Zyber Global

SEPTEMBER 2022 | ISSUE 26

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 26th Edition, September 2022 of Zyber Global Centre's monthly newsletter.

I hope that you are all well and making the most of the last few weeks of summer. We are now in September and 2023 is just five months away!

I am sure we all started with high ideals for what we were going to achieve in 2022.

If you have not done so already, it's time to wheel out those new year resolutions you made. Which do you still have to achieve (and want to)? You can still do it! So, organise yourself, make that action plan and start achieving them.

My team and I are now working on our end of year goals so that we can end the year strong and ease gently into the new year.

2022 has so far been a year where the news has been full of conflicts and disasters happening all over the world. Our thoughts and prayers are with all who are suffering at this time.

The next Stay Safe Online webinar is on the 29 September 2022, so do register now to attend, see https://zyberglobal.com/webinars

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. Stay well!

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Focus

This month's article is on Ransomware: Cause & Effect.

Zyber News

We have a roundup of the latest international cybercrime news.

Zyber Global Events Information

A focus on forums/conferences around the world.

image courtesy Gabrielle_cc, Pixaby

Every great dream begins with a dreamer.
Always remember, you have within you
the strength,
the patience, and the passion
to reach for the stars to change the world.

Harriet Tubman, 1820-1913

Zyber Focus Article

Ransomware: Cause & Effect
by
Esther George, CEO- Zyber Global Centre

Like everyone else during the last two years I have been watching the dramatic rise in cybercrime as cybercriminals took advantage of the increasing number of people who due to the COVID-19 pandemic had to not only work remotely but were also increasingly socialising online as well. Amidst the fear and uncertainty cybercriminals flourished.

The history of ransomware attacks covers slightly over thirty years. As Group-IB states in their report Hi-Tech Crime Trends 2021/2022. Part II. “Corporansom: threat number one,” the first ancestor of the modern ransomware that cybersecurity analysts know today was spread using floppy disks and compact disks (CDs) in 1989 to extort money from users using social engineering techniques. The Trojan, however, could not encrypt data and its creators were unaware of monetization methods other than deception. Group-IB in their report attempted to figure out how the focus of the ransomware industry shifted from advanced targeted attacks to non-targeted affiliate malware distribution programs by looking into the history of how these services had developed.

The ransomware that we are dealing with today, is a far cry from the ransomware of thirty years ago. Ransomware has become a major threat, targeting businesses, government agencies, schools, and even individuals. Ransomware has now developed into a very profitable business with little prospect of being caught. The European Union Agency for Cybersecurity (ENISA) said there was a 150% rise in ransomware attacks between April 2020 and July 2021.

Ransomware attacks have many different appearances and come in all shapes and sizes. But what has really propelled ransomware into the spotlight and been the game changer is the establishment of an industry within the ransomware business, in which operators lease out or offer subscriptions of their malware creations to others for a price -- whether this is a per month deal or a cut of any successful extortion payments.

This is called Ransomware-as-a-Service (RaaS) and enables cybercriminals with low technical capabilities to carry out ransomware attacks. In this way the malware is made available to more buyers, which means lower risk and higher gains for the programmers of the software. Since 2020, we have seen a high increase in the average ransom payment demand.

With all this occurring it was therefore an opportune time for the Council of Europe iPROCEEDS -2 project in cooperation with the USA Embassy in Croatia to organise a regional cybercrime exercise on a ransomware attack.

The iPROCEEDS-2 project, is a joint initiative of the European Union and Council of Europe which aims to enhance the capacities of authorities in Southeast Europe and Turkey to fight organised crime, by strengthening their capabilities to search, seize and confiscate cybercrime proceeds, prevent money laundering on the Internet and to secure electronic evidence.

The regional cybercrime ransomware attack exercise was held in Turkey and there were around 40 delegates attending from 10 countries, they were cybercrime investigators, law enforcement, prosecutors, CERT experts and other digital forensic and electronic evidence experts. All delegates had attended several other relevant cybercrime training courses before the ransomware exercise which meant that they all had a good understanding of the subject.

The exercise involved the delegates having to work as a team to investigate ransomware attack and secure electronic evidence and digital forensics. The delegates used international and domestic cooperation regarding access to data, search, seizure, and confiscation of cybercrime proceeds. There were also practical exercises as part of the scenario covering other topics such as negotiation, blockchain and cryptocurrencies etc. It was a packed four days which resulted in very positive feedback on the training and great appreciation for its being so practical.

Image courtesy Gerd Altmann, Pixabay

In trainings such as this, you learn as much from your fellow trainers and delegates as you share. In conclusion I have set out seven of my learning points below:

1. There is an art to putting together the right team of people with the right skills and expertise that will be able to work effectively together to ensure that they can take a complex and difficult task (such as this) and in a short period of time put together a successful practical ransomware exercise. The operative word is team, and I will look at how to embody some of the lessons I learnt in building the Zyber Global team.

Read the full article including the seven learning points: https://zyberglobal.com/blog

Zyber News Roundup

NATO Investigates Dark Web Leak of Data Stolen from Missile Vendor

Documents allegedly belonging to an EU defense dealer include those relating to weapons used by Ukraine in its fight against Russia.

NATO is investigating the leak of data reportedly stolen from a European missile systems firm, which hackers have put up for sale on the Dark Web, according to a published report. The leaked data includes blueprints of weapons used by Ukraine in its current war with Russia.

