Zyber Global

MAY 2024 | ISSUE 46

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the May edition of Zyber Global Newsletter, the 46th edition! Explore the latest electrifying updates from the world of cybersecurity with our April adventures!

This past April, I was thrilled to participate in the esteemed Insig2 Data Focus 2024 Conference, held in picturesque Zagreb, Croatia. The conference kicked off with riveting speeches from luminaries such as Goran Oparnica, Director of Insig2; Davor Božinović, PhD, Minister of the Interior; and Darko Klier, Deputy Chief State Attorney of Croatia. Speaking on "*AI in the Courtroom*," I emphasized the urgent need for AI legislation and its burgeoning impact on the criminal justice system; urging immediate action to prevent potential injustices. A heartfelt thanks to Insig2 for their outstanding hospitality and for fostering a dynamic platform to explore AI's future in legal frameworks—an incredibly enriching experience!

The adventure continued with a visit to Maribor, Slovenia, a mere two-hour drive from Zagreb. There, I met with Prof. Dr. Ludvik Toplak, President of Alma Mater Europaea. Our discussions on educational and academic innovations were profoundly enlightening, showcasing Alma Mater Europaea's dedication to excellence and innovation.

April also marked the launch of #operationshamrock, a ground-breaking virtual gathering aimed at combatting the global threat of pig butchering. This unprecedented assembly brought together a diverse mix of stakeholders—from social media giants and telecom firms to banking sectors, cryptocurrency exchanges, blockchain analysts, non-profits, academics, and law enforcement at all levels. Spearheaded by Erin West, a US Assistant District Attorney, the meeting was a vibrant brainstorming session on thwarting this pervasive crime. Join the movement on LinkedIn at #operationshamrock.

The month concluded with the 10th Anniversary Annual Conference of the Global Cyber Security Capacity Centre (GCSCC) titled "Cybersecurity Capacity Priorities for Emerging Futures and Systemic Risks," held in Oxford, England. Returning to the GCSCC, which I saw launch over a decade ago with UK government backing, was profoundly rewarding. The conference offered fresh insights into major cybersecurity advancements and provided a delightful opportunity to reconnect with old colleagues, and to forge new connections in this ever-evolving field.

Remember to stay vigilant and informed as we continue to navigate the ever-evolving landscape of cybersecurity.

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Focus Article

Who's in the Crosshairs? Unveiling Cybercrime's Favourite Targets - Arsha Gosine, Head of Research, ZGC.

Zyber News

A roundup of the latest international cybercrime news.

Zyber Global Events Information

A focus on forums/conferences around the world.

Zyber Focus Article

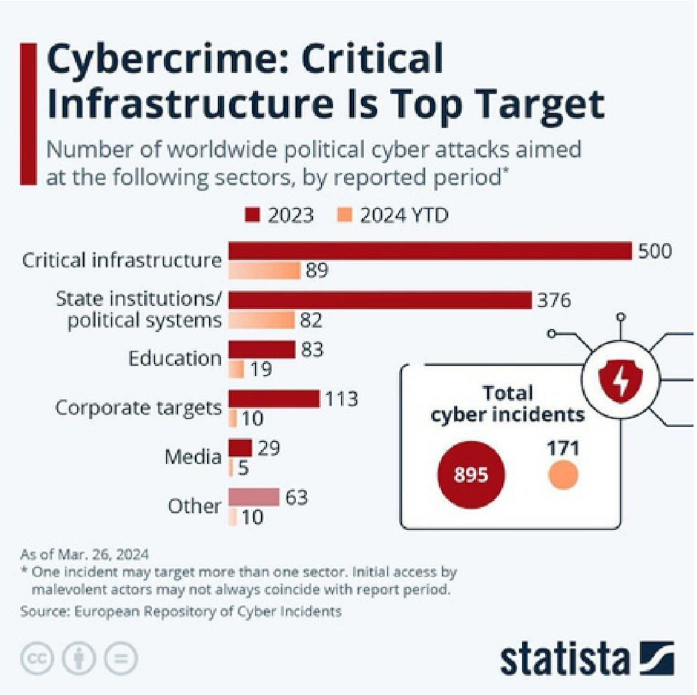
Who's in the Crosshairs? Unveiling Cybercrime's Favourite Targets

Arsha Gosine, Head of Research,ZGC

"The effects of cyberattacks on critical infrastructure can be catastrophic. Security breaches in this sector can be incredibly disruptive to society and are attracting considerable attention from governments and regulatory bodies around the world"

Marcelo Delima, Senior Manager,
Global Solutions Marketing, Thales.

Cybercriminals continue to cast a wide net when seeking out new targets online. We are all too familiar with phone; social media; and email scams and we often hear in the news about business and service industries hacks and scams. Now, researchers have revealed the sectors most commonly targeted by hackers, extortionists, digital spies and online criminals.
A report from the World Economic Forum, published April 22, 2024 provided the following information from Statista who pulled together data from the European Repository of Cyber Incidents (ERCI). The ERCI revealed that critical infrastructure is the main target that cybercriminals go after most frequently. State institutions and political systems are the second most targeted.



