Zyber Global

FEBRUARY 2021 | ISSUE 7

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 7th Edition, February 2021 of Zyber Global Centre's Monthly Newsletter.....

February is one of my favourite months! It is starting to get lighter in the evenings and gives me hope that longer days will soon be with us!

My month had a great start, as on February 2, 2021, I spoke at a really interesting Cybersecurity and Digital Forensic training organised by the Liberia Cybercrime Prevention and Mitigation Agency (LCCPMA). I presented on the Global Prosecutor's e-Crime Network and the vision for the Zyber Global Centre.

On February 4, 2021, I spoke at 'Take a Break' a new initiative of ' A Call to Business'. I shared my journey on my business and how I got here (you will be pleased to know it's the brief version). The talk was recorded so you will soon be able to access it here:http://www.acalltobusiness.co.uk/entrepreneurs-evening

I hope 2021 is treating you well. Enjoy the newsletter and Happy February!!

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Spotlight

The interview spotlight this month is on Alexandru Caciuloiu, UNODC Cybercrime, and Cryptocurrency Advisor and Regional Coordinator for South East Asia and the Pacific.

Zyber News

We have a roundup of the latest international cybercrime news.

Zyber Focus

The focus this month is on the *'Worst Cyber Threats of 2020'* by Esther George, CEO.

Zyber Global Events

The next Stay Safe Online Webinar by Zyber Global is due to take place on February 25, 2021 register now to attend.

Coming Soon:

We have an exciting new webinar series in development for later this year

"We need to improve the compatibility of cyber legislation across the world to combat cybercrime"

ALEXANDRU CACIULOIU

UNODC CYBERCRIME, AND CRYPTOCURRENCY ADVISOR

Zyber Spotlight

Alexandru Caciuloiu, UNODC
Cybercrime and Cryptocurrency Advisor and Regional Coordinator for South East Asia and the Pacific

Dynamic and enterprising, Alex brings a wealth of experience to bear in tackling cybercrime throughout the S.E Asia and Pacific Region.

What are the main cybercrime threats in S.E Asia and the Pacific region and what is being done to respond to the challenge?

From our research and direct engagement with the government and other stakeholders in the region, I can say that all indicators point to a rise in all types of cybercrime. This has been compounded by the COVID-19 pandemic as well. We see a continuous increase in ransomware, business email compromise, phishing, all types of internet frauds but also more technically complex APT`s operating in the region. Cryptocurrency and darknet related crime are also well on the rise, and that includes cryptojacking, crypto exchange hacks, or more criminals in Southeast Asia selling or buying illegal items on the darknet such as drugs, cyber tool kits, and more increasingly child sexual abuse material. Misinformation and disinformation are also at an all-time high. Various messages, phishing emails, instant messaging memes, fake news circulate now, accelerated by the pandemic, as people want to keep abreast of the latest developments on vaccines, government measures, travel restrictions, or even domestic travel opportunities.

Many criminals thus seek to take advantage of these factors and use this opportunity to push out disinformation, advertise for fake vaccines or request money for various pyramid schemes. The fact that the pandemic shows no signs of dimming down, reflects in a smaller number of specialist cybercrime police being able to work to counter it. That is either due to police being diverted to enforce lockdown measures or conduct contact tracing investigations or to them even falling ill.

Cryptocurrency is very topical at the moment, especially Bitcoin. There are many advertisements inveigling the public to invest and it is touted as one of the easiest ways to make money.
Can you tell us how the Working Group is tackling this?

Indeed, Bitcoin is now on everybody`s lips. Given my experience with crypto and darknet starting from INTERPOL it was a natural transition to continue this work with UNODC. By working with the countries in the region we were able to see that there was still a big gap in law enforcement understanding of the criminal use of cryptocurrencies and their capacity to act in this environment and an even wider gap in the regulatory framework in the region.

What advice can you give to the public regarding cryptocurrency?

