Zyber Global
INDEPENDENT CYBERCRIME, CYBERSECURITY, DIGITAL EVIDENCE, LEADERSHIP AND BUSINESS CONSULTANCY
www.zyberglobal.com

MAY 2025 | ISSUE 58

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Here in the UK, May brings not one, but two bank holiday offering some much needed breathing room. Just days ago, we were enjoying sunshine and an early taste of summer with an unexpected heatwave, but as British weather would have it, we're now back to cold winds and rain. Fingers crossed for brighter skies ahead!

On a more positive note, we kicked off the month with our Wisdom of the Crowd webinar on 6 May, featuring Marina Peshovska, Cybercrime Chief Investigator, Skopje, North Macedonia. She delivered an excellent and insightful session on the Admissibility of Electronic Evidence and Cross Border Cooperation a topic that sparked great engagement and discussion.

Our next Wisdom of the Crowd webinar is coming up in July, so stay tuned for more details.

Until then, stay safe, stay curious, and enjoy the rest of your month!

Esther George, CEO Zyber Global Centre

Marina Peshovska

This Month's Features

1. **Zyber Focus Article**
   Inside the New Era of Global Cyber Threats (2023-2025) – Part 1
2. **Zyber News**
   We have a roundup of the latest international cybercrime news.
3. **Zyber Global Events Information**
   A focus on forums/conferences around the world.

Zyber Global – Tel: 07426719579 Privacy Policy Register
To unsubscribe contact us at office@zyberglobal.com

Zyber Focus Article

Inside the New Era of Global Cyber Threats (2023-2025) – Part 1

By Esther George and the Zyber Global Research Team

Cybercrime and cyber enabled attacks surged in 2023–2024, striking governments, businesses, and public services worldwide. The FBI's IC3 reported a 33% jump in losses, totalling $16 billion in 2024, with phishing/spoofing, extortion (ransomware) and data breaches as the top complaint categories. Europol likewise warned that "millions of victims across the EU were attacked and exploited online on a daily basis" in 2023 the Internet Organised Crime Threat Assessment (IOCTA) 2024 stated that ransomware, child sexual exploitation and financial fraud remained the "most threatening manifestations" of cybercrime. The report noted that small and medium sized organizations are prime targets for ransomware groups due to their weaker defences.

National cyber authorities and the World Health Organisation now stress that attacks on sectors like healthcare can be "issues of life and death. " The following survey details the biggest global cyberthreats and incidents from 2023 to date, outlines attackers' tactics and exploited vulnerabilities, and highlights law enforcement successes and lessons learned.

Ransomware: The Perennial Top Threat

Ransomware remains the dominant cyberthreat affecting all sectors. In 2023, law enforcement and security analysts observed a proliferation of "Ransomware as a Service" (RaaS) gangs and attacks. The UK's National Cyber Security Centre bluntly warns that "ransomware remains one of the most acute cyber threats facing the UK. " Criminals typically steal data, encrypt systems or both ("double extortion"), and demand payment in cryptocurrency. Europol notes that a few RaaS operators control much of the market: LockBit was by far the most active provider in 2023, while sophisticated groups like CL0P leveraged Zero-day software flaws, and newcomers like Akira and Medusa emerged. BlackCat (ALPHV), Black Basta and Conti like affiliates also continued to hit critical infrastructure, health, finance and education targets. An international task force disrupted the Hive ransomware cartel in January 2023, helping 1,500+ victim companies and preventing an estimated €120 million in ransom payments.

In February 2024 international law enforcement Agencies including the UK's NCA, FBI, and Europol seized LockBit's dark web leak site and infrastructure during Operation Cronos. LockBit, dubbed "the world's top ransomware threat", had extorted over $120 million from more than 2,000 victims across nearly every industry. Authorities replaced LockBit's data dump site with a seizure notice and obtained decryption keys to assist victims.

Despite recent successes, RaaS continues to evolve as leaked source code from Conti and others has spawned many copycats. Europol notes some affiliates now develop their own ransomware to avoid relying on major providers. These attackers increasingly target small to medium businesses with weak security, knowing they will pay to keep systems online. New tactics include data extortion without encryption and targeting new platforms like Macs. Ransomware remains a persistent global threat over 300 organizations across sectors from medical to manufacturing has been hit by newer strains like Medusa and Akira...

