Zyber Global

MARCH 2023 | ISSUE 32

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to Zyber Global Centre's monthly newsletter - March 2023, the 32nd edition!

Like everyone else, I was saddened and shocked at the death and destructions that the earthquakes that affected Turkey and Syria. Over the last few years, I have been doing a lot of work with colleagues in Turkey and have made some good friends. My prayers and thoughts are with all of those affected.

March is usually the start of spring here, unfortunately no-one has told the weather as it is freezing cold now.

I am looking forward this month to speaking at the DataFocus conference in Zagreb, Croatia on the 21 March 2023. This is the first DataFocus to be held since Covid, let me know if you are planning to attend, it will be great to meet you in person rather than just online.

I was recently interviewed on my views on cybercrime by Frits Bussemaker of the "Institute of Accountability in the Digital Age" and towards the end of the interview I spoke about my new project the Zyber Global Community. You can listen to that interview here: https://i4ada.org/dialogues/esther-george-zyber-global-centre/

The next Stay Safe Online webinar is on the 27 April 2023, so do register early. Spaces are limited!
See: https://zyberglobal.com/webinars

As always, do let us know what topics you would like to see discussed in the April 2023 newsletter. Stay safe!

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Focus Article
This month's article focuses on a 'cyber apocalypse 2023' and highlights from the World Economic Forum, Global Cybersecurity Outlook 2023 Insight Report.

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

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

"Awareness and preparations will help organisations balance the value of new technology against the cyber risk that goes with it. "

World Economic Forum
Global Cybersecurity Outlook 2023
Insight Report
January 2023

Zyber Focus Article

Are we heading for a Cyber Apocalypse?

Arsha Gosine
Head of Research, Zyber Global Centre

It is with great interest that in my research I came across this Forbes Article written by Bernard Marr, entitled '***Cyber Apocalypse 2023: Is the World Heading for a Catastrophic Event?***'

Mr. Marr pointed out that at the World Economic Forum ('the Forum') wrapped up in Davos, Switzerland, Jeremy Jurgens, Managing Director & Head of the Forum's Centre for the Fourth Industrial Revolution while delivering a presentation on the 2023 Global Cybersecurity Outlook report (the report) revealed that 93 percent of those surveyed believe that a 'catastrophic' cyber security event is likely in the next two years. The main reason for this is likely to be constant and more targeted cyberactivity towards businesses and governments as well as increased technology with minimal safeguards and of course let us not forget that it is so easy to purchase the latest hacking software on the dark net.

There is also the projection by the Forum that by 2025 cybercrime will cost the world economy around $10.5 trillion annually, increasing from $3 trillion in 2015. Mr. Marr suggests that it is likely that much of the forecasted $10 trillion in economic damage will be caused by smaller attacks, simply aimed at stealing or extorting money from businesses or individuals.

Mr. Marr pointed out some key points at the Forum namely that the very nature of cybercrime is becoming increasingly unpredictable which is primarily due to technology becoming more and more complex especially with breakthrough technologies such as artificial intelligence (AI).
According to the report, one of the biggest threats is a "mutating" threat. This could take the form of an AI-enabled virus that transforms as it infects various systems and organizations to evade defence systems or even detection.

The Prime Minister of Albania, Edi Rama, whose country suffered an attack that brought down critical infrastructure in 2022, spoke about what he has learned since:
"*It's about viruses that can not only block our way of living but can control it and deviate it. So, it can use our systems like, God forbid, our air transport systems to hit us back. Imagine if there is a cyberattack on our air transport systems that turn a huge number of airplanes that are flying into bombs*".

"*What we learned is that this is something that's absolutely naive to think that … any country can tackle this on its own.*"

Another example was given of a truly devastating cyberattack which was an attempt by Russian-linked groups to hack infrastructure in Ukraine following the 2014 invasion of Crimea, which left 230,000 homes without power. In the run-up to the 2022 invasion, 288,000 attempted cyberattacks were detected against Ukrainian businesses and government infrastructure.

At the Forum, Interpol Secretary-General Jurgen Stock spoke about a 2022 operation by his organization against the west-African cybercrime group Black Axe that recently led to the arrest of 70 individuals. Groups like it are made up of professional hackers, fraudsters, scammers, and money-launderers who have become increasingly proficient at credit card fraud, extortion, identity theft, and ransomware attacks.

So, let us look at some of the key findings of the 2023 Global Cybersecurity Outlook report (the report):
The character of cyberthreats has changed dramatically. Respondents now believe that cyber-attackers are more likely to focus on business disruption and reputational damage. These are the top two concerns among respondents.
– Global geopolitical instability has helped to close the perception gap between business and cyber leaders' views on the importance of cyber-risk management, with 91% of all respondents believing that a far-reaching, catastrophic cyber event is at least somewhat likely in the next two years.
– Following from this, 43% of organizational leaders think it is likely that in the next two years, a cyberattack will materially affect their own organization. This, in turn, means that in many cases, enterprises are devoting more resources to day-to-day defences than strategic investment.
– The data protection and cybersecurity concerns created by geopolitical fragmentation are increasingly influencing how businesses operate and the countries in which they invest.
– Cyber talent recruitment and retention continues to be a key challenge for managing cyber resilience. A broad solution to increase the supply of cyber professionals is to expand and promote inclusion and diversity efforts. In addition, understanding the broad spectrum of skills needed today can help organizations to expand their hiring pools. A number of promising initiatives are already in place, but these tend to focus on small cohorts. Time, thought and investment are needed to make cyber-skills development programmes scalable.

Read the full article: https://zyberglobal.com/blog

Zyber News Roundup

GoDaddy suffered a huge hack that saw criminals steal source code and install malware

An unknown threat actor was sitting in GoDaddy's systems for several years, installing malware, stealing source code, and attacking the company's customers, the web hosting giant has confirmed.

