Zyber Global

APRIL 2022 | ISSUE 21

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 21st Edition, April 2022 of Zyber Global Centre's monthly newsletter.

I was involved this month as a Council of Europe cybercrime specialist as a speaker and facilitator in the fifth Coordination Meeting held in Antalya in Turkey. This was a hybrid meeting with most delegates and speakers attending the actual venue and about ten delegates and I taking part online. It was a very successful and engaging meeting all the richer from having delegates attend remotely.

I must admit that I am amazed at how much the cybercrime /cyber security capacity building landscape has changed in the last two years. Before the pandemic face to face training and meetings were the norm and like everyone else, I wondered how we would ever cope with extensive online trainings and meetings, but we have. The pandemic has taught me that we can do a lot more remotely than I had thought possible. But that is subject to there being fast and reliable broadband connections which is not always available. I remember during the early days of the pandemic where I was a speaker at a completely virtual cybercrime capacity training meeting. Over half of that country's delegates could not attend due to broadband problems.

There is obviously a place for virtual, hybrid and face to face trainings and meetings depending on which best suits your needs at present. I think though that the present trend will continue its steady movement to virtual online training becoming the norm. What do you think?

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

We have asked you to let us know what you want us to write on and you have. Thank You! We have had requests for some articles on cyber money laundering.

We have therefore planned a three-part series on cyber money laundering; this issue begins with an introduction to the topic. We hope that you find it useful.

We continue with our usual features and ask that you continue to engage with us and let us know what topics on cybercrime you would like to hear more of.

The next Stay Safe Online webinar is on the 28 April 2022, so do register early. Stay well!

This Month's Features

Zyber Focus

This article is an '*An Introduction to 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.

Zyber Focus Article

An Introduction to Cyber-Money Laundering

by

Zyber Global Centre Research Team

Cyber money laundering is a type of cyber-enabled financial crime wherein digital systems (online) are used to transfer money obtained from illicit or illegal activities in such a way that the proceeds of these activities look legitimate and can be used without suspicion. As the word “launder” suggests, it is a way to make illegal dirty money transactions look clean and white transactions in order to elude the law enforcement. This cybercrime has become a complex, wide-spread and multi-faceted activity

The traditional money laundering relies on the banking system. Unlike the traditional money laundering, cyber-money laundering relies on various kinds of e-transactions and financial service providers like e-money transactions to "money mules" and remittance services, international wire transfers, transferring by the use of block-chain technologies, e-gaming, e-banking, using specific hardware and software systems so that anonymity can be created and one's location can be untraceable, creating computer bugs and loopholes etc.

WHAT DOES IT INCLUDE AND HOW DO PEOPLE LAUNDER MONEY?

The traditional money laundering usually includes (sometimes one or two phases and sometimes all) three phases which are as follows:-

1.Placement: - In this phase, the proceeds from the illicit activities, i.e. cash or property, are placed into the legitimate financial institutions. This phase is most vulnerable to detection that’s why legislations across the world mostly focus on this stage to detect money-laundering activities and prevent launderers from depositing or converting large amounts of cash at financial institutions or taking cash out of the country. There are many methods used by the money launderers to place the proceeds into the legitimate financial institutions like repaying loans or credit cards with illegal proceeds, gambling and laundering money at casinos, over-invoicing or under-invoicing, phantom shipping wherein no items are actually shipped but the fraudulent documentation is produced to justify the payment done abroad, using a legitimate cash-focused business to blend dirty funds with the day's legitimate sales receipts, using virtual gaming sites to convert illicit money into gaming currency, hiding money in offshore accounts as like this the identity of the real beneficiary will be kept hidden, etc.

2. Layering/Structuring Stage: - In this phase, the proceeds are broken into smaller transactions so that it becomes difficult to detect. The main aim of this phase is to conceal the source of money with the help of a series of transactions and bookkeeping tricks. It is in this stage that the proceeds move across the world electronically, trading in overseas markets so that the government isn’t able to track the financial gains from illegal proceedings so easily. The more layers of financial transactions, the harder it is to trace the funds, particularly if the money is moved offshore.

3. .Integration / Extraction: - In this final phase, the money is integrated back in the economy to the criminals in a way that makes its source appear legitimate. Usually, criminals retrieve the dirty money by purchasing luxurious and expensive assets, for example, art work, properties, jewellery, high-end automobiles, etc.

Cyber-money laundering makes these phases all more complex by bringing in various new aspects of the digital world. There are two types of cyber-money laundering, they are: -

1.Instrumental Digital Laundering: - In this process, one or more constituent phases of money laundering occurs.

