Zyber Global

JULY 2022 | ISSUE 24

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 24th Edition, July 2022 of Zyber Global Centre's monthly newsletter.

I am excited because I am presently working on a Council of Europe iProceeds -2 project targeting crime proceeds on the Internet and securing electronic evidence in South-East Europe and Turkey. I am working with several international cybercrime / cyber security experts, as we are designing and developing the "Mock Trial of an International Ransomware Attack Exercise" to be delivered this month. This is a practical exercise which is very topical for today as it allows the delegates to investigate a ransomware attack that has an international component.

On a sad note, I am mourning a colleague and friend who was active in the international fight against cybercrime Mr Gnanasihamani Kannan. Mr Kannan was the Senior State Counsel, and Senior Director of the Crime Division at the Attorney-General's Chambers in Singapore. I first met Mr Kannan many years ago when I was a Senior Prosecutor and Policy Advisor with the Crown Prosecution Service in London.

I highly valued my discussions on cybercrime over the years with Mr. Kannan as he was always very knowledgeable on most things related to cybercrime and it was a joy to discuss new initiatives etc with him.

I always looked forward to meeting him at the Council of Europe Octopus Conference in Strasbourg. I send my deepest sympathy and caring wishes to his family and colleagues. May he rest in peace!

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

Its summer here in the United Kingdom. The school academic year ends this month, and school holidays begin. I wish everyone planning to travel with their family over the holidays a safe journey.

Don't forget to read our roundup of the latest international cybercrime news! The next Stay Safe Online webinar is on the 28 July 2022 so register now to attend. As usual do get in touch with anything you would like to see more of in the newsletter!

This Month's Features

Zyber Focus

This article is on '*Cyber-attacks on Critical National Infrastructure*'

Zyber News

We have a roundup of the latest international cybercrime news.

Zyber Global Events Information

A focus on forums/conferences around the world.

Istanbul- courtesy Falco - Pixaby

Zyber Focus Article

Cyber-attacks on Critical National Infrastructure

Arsha Gosine, Head of Research,
Zyber Global Centre

Petroleum Refinery
courtesy Carlos Rivadeneira - Pixaby

The rising and continuing danger of cyber-attacks on critical national infrastructure has enormous repercussions for the government and the public in terms of time, money and public confidence. Critical Infrastructure ("CI") is essential to a nation's economy and security. They are usually range from national energy, health, transportation, information and rescue responders' services to private businesses. The CIs are usually targeted for ransomware and sometimes even for 'fun' i.e. because they (the attackers) can cause disruption at such a deep level.

In March 2020, a study on the worldwide status of industrial cybersecurity revealed that almost 3 out of 4 IT security experts are more concerned about cyber assaults on vital infrastructure than about data violation in their organisations.

Malware and ransomware are the most common means of carrying out cyber assaults on critical infrastructure and have been employed in a series of attacks worldwide, including the United States, Ukraine, Japan, and the United Kingdom.[1] All of this is in line with the 2020 World Economic Forum's Global Risk Report, which highlighted a surge in cyber assaults aiming at vital infrastructures such as energy, transportation, and health. The study's finding provides that public and private sectors alike are in danger of being held as hostages from attacks on CIs. It also stated that organized cybercrime organisations are linking with each other and currently have a probability of 0.05% of getting caught by the United States authorities.

Disrupting CIs has become the continual focus of some attackers. The first reported power outage occurred in December 2015 where three companies in the Ukraine were hit by BlackEnergy malware leaving hundreds of thousands of homes without electricity for six hours. This blackout was followed two months later by the news that the Israel National Electricity Authority had been the target of a cyber-attack. The system had to be shut down to prevent the spread of a virus.

Each year cyber-attacks on CIs continue to increase.

In February 2021, a Florida water treatment plant (the Plant) was unsuccessfully targeted by hackers. Sodium hydroxide added to the water supply was raised to poisonous levels. An operator noticed the discrepancy and took effective action. The attacker had exploited a dormant, password-controlled remote access software platform, compromising user credentials, gaining entry into the internet facing system and then moving laterally across the operational network.

