Zyber Global

NOVEMBER 2022 | ISSUE 28

MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

Welcome to the 28th Edition, November 2022 of Zyber Global Centre's monthly newsletter.

Autumn and winter are not my favourite time of the year. I like spring and love summer, so I am not looking forward to the darker mornings and earlier evenings we are beginning to experience.

Being in the UK in October has been pretty eventful, as we saw history being made as we now have our first British Asian Prime Minister Rishi Sunak.

Rishi Sunak is the third British Prime Minister in seven weeks, and our first post-war ethnic minority Prime Minister. The U.K is facing an economic crisis which I pray will get better.

On a more positive note, we have had a very interesting and successful Black History month and Cybersecurity Awareness month, with lots of well attended events across the country. On our events page we have featured three interesting conferences that can be attended in person and/or virtually.

If you would like to have an online cyber health check – do register early for our Stay Safe Online webinar on the 29 November 2022, see https://zyberglobal.com/webinars

We continue with our usual features and ask that you continue to engage with us and let us know what topics on cybercrime you would like to hear more of. Stay safe. Stay well!

BEST REGARDS
ESTHER GEORGE

Esther George, CEO Zyber Global Centre

This Month's Features

Zyber Focus
This month's focus is an article on Stalkerware: Are you being Stalked?
(Zyber Global Research Team)

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

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

Image courtesy Luxstorm @ Pixaby

Stalkerware - also known as spouseware - are powerful surveillance software programs typically sold openly online. On a device, all messages can be read, screen activity recorded, GPS locations tracked and cameras used to spy on what an individual is doing.

-The BBC-

(https://www.bbc.co.uk/news/technology-50166147)

Zyber Focus Article

Stalkerware: Are you being Stalked?

Zyber Global Research Team

Is there a stalker hiding in your electronic devices? Stalkerware is software that tracks a person's location and other personal information, including their Internet activity and social media activities. Yes! an app can stalk you J

The proliferation of Stalkerware has led to concerns about the ethical implications and the potentially dangerous capabilities of such technology. There have been instances where stalkers have used Stalkerware to troll people or send harassing messages when the victim believes they are safe from cyber-threats like this. It is important to remember that this form of online harassment can happen on any electronic device: smart phones, tablets, laptops, desktop PCs...

But you may wonder what exactly is stalkerware? Stalkerware is basically a kind of malware that records every little information if installed on a device and shares it with a third party. Stalkerware is installed and tracks the user without his/her consent. This unwanted program not only breaches your privacy, but it also tracks your location and can therefore put the user at risk.

You may wonder how bad can this be and what can stalkerware apps do? Actually quite a lot!

Stalkerware can monitor, record, track, and illegitimately share everything that a user does on their phone. For example:

- Tracking the user's location in real-time;
- Getting access to the user's call logs;
- Reading the user's messages;
- Taking screenshots;
- Access to the user's camera and microphone;
- Access to social media accounts; and
- Access to the user's gallery.

Different types of stalkerware

These apps disguise and may bypass the privacy policies of the Google Pay Store and Apple Store.

These apps can be classified as:

1. Consumer-grade apps: these are often disguised as child tracking software[1], but are also known as "stalkerware" as they illegitimately track and monitor user's digital world without their consent. These apps are designed to disappear from the home screen to avoid detection.

2. The Employee's Work Apps: these work in a similar way to consumer-grade apps, this has a more formal approach. It would record all SMS, voice, and location activity of business smart phones so that bosses could keep track of their employees. But in such occasions the employees should receive warning of the app's installation, unfortunately that may not be the case.

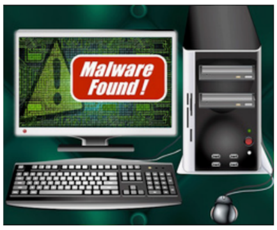
3. The Tracker Apps: these apps, for instance, track SMS messages. However, if you read their marketing copy, you'll find other such tools have been bundled together with the stalkerware.

4. Anti-theft apps: these apps typically enable secret device tracking, and often contain features that could enable remote access to the microphone and camera.

A lot of these companies market such apps to parents so that they can protect their children by tracking and monitoring them. The goal is to reassure concerned parents by sending them details of everything the child does on their devices.