What can I say to the public is that they should try to understand the environment before jumping head first into it.
It all depends on their motivation for adopting such technology. One thing that I can certainly say is that it is not a good or bad thing, it is inherently just a technology like any others. So, if you understand the processes well enough, you can start using it to pay for certain things or even as an investment. It just requires a bit of a higher level of understanding than using cash. And since it`s a distributed and decentralized system, if you have an issue with your wallet or you forget or misplace your password and can`t get back into the wallet, there`s nothing anybody else can do to help you with this. It`s not like with a bank where you can call customer service and reset your password after you go through a verification process. This is what it means that you are totally in control. Ultimately you are the only one responsible for its security.

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

Zyber News Roundup

Fake ICO Consultant Sentenced for Embezzling Cryptocurrency now worth $20 million

A US resident who masqueraded as a cryptocurrency consultant has been sentenced for embezzling cryptocurrency and cash fraudulently obtained from investors.
Jerry Ji Guo, a resident of San Francisco, will spend six months behind bars and has been ordered to pay $4.4 million in restitution for his activities.
The 33-year-old former journalist admitted to reshaping himself as an expert and consultant on cryptocurrency and Initial Coin Offerings (ICOs).
ICOs are investor events that originally formed to give emerging projects an alternative funding route to angel investment or loans. Participants in legitimate ICOs receive project-branded tokens for their contribution, and should the project succeed, this could allow investors to reap substantial profits.
However, ICOs are risky and have paved the way for exit scams and fraud.
In Guo's case, he conned investors by promising he would perform "consultancy, marketing, and publicity services," according to US prosecutors. However, instead of keeping his promise, investor cash and cryptocurrency -- including Bitcoin (BTC) and Ethereum (ETH) ended up being drained from wallets used by companies to deposit funds up-front in order to secure his 'services.
The cryptocurrencies taken from investors have surged in value over the past few years and the combined funds, with cash, are now worth an estimated $20 million. The US Department of Justice Money Laundering and Asset Recovery Section obtained warrants in February 2020 to seize the stolen funds and says that the government "is [now] in a position to return the stolen property to the victims."

Read more:
https://www.zdnet.com/article/fake-ico-consultant-sentenced-for-embezzling-20-million-in-cryptocurrency/?ftag=TRE-03-10aaa6b&bhid=29633521617577276770654057469299&mid=13249228&cid=2354413351

Cyber Attack on the Woodland Trust, UK

The Woodland Trust has been the victim of a sophisticated, high-level cyber-incident, which took place in December 2020.
The Woodland Trust, a peaceful British charity that looks after trees, was struck by a “cyber attack” before Christmas.
Members of the trust, which says that it has planted 43 million trees since its foundation in 1972, were informed of what was inevitably described as a “sophisticated, high-level cyber-incident.” It may not seem obvious what cybercriminals wanted to achieve by targeting the trust, whose online content includes guides on planting trees and how to object to planning permission applications that could result in trees being cut down – but it does have 250,000 registered members.
Chief Executive Darren Moorcroft told Woodland Trust members in an email: “As soon as we became aware of the incident we engaged a group of external specialists who launched an investigation and also took immediate action in order to mitigate the impact.”
He added: “We reported the incident to the Information Commissioner’s Office (ICO), the Charity Commission as well as the Police Cybercrimes Unit.” The charity said in a statement on its website that “no data has been compromised” that it knows of, though it warned members to be vigilant for unusual phonecalls or communications appearing to come from the Trust or from banks.

Read more:
https://www.theregister.com/2021/01/27/woodland_trust_cyber_attack/

Zyber Focus
Worst Cyber Threats of 2020

The year 2020 is already infamous as the year when the world woke up to find that a virus pandemic called COVID 19 was rampaging around the globe causing havoc and mayhem. With the horrendous number of deaths, 2020 turned out to be an "*annus horribilis*" (Latin, meaning "horrible year"). Although like most things it is a matter of perspective, for 'cybercriminals' 2020 was probably their most profitable year yet!
Let's take a walk down memory lane and recall a few of 2020's notable and more interesting breaches and hacks[1].

