Zyber Global

JUNE 2022 | ISSUE 23

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 23rd Edition, June 2022 of Zyber Global Centre's monthly newsletter.

In the United Kingdom we have been celebrating the Queen's Platinum Jubilee to mark 70 years on the throne. The Queen holds the record for being the world's longest reigning living monarch and the longest serving female monarch. The Queen is now the first royal in British history to celebrate a Platinum Jubilee.

A series of celebrations and events took place in London over the special four-day bank holiday weekend from Thursday June 2 to Sunday June 5, in line with the Queen's coronation on 2 June 1953.

It's been a fun weekend with Union flags everywhere and an ever-increasing number of street parties. Starting with the Trooping the Colour procession at Horse Guards Parade and it concluded with a pageant of performers from 54 Commonwealth countries, who marched along The Mall in front of Buckingham Palace and around the nearby streets to celebrate.

I am so glad that I was in London to experience it.

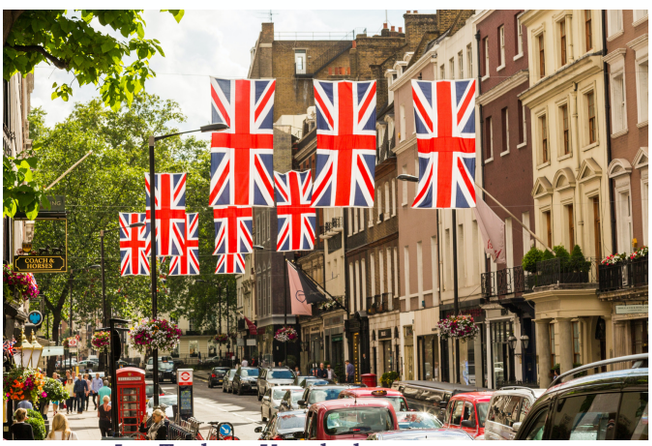
Don't forget to read our roundup of the latest international cybercrime news.

The next Stay Safe Online webinar is on the 30 June 2022 register now to attend.

Let us know what topics you would like to see discussed in future newsletters.

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre



courtesy Ian Taylor - Unsplash

This Month's Features

Zyber Focus

This article is on Cyptocurrency, which is the third and last in a series on '*Cyber-Money Laundering*'

Zyber News

We have a roundup of the latest international cybercrime news.

Zyber Global Events Information

A focus on forums/conferences around the world.

courtesy Matt Antoniolli - Unsplash

Zyber Focus Article

Cyber-Money Laundering: Part III Cryptocurrency

Arsha Gosine, Head of Research, Zyber Global Centre

courtesy Kanchanara - Unsplash

As cryptocurrency continues to grow, it's imperative that the public and private sectors work together to ensure that users can transact safely, and that criminals can't abuse these new assets.
The 2022 Crypto Crime Report (The 2022 Report), Chainalysis.

