Zyber Global

JULY 2021 | ISSUE 12

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 12th Edition, July 2021 of Zyber Global Centre's Monthly Newsletter.....

Here in the U.K, we are patiently awaiting the end of the 'lockdown' period on 19 July 2021. Things do seem to be opening up slowly.

I recently attended (online, of course) a two-day consultation meeting held by the Global Forum on Cyber Expertise (GFCE). https://thegfce.org

The GFCE is a multi-stakeholder community and its aim is to strengthen cyber capacity and expertise globally. I attended sessions on capacity building in Africa and Europe. Some really great aspirational ideas were shared and I am looking forward to seeing how we can all help make them a reality.

Do write in and let us know what topics you would like to see discussed in the August newsletter. We appreciate your feedback!

In the meantime, keep safe

ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Spotlight

The interview spotlight this month is on Matteo Lucchetti, Direttore Operativo, Cyber 4.0

Zyber News

We have a roundup of the latest international cybercrime news.

Zyber Focus

The focus this month is on Ransomware and whether paying ransoms should be made illegal by the Head of Research, Arsha Gosine.

Zyber Global Events

The next Stay Safe Online Webinar by Zyber Global is due to take place on July 30, 2021 register now to attend.

Coming Soon:

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

"In order to successfully combat Cybercrime, we need the three C's: commitment, capacity, and co-operation at both the national and international level "

MATTEO LUCCHETTI

DIRETTORE OPERATIVO,CYBER 4.0

Zyber Spotlight

MATTEO LUCCHETTI, DIRETTORE OPERATIVO, CYBER 4.0

Mr. Lucchetti brings a wealth of experience and knowledge in building creative and innovative solutions to combat cybercrime in both the private and public sectors of cybersecurity.

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

I have been working in the field of cybersecurity and cybercrime for almost 20 years.
I started my journey in the private sector in Italy: at the Italian Banking Association first, where I was in charge of the Italian FI-ISAC, and then Poste Italiane, where I was responsible for the cybersecurity competence center and worked on the start-up of the company's CERT. In this period I also acted as technical leader of the European Electronic Crime Task Force, an information-sharing initiative promoted by the Italian Ministry of Interior and the United States Secret Service.
I then moved to international organizations: first the European Union Agency for Fundamental Rights, based in Vienna, where I worked on data protection issues related to the surveillance programs implemented by intelligence agencies in the EU, and then the Council of Europe, as Programme Manager Cybercrime at the Cybercrime Programme Office based in Bucharest, leading the GLACY+ Project. With time GLACY+ has become a sort of brand, so many might know this already: GLACY+ is a capacity-building initiative co-funded by the European Union and the Council of Europe, whose goal is to strengthen the global criminal justice response to cybercrime by advising on domestic legislation, strategies, and policies, enhancing capacities of judicial authorities, prosecutors and law enforcement officers, developing partnerships with national, as well as regional and international counterparts. I will tell more about it in this interview.
This year, I decided to take a sabbatical from the Council of Europe and return to Italy as I was offered the post of Director of the National Competence Center on Cyber Security, named CYBER 4.0.
I hold a Ph.D. in Systems Engineering, an MSc in Electronic Engineering, and an MSc in Cyber Security, respectively from the Sapienza University of Rome and the Royal Holloway University of London.

Is there a link between Cyber 4.0 and your previous role in capacity building at the Council of Europe?
Definitely. Although the reference target of the action is different, as in the former role it was the criminal justice sector, and in the current role it is the private and public sector working in the cybersecurity field when it comes to training and advisory activities the methodological approach is very much the same. At CYBER 4.0 we aim at developing a train the trainers' approach, through a curriculum of courses that will span from introductory to advanced levels, including specialized technical modules. Similar to what has been done at the Council of Europe, we just finalized the creation of a roster of experts that will support us in the making and the delivery of such programs, until sufficient capacities will have been built within the community of our stakeholders, which could continue delivering the relevant materials to their peers.
Also, we are trying to develop a coherent approach for the international accreditation of the Center and cooperation with similar entities, and we'll do that through the networks that have been established for this purpose in the global community, such as the GFCE and the EU CyberNet Project.

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

Zyber News Roundup

Cyber-Attacks Are Primary Funding Source for North Korea

Cybercrime is now the primary means by which the North Korean state is funded, according to researchers at Venafi.

The security vendor's threat intelligence specialist, Yana Blachman, and her team analyzed publicly available information on state-sponsored attacks directed by the hermit kingdom over the past four years.

They concluded that the Asian dictatorship now monetizes cyber-attacks to circumvent economic sanctions and keep the Kim Jong-un regime alive.

