Zyber Global

JULY 2023 | ISSUE 36

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome cyber sleuths to Zyber Global Centre's monthly newsletter - sizzling July 2023, the 36th edition!

The weather here has been hot and sunny, and I am hoping for more of the same this month.

June was a busy month for cybercriminals and as we surf the waves of this digital ocean, we are finding more cyber sharks ready to take a byte (pun absolutely intended) out of our tranquility. In June, our tales of digital derring-do took us from the chaos of the MOVEit cyber-attack (making its victims wish they had moved it to a more secure platform) to the spin cycle of the SpinOk malware (turning Androids into little green men of mischief).

But seriously, the MOVEit cyber-attack orchestrated by the ransomware gang Clop was a major security incident that resulted in significant data breaches across multiple companies. Those impacted included PricewaterhouseCooper, Ernst and Young, Health Service Ireland, and payroll provider Zellis. The attackers exploited a zero-day vulnerability within the MOVEit infrastructure, which allowed them to infiltrate various networks and steal sensitive data. Notably, Clop attempted to ransom the victims by threatening to release their data unless a certain amount was paid, resulting in multiple corporate information being posted on the darknet.

We are here to ensure you are up-to-date, and ready to tackle the online outlaws of our interconnected world. So, buckle up and log in, so that together, we can tackle these challenges head-on and create a safer cyber environment for all.

Do let us know what topics you would like to see discussed in the next newsletter. Keep safe!

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Focus Article
Why Transparency is required in Reporting Ransomware

Zyber News
We have a roundup of the latest international cybercrime news.

Zyber Global Events Information
A focus on forums/conferences around the world.

"Everybody should want to make sure that we have the cyber tools necessary to investigate cyber crimes, and to be prepared to defend against them and to bring people to justice who commit it."

Janet Reno
Former Attorney General of the United States

Zyber Focus Article

Transparency in Reporting Ransomware

by Arsha Gosine, Head of Research, ZGC

Over the years, we have seen a massive rise in ransomware cases where the ransom is usually paid to avoid leakage of personal data. Many companies feel that it is easier to pay the ransom rather than suffer the wrath of their customers or incur low public confidence which will impact on their business. There are many myths surrounding the reporting of cybercrimes. In this article we debunk some of those myths and show why being transparent is key.

In the United Kingdom (UK), the National Cyber Security Centre (NCSC) and the Information Commissioner's Office (ICO) while separate in their approach, with different responsibilities, both work on cyber incidents that can take down businesses, severely impact national services and infrastructure, and massively disrupt people's day-to-day lives. Both the NCSC and the ICO collaborate to help and support victim companies and organisations.

The NCSC is not a regulator; it provides support to victim organisations in confidence and does not share information about an incident with the ICO without an organisation's express consent. While any breaches of security should be reported to the ICO.

The NCSC and the ICO have identified six misconceptions which discourage companies and organisations from reporting cybercrimes, mainly ransomware. The NCSC and the ICO are both very concerned about the cybercrime incidents which remain unreported because they say that no-one gets to learn from them and they are urging companies and organisations to contact them to seek advice and support. The ICO has also said that they will be favourable to regulatory reports.

So let us look at the six main misconceptions which have been identified as:

1. If I cover up the attack, everything will be ok.
2. Reporting to the authorities makes it more likely your incident will go public.
3. Paying a ransom makes the incident go away.
4. I've got good offline backups, I won't need to pay a ransom.
5. If there is no evidence of data theft, you don't need to report to the ICO.
6. You'll only get a fine if your data is leaked.

Eleanor Fairford, NCSC Deputy Director for Incident Management, said:

"*The NCSC supports victims of cyber incidents every day, but we are increasingly concerned about the organisations that decide not to come forward. Keeping a cyber attack secret helps nobody except the perpetrators, so we strongly encourage victims to report incidents and seek support to help effectively deal with the fallout. By responding openly and sharing information, organisations can help mitigate the risk to their operations and reputation, as well break the cycle of crime to prevent others from falling victim.*"

Myth 1: If I cover up the attack everything will be okay.

How could everything be okay if a company or organisation covers up a ransomware attack and pays off the cybercriminals? The message that is being sent to these cybercriminals is that it is okay to do this and to continue to do so because it is is easy money. Where there is no reporting, no investigation, no information sharing, these attacks will continue to occur and there will be no way to find these cybercriminals. Companies and organisations should be aware that t the NCSC has CISP to facilitate information sharing between organisations, as well as sector information exchanges (IEs) and other trust groups. Keeping a cyber incident hush hush only benefits the cybercriminals.