Read more here: https://zyberglobal.com/blog?blogcategory=Article

Zyber News Roundup

New Framework Targets Rising Financial Crime Threats

Experts are sounding the alarm over a global rise in online fraud, particularly cryptocurrency scams and phishing attacks that increasingly mimic cybercriminal tactics. The FBI reports $9.3 billion in losses from crypto scams alone, while Google recently warned billions of Gmail users about an advanced phishing threat. As cybercrime expands across regions like East and Southeast Asia, countries such as New Zealand are adopting new anti-fraud measures, and international bodies like the United Nations have noted the growing global scope of these scams...

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

Vulnerability Exploitation Is Shifting in 2024-25

While the number of exploited vulnerabilities may have stabilized, the cybersecurity landscape is shifting in more concerning ways. Attackers are now focusing less on consumer applications and more on enterprise technologies such as firewalls, VPNs, and cloud services, which grant higher network privileges and often evade traditional security tools. At the same time, the window between vulnerability disclosure and exploitation is narrowing, with nearly a third of known vulnerabilities being weaponized within a day of becoming public...

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

AI security report warns of rising deepfakes & Dark LLM threat

Check Point Research's first AI Security Report highlights how artificial intelligence is rapidly transforming the cyber threat landscape. The report identifies four major areas of concern: AI-enhanced impersonation, data poisoning and disinformation, AI-powered malware development, and the creation of malicious large language models (LLMs) like FraudGPT and WormGPT. One in 80 generative AI prompts carries a high risk of sensitive data leakage, while one in 13 includes potentially exploitable information, pointing to the growing misuse of AI in criminal operations such as phishing, impersonation, and disinformation campaigns...

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

Building resilience through community

Charities provide essential services to communities, often operating on limited budgets and depending heavily on volunteers. However, their trusted status and stretched resources make them prime targets for cybercriminals and fraudsters. In today's increasingly digital environment, improving resilience to fraud and cybercrime is not just a technical requirement but a fundamental necessity for safeguarding beneficiaries, donor funds, and public confidence.

The sector faces unique challenges, including underinvestment in cybersecurity, lack of dedicated IT teams, and an operational focus...

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

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

IoT Solutions World Congress | 13 – 15 May 2025 | Barcelona, Spain

This congress is the first to focus solely on IoT integrated with cutting-edge technologies such as AI, Network Resilience, Big Data, and cloud computing, positioning it as an excellent opportunity for professionals working in network security, IT administration, and threat detection.

The agenda includes discussions around disruptive cloud and networking technologies, enabling businesses across the globe to scale faster and securely.

SEE MORE >

GOVSEC - Government IT Security | 15 May 2025 | London, UK

Hosting the leading experts and solution providers within government and public sector infosec and cybersecurity. Our GovSec series of events, now in its 11th year, is rightly regarded as the leading UK government security and risk management conference which brings together the leading lights from across the government and public sector.

In collaboration with world-renowned solution providers who are situated at the cutting edge of human and technology-led innovations, Whitehall Conferences GovSec 2025 guarantees to deliver on its promise to provide a platform through which knowledge can be shared, the understanding gained, professional networks expanded and solutions to existing problems discovered.

SEE MORE >

Cybersec Europe 2025 | 21-22 May 2025 | Brussels, Belgium

Cybersec Europe 2025 is a leading cybersecurity event bringing together industry experts, decision-makers, and technology providers to explore IT security, data management, cloud solutions, and artificial intelligence. Taking place on May 21-22, 2025, in Brussels, Belgium, the event features keynote speeches, interactive workshops, and AI-driven matchmaking for networking.

With over 10,000 attendees and 500+ exhibitors expected, Cybersec Europe provides a comprehensive platform for learning, collaboration, and business development. The exhibition floor showcases the latest cybersecurity innovations, while expert-led discussions address emerging threats and industry best practices. Designed for professionals looking to stay ahead in cybersecurity, this event is an essential destination for security leaders across Europe.

SEE MORE >

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**

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.

CLICK HERE

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.

CLICK HERE