2.Integral Digital Laundering: - In this process, all the three phases of money laundering occur.

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

Zyber News Roundup

White House warns: Do these 8 things now to boost your security ahead of potential cyberattacks

It's one thing for tech companies to urge users to enable multi- or two-factor authentication, but now the White House is urging all US organizations to do it because of potential cyberattacks ahead.

Two-factor or multi-factor authentication (MFA) was a concept that needed to be explained carefully to the public a few years ago. It's an approach to cybersecurity that requires users to sign into an account with something they physically possess, such as a phone.

Most companies don't use it, even when it's readily available, according to previously reported data from Microsoft, because they prioritize easy access to information over security. But with the Russian invasion of Ukraine happening now, the US government has now told all organizations that MFA is a must. "Mandate the use of multi-factor authentication on your systems to make it harder for attackers to get onto your system," the White House has warned.

The message comes as the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) ramp up warnings about Russian hacking of everything from online accounts to satellite broadband networks. CISA's current campaign is called Shields Up, which urges all organizations to patch immediately and secure network boundaries.

President Biden said the warnings around improving tech security were "based on evolving intelligence that the Russian government is exploring options for potential cyberattacks."

Read more:
https://www.zdnet.com/article/white-house-warns-do-these-8-things-now-to-boost-your-security-ahead-of-potential-russian-cyberattacks/

FBI and CISA warn over threats to satellite communications networks

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) has warned satellite communications network providers to beef up security.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) has warned satellite communications network providers to beef up security.

The CISA and FBI said in a joint advisory that they are "*aware of possible threats*" to U.S. and international satellite communication (SATCOM) networks. "*Successful intrusions into SATCOM networks could create additional risk for SATCOM network customer environments*," the agencies note.

Read more: https://www.zdnet.com/article/cisa-and-fbi-warn-over-threats-to-satellite-communications-networks/

Man linked to multi-million dollar ransomware attacks gets 66 months in prison for online fraud

An Estonian man connected to multi-million dollar ransomware attacks has received a five-and-a-half-year jail sentence for his involvement in online fraud schemes. The US Department of Justice says Maksim Berezan, a 37-year-old from Estonia, took part in at least 13 ransomware attacks, including seven against American businesses, which cost victims over $53 million in losses.

Berezan was an active member of an online forum designed for Russian-speaking cyber criminals to gather and exchange their criminal knowledge, tools, and services, the DoJ said.

Berezan was arrested in Latvia in November 2020 and extradited to the US where he pleaded guilty in April 2021 to conspiracy to commit wire fraud affecting a financial institution and conspiracy to commit access device fraud and computer intrusions.
Berezan was sentenced to 66 months in prison and ordered to pay $36 million in restitution.

Read more: https://www.zdnet.com/article/man-linked-to-multi-million-dollar-ransomware-attacks-gets-66-months-in-prison-for-online-fraud/

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

International Conference on Cyber Crime and Information Security **April 25-26, 2022** **Tokyo, Japan**	**eCommerce Week 2022: Data and Digitalization** **25 - 29 April 2022** **Geneva, Switzerland and Online**	**National Cyber Crime Conference** **April 26th - April 28th** **Norwood, Massachusetts USA**
The International Conference on Cyber Crime and Information Security aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Cyber Crime and Information Security. 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 Cyber Crime and Information Security.	IThe 2022 ecommerce week will be held under the theme "*Data and Digitalization for Development*", putting a special emphasis on data and cross-border data flows and the crucial role they play in economic and social development. The connectivity-related digital divide is being heightened by an emerging data divide, reflecting the wide differences that exist between and within countries to harness data. Countries with limited capacities to turn data into digital intelligence and business opportunities, and use them for economic and social development, are at a clear disadvantage. The event will also shine a light on how the COVID-19 pandemic has impacted digital transformations globally.	The National Cyber Crime Conference is hosted by the Massachusetts Attorney General's Office. It is one of the premier annual cyber crime and digital evidence training events for law enforcement and prosecutors. Over the course of the past 10 years, the NCCC has become the premier annual cyber crime and digital evidence training event for law enforcement, prosecutors, and forensic examiners. Please be advised that the NCCC is restricted to actively employed law enforcement/prosecutorial agency investigators, forensic examiners, prosecutors and respective support personnel.
For further information: https://waset.org/cyber-crime-and-information-security-conference-in-april-2022-in-tokyo	For further information: https://unctad.org/eweek2022	For further information: https://www.mass.gov/service-details/national-cyber-crime-conference

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