CYBERSPRINT
BREAKTHROUGH SECURITY

EDITORIAL

SUPPLY CHAIN ATTACKS

WHY EVERYONE IS TALKING ABOUT IT AND WHAT YOU NEED TO KNOW

BY **EWARD DRIEHUIS**
SVP STRATEGY CYBERSPRINT

BY **E. DRIEHUIS**
SVP Strategy

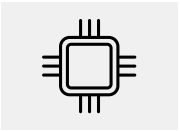
SUPPLY CHAIN ATTACKS

WHY EVERYONE IS TALKING ABOUT IT AND WHAT YOU NEED TO KNOW

The next big thing in cybersecurity might very well be supply chain security. I have followed this evolution closely over the years. Today, supply chain attacks are as abundant as they are elusive. However, as many parties communicate about the dangers and their technical solutions, not much is said about the basics of supply chains attacks. I have written this article based on my personal experiences and knowledge on the subject. I hope it answers most of your questions about the topic, so that you have a solid basis to expand your supply chain security from.

WHAT IS A SUPPLY CHAIN? HOW ARE THEY ATTACKED?

In a cyber context, your supply chain is formed by the third parties needed to achieve your organisation's goals. Since we talk about risk a lot, it's key to understand there are different supply chains with different types of risks:

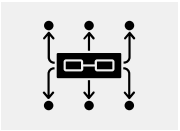


HARDWARE SUPPLY CHAIN

Organisations using hardware (this is of course most enterprises, but specifically data centers, SaaS providers and big tech) increasingly worry about the risk of an unmonitored supply chain. In 2018, this led to a widely criticised Bloomberg article[1] on a Chinese chip making its way into hardware belonging to American companies. The worries remain, and every now and then snippets of evidence of hardware supply chain attacks enter the main stream.

SOFTWARE SUPPLY CHAIN

Organisations using software (which means all of them) are confronted with an increased volume of attacks and risks. The 2019 Citrix breach[2] and the 2020 Solarwinds attack[3] were two recent ones. The 2017 Notpetya attack[4], one of the most destructive ones ever, was traced back to a hacked update service of the Ukrainian MeDoc software provider. Tens of thousands of organisations using these companies' software were at risk.



INFRASTRUCTURE SUPPLY CHAIN

Almost every organisation requires specialist IT companies to perform service updates to their infrastructure. These connections are leveraged by attackers who use the MSPs as a stepping stone to their intended target. The Cloudhopper attack[5] had been going on for a year when it broke the news in 2018.

HOW BAD IS IT?

The unfortunate thing is: nobody really knows.
It is almost impossible to get definitive numbers. In case of incidents, victims usually call an incident response team. These are governmental as well as commercial teams, and depending on your type of organisation, you call one or both of them. An incident response team is (almost always) bound by Non-Disclosure Agreements. The events might impact stocks and company value, so a lot of organisations keep events close to the chest. Most people I know in incident response have investigated supply chain attacks over the last four years or so, including myself. Everyone has their personal experiences, but there's no central registration. Some larger international incident response organisations (like FireEye's Mandiant team) do enough of these jobs to discern some global trends. But the wider community needs initiatives like Mitre's ATT&CK framework[6], which aims to be a register of tactics, techniques and attackers.

A second, more bleak reason why accurate figures are hard to determine, is that adversaries leveraging the supply chain are good at their jobs. A large percentage of attacks go undetected, while other incidents might have been detected but were not traced back to the supply chain. It often happens the attackers have had access to systems long before the attack is weaponised. Especially espionage attacks are executed with the aim to avoid damaging or interrupting operations as much as possible. I fear we're only detecting a small percentage of attacks.

Talking to professionals, the consensus I encounter is that

- Supply chain attacks are on the rise
- Most professionals have dealt with these events personally
- There is no clear solution

WHO ARE THESE ATTACKERS?

Hardware and software supply chain attacks would likely and largely be nation state sponsored. Although proof of hardware supply chain attacks is few and far between, software supply chain attacks require a hefty amount of bespoke, specialist effort. It's largely reserved for those well-funded groups.

Infrastructure supply chain attacks started in the espionage world, though the more ambitious criminals leveraged these methods fairly quickly as well. The Mitre's ATT&CK framework[6] shows that many of the nation state sponsored groups dedicated to espionage are (sometimes loosely) tied to the Chinese government. Over the last years, they've established a reputation of having the most espionage groups leveraging the supply chain.

We need to have a sense of perspective about this: espionage is day-to-day business for any self-respecting economy, including Western nations. Almost no-one is innocent.

HOW DO THEY DO IT?