Legality of stalkerware

The legal frameworks pertaining to the legality of stalkerware apps in different countries varies greatly depending on the possible legitimate use of the app discussed above. In most cases, placing stalkerware on a user's device and recording their actions without their consent is illegal. It is also important to understand that in most countries the legal liability for such stalkerware can lie with the person using it rather than its developer, especially in dual-use cases.



The combination of activities that stalkerware tracks, stores and shares is illegal at least in some jurisdictions as it violates the user's privacy and is also against GDPR rules. It is important to be understood here that many countries do not directly forbid/criminalize its development and distribution. However, it is becoming more regulated. Thus, stalkerware seems to be moving out of the gray area it's been hiding in.

For example, in April 2021, the U.S. Federal Trade Commission for the first time banned an app Support King, LLC, which did business as SpyFone.com, and its developer from selling stalkerware.

Once installed, it can be very hard to detect stalkerware, since these apps are designed to be hidden from the users of the device. These apps are designed to convert their icon to that of a calculator or calendar app or system setting or battery saver, etc. Earlier versions of android allowed any app to hide their icons from a phone's home screen.

In a study conducted by Norton Life Lock in 2021, the number of devices infected with stalkerware jumped 63 percent. In 2019 the U.S. Department of Homeland Security (DHS) released an article warning mobile users about the increasing use of spyware apps.

The US-CERT (Computer Emergency Response Team) has also raised concerns about an increase in Stalkerwares after the Federal Trade Commission (FTC) marked its first case, FTC's settlement with Retina-X Studios, LLC against stalking apps (also known as stalkerware). A case was filed against a company named Retina-X that developed and distributed stalking apps that could track smart phone activities like call history, text messages, photos, locations, browser history, and more.

Read the full article: https://zyberglobal.com/blog

Zyber News Roundup

Hacker steals $300K from Olympus DAO, then returns it all the same day

Olympus DAO is the latest target of a crypto cyberattack, as a thief made off with 30,000 OHM tokens—worth about $300,000—early this morning. But the attacker either had a change of heart or was a white hat hacker all along, as they sent back the funds to the DAO hours later.

Community members were first alerted to the exploit early Friday morning on Discord.
"*This morning, an exploit occurred through which the attacker was able to withdraw roughly 30K OHM ($300K) from the OHM bond contract at Bond Protocol*," the post read. "*This bug was not found by three auditors, nor by our internal code review, nor reported via our Immunefi bug bounty.*"
Olympus said that a phased rollout put a "*limited amount of funds at risk*," and the amount stolen was a fraction of the potential $3.3 million bounty the attacker would have been able to claim on bug-hunting website Immunefi for reporting the exploit.

"*We have closed the affected markets and all other funds are safe*," Olympus added. In the announcement, the DAO team said it was exploring the best way to fully compensate all affected bonders. Just hours later, however, Olympus DAO updated the community with better news: all the tokens had been returned by the attacker.

Launched in May 2021, Olympus DAO is a decentralized reserve currency protocol based on the OHM token. OHM tokens are backed by a basket of assets (such as DAI and FRAX) held in the Olympus treasury. Since January 2022, Olympus has offered a potential maximum $3.3 million bounty focused on Olympus smart contracts and applications to prevent the loss of DAO funds.

Read more:
https://finance.yahoo.com/news/hacker-steals-300k-olympus-dao-223639476.html

Criminals are starting to exploit the metaverse, says Interpol. So, police are heading there too

The International Criminal Police Organization, aka Interpol, has launched its 'global police Metaverse' as part of an effort to train members how to police in a virtual world.
Last week, Interpol unveiled what it says is the "the first ever Metaverse specifically designed for law enforcement worldwide." It says the "Interpol Metaverse" gives officers around the world the tools for cross-border knowledge sharing via avatars, and to take immersive training in forensic investigation and other policing activities.
Interpol has also created an expert group on the metaverse to represent law enforcement concerns about the new virtual world. "*Criminals are already starting to exploit the Metaverse,*" Interpol warned. "*As the number of Metaverse users grows and the technology further develops, the list of possible crimes will only expand to potentially include crimes against children, data theft, money laundering, financial fraud, counterfeiting, ransomware, phishing, and sexual assault and harassment,*" it said.

"*For law enforcement, some of these threats are likely to present significant challenges, because not all acts that are criminalized in the physical world are considered crimes when committed in the virtual world,*" it warned.

