FEBRUARY 2022

# inside zhero

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

## MESSAGE FROM IZAK

In the cybersecurity landscape, a threat that is becoming increasingly troublesome is digital supply chain attacks. SolarWinds, Microsoft Exchange Server and Kaseya, immediately come to mind - not to mention the disruptions to businesses as a result of these breaches.

Christopher Graham, a privacy and information security lawyer, tweeted:

*“The knock-on effect of a data breach can be devastating for a company. When customers start taking their business — and their money — elsewhere, that can be a real body blow.”*

In this issue of Inside Zhero, we look at the causes of supply chain attacks, what the knock-on effects are, and ultimately, how you can avoid them.

You don’t have to be a victim.

Izak Oosthuizen
Bestselling Author and
Founder and MD of Zhero

# A GROWING CYBER THREAT

Have you ever heard of killing two birds with one stone? Cybercriminals have, as they are cunningly exploiting a form of attack that can breach multiple targets instead of laboriously breaching one at a time. The so-called 'supply chain attack' is now popular in which a business is breached through vulnerabilities in its supply network, usually as a result of poor cybersecurity, or a lack thereof.

Supply chain attacks, also referred to as value-chain attacks or backdoor breaches, often go unnoticed as they are difficult to detect or trace.

The results of such a breach would be catastrophic to your business, as it could bring operations to an immediate halt and expose sensitive data.

**WHAT IS A SUPPLY CHAIN ATTACK?**

A supply chain attack, also called a value-chain or third-party attack, occurs when someone infiltrates your system through an outside partner or provider with access to your systems and data.

The European Union Cybersecurity Agency (ENISA) predicts a 4-fold increase in supply chain attacks in 2022. These threats have the potential to do great reputational and financial damage to businesses and their stakeholders.

Eran Orzel, a Senior Director at Argon, says:

*“The number of attacks over the past year and the widespread impact of a single attack highlights the massive challenge that application security teams are facing. Unfortunately, most teams lack the resources, budget, and knowledge to deal with supply chain attacks.”*

# WHAT HAPPENS IN A SUPPLY CHAIN ATTACK?

Cybercriminals see supply chain attacks as a massive leap forward in their quest to paralyze IT systems, steal data, and make money. Most companies don't have the resources to develop their own software applications. Instead, they obtain off-the-shelf component software from third-party vendors. This software often contains unpatched vulnerabilities. Cybercriminals use these as a backdoor into their victims' systems.

After obtaining access, the software is infected with malware which roams freely throughout the application with the same trust and permissions as the original application.

One of the biggest supply chain attack threats occurs when a software vendor is hacked. This means that the malware is passed on to the vendors' clients and possibly even further down the supply chain. This phenomenon has a ripple effect. Look at this simple example:

- A vendor supplies 1000 businesses with infected software.
- Each of these businesses has 1000 clients.
- A single supply chain attack has the potential to disrupt 1000 x 1000 operations. That's 1 million breaches, not including the software vendor.

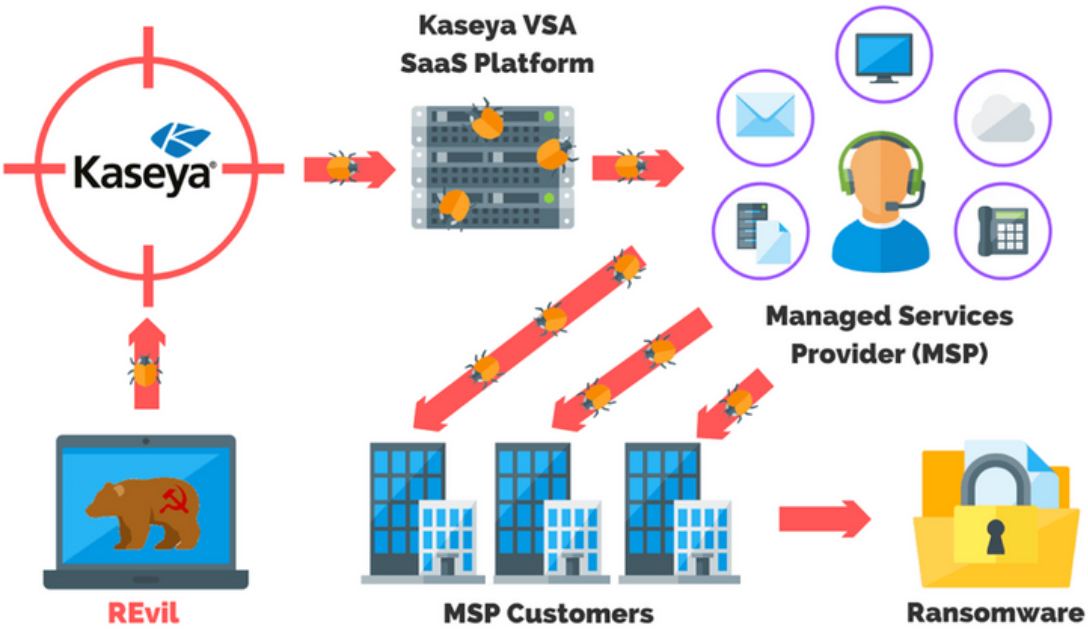
Today, the average software project has 203 dependencies. If a popular app includes one compromised dependency, every business that downloads from the said vendor will also be compromised. Therefore, the total number of affected businesses can be exponential.