Cybercrime: Critical Infrastructure Is Top Target

Number of worldwide political cyber attacks aimed at the following sectors, by reported period*

As of Mar. 26, 2024
* One incident may target more than one sector. Initial access by malevolent actors may not always coincide with report period.
Source: European Repository of Cyber Incidents

The ERCI data showed that the healthcare sector accounts for 14.2 % of all attacks targeting critical infrastructure. This included ransomware attacks; the theft of confidential patient healthcare records; and the disruption of care services in healthcare organisations. Financial organisations are another major target, accounting for 8.3% while telecommunications, transport, and the energy sectors are targeted on a regular basis.

Some examples of critical infrastructures affected by cyberattacks over the last few years:

(i) In 2020, a highly sophisticated cyber intrusion that inserted a backdoor into the product was found in a software application made by Solarwinds. The hackers created a backdoor in the third-party software, in this case the SolarWinds Orion Platform, through which they accessed and impersonated users and accounts of victim organizations. The malware also accessed system files and blended in with legitimate SolarWinds activity without detection, even by antivirus software.

As customers downloaded the Trojan Horse installation packages from Solarwinds, the cybercriminals were able to access the systems running the Solarwinds products. The hackers used a method known as a supply chain attack to insert the malicious code into the Orion system. A supply chain attack works by targeting a third party with access to an organization's systems rather than trying to hack the networks directly. SolarWinds was a perfect target for this kind of supply chain attack because their Orion software is used by many multinational companies and government agencies; all the hackers had to do was install the malicious code into a new batch of software distributed by SolarWinds as an update or patch.

(ii) In 2021, Colonial Pipeline, a US fuel pipeline operator was targeted the FBI confirmed that a ransomware attack organized by a cybercrime group called DarkSide forced the Colonial Pipeline into a voluntary shut down. During the six-day outage, panic buying caused a gas shortage across more than a dozen states in the southeast.
Pipeline Colonial is the most extensive pipeline system for refined oil products in the USA. The stoppage of the pipeline that delivers approximately half of the fuel across the southeast caused nearly 9 out of 10 gas stations in Washington, D.C., to be out of gas. The fuel was not only unavailable but also caused gas stations to increase prices dramatically. The cost nearly tripled in states such as Virginia, where pumping gas for $7 a gallon was a typical sight. And again, this was only available to drivers who were "lucky enough" to find a gas station that still had any fuel left. Some gas stations tried to battle panic buying by limiting the amount of gas purchased per customer.

After days of negotiations, anonymous sources, quoted by CNBC, said that Colonial Pipeline even paid approximately $5 million ransom to the hackers, even though government agencies strongly advised them not to pay the ransom as such actions encourage the hackers to keep extorting other companies.

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

Zyber News Roundup

Europol Operation shutters 12 scam call centers and cuffs 21 suspected fraudsters

A Europol-led crackdown named "Operation Pandora" has successfully dismantled a large-scale phone scam operation, shutting down 12 call centers and arresting 21 individuals across Albania, Bosnia-Herzegovina, Kosovo, and Lebanon. These centers were implicated in orchestrating thousands of fraudulent calls daily, including deceptive police impersonations, investment scams, and romantic cons, with an estimated prevention of financial losses exceeding €10 million. The operation was triggered by a vigilant bank teller in Freiburg, Germany, who suspected a customer attempting to withdraw a large sum was the victim of a scam, leading to the initial scammer's arrest and subsequent investigations. Further investigations revealed that the criminal network made over 28,000 scam calls in just 48 hours, using sophisticated methods to extract money from unsuspecting victims across Europe. German authorities, deploying over 100 officers, traced these calls to their origins, discovering specific crime specializations in each country's call centers. This massive police effort, which included extensive monitoring and direct warnings to potential victims, culminated in coordinated raids on April 18 involving hundreds of officers across multiple countries, seizing significant amounts of digital and physical evidence along with cash and assets worth €1 million. The operation highlights the complex nature of modern telecommunication fraud and the importance of international cooperation in tackling such widespread criminal networks.

Read more: **https://www.theregister.com/2024/05/03/operation_pandora_europol/**

INTERPOL, security stakeholders proffer solutions to cybercrime challenges

Stakeholders in the cybersecurity sector and representatives from Interpol gathered to address cybercrime challenges in Africa at "INTERPOL'S 10th African working group cybercrime units meeting for African heads." The meeting featured key figures including Interpol's Director of the Cybercrime Directorate Unit, Craig Jones, and the Inspector General of Police, Kayode Egbetokun, alongside Interpol's Vice President for Africa, Garba Umar. Discussions focused on enhancing collaboration among member nations to tackle the global menace of cybercrime, recognizing the need for a unified approach due to the transnational nature of cyber threats that affect individuals, businesses, and governments worldwide.