Cryptocurrencies are digital money that is not issued by a bank. One can trade and invest these currencies like any other and there are virtually no barriers to entry. The absence of regulation means the market can go up incredibly fast.
During the lockdown, the total value of all cryptocurrencies increased from about £175bn to more than £1.75tn.
In May last year, the National Crime Agency (NCA) warned that 'criminals increasingly used cryptocurrencies to facilitate money laundering [in the last 12 months], at least in part because the pandemic made it harder to move cash'. The NCA also found that cryptoassets were being used more and more by criminals to 'buy and sell commodities, such as drugs, using online marketplaces found on the dark web'.
In July last year, the Metropolitan Police seized nearly £180 million worth of cryptocurrency in a record- breaking ongoing investigation into international money laundering.
The Metropolitan Police Deputy Assistant Commissioner Graham McNulty had this to say: "Proceeds of crime are laundered in many different ways. While cash still remains king in the criminal world, as digital platforms develop we're increasingly seeing organised criminals using cryptocurrency to launder their dirty money.
The detectives on this case have worked tirelessly and meticulously to trace millions of pounds worth of cryptocurrency suspected of being linked to criminality and now being laundered to hide the trail".
He added: "*Whilst some years ago this was fairly unchartered territory, we now have highly trained officers and specialist units working hard in this space to remain one step ahead of those using it for illicit gain*".
Primarily, cybercriminals dealing in cryptocurrency usually share one goal, which is to launder their ill-gotten funds by first moving it to a safe place, hidden away from the authorities and eventually converting it into 'clean' cash.
The 2022 Report by blockchain data company Chainalysis stated that criminals laundered $8.6bn (£6.4bn) of cryptocurrency in 2021, which was up by 30% from the previous year. The 2022 Report also stated that "Law enforcement can strike a huge blow against cryptocurrency-based crime and significantly hamper criminals' ability to access their digital assets by disrupting these services. An example of this was when, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned two of the worst-offending money laundering services — Suex and Chatex — for accepting funds from ransomware operators, scammers, and other cybercriminals".
Gary Cathcart, head of financial investigation at the NCA said: "*Whilst the vast amount of cryptocurrency use and exchange is for legitimate reasons, organised criminals have identified the benefits that cryptocurrency provides them. There are parts of the cryptocurrency structure that are being exploited to launder criminal cash, particularly from drug dealing. The growing menace of ransomware also utilises cryptocurrencies as its payment mechanism. Law enforcement is responding to this adoption by criminal gangs and cryptocurrency seizures are increasing. Legislative changes are also being progressed to assist with the response to cryptocurrencies being used in illicit finance practices.*"
It seems that it is incredibly difficult to ascertain cryptocurrency's role in the laundering of funds derived from traditional offline crimes because in those cases, the cryptocurrency isn't moving from addresses that have been previously identified as associated with crime, but rather it is initially deposited as fiat currency with no evidence of its criminal origins visible on the blockchain. The only way someone could know the origins of those funds is if they were already investigating the criminals in question. This is where blockchain analysis comes in, which is the process of inspecting and identifying, clustering, modelling and visually representing data on a cryptographic distributed ledger known as blockchain. The goal of blockchain analysis is discovering useful information about the different actors transacting in cryptocurrency.

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

Zyber News Roundup

Suspected phishing email crime boss cuffed in Nigeria

Interpol and cops in Africa have arrested a Nigerian man suspected of running a multi-continent cybercrime ring that specialized in phishing emails targeting businesses.

His alleged operation was responsible for so-called business email compromise (BEC), a mix of fraud and social engineering in which staff at targeted companies are hoodwinked into, for example, wiring funds to scammers or sending out sensitive information. This can be done by sending messages that impersonate executives or suppliers, with instructions on where to send payments or data, sometimes by breaking into an employee's work email account to do so.

The 37-year-old's detention is part of a year-long, counter-BEC initiative code-named Operation Delilah that involved international law enforcement and started with intelligence from cybersecurity companies Group-IB, Palo Alto Networks Unit 42, and Trend Micro.

"*The arrest of this alleged prominent cybercriminal in Nigeria is testament to the perseverance of our international coalition of law enforcement and Interpol's private sector partners in combating cybercrime*," Garba Baba Umar, Assistant Inspector General, Nigeria Police Force, said in a statement this week.

Read more: **https://www.theregister.com/2022/05/26/nigerian_phishing_arrest/**

This era of big tech exceptionalism has got to end: Australian eSafety Commissioner

Much like how car manufacturers had to be forced to implement safety features such as seat belts, Australian eSafety Commissioner Julie Inman Grant believes social platforms and tech giants need to be guided by international standards.

"What we're saying is this era of technological exceptionalism has got to end," Inman Grant said on a panel at the World Economic Forum.

"*We've got food safety standards, we've got consumer protection laws, we need the companies assessing their risks and then building the potential protections in as a forethought, rather than an afterthought ... embedding those digital seatbelts and erecting those digital guardrails*."

As the world hurtles towards a future that could include augmented reality, metaverses, and other different realities, Inman Grant said such experiences could be supercharged, and that also includes when users are harmed in such environments.

