Zyber Global

FEBRUARY 2023 | ISSUE 31

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to Zyber Global Centre's monthly newsletter - February 2023, the 31st edition!

As I keep saying, February is one of my favourite months, it's when I start to believe that the dark nights of winter will soon be a thing of the past. It's when I start to experience it getting lighter in the evenings and I rejoice knowing that spring will soon be with us. It's still quite cold in London, if only the weather would be just a little warmer, I would be really overjoyed but I guess that you can't have everything.

I was glad to hear that the 'DataFocus Conference' is being held this year.

DataFocus is an international conference, that is organized by INsig2. They bring together law enforcement investigators, prosecutors, judges, court expert witnesses etc where they share their experiences with digital evidence and digital forensic investigations. I used to attend the DataFocus conference pre Covid and really enjoyed them, so I will make an effort to attend this year.

DataFocus 2023 will be held at the Hilton Garden Inn hotel in Zagreb, on Tuesday, March 21st 2023, under the sponsorship of the Croatian Minister of Interior, Mr. Davor Božinović.

DataFocus is free to attend, so register now at: https://insig2.com/en/conference/datafocus-2023

The next Stay Safe Online webinar is on the 28 February 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 March 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 is a round-up of Cybercrime highlights last year and what to expect in 2023.

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

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

""As we enter 2023, it's important that organizations not relegate cybersecurity to the back burner. Threat actors are opportunistic and thrive in times of uncertainty. Perhaps the most important step any organization can take in 2023 is fostering a culture of awareness and establishing a security foundation. If they focus on doing these two things, they will be much better prepared for the new year and beyond"
Stu Sjouwerman
Forbes Councils Member
Forbes Technology Council

Zyber Focus Article

Cybercrime Trends: Looking Backwards Looking Forwards

Arsha Gosine
Head of Research, Zyber Global Centre

Year on year there continues to be an increase in cybercrime and cybersecurity attacks. It is certain that this year will be no exception as cyber criminals seek new and sophisticated opportunities to exploit online services worldwide while law enforcement use creative means to catch them.

Let us look at some of the cyber-attacks that took place last year. Bob Carver, CISM, CISSP, M.S. provides a sample of cybercrimes/attacks in 2022:

·Ukraine was the target of wiper malware from Russia, which interrupted any cyber system which could have been useful to the Ukraine government and the war effort.

·The Lapsus$ group started their phishing campaigns and hacking spree in early 2022 where they stole from Samsung, Ubisoft, Microsoft, Nvidia and eventually Okta.

·In November 2022, the island nation of Vanuatu was hit by a cyberattack that took much of the country offline causing all government agencies to work with pen and paper. In addition, Costa Rica, Albania and Montenegro suffered similar damaging cyberattacks.

·Ransomware groups continued unabated, especially hitting national agencies and infrastructure, schools, healthcare organizations, and private companies around the world. Ransomware as a Service (RaaS) continued to be a popular way to enter the cybercrime business with no coding skills and limited funds.

·One of the largest cybersecurity insurers in the world, Lloyds of London, announced that they would no longer pay claims that were caused by Nation States stating that they fell under the Force Majeure clause, events that were beyond anyone's control. Shortly after, Lloyds was breached.

·Twitter had much of their personal account information stolen due to an API vulnerability. Then there were outages and posts from fringe hate groups getting a free pass.

·Finally, last but not least, Lastpass, a popular password manager got breached. It was first reported that this breach only involved a development environment; however, it was later discovered that entire password caches were stolen from many of their customers.

So, we can conclude that 2022 was a hive of activity in many areas. Hopefully lessons were learnt and companies and governments invested in cyber-security and shored up their infrastructure in relation to this

Let us look briefly at some of the 2023 predictions.

1. **Crypto Scams and 'Pig Butchering'** - Using translation programs to communicate with global victims, scammers looking for a payout launch what authorities call "pig butchering" scams. They'll message someone's phone, dating app or WhatsApp with a "Hey, are we still on for lunch Friday?" The goal is to see if they can get a response and then build an online friendship. Eventually, they'll ask if the victim knows anything about crypto to lure them onto a sham website where the fraudsters say a friend made a lot of money. If the victim invests, they'll see rapid returns that lure them into pouring in more money. The scammers are basically "fattening the pig" until it's time to butcher it—when they take all the money out of the account.

2. **Theft of Digital Likeness** - With the rapid development of "deep fake" environments, there will be markets for "digital likeness" of various people including celebrities, executives, politicians and the like. With access to the voices, mannerisms and 3D profiles of these people, deep fakes will become better than ever (Bob Carver, CISM, CISSP, M.S. writing on Linked In).

Stu Sjouwerman (the founder and CEO of KnowBe4 Inc., a security awareness training and simulated phishing platform, and is also a member of Forbes) said that the rise of deepfakes (synthetically manipulated audio, video and images) as a tool to build a layer of trust into scams and social engineering attacks will increase exponentially. The maturity level of deepfakes technology is convincing enough to trick most unsuspecting people ....