Integrated defense company MBDA Missile Systems, headquartered in France, has acknowledged that data from its systems is a part of the cache being sold by threat actors on hacker forums after what appears to be a ransomware attack. Contradicting the cyberattackers' claims in their ads, nothing up for grabs is classified information, MBDA said. It added that the data was acquired from a compromised external hard drive, not the company's internal networks. NATO, meanwhile, is "assessing claims relating to data allegedly stolen from MBDA," a NATO official told Dark Reading on Monday. "We have no indication that any NATO network has been compromised," the official said.

MBDA acknowledged in early August that it was "the subject of a blackmail attempt by a criminal group that falsely claims to have hacked the company's information networks," in a post on its website. The company refused to pay the ransom and thus the data was leaked for sale online, according to the post.

MBDA reported $3.5 billion in revenue last year and counts NATO, the US military, and the UK Ministry of Defense among its customers.

The company is working with authorities in Italy, where the breach occurred.

Read more: https://www.darkreading.com/vulnerabilities-threats/nato-investigates-leak-of-data-stolen-from-missile-vendor

Student Loan Breach Exposes 2.5M Records

2.5 million people were affected, in a breach that could spell more trouble down the line.
EdFinancial and the Oklahoma Student Loan Authority (OSLA) are notifying over 2.5 million loanees that their personal data was exposed in a data breach. The target of the breach was Nelnet Servicing, the Lincoln, Neb.-based servicing system and web portal provider for OSLA and EdFinancial, according to a breach disclosure letter. Nelnet revealed the breach to affected loan recipients on July 21, 2022 via a letter.

"[Our] cybersecurity team took immediate action to secure the information system, block the suspicious activity, fix the issue, and launched[sic] an investigation with third-party forensic experts to determine the nature and scope of the activity," according to the letter.

By August 17th, the investigation determined that personal user information was accessed by an unauthorized party. That exposed information included names, home addresses, email addresses, phone numbers and social security numbers for a total of 2,501,324 student loan account holders. Users' financial information was not exposed.

According to a breach disclosure filing submitted by Nelnet's general counsel, Bill Munn, to the state of Maine the breach occurred sometime between June 1, 2022 and July 22, 2022. However, a letter to affected customers pinpoints the breach to July 21. The breach was discovered on August 17, 2022.
It's unclear what the vulnerability was.

Read more: https://threatpost.com/student-loan-breach-exposes-2-5m-records/180492

Block Faces Class Action Suit After 2021 Breach

Payments giant Block is being taken to court by former customers who claim its negligence led to an insider stealing their personal information last year.

A December 2021 breach at the firm's subsidiary Cash App enabled a former employee at the firm to steal the personal information of over eight million customers.

Lawyers for two of those victims filed a class action lawsuit in the Northern District of California. They're alleging that Block "failed to maintain reasonable and adequate data security measures to safeguard customers' private information," which ultimately enabled the unauthorized insider access.

The plaintiffs are also arguing that the four-month delay between the breach and Block's notification to the Securities and Exchange Commission (SEC) was unreasonably long, and that when it came, "the defendant's notice of the data breach was not just untimely but woefully deficient." The complaint cites the California Customer Records Act, Texas Deceptive Trade Practices Act and other laws which it is claimed Block has broken.

The lawsuit was filed in a week when Block founder Jack Dorsey's other business, Twitter, came under intense scrutiny after a whistleblower disclosure from its former head of security was made public. There is some crossover between the cases, notably allegations that access policies for insiders were too lax at both firms.

Read more:
https://www.infosecuritymagazine.com/news/block-faces-class-action-suit/

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

Cybercrime & Technical Investigations Training Conference (CYCON) **September 14-16, 2022 i** **Glynco, Georgia**	**International Conference on Cyberterrorism, Cyberthreats and Cybercrime** **September 22-23, 2022** **London, United Kingdom**	**1st Annual** **e-Crime & Cybersecurity Congress Switzerland** **28th September 2022** **Courtyard by Marriott Zurich North**
The Federal Law Enforcement Training Centers (FLETC) Glynco, Georgia cordially invites you to attend the fourth Cybercrime & Technical Investigations Training Conference (CYCON-2022), scheduled to run between September 14th – 16th, 2022, at FLETC in Glynco, Georgia. Our goal is to foster education and awareness of current threats and innovations, which impact how law enforcement investigates cybercrime and how they conduct technical investigations. During this year's event, we will discuss how FLETC is streamlining its Cyber training to better meet the needs of law enforcement in the current operating environment. Attendees will experience exhibits, lectures, demonstrations, and hands-on labs. Although CYCON 2020 was a virtual event, CYCON-2022 will be conducted in-person.	Cyberterrorism, Cyberthreats and Cybercrime Conference aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Cyberterrorism, Cyberthreats and Cybercrime Conference. 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 Cyberterrorism, Cyberthreats and Cybercrime Conference.	Securing critical business sectors - Finance, healthcare, infrastructure and local government are all key targets: are they doing enough? Switzerland, arguably, came late to cybersecurity. It was only in 2019 that the Federal Council created the NCSC, which is part of the FDF General Secretariat. But more recently, the growing significance of cybersecurity to the country and core sectors such as finance has become clear. This year, the Federal Council is looking to reinforce and restructure the NCSC and turn it into a Federal Cybersecurity Office. In addition, the government has just announced the establishment of a financial sector cybersecurity association, aimed at increasing the cyber resilience of the country's financial sector. The drivers of these changes are clear: Switzerland is increasingly a target for cyberattacks.
For further information https://www.fletc.gov/cybercrime-technical-investigations-training-conference-cyco	For further information: https://waset.org/cyberterrorism-cyberthreats-and-cybercrime-conference-in-september-2023-in-london	For further information: https://akjassociates.com/event/switzerland

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