Zyber Global

AUGUST 2022 | ISSUE 25

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 25th Edition, August 2022 of Zyber Global Centre's monthly newsletter.

Summer is well and truly here and the UK has been through a heat wave to prove it!
I was lucky last month to spend a week working in Izmir, Turkey with the Council of Europe iProceeds - 2 project in cooperation with the USA Embassy in Croatia. It was a regional cybercrime exercise on a ransomware attack (the weather was hotter than in the UK but being in an air-conditioned hotel made the heat and sun enjoyable).
The iProceeds -2 project is aimed at targeting crime proceeds on the Internet and securing electronic evidence in South-East Europe and Turkey. The regional exercise went really well and as requested by some readers we will be doing an article on it soon.
Meanwhile, back at home, we have a summer of sport with the The Commonwealth Games 2022 which has just begun and is being held in Birmingham. Like everyone else I am looking forward to following the action online. The UEFA European Women's Championship recently concluded with England's success. This is the first major football tournament that England has won since 1966, so we will be celebrating this for some time to come! Well done to England's lionesses for their great achievement!
We continue with our usual features and ask that you continue to engage with us and let us know what topics on cybercrime you would like to hear more of. The next Stay Safe Online webinar is on the 3oth August 2022, so do register early. Stay well!

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Focus
This article is the last one on *'Cybercrime's effect on Critical National Infrastructure'.*

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

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

Izmir, Turkey

Zyber Focus Article

The Impact of Cyber-Crime on the Energy Sector

Arsha Gosine
Head of Research, ZGC

In the last article, we looked at the effect of cybercrime generally on the critical national infrastructure. In this article we are going to focus on the continuing and burgeoning effect that cybercrime has on the energy sector and the way forward for the United Kingdom (UK). From all reports it seems that the energy sector is facing a serious challenge from cyberattacks. In February this year, IBM brought out their 2022 X-Force Threat Intelligence Index which found that the energy sector accounted for 24 percent of cyber attacks followed by manufacturing and financial services which each received 19 percent respectively of attacks, increasing pressure on supply chain challenges and energy costs. The UK was one of the top three most attacked country (in Europe) in 2021, followed by Germany and Italy.

"*Cyber criminals worldwide are becoming increasingly resilient, resourceful, and stealthy in their pursuit of critical data*" said Laurance Dine, global partner, X-Force Incident Response at IBM.

These findings highlight an urgent need for 'cyber-resilience' in the energy sector as cyber-criminals will continue to seek out the vulnerabilities and weaknesses within organisations to disrupt key services primarily because it is a wealthy industry that is 'ripe for pickings' and perhaps there is the challenge of being able to bring down critical national infrastructure. Cyber-criminals are creative and inventive when it comes to exploiting and attacking networks and taking control remotely and holding to ransom.

So what is cyber-resilience? As we have seen, no cyber-security is fool-proof. Breaches for ransomware are becoming the norm. As a result, organisations are beginning to take a new approach to mitigating their cyber-risks. Ryan Weeks, CISO, Datto says that a traditional cyber-security strategy is no longer enough. Instead, organisations must shift from prevention to an 'assumed breach' mentality – operating as though a breach has already happened, and ensuring they can recover fast, with minimal damage to operations. Rather than relying on a protective layer of firewalls, anti-malware solutions and intrusion prevention, businesses increasingly understand the need to build cyber resilience beyond these first lines of defence. In addition to well-established cyber security practices, cyber resilience encompasses incident response, as well as business continuity and disaster recovery (BCDR). Incidents will almost certainly happen, and the focus is on keeping systems up and running during recovery, to speed up restoration, reduce downtime and minimise the overall impact of an attack.

"*Cyber resilience hinges primarily on people and processes. Technology investments come second, and they should be made based on the needs of people and processes, not vice versa*". Ryan Weeks, CISO, Datto.

As cyber-criminals continue to target the energy and other critical national infrastructure, I believe that companies can also benefit from sharing information within their sector and work together to thwart and help face active threats. The strength of the energy sector lies in working together. The European Energy Information Sharing & Analysis Centers (EE-ISACs) allow companies to share information without disclosing trade secrets. Sharing cyber-security information is a critical component in staying protected from these emerging threats. We saw this when other pipeline companies were not hit following the Colonial Pipeline breach signaling that perhaps information had been shared so the other companies could tighten their IT systems.

The UK government recently published its National Cyber Strategy and Government Cyber Security Strategy 2022-2030 (the Strategy), setting out measures to strengthen security of critical infrastructure. Additionally, amendments to the Network and Information Systems (NIS) regulations are being proposed, to improve the cyber resilience of UK businesses. The Government's latest Annual Cyber Sector Report showed a record investment in the cyber security sector last year, with revenues exceeding £10 billion.

The UK's National Cyber Strategy 2022 heralds a change in how the government views cyber security and sets its position as an international "cyber power". This term is used frequently throughout the strategy, and emphasizes the significant shift and wide approach in how the government views cyber space. There is also a focus on the "ability of a state to protect and promote its interests in and through cyber space" instead of just security.

