Zyber Global

AUGUST 2021 | ISSUE 13

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 13th Edition, August 2021 of Zyber Global Centre's Monthly Newsletter.....

I hope that you are all well and enjoying the summer break. The weather in the UK is very changeable and we are having spells of good weather mixed with days of rain.

Any way we can ignore all of that, as we have the Olympic Games Tokyo to amuse and divert us. In the medal's table, Great Britain (GB) is presently in the top 10, so we are very happy. Pity about the 8 hour time difference but we are hoping for team GB to get a lot more medals.

Do write in and let us know what topics you would like to see discussed in the September newsletter.

We always appreciate your feedback!

In the meantime, keep safe.

BEST REGARDS

ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Spotlight

The interview spotlight this month is on Yves Vandermeer, Chairman, European Cybercrime Training and Education Group, Brussels, Belgium.

Zyber News

We have a roundup of the latest international cybercrime news.

Zyber Focus

The focus this month is an article on 'Darknetlive' by Professor Zvonimir Ivanovic, University of Criminal Investigation and Police Studies, Belgrade Serbia.

Zyber Global Events

The next Stay Safe Online Webinar by Zyber Global is due to take place on August 31, 2021 register now to attend.

Coming Soon:

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

"Education, again, should be a key for the future. All citizens need to get some awareness about IT security and implement some daily "digital hygiene".

YVES VANDERMEER

CHAIRMAN, EUROPEAN CYBERCRIME TRAINING AND EDUCATION GROUP, BRUSSELS, BELGIUM

Zyber Spotlight

YVES VANDERMEER
Chairman, European Cybercrime Training and Education Group, Brussels, Belgium

Mr. Vandermeer is a dedicated educator and innovator in the field of cybercrime. He has designed many tools and processes to assist Law Enforcement Agencies in their quest to stop cybercriminals. He is an avid photographer!

Can you tell us about yourself and your journey to where you are today?

In the eighties, I applied to become a police officer in the Belgium Gendarmerie. Prior to this I taught mathematics.

After a few years in the Belgium Gendarmerie, I became an instructor in the school for ranked officers. During the nineties, the Gendarmerie created the Digital Forensics Unit to support serious crimes investigations which I immediately applied for as I was already developing software as a hobby in my free time. At that time, we were four geeks supporting all major investigations in the country. Due to the lack of standards and financial resources, we developed our "home-made" software tools and started to define the digital forensic processes trying to follow the evolution of the technology like, for example, the Live Data Forensics. When the police forces merged in 2001, I continued to work in the newly created Federal Computer Crime Unit. I honed and improved my expertise in file systems and computer networks. In the meantime, I started sharing my experience and knowledge during internal training activities.

In 2009, the University College of Dublin organised an MSc in Computer Forensics and Cybercrime Investigations, under the aegis of the "Falcone" EU funded project. I, along with 30 other colleagues from EU Member States, Law Enforcement Agencies successfully completed the course.

Later on, I was appointed to represent Belgium in the European Cybercrime Training and Education group and was subsequently elected its Chair in 2013, taking over from Paul Gillen who was one of the founders of the group.

I also lecture on Digital Forensics and Cybercrime at the Norwegian Police University College having left the Belgian Federal Police in 2017.

As a former police officer in the Federal Computer Crime Unit, Belgium, can you share some of the challenges you faced in investigating cybercrime and how you overcame them.

Initially, I was involved in all types of serious crimes investigations, including child abuse, corruption and terrorist cases. Later on, hacking and cyber-attack cases took a bigger part of my duties.

Besides the complexity of some infrastructures, the primary stress factor is time. Electronic evidence may deliver an impressive amount of investigation clues but it can be highly volatile, and some early countermeasures taken by the victim or the suspect can compromise it.

We were able to overcome the time challenge, at least partially, by working in small but strongly coordinated teams and applying flexible processes adapted to the IT and criminal context. On the crime scene, the salt grain, often linked with human behaviour, may compromise all that was earlier professionally planned

In my opinion, teamwork is the best approach, as it allows us to share the tasks and improve the quality of the investigation.

What is the European Cybercrime Training and Education Group (ECTEG) and what does it do?

ECTEG, initially named "Europol Working Group on the Harmonisation of Cybercrime Investigation Training", was created in 2007 by Law Enforcement and University representatives supported by Europol. The founders were "believers" that something needed to be done to improve the quality and access to cybercrime training materials.