The attackers breached GoDaddy's cPanel shared hosting environment and used that as a launch pad for further attacks. The company described the hackers as a "sophisticated threat actor group". The group was eventually spotted in late 2022 when customers started reporting that traffic coming to their websites was being redirected elsewhere.

GoDaddy now believes that the data breaches that were reported in March 2020 and November 2021 were all linked and part of a multi-year campaign by a sophisticated threat actor group that, among other things, installed malware on their systems and obtained pieces of code related to some services within GoDaddy,"

During the November 2021 incident, the user data of some 1.2 million of its customers were accessed by the attackers. This included both active and inactive users, with email addresses and customer numbers being exposed.

In a statement published in February 2023, the web hosting giant claims to have employed an external cybersecurity forensics team, and brought in law enforcement agencies from all over the world to investigate the matter further.

Read more:
https://www.techradar.com/news/godaddy-suffered-a-data-breach-over-three-years

Royal Mail Hung Tough in LockBit Ransom Negotiations

Negotiators for the Royal Mail apparently played hardball with LockBit over a ransom demand that the mail service said was too high, prompting the attackers to lower their ask and reset the ransom deadline. Insights into how ransoms are negotiated are few and far between, but the leaked transcript of chat logs showed the tactics taken by the UK's National Cyber Security Centre (NCSC) and National Crime Agency (NCA).

"*Under no circumstances will we pay you the absurd amount of money you have demanded*," an unidentified Royal Mail negotiator said, according to a Techcrunch report, which showed screenshots of a transcript posted by LockBit. "*We have repeatedly tried to explain to you we are not the large entity you have assumed we are, but rather a smaller subsidiary without the resources you think we have. But you continue to refuse to listen to us. This is an amount that could never be taken seriously by our board.*"

"*The fact that these cybercriminal gangs operate using business models borrowed from the legitimate business world shows how sophisticated they've become*," said Mike Parkin, senior technical engineer at Vulcan Cyber.

The January attack compromised Royal Mail's ability to deliver some items internationally and came with a hefty ransom of around $80 million, or what the attackers calculated was 0.5% of Royal Mail's annual revenue. After the mail service spurned the initial demand, the miscreants lowered the ransom to $70 million. Although much of the disruption has been resolved, Royal Mail is still suffering the effects of the attack.

Darren Guccione, CEO and cofounder at Keeper Security. "It's *also important to note that in many cases, the payment of a ransom doesn't guarantee the cybercriminal will decrypt a victim's files or reinstate access to their systems. They are criminals and, as such, they cannot be trusted.*"

Read more:
https://securityboulevard.com/2023/02/royal-mail-hung-tough-in-lockbit-ransom-negotiations/

European & American Hackers Attack China

Chinese cyber security experts say that a hacking group, which draws its principal members from Europe and North America, has been launching cyber attacks against China, posing a serious threat to China's national cyber security.

The hacking group, which has been named Against The West (ATW), is claimed by Chinese sources to have exposed sensitive information, including source code and databases of critical information systems related to China. Since last year, ATW has intensified large-scale intrusion, detection and supply chain attacks on Chinese networks.

China has itself been launching cyber attacks on both its allies and competitors. In 2022 Chinese state-sponsored hacking group successfully compromised the computer networks of at least six US state governments. These hacking attacks have been going on for some time by different countries against others.

Read more:
https://www.cybersecurityintelligence.com/blog/european-and-us-hackers-attack-china-6798.html

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

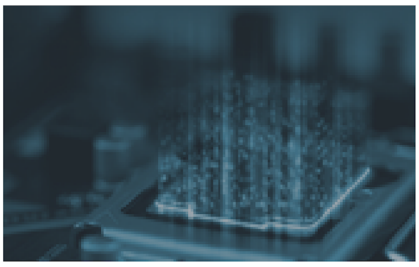
18th International Conference on Cyber Warfare and Security **Hybrid: Towson, Baltimore County, Maryland, USA** **9 - 10 March 2023**	**International Conference on Cyberlaw and Cybersecurity ICCC** **London, United Kingdom** **16 – 17 March 2023**	**DataFocus 2023** **Hilton Garden Inn, Zagreb, Croatia** **21 March 2023**
We are pleased to invite you to participate in the 18th International Conference on Cyber Warfare and Security (ICCWS) to be held on 9-10 March 2023 at the Towson University, Baltimore County, Maryland, USA. This conference goes to the heart of all matters relating to cybersecurity. It will bring together distinguished cybersecurity researchers and practitioners worldwide to explore innovative solutions in addressing complex cybersecurity problems.	International Conference on Cyberlaw and Cybersecurity aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Cyberlaw and Cybersecurity. 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 Cyberlaw and Cybersecurity.	DataFocus is an international conference, that has been successfully organized by INsig2, every year since 2012, and attended by more than 200 participants each year, from the whole world. DataFocus is all about exchanging experiences. We bring together law enforcement investigators, prosecutors, judges, court expert witnesses and let them talk about their experiences with digital evidence and digital forensic investigations. DataFocus will be held under the sponsorship of Croatian Minister of Interior, Mr. Davor Bozinovic who will open the conference with an introductory speech. The conference will feature a variety of keynote speakers, panel discussions, exhibitors, and workshops. Attendees will have the opportunity to learn from industry leaders, network with their peers, and gain valuable insights into the latest trends and technologies in the field. **Admission is free of charge for all the attendees.**
For further information **https://www.academic-conferences.org/conferences/iccws/**	**For further information** **https://waset.org/cyberlaw-and-cybersecurity-conference-in-march-2023-in-london**	**For further information** **https://insig2.com/en/conference/datafocus-2023**

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