, there are challenges in communication and coordination. Managing the response to a cyber incident in an international environment requires coordinated communication between various internal teams and external partners. Challenges include differences in time zones, language barriers and cultural differences in business.

Effective communication protocols and cooperation tools can help ensure that all parties communicate in a timely and clear manner during incident management. It must be understood that for an attacking company it is an open space, while for internal teams it is an complex structure of legal, economic and other constraints, where individual teams or parts of teams can even have conflicting interests. The famous "*blame-game*" and "*elephant-in-the-room*" situations are part of complex incident situations and one should be prepared to recognize them and prevent them as much as possible, since their consequences are often more devastating than the incident itself, and they should definitely be understood as part of the damage that the incident creates.

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

Look out for more insights on this in our July 2024 Newsletter. Stay connected!

Zyber News Roundup

EUK: BBC Pension Scheme Breached, Exposing Employee Data

The BBC has confirmed a breach of its pension scheme, exposing the personal data of over 25,000 current and former employees, including names, National Insurance numbers, dates of birth, and home addresses. The attackers copied files from a cloud-based storage device, though no phone numbers, email addresses, bank details, financial information, usernames, or passwords were compromised. The BBC has apologized for the breach and is taking it "extremely seriously," working with specialist teams to secure the source and implement additional security measures.

There is no evidence that the incident was a ransomware attack, and the data files involved were copies, not affecting the pension scheme's operations. The BBC warns impacted employees to be vigilant for unexpected communications requesting personal details. Cybersecurity experts caution that exposed personally identifiable information (PII) could be sold on dark web marketplaces, leading to fraud, identity theft, and spear phishing attacks. Impacted individuals are advised to monitor their bank and credit card accounts and consider using identity monitoring services. The BBC was also reportedly affected by the MOVEit zero-day vulnerability in 2023.

Read more:
https://chatgpt.com/c/53e58ce3-fa7c-4837-be2b-218d1876cb77

Advance Fee Fraud Targets Colleges With Free Piano Offers

A malicious email campaign using piano-themed messages has been targeting students, faculty at North American colleges, and various industries since January 2024 to perpetrate advance fee fraud (AFF) scams. Discovered by Proofpoint, the campaign has sent over 125,000 emails offering a free piano, directing respondents to a fake shipping company that demands delivery payments, and collecting personal information. Payments are accepted via Zelle, Cash App, PayPal, Apple Pay, and cryptocurrency.

A Bitcoin wallet linked to the scammers has processed over $900,000, suggesting multiple actors' involvement. Despite varied sender addresses, the scam emails have consistent content and use free email services. Proofpoint's investigation revealed part of the operation is based in Nigeria. These scams rely on social engineering and diverse payment methods, prompting Proofpoint to advise vigilance against unsolicited emails offering deals that seem too good to be true.

Read more:
https://www.infosecurity-magazine.com/news/aff-targets-colleges-free-piano/

Cybercrime study finds global human-initiated digital attack rate up 19%

The expanding scale of cybercriminal activity, particularly in e-commerce and North America, is highlighted in LexisNexis Risk Solutions' annual cybercrime report, "Confidence Among Chaos." Analyzing data from 92 billion transactions in 2023, the report reveals a 19% year-over-year increase in global human-initiated digital attacks, with significant spikes in North America's attack rate, surpassing that of Latin America. Although e-commerce transactions grew modestly by 7% due to economic factors, fraudsters' activity surged, with an 80% year-over-year increase in human-initiated attacks, particularly focusing on account takeovers.

Key findings include the dominance of third-party account takeover fraud, constituting 29% of reported fraud, and a 40% increase in human-initiated attacks to 1.3 billion. Remote scam centers in South-East Asia are identified as significant sources of fraud, and businesses face new challenges in combating bot attacks, which have evolved to mimic human behavior and evade detection. The report underscores the importance of advanced bot detection technologies and proactive measures to counteract sophisticated cybercriminal operations.

Read more:
https://chainstoreage.com/cybercrime-study-finds-global-human-initiated-digital-attack-rate-19

New PyPI Malware "Pytoileur" Steals Crypto and Evades Detection

Cybersecurity researchers have discovered "pytoileur," a malicious package on the Python Package Index (PyPI) that posed as an "API Management tool written in Python." This package contained hidden code that downloaded trojanized Windows binaries capable of surveillance, persistence, and cryptocurrency theft. Sonatype's automated malware detection systems flagged and removed the package, which had been downloaded 264 times, revealing it used deceptive metadata and extensive whitespaces to avoid detection, executing a base64-encoded payload to install the malicious "Runtime.exe" binary.

Further investigation indicated that pytoileur is part of a broader campaign involving multiple malicious PyPI packages, such as "gpt-requests" and "pyefflorer," using similar techniques to distribute trojanized binaries. This ongoing campaign employs tactics like base64 encoding to hide malicious payloads and targets user data and cryptocurrency assets through clipboard hijacking, keylogging, and remote webcam access. Sonatype notes that the reemergence of such malicious packages reflects threat actors' strategies to recycle old tactics and expand their target range across various developer niches.

Read more: https://www.infosecurity-magazine.com/news/pypi-malware-pytoileur-steals/

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

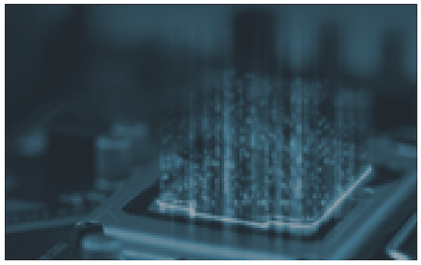
International Conference on CyberCrime and Computer Forensics (ICCCF) Adelaide, Australia. 12 – 14 June 2024	**Conference on Digital Trust, Digital Identity and Blockchain Edinburgh Napier University, Scotland 26 June 2024**	**Cyber Security Capacity Centre Oxford Martin School, University of Oxford, UK 30 April 2024**
Join us for The International Conference on CyberCrime and Computer Forensics (ICCC) is a key platform for discussing cybercrime and computer forensics. Australia's cybersecurity strategy emphasizes the need to curb cybercrime and enhance cyber resilience. The conference theme, "The future of geopolitical security - the cyber connections," explores the impact of emerging technologies like AI, quantum computing, and social media on cybercrime and geopolitical security, urging stakeholders to anticipate their future roles in these areas.	Our world is transforming from a legacy world into one which is built on digital methods. A core part of this must be the drive towards integrating privacy, digital trust and security into the design of these systems. Convened by Professor Bill Buchanan of our Edinburgh Napier Centre for Cybersecurity, IoT & Cyberphysical Systems, this conference will investigate areas of digital trust, digital identity and blockchain.	It is now 22 years since the European Conference on Cyber Warfare and Security (ECCWS) was established. It has been held in Greece, Ireland, Germany, Finland, Estonia, Portugal, to mention only a few of the countries which have hosted it. This conference attracts an interesting combination of academic scholars, military personnel, practitioners and individuals who are engaged in various aspects of the cyber security community. ECCWS is generally attended by participants from more than 30 countries. The Journal of Information Warfare regularly publishes a number of the papers presented at this conference.
For further information **https://www.icccf.org**	**For further information** **https://innovationhub.napier.ac.uk/news-and-events/events/conference-on-digital-trust-digital-identity-and-blockchain**	**For further information** **https://www.academic-conferences.org/conferences/eccws/** -

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