Zyber Global

JANUARY 2021 | ISSUE 6

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 6th Edition, January 2021 of Zyber Global Centre's Monthly Newsletter

Our team wishes you a very prosperous and happy New Year.

May this year be full of new achievements that will bring you success and prosperity. For us, at Zyber Global, the New Year means new opportunities. As the New Year approached, we took some time to reflect on our achievements in 2020.

This Month's Features

Zyber Spotlight

The interview spotlight this month is on Mr. Virgil Spiridon, Council of Europe

Zyber News

We also have a roundup of the latest international cybercrime news.

Zyber Focus

Sharing a blog from the International Monetary Fund (IMF).

Zyber Global Events

The next Stay Safe Online Webinar by Zyber Global is on the 28th of January 2021. Register now to attend.

Esther George, CEO Zyber Global Centre

" The Council of Europe is currently working with approximately one hundred and fifty (150) countries to set standards and measures and, to harmonise national laws so that there is a combined response to the threat of cybercrime....."

Virgil Spiridon
Head of Operations, Cybercrime Programme Office
Council of Europe

Continued from page 1.....

What went well and what lessons we learned that would help us to do better and be even more successful in 2021.
On a personal note, one of my goals is to read at least one non-fiction book a week. I guess you would have also done something similar and made your own resolutions.

Last month, I was in the process of writing an article covering the worst cyber threats experienced in 2020. When I heard of what is one of the worst hacks ever called “SolarWinds Breach”.

The SolarWinds Breach appears to be widespread especially in the USA, however, it’s probably best to assume that if your company was using SolarWinds Orion software last year (2020), you may also have been hacked. You can read more on the SolarWinds Breach in our roundup of the latest international cybercrime news.

Also, do let me know if you would like to hear more about the '*worst cyber threats experienced in* 2020'. I would be more than happy to include the article in a future newsletter, based upon your feedback. So do get in touch!!

In the meantime, we are back in lockdown in the UK, and I know it's the same for other countries. So to all our readers:
Be Well and Stay Safe.

ESTHER GEORGE
Editor and CEO Zyber Global Centre

Zyber News Roundup

SolarWinds: The more we learn, the worse it looks!!
In March of 2020, Americans began to realize that the coronavirus was deadly and going to be a real problem. What no Americans knew then was that at about the same time, the Russian government's hack of SolarWinds's proprietary software Orion network monitoring program was destroying the security of top American government agencies and tech companies. There were no explosions, no deaths, but it was the Pearl Harbour of American IT.
Russia, we now know, used the SolarWinds' hacked program to infiltrate at least 18,000 government and private networks. The data within these networks, user IDs, passwords, financial records, source code, you name it, can be presumed now to be in the hands of Russian intelligence agents. The Russians may even have the crown-jewels of Microsoft software stack: Windows and Office. While President Donald Trump has completely ignored the actions of Russian President Vladimir Putin's government, America's Cybersecurity Infrastructure and Security Agency (CISA) said the hacks posed a "grave risk" to US governments at all levels. Worse was revealed. Over the Christmas season holidays, the CISA said that all US government agencies must update to Orion's 2020.2.1HF2 version by the end of the year. If they can't, they must take these systems offline.
Why? Because yet another SolarWinds' Orion vulnerability was being used to install the Supernova and CosmicGale malware. This security hole, CVE-2020-10148, is an authentication bypass in the Orion API that allows attackers to execute remote code on Orion installations.

Continued on page 4.....

Zyber Spotlight

VIRGIL SPIRIDON
HEAD OF OPERATIONS
CYBERCRIME PROGRAMME OFFICE,
COUNCIL OF EUROPE

Virgil works tirelessly throughout the world, using his skills and practical expertise to assist countries in developing their practices and procedures to deliver a national and global response to the continuing threat of cybercrime.

Can you tell us a bit about yourself and your journey to where you are today in your career?

I am Romanian and I began my career in 1997 as a police officer in the Romanian Police Force. I worked in different areas building my experience in investigative techniques and then moved on to building capacity and developing policies and strategy in areas such as financial crimes and cybercrime.

In 2003, I was appointed as the Head of a Department with a newly formed Cybercrime Unit. The Central Unit started with three (3) persons and over the years, I built up and developed the Cybercrime Unit to respond proactively to cybercrime. I ensured that training was made available and appointed sections to deal specifically with crimes such as internet fraud, card payment fraud, and other cybercrime incidents.

