DECEMBER 2021

inside zhero

Let's take a look at what is happening at Zhero

MESSAGE FROM IZAK

The festive season is upon us again and I always find this a useful time to reflect on the events of the past year. To my mind, it has been nothing short of chaotic from a global IT perspective. The apocalyptic ransomware attacks for instance, on the likes of SolarWinds, Kaseya and Colonial Pipeline. However, total chaos presents an opportunity to improve. Consider the words of Jok Church, the American cartoonist, for a moment:

"Chaos does not mean total disorder. Chaos means a multiplicity of possibilities."

I believe that by delivering better IT faster, it is possible to eradicate everybody's IT chaos. Moving forward into the New Year, we can all then look forward to an online world that is safe and secure - and free from any chaos.

Wishing my loyal clients and talented staff a peaceful festive season and a prosperous 2022.

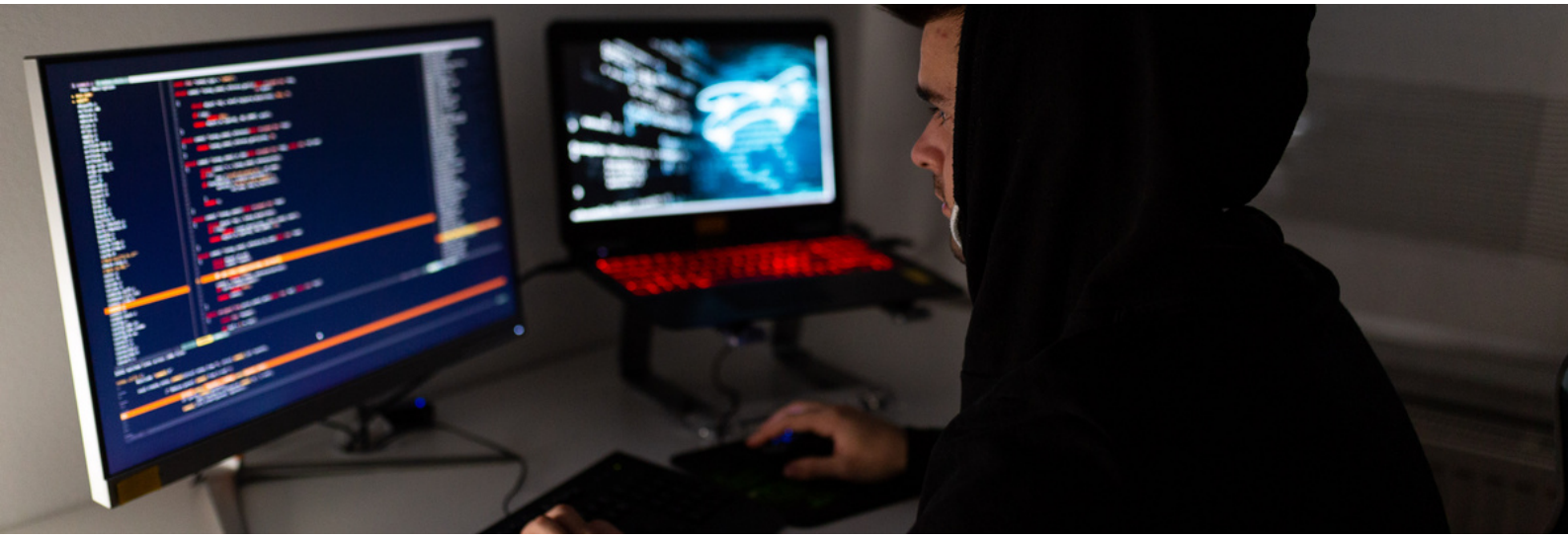
Izak Oosthuizen
Bestselling Author and
Founder and MD of Zhero

RANSOMWARE APOCOLYPSE

To say that ransomware attacks have bordered on apocalyptic levels in 2021 is an understatement. According to U.S. internet and cybersecurity provider, SonicWall, the world expects to record 714 million attempted ransomware attacks by the close of this year.

That's a 134% increase over the total for 2020. While some of these attacks have been rendered harmless, others show that ransomware is a significant threat to global business.

For hackers, this form of cyber exploitation means big business and it is estimated that ransomware costs will exceed $20 billion in 2021. Here are 4 examples of how hackers upended our way of life and caused IT chaos in their quest for a big payday.



ACER - $50 MILLION

In March, Taiwanese electronics giant, Acer, was hit by a ransomware attack by the notorious Russian Hacker group, REvil, demanding $50 million. Breached data included confidential financial and banking information. When Acer tried to negotiate the ransom down to $10 million, REvil released some of the exfiltrated data onto the dark web and doubled the ransom amount to $100 million. Whether Acer paid the amount cannot be confirmed.

SOLARWINDS - $90 MILLION

In early 2021, a Texas-based managed services provider (MSP) was hacked when malicious code was injected into the company's Orion software system. In March, SolarWinds unknowingly sent out software updates to its 33,000 customers which included the hacked code.

Of these, 18,000 installed the updates and were left vulnerable to hackers. Companies affected included Microsoft, Intel, Cisco and Deloitte. Russia's Foreign Intelligence Service, SVR, demanded a massive $90 million in ransom.

SolarWinds did not pay the ransom but instead spent $19 million to investigate and remediate the cyber incident.