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

Zyber News Roundup

Scammers offer streaming services, giveaways, and a fake cyber currency to cash in on the Olympic Games

Kaspersky experts analyzed Olympic-related phishing attacks and found fake pages offering streaming services, tickets to events that won't have spectators, and even a fake Olympic Games virtual currency.

Olga Svistunova, a security expert at Kaspersky, said that cyber criminals always use popular sports events as bait for their attacks. Security experts recommend that security teams recognize this standard tactic and incorporate an awareness of current events into threat monitoring. Even under the unusual circumstances of this year's games, bad actors have found a way to use the event to their advantage.

"For example, this year, we discovered an interesting phishing page selling an 'Olympic Games Official Token,'" Svistiunova said. "There is no real equivalent of such a thing, that means that cybercriminals are not only faking already existing baits but also coming up with their own new sophisticated ideas."

Security experts found a website selling a virtual currency that is supposed to be a support fund for Olympic athletes. The lure is financial help for an athlete in need but there is no official Olympic token. The only person who benefits is the scammer.

Kaspersky's analysis found several creative ways scammers are taking advantage of the buzz around the Olympic Games.

Kaspersky experts also found phishing pages disguised as official Olympic websites. Scammers looking to capitalize on interest in the Olympics create fake pages that look official and connected to the International Olympic Committee.

Read more:

https://www.techrepublic.com/article/scammers-offer-streaming-services-giveaways-and-a-fake-cyber-currency-to-cash-in-on-the-olympic-games/

EU Proposes Law to 'Ensure Full Traceability' of Crypto Transfers, Ban Anonymous Wallets

The European Commission presented a set of legislative proposals aimed at strengthening the EU's anti-money laundering and countering terrorism financing (AML/CFT) rules. Among the proposals is a revision of the 2015 Regulation on Transfers of Funds "to trace transfers of crypto-assets."

The proposals take into account "new and emerging challenges linked to technological innovation," including "virtual currencies, more integrated financial flows in the Single Market and the global nature of terrorist organisations," the Commission explained.

At the heart of the proposed legislative package is the creation of a new "EU-level Anti-Money Laundering Authority (AMLA)." It will be "the central authority coordinating national authorities to ensure the private sector correctly and consistently applies EU rules."

The proposals also include "full application of the EU AML/CFT rules to the crypto sector."

Read more:

https://news.bitcoin.com/eu-proposes-law-to-ensure-full-traceability-of-crypto-transfers-ban-anonymous-wallets/

The world's top ransomware gangs have created a cybercrime "cartel"

Several of the largest Russian ransomware cybercriminal gangs have partnered up and are sharing hacking techniques, purloined data-breach information, malware code, and technology infrastructure.

Hacking groups frequently collaborate, break up, shut down, rebrand, and regroup. Several groups in the so-called cartel cluster announced a collaboration in July 2020, then disbanded in November.

The new cluster of gangs is potentially more powerful, DiMaggio (Chief Security Strategist at Analyst1) said, because of its links to other threat actors in the cybercriminal ecosystem.

Continue reading:

https://www.cbsnews.com/news/ransomware-cybercrime-cartel-wizard-spider-viking-spider-lockbit-twisted-spider/

Zyber Focus

Darknetlive

Professor Zvonimir Ivanovic
University of Criminal Investigation and Police Studies, Belgrade Serbia.

Introduction

The darknet (or Dark Net or Dark Web) is a network that can only be accessed with specific software, configurations, or authorization, it is not reachable through standard browsers and/ or search engines, and is often using non-standard communications protocols. Almost all sites on the so-called darknet hide their identity using the Tor encryption tool.

Because of the anonymity of the browsing experience on the darknet many people use it to engage in activities that are semi-legal or illegal. Activities such as buying and selling drugs, weapons, and pornography are common on the darknet.

Tor is a free software for enabling anonymous communication. The name Tor is an acronym derived from the original software project name The Onion Router. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of thousands relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.

Onion routing is implemented by encryption, nested like the layers of an onion, used to anonymize communication. Tor encrypts the original data, including the destination address, multiple times and sends it through a virtual circuit comprising successive, randomly selected Tor relays.

The most common uses for websites on Tor hidden services are “criminal, including drugs, illicit finance and pornography involving violence, children and animals.”

ANITA Horizont 2020 Project

The Darknet is so prolific in its nefarious activities that, there are many on-going projects in the EU dedicated to developing new tools to equip the law enforcement agencies (LEAs) to bring down these websites.

One such project is the ANITA H2020, which is aimed at improving the investigation capabilities of LEAs by delivering a set of tools and techniques to efficiently address online illegal trafficking of counterfeit/falsified medicines, New Proactive Substances, drugs, and weapons.