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

Courtesy Rosy, Pixaby

Zyber News Roundup

Morocco hands America one of its most wanted cybercriminals - Sebastien Raoult

French cybercriminal Sebastien Raoult was extradited from Morocco to the United States on January 25, as a result of a procedure set up as part of the bilateral agreements between the two nations for criminal justice system cooperation.

According to US law, the 22 years old Sebastien Raoult could receive a maximum sentence of potentially over 116 years in jail for his crimes. He was first arrested on June 1 at the Rabat international airport, while trying to board a flight to Brussels, Belgium. His arrest followed an Interpol red notice issued against him by a Washington State prosecutor, where the US demands his extradition for cyber criminality and cyber fraud.

He is being placed under arrest for offenses involving impersonation, cyber fraud, and involvement in the "Shiny Hunter" criminal network, which the US government claims are responsible for coordinated information attacks on numerous foreign businesses and contractors.

Read more:
https://en.hespress.com/57573-morocco-hands-america-one-of-its-most-wanted-cybercriminals-sebastien-raoult.html

GoTo admits: Customer cloud backups stolen together with decryption key

GoTo is a well-known brand that owns a range of products, including technologies for teleconferencing and webinars, remote access, and password management.

If you've ever used GoTo Webinar (online meetings and seminars), GoToMyPC (connect and control someone else's computer for management and support), or LastPass (a password management service), you've used a product from the GoTo stable.

You've probably not forgotten the big cybersecurity story over the 2022 Christmas holiday season, when LastPass admitted that it had suffered a breach that was much more serious than it had first thought. Now, unfortunately, it's parent company GoTo's turn to admit to a breach of its own – and this one also involves a development network break-in.

On 2022-11-30, GoTo informed customers that it had suffered "a security incident", summarising the situation as follows:
Based on the investigation to date, we have detected unusual activity within our development environment and third-party cloud storage service. The third-party cloud storage service is currently shared by both GoTo and its affiliate, LastPass.

Two months later, GoTo has come back with an update, and the news isn't great:
[A] threat actor exfiltrated encrypted backups from a third-party cloud storage service related to the following products: Central, Pro, join.me, Hamachi, and RemotelyAnywhere. We also have evidence that a threat actor exfiltrated an encryption key for a portion of the encrypted backups. The affected information, which varies by product, may include account usernames, salted and hashed passwords, a portion of Multi-Factor Authentication (MFA) settings, as well as some product settings and licensing information.

The company also noted that although MFA settings for some Rescue and GoToMyPC customers were stolen, their encrypted databases were not.
Read more:
https://nakedsecurity.sophos.com/2023/01/25/goto-admits-customer-cloud-backups-stolen-together-with-decryption-key/

Most Federal Agencies Ignored GAO's Cybersecurity Recommendations

Nearly 60% of the cybersecurity recommendations made by the US Government Accountability Office (GAO) since 2010 have yet to be implemented by federal agencies.
The Office unveiled the figures in a release last Thursday, adding that out of 335 public recommendations, 190 still needed to be implemented. "*Until these are fully implemented, federal agencies will be more limited in their ability to protect private and sensitive data entrusted to them,*" GAO wrote.
According to the Office, the September 2018 National Cyber Strategy and the National Security Council's accompanying June 2019 Implementation Plan released by the White House addressed some of the characteristics of national strategies but not all of them.

Specifically, GAO explained that purpose, scope and methodologies processes were implemented alongside organizational roles, responsibilities and coordination operations. Integration and implementation efforts had also been acknowledged.

Read more: **https://www.infosecurity-magazine.com/news/federal-agencies-ignore-gaos/**

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

Cybersecurity Standardisation Conference 2023 Hybrid: Renaissance Brussels Hotel / Virtual 7 February 2023	**International Conference on Cyberlaw, Cybercrime and Cybersecurity Barcelona, Spain 16 – 17 February 2023**	**International Conference on Cybersecurity and Cyber Threats Buenos Aires, Argentina 20 - 21 February 2023**
The European Standardisation Organisations CEN, CENELEC and ETSI, are pleased to join forces with ENISA, the EU Agency for Cybersecurity, to organise the 7th Cybersecurity Standardisation Conference 'European Standardisation in support of the EU Legislation' The 2023 programme of this well-recognized conference will have dedicated sessions on standardisation activities in the areas related to the emerging EU legislation: • Proposed Cyber Resilience Act • Reviewed eIDAS Regulation • RED Directive, proposed EU Chips Act, Data Act, AI Act and others.	International Conference on Cyberlaw, Cybercrime 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, Cybercrime 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, Cybercrime and Cybersecurity.	This International Conference on Cybersecurity and Cyber Threats aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Cybersecurity and Cyber Threats. 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 Cybersecurity and Cyber Threats.
For further information https://www.enisa.europa.eu/events/cybersecurity_standardisation_2023	**For further information https://waset.org/cyberlaw-cybercrime-and-cybersecurity-conference-in-february-2023-in-barcelona**	**For further information https://waset.org/cybersecurity-and-cyber-threats-conference-in-february-2023-in-buenos-aires**

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