MARCH 2022

inside zhero

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

MESSAGE FROM IZAK

It was inevitable. While the events that have unfolded as a result of the Russian invasion of Ukraine are devastating, there is more to this conflict than meets the eye.

Ukraine has a long history of being a victim of cyberattacks, mostly at the hand of Russian hackers. Associated Press recently reported:

"Cyberattacks have been a key tool of Russian aggression in Ukraine since before 2014 when the Kremlin annexed Crimea. Their intent can be to sow panic, confuse and distract."

In this issue of *Inside Zhero*, we take a look at how Ukraine has been embattled with Russia on the cybersecurity front. We will also analyse the implications of this battle on businesses and our digital world. There's so much more than panic, confusion and distraction.

Izak Oosthuizen
Bestselling Author and
Founder and MD of Zhero

THE GLOBAL CYBER CONFLICT

On 24 February, the world looked on in despair as Russia invaded Ukraine. Missiles rained down, flattening hundreds of buildings in major Ukrainian centres. In the small town of Schastia, 90% of the buildings have been damaged or destroyed. On the civilian front, the death toll has risen to over 636, including the killing of Kirill Yatsko, an 18-month-old boy. These horrors are the sad story of collateral damage in any war.

The reality is that the current Russian-Ukrainian military conflict has the potential to explode internationally, and not only in the realm of conventional warfare. Instead, cybersecurity experts in the UK and the United States fear that 'the big one' will come soon, a day that will see Russian hacking paralyzing the global internet in retaliation for the economic sanctions levered by the West. In a world where interdependence on data and technology is the name of the game, is cyberwar destined to become reality?

RUSSIA – A MASTERMIND HACKER

"It was like a war before the war." ~ Deutsche Well

The same day that Russia invaded Ukrainian territory, vital government websites in the country, including that of the parliament and the Foreign Ministry, were hit by the destructive Cyclops Blink virus causing massive DDoS attacks.

WHAT IS A DDoS ATTACK?

A DDoS or Distributed-Denial-of-Service is an attempt by botnets to bring down a server, network, website or device with a flood of Internet traffic. A DDoS attack can be compared to an unexpected traffic jam on a motorway preventing vehicles from getting to their destination.

Data-wiping malware, aka HermeticWiper, was identified on 100s of Ukrainian computers with the ability to destroy great quantities of data without detection. This was not the first time that Ukraine was a victim of Russian hacking. In 2015, hackers from the former USSR managed to knock out power for approximately 230,000 customers in Western Ukraine. In 2017, Russia struck again. This time with NotPetya, malware that infected computers in more than 64 countries and cost the global economy the equivalent of £7 billion.

CALLING ALL HACKERS

While Russia may be keeping its cards close to the chest, Ukraine has adopted a completely different stance. The country under siege has enlisted more than 400,000 cybersecurity experts for its IT Army. The crowdfunded government initiative used the Dark Web and social media app Telegram to recruit volunteers with the intention of digitally disrupting Russian government and military targets. Victor Zhora, Deputy Chief of Ukraine's Information Protection Service, said in a briefing:

"Our friends, Ukrainians all over the globe, are united to defend our country in cyberspace. Ukraine is working to do everything possible to protect our land in cyberspace, our networks, and to make the aggressor feel uncomfortable with their actions."

The irony is that while the West supports Ukraine in its military efforts and countries such as the UK, Canada and Denmark have opened the door for their citizens to enlist in Ukraine's international territorial defence legion, many frown down upon Ukraine's cyber militia. Put simply, hacking is illegal and a crime.

WHAT EXPERTS SAY

Paul Chichester, the Director of Operations at the National Cyber Security Centre (NCSC), warned that UK businesses need to prepare themselves for possible Russian-initiated cyberattacks and said:

"While we are unaware of any specific cyber threats to UK organisations in relation to events in Ukraine, we are monitoring the situation closely and it is vital that organisations follow the guidelines to ensure they are resilient. Over several years, we have observed a pattern of malicious Russian behaviour in cyberspace. Last week's incidents in Ukraine bear the hallmarks of similar Russian activity we have observed before."

In the United States, the Cybersecurity & Infrastructure Security Agency (CISA), has expressed similar sentiments. CISA has warned businesses and individuals to prepare for an onslaught of Russian cyberattacks that could even culminate in global cyberwar. According to Forbes, the agency said in its warning:

"Every organization—large and small—must be prepared to respond to disruptive cyber activity."

TOP 2022 CYBERSECURITY TRENDS

As companies and countries watch the latest chapter of the Russian war in Ukraine unfold, they should prepare for an increase in cyber attacks in the coming months. Here are the top 5 cybersecurity predictions, exacerbated by the Russian-Ukraine war, for 2022 and beyond:

- Ransomware will surge and you will see a big increase in digital supply chain attacks.
- There will be a significant increase in sophisticated and damaging DDoS attacks.
- Cyber insurance will become much more expensive, especially for SMEs.
- The global spend on cybersecurity will be an estimated £60 billion by 2025.
- Investment in Zero Trust security will grow from £15 billion in 2021 to £40 billion in 2026.

While some attacks, such as attacks on infrastructure, are nearly impossible for companies to prepare for, there are steps businesses and individuals should take as a matter of course: make sure software is up to date and patched, check that you have effective and up-to-dated malware and antivirus software, and ensure that all important data is backed up in a safe location.

MEET THE TEAM

Thomas Buys

PROJECTS ENGINEER

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

I've always had a fascination with how data is transmitted. When it came time to choose a career path 17 years ago, the choice to go into IT was easy as it's a rapidly expanding ever-changing industry and the scope for different levels of knowledge is vast.

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

Problem-solving, having the knowledge to identify problems onsite and offering resolutions. For example, troubleshooting a network device that's offline or general PC problems.

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

I enjoy being the onsite face of the company, working directly with clients, and teaming up with colleagues to resolve problems.

4. How would you describe yourself?

Slightly shy and reserved but confident in conversation.

5. Do you have any hidden talents or hobbies?

I used to ride motocross, enduro, and any petrol-fuelled two-wheel offroad vehicles. I also love flying stunt kites. There was a stage in my life when I went into tree felling.

6. Are you a sports fan?

Yes, I follow the F1 season and MXGP calendar throughout the year.
I'm a bit of a racing fanatic. I also enjoy watching cricket tournaments and occasionally rugby.

7. What is your favourite film?

Most recently a series called The OA.