"*If we don't learn the lessons of the web 2.0 world and start designing for the governance and safety by design, and security and privacy for the metaverse world -- I mean, what could possibly go wrong with full sensory haptic suits, hyper-realistic experiences, and teledildonics all coming together in the metaverse?*" the commissioner said.

"*I think we're going to have to think about a recalibration of a whole range of human rights that are playing out online -- from freedom of speech, to the freedom to be free from online violence, or the right of data protection, to the right to child dignity.*"

Inman Grant earlier told the forum that freedom of speech does not equate into a total free-for-all, and her agency had seen success in getting harmful content taken down.

Read more: https://www.zdnet.com/article/this-era-of-big-tech-exceptionalism-has-got-to-end-australian-esafety-commissioner/

Crypto Hacks Aren't a Niche Concern: They Impact Wider Society

Million-dollar crypto heists are becoming more common as the currency starts to go mainstream; prevention and enforcement haven't kept pace.

The attack against the Ronin Network in March was quickly speculated to be one of the largest cryptocurrency hacks of all time. Approximately $540 million was stolen from the cryptocurrency and NFT games company in a combination of USDC and Etherium, with $400 million of the stolen funds owned by customers playing the game Axie Infinity.

This attack was the latest in a string of thefts perpetrated against crypto and should be a jolt to both the digital asset and cybersecurity communities to bring the security of cryptocurrencies into line.

The current vogue of large-scale crypto heists goes as far back as the 2014 Mt. Gox hack (another cryptocurrency exchange built around a game, Magic: The Gathering), which went into bankruptcy after losing $460 million of assets.

However, the trend has been gathering pace. In the months leading up to the Ronin Network attack, cybercriminals stole nearly $200 million worth of cryptocurrency from the crypto trading platform BitMart, attacked 400 Crypto.com users, and orchestrated NFT-related scams, to name but a few incidents. There is often an uncomfortable tendency to see these attacks as something that takes place in isolation in a remote part of the Internet when they actually have a huge impact on thousands of people

Read more: **https://www.darkreading.com/attacks-breaches/crypto-hacks-aren-t-a-niche-concern-they-impact-wider-society**

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

CYBERTECH Global, **June 13-14, 2022** **Dubai,** **United Arab Emirates**	**ISMG Fraud Summit,** **June 16,2022** **Online**	**Infosecurity Europe,** **June 21-23, 2022** **Excel London**
The Cybertech Global Conference 2022 returns to Dubai for the second time in full scale after Covid and is being held on the 13 to 14th of June 2022. This event will highlight the latest technological innovations, challenges and solutions to combat threats within the global cyber arena. It will feature internationally renowned cybersecurity leaders, including representatives from government offices and industry organizations. With a grand exhibition hall and a cutting-edge conference, Cybertech Global gathers thousands of C level decision makers and brings new market opportunities for multinational corporations, startups, private and corporate investors, venture capital firms, government entities and academia.	The 2022 Fraud Summit, hosted by the Information Security Media Group (ISMG), is part of the virtual and hybrid summit event series presented by the organization. The annual Fraud Summit brings leaders and key decision-makers together to connect and learn from each other's success, as well as challenges, in an interactive educational environment to better combat fraud. Speakers at this year's event include security leaders from Google Cloud, Visa and the World Health Organization, among others.	Infosecurity Europe is a large event with security vendors exhibiting alongside conference content. An ever-demanding environment for cybersecurity professionals is worsened by blackmailers, terrorists - even hostile nation states. A rise in social engineering attacks, large scale third-party incidents, and constantly evolving human risk factors has resulted in security threats emerging as one of the most contemporary, prominent risks to businesses, civil society, and democracies; undermining the very fabric of our communities. This is why Infosecurity Europe wants to nurture a knowledge-sharing culture. We are calling on information and cybersecurity professionals to cooperate. We must instill ethics, promote diversity, improve global talent, and design a world that is safer for all. Together we are stronger.
For further information: **https://dubai.cybertechconference.com**	For further information: **https://ismg.events/summit/cybersecurity-summit-fraud-2022**	For further information: **https://www.infosecurityeurope.com/en-gb/whats-on/conference.html**

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