CNA - $40 MILLION

Also in March, CNA Financial, one of the largest insurance companies in the United States, suffered a ransomware attack that blocked access to the company's network and stole its data. The Russian syndicate, Evil Corp. demanded $60 million in ransom. Following negotiations, CNA paid them $40 million in late March.

COLONIAL PIPELINE - $5 MILLION

In May, another Russian hacking group, DarkSide, breached the IT systems of Colonial Pipeline, the largest pipeline system for refined oil products in the United States. The ransomware attack disrupted fuel supplies to the East Coast of the United States for 5 days. DarkSide demanded $5 million in ransom which Colonial Pipeline paid in bitcoin. In June, the FBI recovered $2.3 million of the payment.

KASEYA – $50 MILLION

In July, the Florida-based software and automation company, Kaseya, was hacked when REvil broke into the networks of about 50 MSPs that used its products. As a result, more than 1,500 companies that were supported by these MSPs had their data compromised and were paralysed. Revil wanted $50 million for the release of a decryptor key. Kaseya refused to pay and provided clients with its own decryption software.

CYBERCRIME AT CHRISTMAS

Cybercrime, whether it be ransomware, phishing, identity theft, or anything else, is always prevalent. But cybercriminals know all too well that Christmas is the busiest time of year for internet retailers and that more people than ever will be using their devices to make purchases and surf the web.

Here are 4 ways that hackers can turn your Christmas festivities into chaos and misery:

- **Email Banking Scams –** Posing as your financial institution is one of the most common ploys that scammers use. Via an unsolicited email, clueless victims are asked to login to their accounts and update personal details. They then say goodbye to their money. Banks will never ask to login in from a link in an email and are also unlikely to contact you for your personal information.

- **Phishing Scams –** Provided that they have your consent, over the Christmas period you will be bombarded by marketing emails from genuine retailers encouraging you to make a last-minute purchase. Hackers know this and send out mail pretending to be Amazon, eBay or any other reputable e-tailer. Remember that if an email describes an offer that seems too good to be true, it probably is.

- **HTTP Sites -** Most e-commerce websites in which you input your personal data or credit card details offer a secure connection or HTTPS certificate. These are easily identified by the padlock symbol in the browser. Although not all are dangerous, unsecure HTTP websites don't encrypt traffic between you and the server. As such, it's extremely easy for any hacker with the know-how to steal information from these sites. If you don't spot the padlock, it's probably best to do your Christmas shopping elsewhere.

- **Phone Scams –** Phone scams are increasingly becoming the norm. If you receive a call claiming to be a customer adviser from your bank, or the manufacturer of that shiny new laptop or smartphone you got last Christmas, always ask for their credentials. Never give out any personal details or passwords to someone who makes an unsolicited call to you. Also, don't let hackers scare you. Some may call and say that your National Insurance number has been compromised, that your bank accounts are now frozen, and that you need to take action. The call may even sound professional and sincere. Don't listen. It's a scam. Hang up.

STAY SAFE THIS HOLIDAY SEASON

Christmas doesn't need to be chaotic. There's no need to feel threatened when shopping online. If you use your common sense and apply these 6 tips when buying gifts for your loved ones and friends, you can shop safely and securely.

- **Use secure networks when shopping online** and only window shop on public Wi-Fi. Public Wi-Fi can be hacked by someone with the right tools, exposing your passwords, billing information, and other sensitive data.

- Make sure your **apps are downloaded from a trusted source**, such as the Android Market, Apple App Store or the Amazon App Store. When you download the app, it will ask for various "permissions." Be sure to read through them and decide if they make sense – or not.

- **Lock your devices** so that your credentials, bank details and other personal data are not exposed to prying eyes. It only takes a second to unlock but it could take years to recover from serious financial loss.

- Where possible, **use Two Factor Authentication** (2FA) when accessing websites, even those with HTTPS certificates. Using 2FA will preclude hackers from gaining access to your personal data. Most banks and retailers like Amazon, Apple and eBay require 2FA.
- Before you shop, check that your **device is updated** with the latest antivirus.

- **Use credit, not debit.** Credit cards offer much more protection and less liability if your information were to be compromised. Debit cards are linked directly to your bank account so you are at much more risk of fraudulence if a cybercriminal were to obtain this information.

MEET THE TEAM

Enrico Marais

SERVICE DESK ENGINEER

1. What made you realise you want to go into the IT industry?

I had a friend who was into computers. He introduced me to IT and after I matriculated, I decided to study IT. I started with fixing computers etc. and that helped me grow to where I am today.

2. What's your most-used productivity skill?

By constantly communicating with clients, I would always need my phone.

3. What do you enjoy the most about your job?

The most rewarding is getting a thank you and a well done from an employee or customer. It feels good to see a smile on a customer's face after resolving an issue and getting a 5-star rating.

4. How would you describe yourself?

I am a very friendly and approachable person. When I started working at Zhero I noticed that when the guys had questions, they often came to me because I am always willing to assist. I never say no and I enjoy helping others out. I am the go-to guy.

5. Do you have any hidden talents or hobbies?

Outside of work I am a BIG motorcycle fanatic. I've owned 23 motorcycles and have built my own in my free time. I even have my own YouTube channel about it.

6. Are you a sports fan?

I'll watch rugby when it is a big game, but I am really more into Rally or Moto GP. I would rather be in the garage working on my bike.

7. What is your favourite film?

Any movie that involves Jason Statham or Keanu Reeves.