The Plant had used multiple computers running an aged version of Microsoft Windows to monitor the facility remotely, and all of the computers shared a single password to access an apparently disused version of the plant's remote management software.

The revelations highlighted evidence of poor cybersecurity hygiene at the plant, whose unexpected compromise has raised awareness of the nation's vulnerability to industrial cyberattacks.

The former director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, Chris Krebs, said that the Oldsmar, Florida hack highlights how dire the challenge is. "Unfortunately, that water treatment facility is the rule rather than the exception," Krebs wrote in a column for The Hill. "When an organization is struggling to make payroll and to keep systems on a generation of technology created in the last decade, even the basics in cybersecurity often are out of reach." Cybersecurity experts have described the incident affecting Oldsmar, Florida, as a wake-up call.

The latest major hack occurred in May 2021, where a small group of hackers launched a ransomware attack on Colonial Pipeline (Colonial), which is the United States' largest pipeline network for the delivery of refined petroleum. This attack caused disruption and mayhem. Colonial had to shut its main lines for five days while they dealt with the issue. The repercussions were far-reaching. It affected any form of transport and prices for fuel sky rocketed.

CIs are the backbone of today's economic and social well-being. Improving their protection against cyber assaults has to become a priority of the authorities worldwide and a collaborative affair.

In the next article, we will go into more detail on the impact of cybercrime on the critical national infrastructure and the way ahead.

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

Zyber News Roundup

“Missing Cryptoqueen” hits the FBI’s Ten Most Wanted list

The US Federal Bureau of Investigation (FBI) famously maintains a Ten Most Wanted Fugitives list. Currently, nine of them are men, suspected of 22 different offences between them.

One of them, however, newly added and the only woman on the list, breaks the mould.

According to the FBI, Ruja Ignatova, widely known as the Cryptoqueen, and famously dubbed the “Missing Cryptoqueen” by the makers of a popular BBC podcast series:

...is wanted for her alleged participation in a large-scale fraud scheme. Beginning in approximately 2014, Ignatova and others are alleged to have defrauded billions of dollars from investors all over the world. Ignatova was the founder of OneCoin Ltd., a Bulgaria-based company that marketed a purported cryptocurrency. In order to execute the scheme, Ignatova allegedly made false statements and representations to individuals in order to solicit investments in OneCoin. She allegedly instructed victims to transmit investment funds to OneCoin accounts in order to purchase OneCoin packages, causing victims to send wire transfers representing these investments. Throughout the scheme, OneCoin is believed to have defrauded victims out of more than $4 billion.

Some of the henchpeople in the OneCoin crew have already been convicted of scam-related offences, including Ignatova’s brother, Konstantin Ignatov, who allegedly took over the reins of the OneCoin empire when his sister dropped out of sight in 2017.

The reward for information leading to her arrest is listed as “up to $100,000”.

Read more: **https://nakedsecurity.sophos.com/2022/07/01/missing-cryptoqueen-hits-the-fbis-ten-most-wanted-list/**

Channel Islands used to Launch Global Cyber-Attacks

Jersey is part of the Channel Islands, a British territory located in the English Channel close to the coast of France. Usually associated with its wealthy residents and low tax regime and a target for attack, it turns out the island is also being used as a base for cyber crime. Computers have recently been hijacked and used to launch cyber attacks against organisations in a number of different countries.

The Channel Islands see more than 10 million incoming cyber attacks every month. In particular, the islands' have frozen the assets of Russian banks and billionaires with close links to President Putin.

Now, the Jersey government’s Cyber Emergency Response Team, (CERT.JE) has said that recently 5 to 13 compromised Jersey IT machines have been used to target computers in the United States, Germany and Hungary, but so far it is not known who was behind the attacks.

CERT.JE also revealed that it is being expanded to counter an anticipated increase in cyber crime, driven by several factors, including the Russian invasion of Ukraine.