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

Zyber News Roundup

Cyber-Criminal Offers 5.4m Twitter Users' Data

A database containing 5.4m Twitter users' data is reportedly for sale on a popular criminal forum. Twitter is investigating the issue, which the seller said exploited a vulnerability in its systems reported in January.

The seller, using the nickname 'devil,' advertised the data on the Breached Forums site and demanded at least $30,000 for it. They said that the database contains the phone numbers and email addresses of users, including celebrities and companies.

The hack reportedly exploits a vulnerability first reported by a HackerOne user known as 'zhirinovskiy.' That bug enabled "an attacker with a basic knowledge of scripting/coding" to find a Twitter user's phone number and email address, even if the user has hidden them in privacy settings. The attacker explained how to exploit the bug in their HackerOne report. Twitter acknowledged the bug and fixed it five days later.

The sale was first reported by RestorePrivacy, which has also downloaded and verified the dataset. Twitter told the publication that it is investigating the situation but provided no other information. Twitter users are unhappy that the company has apparently failed to notify them of the breach.

Read more: https://www.infosecurity-magazine.com/news/criminal-twitter-users-data/

Cyber hackers threaten Bedford school, demanding '£500k or else'

Hive Ransomware Group has hacked Wootton Upper School and threatened to post sensitive data unless the school pays out £500,000.

In a message to students and parents, the cyber hackers claim to have infiltrated Wootton networks a number of weeks ago and "managed to encrypt all of Wootton organisation servers", including Kimberley College.

The Hive Ransomware Group went on to say it had managed to exfiltrate sensitive data such as home addresses, bank details, medical records and students' psychological reviews – and plans to leak it UNLESS the school meets its ransom demands.

The post said: "*We are very well informed and precise in our operations, so we know that Wootton have cyber insurance that reaches £500k.*" And it added: "*If Wootton management decide to move on with their plan and refuse to negotiate, we are going to release all of the stolen data online for everyone to see. All of your child's private information will be online for everyone and for free*".

In a detailed post on the school website, executive principal Michael Gleeson, said: "*I can now confirm that the trust suffered a cyber incident and we are now in the process of putting in place a plan that will enable our IT system to be re-built. We are aiming to get everything back up and running as quickly as we can.*" Mr Gleeson also said as this type of incident has been linked to criminal groups, it has reported the breach to police as well as the Department for Education and the council.

Read more: https://www.bedfordtoday.co.uk/education/cyber-hackers-threaten-bedford-school-demanding-ps500k-or-else-3784035

European Police Arrest 100 Suspects in BEC Crackdown

European police have released details of two major operations against business email compromise (BEC) fraudsters, which resulted in the arrest of close to 100 suspects.

Operation Wine Cellar and Operation Theatre were carried out in November 2021 but are only now being made public due to operational reasons, Europol said. They were carried out by the Anti-Economic Crime Department of the Budapest Metropolitan Police with the support of Europol's European Financial and Economic Crime Centre.

The Budapest Metropolitan Police made the arrests after working its way through two complex fraud cases. They involved an organized crime group in the region which targeted state-owned companies with fake invoices.

The gang is said to have used a "sophisticated money laundering infrastructure" to obfuscate the flow of proceeds from these crimes and hamper investigator efforts to track it down.

Read more: https://www.infosecurity-magazine.com/news/european-police-100-suspects-bec/

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

Council of Europe (COE) and PILON Cybercrime Working Group webinar 'Cybercrime Legislation in the Pacific: Sharing Perspectives on Recent Progress': **5 August, 12-2pm Canberra time**	**International Conference on Cybercrime Investigation and Digital Forensics** **August 16-17, 2022** **Tokyo, Japan**	**11th International Workshop on Cyber Crime (IWCC 2022) held in conjunction with the 17th International Conference on Availability, Reliability and Security** **August 23 – August 26, 2022 in Vienna, Austria,**
The webinar will discuss recent progress in harmonising and updating legal frameworks on cybercrime and electronic evidence, in line with international standards (i.e., Budapest Convention) as a crucial milestone in equipping relevant authorities in the region to address cybercrime issues. The webinar will offer Pacific countries the opportunity to share the approach their country has taken, and discuss the merits of solutions to further strengthen the criminal justice response in the region. We are very pleased to announce that the webinar will feature presenters from Kiribati and Tonga, which are at different stages in the consideration and implementation of cybercrime legislation.	International Conference on Cybercrime Investigation and Digital Forensics aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Cybercrime Investigation and Digital Forensics. 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 Cybercrime Investigation and Digital Forensics.	Today's world's societies are becoming more and more dependent on online services – where commercial activities, business transactions and government services are realized. This tendency has been especially visible during the COVID-19 epidemy. This fact, as well as the recent Russia's aggression on Ukraine, have led to the fast development of new cyber threats and numerous information security issues which are exploited by cyber criminals. The inability to provide trusted secure services in contemporary computer network technologies has a tremendous socio-economic impact on global enterprises as well as individuals.
For further information: https://us06web.zoom.us/meeting/register/tZcof-yvqj4jGdLdoK28eI0v-2JfAeXKMoGh	For further information: https://waset.org/cybercrime-investigation-and-digital-forensics-conference-in-august-2022-in-tokyo	For further information: https://www.ares-conference.eu

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**

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