# KASEYA AS A CASE IN POINT

The supply chain attack on Miami-based software vendor Kaseya in July 2021 is one of the most damaging ransomware attacks in history, involving a whopping $70 million ransom. Kaseya provides IT Managed Service Providers (MSPs) with Remote Monitoring and Management (RMM) software. The MSPs install the RMM tools on client workstations and servers to monitor their emails, phone systems, firewalls, switches and other network devices.

Last year, the Russian Ransomware-as-a-Service (RaaS) operation, REvil injected zero-day exploits into Kaseya's software platform  This allowed them to gain access and distribute malicious software to its MSP clients which were then passed along to the respective clients of the MSPs. Each company targeted by the supply chain attack was held ransom, causing massive disruption to U.S. businesses, transport systems, schools and chain stores, with hundreds being forced to temporarily cease operations. Victims were also identified in other countries including the UK, South Africa, New Zealand, Canada and Indonesia.

This is an illustration of the occurrence:



# WHAT CAN I DO?

By design, supply chain attacks are often difficult to identify or trace due to their complexity. By implementing the following 6 strategies, you will make life much more difficult for cybercriminals to gain access to your IT system:

- **Implement Honeytokens -** Honeytokens are fake resources posing as sensitive data. A hacker is often fooled into believing that these are valuable assets and when they interact with them, a signal is activated. This will give you an advance warning of any potential and real breach.

- **Implement Zero Trust -** Zero Trust is underpinned by the principle of 'never trust, always verify'. Unlike traditional cybersecurity models in which all users were considered trustworthy once they have passed the network perimeter, Zero Trust embodies a much more cynical and dynamic approach. It uses the principle of least privilege (POLP) which limits access to data and applications only to those who need it. The knock-on effect is that the potential lateral movement of hackers through a network is almost eradicated. Furthermore, Zero Trust enforces strict device authentication and authorization throughout an IT network.

- **Employee Education -** Your staff are often the gateway to malicious intrusion and can be tricked into allowing a hacker access to the cyber ecosystem. Scam emails and phishing attacks are the most common form of trickery, asking for login details and other credentials. Always provide your employees with ongoing cybersecurity education and training that cover all forms of cyber attacks.

- **Minimize Access -** Minimizing access to sensitive data should be inherent to your Zero Trust policy. Firstly, identify all sensitive data access points. This way you will know all the employees and third-party vendors accessing your sensitive data. You then need to keep accounts to a minimum – the more people have access, the greater the risk. Considering that vendors are the first targets in a supply chain attack, scrutinize and cull their access where possible.

- **Identify Vendor Leaks -** According to the latest research, companies have a 27.7% chance of suffering a data breach, and almost 60% of these breaches are linked to third parties. When you focus on the mitigation of third-party data breaches, overall data breaches stemming from supply chain attacks will be reduced significantly.

- **7 questions to ask your suppliers -** Ensure your business stays ahead of the threat by asking your suppliers 7 key cybersecurity questions. This checklist will enable you to identify potential threats in your supply chain and act on them. **Click here** to download your 7-step checklist and start crushing the IT risk.

# MEET THE TEAM

## Jordan Van Vuren

**JUNIOR ACCOUNTANT**

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

I get the chance to experience something new. Accounting is always the same process and in this industry, I learn how to do it in a different way.

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

That would definitely be Xero and Zhero Wait. They speak the same language and make work easier.

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

I have the chance to be better. I take stock of details and I learn how to be more present.

**4. How would you describe yourself?**

I am very outgoing and I have a good sense of humour. I'm also very self-driven and I like to work in teams.

**5. Do you have any hidden talents or hobbies?**

I did try magic but it didn't go very well. I use to play hockey when I was younger and I enjoy fishing.

**6. Are you a sports fan?**

Absolutely! I watch basically anything. Lately, I've been watching the Winter Olympics. I'm also a fan of Rugby and Soccer.

**7. What is your favourite film?**

I like to watch the movie Star Wars. I also enjoyed Game of Thrones, Harry Potter and North and South featuring Patrick Swayze.