However, global democracies must take more assertive action to mitigate the cyber-threat from North Korea or risk the funding model being exported to Myanmar, Belarus and other countries shunned by the international community, Blachman warned.

In 2019, the United Nations issued a report claiming that the Kim regime had managed to generate as much as $2 billion from attacks on banks and cryptocurrency exchanges, in part to raise money for its nuclear weapons program.

Read more: https://www.infosecurity-magazine.com/news/cyberattacks-primary-funding-north/

'Pen tester' FIN7 hacking group member lands seven-year prison term

A "high-level" member of FIN7 has been sentenced to a seven-year term for his role in the cybercriminal group.

On Thursday, the US Department of Justice (DoJ) named Andrii Kolpakov, a 33-year-old from Ukraine, as a past member of FIN7 who served as an attacker internally referenced as a penetration tester.

According to US prosecutors, Kolpakov was involved in FIN7 from at least April 2016 until his arrest in June 2018, when he was picked up by law enforcement in Spain and extradited to the United States a year later. The former hacker managed teams of attackers responsible for compromising the security of target systems, including businesses in the US.

FIN7, also sometimes referred to as Carbanak, specialized in the theft and sale of consumer records from Point-of-Sale (PoS) systems from companies. The malware used by the group would be used to harvest payment card details that were then used to conduct fraudulent transactions or were sold on.

The DoJ estimates that in the US alone, over 6,500 PoS systems at more than 3,600 business locations were infiltrated by FIN7, leading to the theft of tens of millions of debit and credit cards, as well costs of over $1 billion that had to be shouldered by victims.

In June 2020, Kolpakov pleaded guilty to one count of conspiracy to commit wire fraud and a further count of conspiracy to commit computer hacking. He has now been sentenced to seven years in prison and has been ordered to pay $2.5 million in restitution.

Read more: https://www.zdnet.com/article/pen-tester-fin7-hacking-group-member-sent-behind-bars-for-seven-years/

Cyber Security in the Crypto World

A number of crypto-currencies have been the victim of ransomware attacks by hackers and some like Ethereum Classic and ZenCash have lost $millions because of blockchain security problems.

Blockchain has grown rapidly in recent years, but it is not immune to security attacks. Because of the way blockchain works, the data on the chain is potentially viewable by all users and this can lead to both security and privacy issues.

Bitcoin is basically an online currency, it is intangible and decentralised and no government has control over it. Every bitcoin is stored in a "digital wallet" and it uses blockchain technology where every single transaction is recorded there and although blockchain technology is very secure in theory, it is estimated that 33% of Bitcoin trading platforms have been hacked.

The problem of security comes from the use of keys and the transactions on the blockchain. A key is a set of letters and numbers that is the unique correspondence for your Bitcoin. It is secure, but once you put it into a Bitcoin wallet or on a trading platform, the security of that platform becomes vital. If someone accesses the key, the currency can be removed elsewhere. Hackers can target this security flaw and use it as a method to steal the money.

Read more:
https://www.cybersecurityintelligence.com/blog/cyber-security-in-the-crypto-world-5701.html

Zyber Focus

Hacker Ransom Payment Debate

Recent articles on ransomware have highlighted a current debate on whether paying ransoms to hackers should be made illegal. We see that ransomware attacks can have a devastating impact (emotional and financial) on organisations, with victims requiring a significant amount of recovery time and substantial monies to reinstate critical services. These events can also be high profile in nature, with wide public and media interest.

Before we look at the arguments for and against, let us look at what is ransomware and how does it work.

The Oxford Dictionary defines ransomware as a type of malicious software designed to block access to a computer system until a sum of money is paid.

McAfee (an American global computer security software company) expands on this definition, saying that:

'Ransomware is malware that employs encryption to hold a victim's information at ransom. A user or organization's critical data is encrypted so that they cannot access files, databases, or applications. A ransom is then demanded to provide access. Ransomware is often designed to spread across a network and target database and file servers, and can thus quickly paralyze an entire organization. It is a growing threat, generating billions of dollars in payments to cybercriminals and inflicting significant damage and expenses for businesses and governmental organizations.'