1. When attackers have selected their target, they first map out the organisation's relations using open source intelligence (OSINT) and espionage sources. To get to a target, they will often use very generic social engineering techniques such as (spear) phishing or watering holes on these suppliers. The intelligence is used to create a more credible story. Sysadmins are often a great target due to their elevated rights. And should such an attampt fail, it looks like any regular criminal phishing attack, making plausible deniability easy.

2. The next step is to silently recon to "island hop" into the final target. The supplier's sysadmin might have a VPN or email relation with the target organisation. The tools they use aren't always super advanced. It's a matter of economics: achieve the best effect with the least investment. Although nation states can create new malware, they often won't do it because of budgeting.

3. Once in the target's environment, it really depends on the intended goal what happens next. Ransomware criminals will try to find and destroy backups before encrypting files. Spies will try to stay undetected and find intellectual property or pricing plans. Both criminals and spies will try to exfiltrate data undetected.

WHY IS IT HARD TO MANAGE?

A big part of the problem arises from the fact your supply chain's IT isn't managed by you. The challenge organisations are trying to tackle is to get control over digital risk in someone else's company, linking back to their own systems. This is hard for multiple reasons.

- Historically, the industry has focussed on periodical snap shot audits and arbitrary security scores. It certainly means something if a supplier is ISO certified. And if they score a very nice risk score above the industry average of 780, that says something too. Unfortunately, an attacker's chances of succes are defined by the attack surface, rather than by their target's credentials and certificates.
- Attack surfaces, or digital footprints, are difficult to manage for anyone. Over the last years, tremendous progress has been made, and digital risk and attack surface management is now supported by data science and AI. As organisations have only just begun to manage their own attack surface, they now also need a way to manage the attack surfaces of all their suppliers.
- Average mid-sized enterprises already have over 100 infrastructure suppliers (according to our own research into 350 European enterprises). Just one small gap in any of them might lead to compromise within your organisation.

Criminals don't care about your certifications. Spies don't care about your risk score. If you want to be in control of the expanding complexity, findings ways to gain actionable insights into these attack surfaces might be your path. Again, there's no clear consensus among practitioners, but at least from personal experience, I have seen CISOs embark on this path successfully.

> " CRIMINALS DON'T CARE ABOUT YOUR CERTIFICATIONS. SPIES DON'T CARE ABOUT YOUR RISK SCORE. "

HOW TO GAIN CONTROL

It's always easier said than done, but my advice is to:

- Limit your IT dependencies if you can;
- Have in-house knowledge if you can;
- Continuously monitor your attack surface and get as complete a picture you can. Bad guys will inevitably leverage your blind spots;
- Take infrastructural dependencies into account and add them to your watchlist. These dependencies are the ones the bad guys might be able to find, too;
- Define the top strategic suppliers and add them to your continuous watchlist. Watch their infrastructure, or the part of their infrastructure which overlaps with your digital footprint;
- Invest time and effort to manage the process, and include it in compliance and governance[7].

WRAPPING UP

As we're developing more tools and insights into this challenge, we've gained enough sense of reality to see resilience is a continuous battle. Many forward-thinking organisations know how to protect themselves within the boundaries of company goals and budgets. We now find a need to expand our scope. Much in the same way as "hackers don't care for what is under your direct control or not", they don't care where your IT ends and your suppliers' begins. I feel the supply chain is our next big blind spot. In order to be in control, we have no choice than to start looking here.

EWARD DRIEHUIS has been a security veteran for over 24 years, describing himself as having a "tech heart, design mentality, business drive". He's got a proven track record in innovative leadership in start-ups and largeenterprises. Eward is an established speaker in the media and at international events such as RSA and FS-ISAC,drawing upon his years of experience of fighting cyber threats together with banks, law enforcement and corporates.

Before joining Cybersprint, Eward spent three years as CMO at SecureLink, Europe's largest cyber security provider, including being responsible for research. He has also spent nine years at Fox-IT heading their Threat Intelligence and Advanced Analytics products. Earlier in his career, Eward's roles included CTO and Business Director in several IT and software companies.

ABOUT THE AUTHOR

SOURCES

1. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
2. https://krebsonsecurity.com/2020/02/hackers-were-inside-citrix-for-five-months/
3. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
4. https://www.forbes.com/sites/thomasbrewster/2017/06/27/medoc-firm-blamed-for-ransomware-outbreak
5. https://www.reuters.com/article/us-china-cyber-hpe-ibm-exclusive-idUSKCN1OJ2OY
6. https://attack.mitre.org/groups/
7. https://www.cybersprint.com/whitepaper-it-governance

ABOUT CYBERSPRINT

Cybersprint helps organisations achieve instant control over their visible and hidden digital risks to mitigate cyber threats related to their business, brand, online data and employees.

Our Our Attack Surface Management platform provides a continuous and automated process of identifying and managing your attack surface and associated external digital threats.

Visit www.cybersprint.com