Myth 2: Reporting to the authorities makes it more likely your incident will go public.

If an organisation experiences a cyber attack, reporting it to the NCSC or law enforcement means that they can access the wealth of advice and support available. One of the responsibilities of NCSC Incident Management is to provide direct support to affected organisations where there is a national impact and working with the appointed incident response provider. The NCSC respects confidentiality and do not proactively make information public, or share it with regulators without the organisations' consent. In fact, the NCSC has extensive communications support available to help navigate the incident and to manage media coverage and active communications.

Myth 3: Paying a ransom makes the incident go away.

In a ransomware attack, the files and computers are usually encrypted, the data is stolen and the organisation has to pay a large sum of money to get back the data. and the decryption key. The decryption process can be lengthy and cumbersome – attackers sometimes accidentally double-encrypt data meaning it can't be decrypted, or data is deleted so then is unrecoverable. In one case, restoration from backups was actually quicker than using the decryption key itself. The NCSC says that paying a ransom is basically accepting a pinky promise from criminals that they will decrypt your network or not leak stolen data. Nothing is guaranteed and one should bear in mind that organisations that pay the ransom are likely to be targeted again. Estimates vary but it's suggested that around one third of all organisations affected by ransomware are attacked again. It's basically rewarding criminals for their efforts and makes it more likely they'll carry out more attacks against other organisations, ultimately making the broader threat landscape worse. The ICO's point of view is that paying ransoms doesn't reduce the risk to individuals, it's not a mitigation under data protection law, and isn't considered a reasonable step to safeguard data.

In conclusion, the message from the NCSC and the ICO is **'Don't succumb to their (cybercriminals) techniques! Seek support and communicate early to avoid an investigation later into an incident you tried to hide. Don't feed the cycle! '**

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

Zyber News Roundup

2,700 people tricked into working for cybercrime syndicates rescued in Philippines

Philippine police backed by commandos staged a massive raid on Tuesday and said they rescued more than 2,700 workers from China, the Philippines, Vietnam, Indonesia and more than a dozen other countries who were allegedly swindled into working for fraudulent online gaming sites and other cybercrime groups.

The number of human trafficking victims rescued from seven buildings in Las Pinas city in metropolitan Manila and the scale of the night-time police raid were the largest so far this year and indicated how the Philippines has become a key base of operations for cybercrime syndicates.

Cybercrime scams have become a major issue in Asia with reports of people from the region and beyond being lured into taking jobs in countries like strife-torn Myanmar and Cambodia. However, many of these workers find themselves trapped in virtual slavery and forced to participate in scams targeting people over the internet.

Brig. Gen. Sydney Hernia, who heads the national Philippine police's anti-cybercrime unit, said police armed with warrants raided and searched the buildings around midnight in Las Pinas and rescued 1,534 Filipinos and 1,190 foreigners from at least 17 countries, including 604 Chinese, 183 Vietnamese, 137 Indonesians, 134 Malaysians and 81 Thais. There were also a few people from Myanmar, Pakistan, Yemen, Somalia, Sudan, Nigeria and Taiwan.

Workers were lured with high salary offers and ideal working conditions in Facebook advertisements but later found out the promises were a ruse, officials said.

Read more:
https://abcnews.go.com/Technology/wireStory/philippine-police-raid-alleged-cybercrime-buildings-rescue-2700-100404991

UK hacker busted in Spain gets 5 years over Twitter hack and more

The Twitter hack happened in July 2020, when a small group of cybercriminals ended up in control of a small number of Twitter accounts and used them to talk up a cryptocoin fraud. The accounts included Bill Gates, Elon Musk, Kanye West, Joe Biden, Barack Obama, Jeff Bezos, Mike Bloomberg, Warren Buffett, Benjamin Netanyahu, Kim Kardashian, and Apple. One of the suspects in that case was Joseph O'Connor, then 21, who wasn't in the US, and who eluded US authorities for a further year until he was arrested on the Costa del Sol in Spain in July 2021.