While the Ransomware Task Force (RTF) (a U.S led team convened in early 2021, comprising a broad coalition of volunteer experts from industry, government, law enforcement, civil society, cybersecurity insurers, and international organizations) provides that:

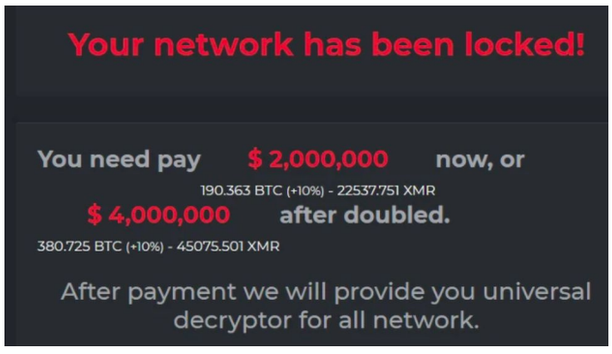
'Ransomware is not just financial extortion; it is a crime that transcends business, government, academic, and geographic boundaries. It has disproportionately impacted the healthcare industry during the COVID pandemic, and has shut down schools, hospitals, police stations, city governments, and U.S. military facilities.

It is also a crime that funnels both private funds and tax dollars toward global criminal organizations. The proceeds stolen from victims may be financing illicit activities ranging from human trafficking to the development and proliferation of weapons of mass destruction.

So let us have a look at how it works. Ransomware uses asymmetric encryption. This is cryptography that uses a pair of keys to encrypt and decrypt a file. The public-private pair of keys is uniquely generated by the hacker. The private key to decrypt the stolen files is usually stored on the hacker's server. The private key is only made available to the victim after the ransom has been paid, though as seen in recent ransomware incidents that has not always been the case. Without access to the private key, it is nearly impossible to decrypt the files that are being held for ransom.

Ransomware (and other malware) is usually distributed using email spam campaigns or through targeted attacks. Malware needs an attack vector to establish its presence on an endpoint. After its presence is established, malware stays on the system until its task is accomplished.

The ransomware drops into and executes a malicious binary on the infected system. This binary then searches and encrypts valuable files, such as Microsoft Word documents, images, databases, and so on. The ransomware may also exploit the system and network vulnerabilities to spread to other systems and possibly across entire organizations. Once files are encrypted, ransomware prompts the user for a ransom to be paid within 24 to 48 hours to decrypt the files, or they will be lost forever. If a data backup is unavailable or those backups were themselves encrypted, the victim is faced with paying the ransom to recover personal files. Often a message –see below- is plastered across the screen.



In February 2020, DarkSide, one of the many prolific ransomware groups held Colonial Pipeline Company, USA to hostage by disrupting the distribution of fuel in the United States.

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

Zyber Global Events

The next **Stay Safe Online Webinar** by Zyber Global is due to take place on July 30, 2021. Register now to attend.

OTHER CYBERSECURITY EVENTS

Policing Cybercrime Digital Conference **United Kingdom** **16 July 2021**	**Blockchain and Internet of Things Conference (BIOTC 2021)** **Vietnam** **8-10 July 2021**	**Black Hat USA 2021** **United States of America** **31 July – 5 August 2021**
Westminster Insight's Cybercrime Conference brings together cyber experts from law enforcement, government, criminal justice, private industry, international organisations, and academia to explore how we can respond to the rapidly evolving digital nature of crime. The law enforcement cybercrime network has expanded over recent years with the launch of regional and local force cybercrime units working in collaboration with the National Crime Agency's National Cybercrime Unit and GCHQ's National Cyber Security Centre. But more needs to be done to make progress in the pursual, investigation, prevention, and prosecution of cybercrime. Attend to hear about the latest cyber threats, trends, and strategies from a local level through to international serious and organised crime. Explore the role the police play, how they work with others, and the way the police service is organised, in order to meet the evolving digital threat.	The 3rd Blockchain and Internet of Things Conference (BIOTC 2021) aims to provide a forum for researchers, practitioners, and professionals from the industry, academia, and government to discourse on research and development, professional practice in Blockchain, and the Internet of Things. BIOTC 2021 will be held in Ho Chi Minh City, Vietnam during July 8-10, 2021. Scholars and researchers working in the field of Blockchain and the Internet of Things from all over the world are expected to attend the conference and share their experiences and lessons with other enthusiasts, and develop opportunities for cooperation.	Now in its 24th year, Black Hat USA is excited to present a unique hybrid event experience, offering the cybersecurity community a choice in how they wish to participate. Black Hat USA 2021 will open with four days of Virtual Trainings (July 31-August 3) conducted in real-time online, with all instructors accessible throughout each class. The two-day main conference (August 4-5) featuring Briefings, Arsenal, Business Hall, and more will be a hybrid event—offering both a Virtual (online) Event and a Live, In-Person Event in Las Vegas.
For further information: https://westminsterinsight.com/event/3632/Policing_Cybercrime_Digital_Conference	For further information: http://www.biotc.net/index.html	For further information: https://www.blackhat.com/us-21/

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