This is achieved through appropriate knowledge modelling and reasoning services; discovery and monitoring of new and existing online marketplaces; resolving criminal identities in social networks and web and identification of authors and web contents; unmasking of fake information, disinformation and camouflage of the real nature of information; insights on criminal groups relevant and related to trafficking of illegal products; discovery and understanding of trends and behavioural patterns; revealing, tracking, and monitoring of payments and transactions in crypto-currency networks;

interoperability with available relevant investigation systems already in place and operation at and for LEAs. This will support the LEAs in more effective investigation activities by using online contents and information obtained under a lawful warrant (see https://www.anita-project.eu/)

The ANITA Horizont 2020 Project aims are:

- To boost the Law Enforcement’s investigation process and to significantly increase their operational capabilities; and
- To significantly facilitate the novice officers training process and to optimise the learning curve.

This project uses an online and offline platform for different searches and intelligence gathering data, and also for the investigation management and chain of evidence preserving. The platform, which is the basis of the project, has already been provided for certain LEAs which enables the activation of different tools beneath the platform. Tools include instant translation text to text; speech to text and even picture or video to text; image and video annotation; text writer profiling; knowledge graph and intelligence; trends analysis of criminal activities on the dark net; blockchain analysis; and scrapping of the darknet markets with offline and online analysis of those, etc. These tools on the platform are used in real time, offline and online, and the real result is also provided with a possibility to export files in pdf or json form. This is done to have human reading interface for judges and prosecutors, and to be used in other forms of different commercial software products for forensics utilisation.

There are plans for training of the system or Artificial Intelligence to help in the training of the future police officers in using the platform. This is planned to be used in ‘eyes gaze’ analysis, and behaviour of the trainees to gather that information which is needed for the neural computing environment to create a base for help in future trainings. The platform is to be used in gathering information and providing analysis of the entities inputted in the system and proposing connections and relations between entities through enforcing powerful tools beneath the platform.

Continue reading:
https://zyberglobal.com/my-blog

Zyber Global Events

The next **Stay Safe Online Webinar** by Zyber Global is due to take place on August 31, 2021. Register now to attend.

OTHER CYBERSECURITY EVENTS

DEF CON 29 **Las Vegas, Nevada** **USA** **August 5-8, 2021**	**30th Usenix Security Symposium** **Vancouver, BC** **Canada** **August 11-13, 2021**	**The 2021 International Workshop on Cyber Security (CSW 2021)** **Stockholm, Sweden** **August 13 - 15, 2021**
An extremely popular event in Las Vegas is DEF CON, one of the oldest and largest security conferences in the world. The conference begins each year when the sister event, Black Hat USA, ends, so you can expect many similar topics and themes. Previous DEF CONs offer: • Several tracks of speakers about computer- and hacking-related subjects; and • Cyber-security challenges and competitions, including their flagship, *Capture the Flag* game The event features speakers, contests, vendors, workshops, demo labs, and entertainment, not to mention plenty of opportunities to network with the world's top hackers and potentially get headhunted by government officials: federal law enforcement agents from the FBI, DoD, United States Postal Inspection Service, and other agencies regularly attend DEF CON.	The Usenix Security Symposium is a three-day virtual conference that includes dozens of refereed paper presentations and invited talks and various sessions about the latest advances in the security and privacy of computer systems and networks. The event brings together researchers, practitioners, system administrators, system programmers, and others to share and explore the latest advances in the security and privacy of computer systems and networks. Keynote Address: **Susan Landau,** Bridge Professor in Cyber Security and Policy at The Fletcher School and the School of Engineering, Department of Computer Science, Tufts University and Visiting Professor, Department of Computer Science, University College, London.	The purpose of the CSW 2021 is to have in-depth discussions on Cyber Security. We intend to bring together some of the leading international research leaders, thought leaders, scholars, and others interested parties, involved in Cyber Security, to provide a platform for real information exchange and advancement of the field of Cyber Security. It is now well accepted that Cyber Security must be approached from a multi-disciplinary angle – from the technical sciences like Computer Science and Engineering to the human sciences like Psychology, Education, and human behavior. Solutions to create real cybersecurity resilience will have to include all such disciplines, and such new solutions are urgently needed. During the conference, we will have keynote speeches, plenary lectures, and research contributions reflecting the newest developments in Cyber Security and Cyberspace.
For further information: https://defcon.org	For further information: https://www.usenix.org/conference/usenixsecurity21	For further information: http://www.cybersecurityworkshop.org

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