O'Connor was extradited to the US in April 2023, pleaded guilty in May 2023, and has now been sentenced. He wasn't convicted only of the Twitter cryptocoin scam he was convicted of multiple offences: conspiracy to commit computer intrusions, conspiracy to commit wire fraud, conspiracy to commit money laundering, making extortive communications, stalking, and making threatening communications.

He received a five-year prison sentence, followed by three years of supervised release, and he was ordered to pay $794,012.64 in forfeiture.

Read more:
https://nakedsecurity.sophos.com/2023/06/26/uk-hacker-busted-in-spain-gets-5-years-over-twitter-hack-and-more/

DOJ Falters on Prosecution of Cybercrimes Due to Unequal Application of the Computer Fraud and Abuse Act

The recent policy changes by the U.S. Department of Justice (DOJ) regarding selective prosecutions under the Computer Fraud and Abuse Act (CFAA) have inadvertently broadcasted limitations in the DOJ's ability to handle multiple cases simultaneously. The CFAA, enacted in 1986, aimed to mitigate cybercrimes by criminalizing unauthorized access to computers. Its broad applications include penalizing hackers and addressing insider threats where employees exceed their authorized access or continue access after their employment has ended.

However, recent DOJ announcements imply that defendants will not be charged in some "exceeds authorization" cases, barring exceptions, leading to criticism about the overbroad and vague nature of the policy, and raising concerns about the potential implications on industrial security and deterrence of cyber theft.

Two similar cases in the real estate and entertainment industries (CREXi and Ticketmaster respectively) expose the seemingly unequal enforcement of the CFAA. While the DOJ intervened with criminal charges against Ticketmaster for unauthorized access to a competitor's computer, the CREXi case, despite a comparable fact pattern, has seen no such intervention.

This selective application of the new policy seems to extend to the DOJ's strategy towards foreign actors, with inconsistent handling of cases involving theft of American companies' intellectual property. This inconsistency and lack of clarity in enforcement of the CFAA threatens industrial security in the face of escalating domestic and international cybersecurity threats.

Read more:
https://ipwatchdog.com/2023/06/24/doj-falters-prosecution-cybercrimes-due-unequal-application-computer-fraud-abuse-act/id=162647/

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

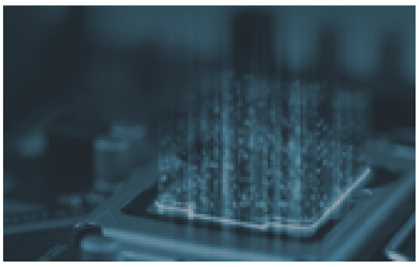
Internet 2.0 Conference USA 2023 **Nevada, Las Vegas USA** **10 July 2023**	**Data Connect Conference** **Columbus, OH** **20-21 July 2023**	**International Conference on Digital Forensics and Cyber Crime** **Zurich, Switzerland** **24 - 25 July 2023**
Internet 2.0 is a term used to characterize the future version of the internet, which is more intelligent, more connected, and more secure. The conference will address the problems and opportunities given by Internet 2.0. The conference delves into a wide variety of subjects, some of which include blockchain, artificial intelligence, cybersecurity, and the Internet of Things (IoT), amongst others. Internet 2.0 Conference is the place to be if you have an interest in gaining knowledge about the most recent issues of concern, such as the use of big data, AI, and NLP in enhancing the customer experience; cybersecurity scams; and ways to identify, report, and prevent spam and fraudulent activities in the tech world.	The annual DataConnect Conference brings together industry leaders, technical experts and entrepreneurs to discuss the latest trends, advancements, technologies, and innovations in data, analytics, machine learning, and AI. • Learn from high-quality content delivered by thought leaders through keynotes, presentations, engaging panel discussions, and expert-led workshops. • Collaborate with peers and network with experts. • Connect with the global data community with non-stop networking opportunities.	The International Conference on Digital Forensics and Cyber Crime aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Digital Forensics and Cyber Crime. 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 Digital Forensics and Cyber Crime.
For further information **https://infosec-conferences.com/event-series/internet-2-0-conference/**	**For further information** **https://www.dataconnectconf.com**	**For further information** **https://waset.org/digital-forensics-and-cyber-crime-conference-in-july-2023-in-zurich**

Zyber Global Online Events

Our Online Courses with INsig2
Sign up now at https://insig2-and-zyberglobal.learnworlds.com/
Special discount: 15% Use Code: zyber

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