Read more: https://guardian.ng/news/interpol-security-stakeholders-proffer-solutions-to-cybercrime-challenges/

USA: Sen. Lindsey Graham's phone being investigated for potential hack

Senator Lindsey Graham disclosed that the FBI is currently in possession of his phone following an incident where he received a deceptive message from someone posing as Senate Majority Leader Chuck Schumer. This revelation came during a panel discussion at The Hill and Valley Forum, emphasizing the vulnerabilities even high-ranking officials face regarding cybersecurity threats. Graham's office has not specified whether the suspicious activity was related to a call or a text, and declined to comment on the type of phone involved, while the Sergeant at Arms is investigating the potential hack.

This incident underscores the broader issue of cybersecurity threats targeting lawmakers, highlighted by past events where phones were manipulated into surveillance tools and other security breaches involving personal data of Congress members. Just recently, software capable of converting phones into surveillance devices was banned by the Treasury Department following its deployment against other U.S. legislators, illustrating the ongoing risks and the importance of stringent security measures to protect sensitive communications.

Read more: https://www.nbcnews.com/politics/congress/sen-lindsey-grahams-phone-investigated-potential-hack-rcna150507

Scammers bilked older Americans out of $3.4 billion last year, often using cryptocurrency

In 2023, at least 101,000 Americans aged 60 and older fell victim to digital fraud, suffering substantial financial losses averaging $33,915 per person, totaling approximately $3.4 billion, according to a report from the FBI's Internet Crime Complaint Center (IC3). The report highlighted a significant 11% increase in complaints from the previous year, with a disturbing rise in scams involving cryptocurrencies, which accounted for nearly 40% of the total losses, amounting to about $1.33 billion. These crypto-related frauds often started as romance or confidence scams that later transitioned into sophisticated cryptocurrency investment schemes, leveraging social and dating platforms to exploit victims.

The FBI has emphasized that combatting financial exploitation of the elderly remains a top priority, noting a 14% increase in overall complaints from this demographic in 2023. The most prevalent type of fraud reported involved call center or tech support scams, where fraudsters posed as representatives from well-known companies to deceive victims into believing their accounts were compromised and that their funds needed to be secured, often leading to devastating financial and personal consequences.

Read more:
https://www.nbcnews.com/business/consumer/older-americans-lost-thousands-of-dollars-to-cybercrime-2023-how-why-rcna150191

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

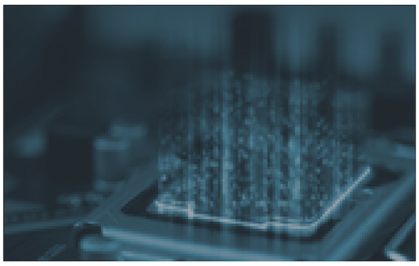
7th Intl. Conference on Big Data, Cybersecurity & Artificial Intelligence **Edinburgh Napier University, Scotland.** **15 May 2024**	**45th IEEE Symposium on Security and Privacy** **San Francisco, CA, USA** **20- 23 May 2024**	**16th International Conference on Cyber Conflict: Over the Horizon** **Tallin, Estonia** **28 - 31 May 2024**
The Cyber Academy, a part of the School of Computing, Engineering & the Built Environment (SCEBE) has been organising the Big Data conference for a decade now (with a gap during the COVID pandemic of course). The event is now back in full force, in person, at our state-of-the-art facilities of The Business School at our Craiglockhart campus in Edinburgh. We have decided to adapt the title each year, to reflect a focal point of interest. In 2023 it was called Big Data, Cybersecurity and Critical Infrastructure. This year, the event is called Big Data, Cybersecurity & Artificial Intelligence (AI) to reflect the enhanced interest in this tech that is changing things extremely fast. With a focus on Artificial Intelligence, this conference will be a little different than usual. A variety of speakers will be talking about the different faces of AI, from business and academia to cybercrime and war.	Since 1980, the IEEE Symposium on Security and Privacy has been the premier forum for presenting developments in computer security and electronic privacy, and for bringing together researchers and practitioners in the field. The 2024 Symposium will mark the 45th annual meeting of this flagship conference. The Symposium will be held on May 20-22, and the Security and Privacy Workshops will be held on May 23.	Throughout the years, the annual International Conference on Cyber Conflict, CyCon, organised by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), has established itself as a major multidisciplinary conference on the technical, legal, policy, strategy and military perspectives of cyber defence and security. In just over a decade, CyCon has also become a community-building event for cyber security professionals, drawing over 600 participants each spring to the Estonian capital Tallinn. CyCon proceedings are sponsored by the IEEE, ensuring the academic online publication and the standards of the research. CCDCOE produces hard copies of the proceedings and the articles will also be published on the Centre's website.
For further information **https://www.eventbrite.co.uk/e/7th-intl-conference-on-big-data-cybersecurity-artificial-intelligence-tickets-884919617397**	**For further information** **https://sp2024.ieee-security.org/index.html**	**For further information** **https://cycon.org**

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