The Guernsey Financial Services Commission is urging firms to ensure they have sophisticated cyber security software in place should their systems come under attack.

Read more:
https://www.cybersecurityintelligence.com/blog/channel-islands-used-to-launch-global-cyber-attacks-6371.html

US watchdog is worried cyber insurance won't cover 'catastrophic cyberattacks'

The US government's cyber insurance only covers certain events and maybe not ones that could destroy IT systems.

The US Government Accountability Office (GAO) has called for a federal response to insurance for "catastrophic" cyberattacks on critical infrastructure. A functioning insurance market is essential for businesses, consumers and, as GAO highlights, for critical infrastructure operators.

The GAO, which audits the trillions of dollars the US government spends each year, warns that private insurers and the US government's official terrorism risk insurance -- the Terrorism Risk Insurance Program (TRIP) -- may not be able to cover catastrophic financial loss arising from cyberattacks.

“Cyberattacks may not meet the program's criteria to be certified as terrorism, even if they resulted in catastrophic losses. For example, attacks must be violent or coercive in nature to be certified," the GAO said.

Read more: **https://www.zdnet.com/article/us-watchdog-is-worried-cyber-insurance-wont-cover-catastrophic-cyberattacks/**

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

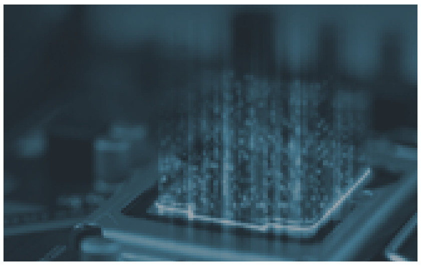
PhilSec Hybrid Event **July 12 - 13, 2022** **Manila, Philippines**	**The Future of Cyber Security** **Virtual Conference** **July 13 -14, 2022**	**Cyber Security for Government Summit 2022,** **July 26-28, 2022** **Hotel Swissôtel Sydney, Australia**
The National Cybersecurity Plan 2022 (NCSP) was created by the Philippines' Department of Information and Communications Technology (DICT) with the goal of making the country cyber secure. According to many projections, the government would need to spend more than $20 billion on cybersecurity between 2017 and 2025 to compete with "global best-in-class countries." Tradepass will host the 2nd edition PhilSec on July 12–13, 2022, to optimize DICT's efforts. The event will bring together 600+ cybersecurity specialists (both in-person and online), including the heads of information security, risk, compliance, forensics, and cyber law from the Philippines' biggest public and private companies.	COVID-19 has changed the workplace forever, with many firms saying they will implement more home working even after the pandemic is over. It can increase efficiency, but this approach also requires a greater focus on cyber security. As businesses continue to realise the benefits of remote working, cyber security has never been more important. The conference will feature topics relevant to the current COVID-19 working environment as a huge number of employees across all industries continue to work from home. There is no doubt that cyber-criminals are jumping on opportunities to exploit employees working remotely during coronavirus, and the number of cyber-attacks will continue to increase, according to Europol. Indeed, cyber-criminals are already profiting from the pandemic, with email phishing campaigns designed to steal employees' credentials and compromise business systems.	The Cyber Security for Government Summit offers an in-depth look at how national and international organisations are building their cyber-defences, in an increasingly vulnerable environment. The program offers practical knowledge to develop a cyber threat intelligence program as cyber-attacks escalate. This trend is highlighted by governments being warned to improve resilience in a heightened threat environment. The agenda also spotlights the action plan to build the government's cyber-resilience capability, together with a look at future cyber security funding, amendments to cyber security legislation, and cyber security policies across all tiers of government. The agenda is tailored for cyber and information security professionals directly responsible for protecting government assets, critical infrastructure, and data against malicious actors.
For further information: **https://philsecsummit.com**	For further information: **https://www.cybernewsgroup.co.uk/events/the-future-of-cyber-security-july/**	For further information: **https://publicspectrum.co/events/cyber-security-for-government-summit-2022/**

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