JANUARY:
Travelex: Travelex services were pulled offline following a malware infection. The company itself and businesses using the platform to provide currency exchange services were all affected.
FEBRUARY:
Denmark's government tax portal: The taxpayer-identification numbers of 1.26 million Danish citizens were accidentally exposed.
MARCH:
Marriott: The hotel chain suffered a cyberattack in which email accounts were infiltrated. 5.2 million hotel guests were impacted.
APRIL:
Lendf.me: $25 million in cryptocurrency was stolen from the Lendf.me platform.
MAY:
Pakistani mobile users: Data belonging to 44 million Pakistani mobile users was leaked online.

[1] My thanks to Charlie Osbourne of ZD Net who wrote two articles in December 2020, listing all the data breaches, etc in 2020. Both articles listed below are well worth a read:
2020's worst cryptocurrency breaches, thefts, and exit scams By Charlie Osborne for Zero-Day December 7, 2020
The biggest hacks, data breaches of 2020 By Charlie Osborne for Zero-Day December 7, 2020

JUNE:
BTC-e: New Zealand law enforcement froze $90 million in BTC-e assets as part of a money laundering investigation.
JULY:
GPay Ltd: UK regulators shut down GPay for scamming cryptocurrency investors by using fake celebrity endorsements.
AUGUST:
Experian, South Africa: Experian's South African branch disclosed a data breach impacting 24 million customers.
SEPTEMBER:
• Norwegian Parliament discloses cyber-attack on internal email system says hackers gained access and downloaded content for "a small number of parliamentary representatives and employees."
• Finland says hackers accessed MPs' email accounts. The Finnish Parliament cyber-attack took place around the same time Russian hackers breached the Norwegian Parliament's email system but was only discovered in December 2020.

"NHS: A relatively unsophisticated attack and could have been prevented by ... following basic IT security best practice" National Audit Office

OCTOBER:
UN IMO: The United Nations International Maritime Organization (UN IMO) disclosed a security breach affecting public systems.
NOVEMBER:
Silk Road: The US Justice Department seized $1 billion in Bitcoin, said to be from the now-defunct Silk Road marketplace.
DECEMBER:
Solar Winds hack: A suspected nation-state sophisticated cyber-attack of SolarWinds which led to the distribution of a tainted version of the SolarWinds Orion network monitoring tool, compromising their customers.

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

Zyber Global Events

The next **Stay Safe Online Webinar** by Zyber Global is due to take place on February 25, 2021. Register now to attend.

OTHER CYBERSECURITY EVENTS

International Conference on Cyberlaw February 14 -15, 2021	**VIRTUAL CYBERSECURITY SUMMIT: SOUTH EAST ASIA** February 23-24, 2021 at 9 am SGT	**Cyber World Virtual Event** March 2, 2021
The International Conference on Cyberlaw 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. 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 .	With the ongoing pandemic, cybersecurity professionals have been stretched plenty, for enhancing corporate agility and also reduce risk, to ensure resilience. As the region witnessed a meteoric rise in online fraud, phishing scams in 2020, CISOs are expected to rethink security and risk strategies in 2021. Join the 2021 South East Asia virtual summit series on February 23-24, 2021. Gain insight from the InfoSec thought leaders on the myths and realities about deploying new frameworks, applying lessons learned, and think strategically, moving beyond the assumption that a bigger team is the best way to respond to increased risk.	The cyber security leadership of the world's largest public and private organisations gather online this March at the Cyber World Virtual Cyber Security Congress. 100s of attendees will attend, representing major players from across the Banking & Finance, Oil & Gas, Retail, Healthcare, Automotive, Electronics, FMCG, Pharmaceuticals, Tourism, and Manufacturing industries. The senior delegation boasts IT security leaders in the form of: CISO, CIO, Head of IT & Security/Network Infrastructure & System/ IT Audit/Cyber Security, Directors of Risk, Information Security & privacy, and Data Protection Officers.
For further information: https://waset.org/cyberlaw-conference-in-february-2021-in-london	For further information: https://events.ismg.io/event/virtual-cybersecurity-summit-south-east-asia-2021/	For further information: https://world.cyberseries.io/overview/

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