On November 23, 2001, Romania signed the Budapest Convention on Cybercrime which came into force on September 1, 2004. This meant that a lot of work had to be done to ensure that legislation and policies were in place and that officers were well trained to respond and handle these types of cases from investigation to prosecution. To that end, I worked closely and collaboratively with international colleagues to obtain the best training and development in this area.

By the time I moved to the Council of Europe, the Unit had thirty-five (35) members of staff and there were fourteen (14) field offices with around two hundred (200) staff. The Cybercrime Unit now has the capacity to deal with every aspect of cybercrime and are often first responders to these types of crimes.

What are some of the challenges facing countries in cybercrime and cybersecurity?

Some of the challenges relate to the competence and capacity of countries to develop their legal and technical tools to access and preserve data.

Lack of resources; training on the different aspects of technology; the plethora of new devices on the market and the inability to investigate these; the many different software applications for online investigations; and the lack of legal instruments between the private sector and law enforcement.

I believe that a strong commitment is required from governments. They have to first recognise the havoc that cybercrime can wreak on societies and companies. They have to be aware of the ramifications and understand the havoc that cybercrime can unleash on society and ensure that they are a part of the conversation to put measures in place to respond to that ongoing threat.

For the full interview, see:
https://zyberglobal.com/my-blog

Zyber News Roundup

Zyber News RoundUp cont'd.....

Sen. Mark Warner (D-Virginia), ranking member on the Senate Intelligence Committee, told the New York Times the hack looked "much, much worse" than first feared. "The size of it keeps expanding."

Read more:
https://www.zdnet.com/article/solarwinds-the-more-we-learn-the-worse-it-looks/

Did you know that Phone scammers were able to get 270% more personal information in 2020 than in 2019!

The 2020 COVID-19 pandemic had a profound effect on Americans who inadvertently released sensitive, personal, and private information, and as a result, suffered financial loss.

First Orion's Annual Phone Scam Call Report exposed how scammers were able to get 270% more personal information in 2020 than they did in 2019.

Be it distraction or fear, people were providing sensitive information at an alarming rate; they were giving the bad actors their Social Security numbers and credit card information six times more frequently, year-over-year.

Whether it was someone looking for a light at the end of the dreary, isolative sheltering-at-home, or someone who is just hopeful, but vulnerable, financial theft was the most egregious. Scammers were most successful by using a ruse for COVID-19, prizes, awards, and student loans, or impersonating bank officials.

First Orion found that financial loss was reported as 20% of consumers disclosed their ages to scammers and 18% shared their bank information.

First Orion offered the following tips for consumers:

- Use whatever protection your mobile carrier offers, and consult with it about anything that is unclear.

.

- It may seem obvious, but don't answer phone numbers you don't recognize.
- A scammer benefits from a person's innate curiosity, concern about an emergency call they might be missing, or a job-related call they're waiting for.

.

- If you do accidentally answer a suspicious call, never, ever give personal information. Only do so if you know the caller is legit. You can visit the company's website to get the official number and call to speak with someone from the organization.

.

- But if you only realize after hanging up that you've likely given personal information to a scammer, there are verified non-profit organizations designed to help you after the fact. The Identity Theft Resource Center has a number of resources, including phone support.

Read more:
https://www.techrepublic.com/article/phone-scammers-were-able-to-get-270-more-personal-information-in-2020-than-in-2019/

Zyber Focus

Cyber Risk is the New Threat to Financial Stability by Jennifer Elliott and Nigel Jenkinson.

First published on December 7, 2020, on the website of the International Monetary Fund's (IMF) and reprinted here, courtesy Mr. Glenn Gottselig, Editor, IMF Blog
Link to the blog on the IMF website can be accessed here:
https://blogs.imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-financial-stability/

Many of us take for granted the ability to withdraw money from our bank account, wire it to family in another country, and pay bills online. Amid the global pandemic, we've seen how much digital connection matters to our everyday life. But what if a cyberattack takes the bank down and a remittance doesn't go through?

"***As we become increasingly reliant on digital financial services, the number of cyberattacks has tripled over the last decade and financial services continue to be the most targeted industry".***

As we become increasingly reliant on digital financial services, the number of cyberattacks has tripled over the last decade, and financial services continue to be the most targeted industry. Cybersecurity has clearly become a threat to financial stability. Given strong financial and technological interconnections, a successful attack on a major financial institution, or on a core system or service used by many, could quickly spread through the entire financial system causing widespread disruption and loss of confidence. Transactions could fail as liquidity is trapped, household and companies could lose access to deposits and payments. Under extreme scenarios, investors and depositors may demand their funds or try to cancel their accounts or other services and products they regularly use.