"*For many, the Metaverse seems to herald an abstract future, but the issues it raises are those that have always motivated Interpol – supporting our member countries to fight crime and making the world, virtual or not, safer for those who inhabit it,*" said Interpol secretary, General Jürgen Stock

Read more: https://www.zdnet.com/article/criminals-are-starting-to-exploit-the-metaverse-says-interpol-so-police-are-heading-there-too/

Facebook users sue Meta for bypassing beefy Apple security to spy on millions

After Apple updated its privacy rules in 2021 to easily allow iOS users to opt out of all tracking by third-party apps, so many people opted out that the Electronic Frontier Foundation reported that Meta lost $10 billion in revenue over the next year. Meta's business model depends on selling user data to advertisers, and it seems that the owner of Facebook and Instagram sought new paths to continue widely gathering data and to recover from the suddenly lost revenue. Last month, a privacy researcher and former Google engineer, Felix Krause, alleged that one way Meta sought to recover its losses was by directing any link a user clicks in the app to open in-browser, where Krause reported that Meta was able to inject a code, alter the external websites, and track "anything you do on any website," including tracking passwords, without user consent.

Now, within the past week, two class action lawsuits from three Facebook and iOS users—who point directly to Krause's research—are suing Meta on behalf of all iOS users impacted, accusing Meta of concealing privacy risks, circumventing iOS user privacy choices, and intercepting, monitoring, and recording all activity on third-party websites viewed in Facebook or Instagram's browser. This includes form entries and screenshots granting Meta a secretive pipeline through its in-app browser to access "personally identifiable information, private health details, text entries, and other sensitive confidential facts"—seemingly without users even knowing the data collection is happening.

A Meta spokesperson provided Ars with a statement: "These allegations are without merit, and we will defend ourselves vigorously. We have carefully designed our in-app browser to respect users' privacy choices, including how data may be used for ads."
Read more: https://arstechnica.com/tech-policy/2022/09/lawsuits-say-meta-evaded-apple-privacy-settings-to-spy-on-millions-of-users/

Zyber Global Events Information Page

GLOBAL CYBERSECURITY EVENTS

UK CyberWeek **Business Design Centre, London N1** **3 - 4 November 2022**	**International Conference on Promoting the Role of Women in Preventing, Investigating and Prosecuting Cybercrime** **San Jose, Costa Rica** **10 - 11 November 2022**	**The Virtual International Conference on Cyberlaw, Cybercrime & Cybersecurity** **23 - 25 November 2022 - Online**
Where UK Businesses fight back against cyber crime. We are all in this together, but we believe there is a knowledge gap between the expertise of the cyber community and UK businesses leaders. We want to close that gap. Everyone has their part to play – policymakers, businesses, cyber professionals, IT departments, cyber vendors, software developers, law enforcement, media, and educators. Join the community fighting back at UK Cyber Week. We're bringing everyone together to level up UK cyber security, demystify jargon, share the latest thinking, and learn from truly world-class experts. Our promise is that everyone, no matter how much or how little expertise they have, leaves knowing more and is better equipped. UK Cyber Week's live flagship event is free to attend.	Women have a crucial role to play in effective criminal justice responses to cybercrime, whether as policymakers or legislators developing and adopting legislation on cybercrime, or as law enforcement, prosecutorial or judicial practitioners investigating and prosecuting offences. This conference will further promote the role of women in preventing, investigating, and prosecuting cybercrimes and other crimes involving electronic evidence, through a 1.5-day event of plenaries, and thematic and practitioner workshops.	The International Conference on Cyberlaw, Cybercrime & Cybersecurity 2022 is taking place from 23rd to 25th November 2022, (in virtual mode), organized by Cyberlaws.Net and Pavan Duggal Associates, Advocates, Supreme Court of India. The Conference 2022 is currently being supported by Department of Legal Affairs, Ministry of Law & Justice, Government of India, Ministry of Electronics & Information Technology, Government of India and United Nations' University for Peace, and other national and international stakeholders. The Conference 2022 will have different sessions with more than 165 speakers over three-day deliberations from different parts of the world discussing and deliberating upon some of the important aspects, issues and challenges concerning cyberspace.
For further information **https://www.ukcyberweek.co.uk**	**For further information** **https://www.coe.int/en/web/international-conference-women-cybercrime**	**For further information** **https://cyberlawcybercrime.com**

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