Hacking tools are now cheaper, simpler, and more powerful, allowing lower-skilled hackers to do more damage at a fraction of the previous cost. The expansion of mobile-based services (the only technological platform available for many people), increases the opportunities for hackers. Attackers target large and small institutions, rich and poor countries, and operate without borders. Fighting cybercrime and reducing risk must therefore be a shared undertaking across and inside countries.

While the daily foundational risk management work — maintaining networks, updating software and enforcing strong 'cyber hygiene' — remains with financial institutions, there is also a need to address common challenges and recognize the spillovers and interconnections across the financial system. Individual firm incentives to invest in protection are not enough; regulation and public policy intervention is needed to guard against underinvestment and protect the broader financial system from the consequences of an attack. In our view, many national financial systems are not yet ready to manage attacks, while international coordination is still weak. In new IMF staff research, we suggest six major strategies that would considerably strengthen cybersecurity and improve financial stability worldwide.

Cyber mapping and risk quantification
The global financial system's interdependencies can be better understood by mapping key operational and technological interconnections and critical infrastructure. Better incorporating cyber risk into financial stability analysis will improve the ability to understand and mitigate system-wide risk. Quantifying the potential impact will help focus the response and promote stronger commitment to the issue. Work in this area is nascent—in part due to data shortcomings on the impact of cyber events and modelling challenges—but must be accelerated to reflect its growing importance.

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

Zyber Global Events

Zyber Global's ***Stay Safe Online Webinar*** is Thursday 28th January 2021 at 1600 hours GMT. ***Register now to attend.***

OTHER CYBER SECURITY EVENTS

International Conference on Cybersecurity and Digital Forensics, Singapore January 11-12, 2021	**International Conference on Cybersecurity, Crime and Threats, Rome, Italy** January 18-19, 2021	**International Conference on Cybercrime, Cyberterrorism and Jurisdiction (ICCCJ) 2021.** **Sydney, Australia** January 28 -29 2021
This conference aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Cybersecurity and Digital Forensics. 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 Cybersecurity and Digital Forensics	This conference will provide 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 Cybersecurity, Crime and Threats .	This conference aims to bring together leading academic scientists, researchers, and research scholars to exchange and share their experiences and research results on all aspects of Cybercrime, Cyberterrorism and jurisdiction. 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 field of Cybercrime, Cyberterrorism and Jurisdiction
For further information: https://waset.org/cybersecurity-and-digital forensics-conference-in-january-2021-in-singapore	For further information: https://waset.org/cybersecurity-crime-and-threats-conference-in-january-2021-in-rome	For further information: https://waset.org/cybercrime-cyberterrorism-and-jurisdiction-conference-in-january-2021-in-sydney

Zyber Global Online Events

Our Online Courses with INsig2
Sign up now at https://insig2-and-zyberglobal.learnworlds.com/
For an extra 15% off use coupon code ZYBER
during checkout.

Courses per sectors

Legal Entities
Judges, lawyers and public prosecutors
Customized courses for legal entities on deeper aspects of digital forensics and forensic value of the evidence while collecting, processing, and presenting digital evidence in criminal and administrative proceedings. a subheading

Law Enforcement
First responders, forensic investigators and analysts
Customized courses for law enforcement officials on procedures, techniques, and tools used in digital forensic analysis and how to apply them in their forensic investigations.

Private Sector Corporations and small businesses.
Customized courses for various 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 Reading
- Quiz after each chapter
- Case study final exam

At the end of each course, you will be issued a completion e-certificate which is immediately printable for your records. Certificates brings you CPD (Continuing Professional Development), CPE (Continuing Professional Education), CLE (Continuing Legal Education) points. The number of points depends on the course.

Discounts

Use the code **ZYBER** and get 15% off on your first-time purchase.
Special discount for groups of 10+ participants on all courses. The bigger the group, the bigger the discount.

Bundles

Stay on your digital forensics learning path and get the most from your e-learning experience by using course bundles. https://bit.ly/3lNRYsj

Free Courses
Password Management

The course covers different lock security methods, guidelines on securely storing your passwords, various password managers and how to use them
https://bit.ly/3eMu7FD