Digital Security
Progress. Protected.

Ransomware: The need to protect the weakest link, your supply chain

So far in our ransomware series, we have looked at the basics of ransomware, Remote Desktop Protocol and email compromises. In this blog, we take a look at how businesses can be attacked through their supply chains.

What is a supply chain?

A supply chain is a network between a company and its suppliers to produce and distribute a specific product or service. **It consists of everything between the raw materials and the product that hits the shelves**. The chain is typically made up of the supplier of the raw materials, the manufacturer, the distributor and the retailer.

When it comes to security, **the supply chain is only as strong as its weakest link**. Attacking the supply chain at any point along its length will have consequences throughout. When the environment is digital rather than physical, the ramifications are the same. By breaching just one vendor, bad actors may eventually be able to gain unrestricted and hard-to-detect access to large sections of vendor's business partners and customer base.

Playing the odds

This explains why large vendors are constantly being targeted. Their solutions are used in homes and businesses around the globe. Attack Microsoft Exchange and you attack millions of people worldwide in one hit. Threat actors are simply playing the odds in their ambition to drop malware, including ransomware, on victims' email servers.

This is exactly what happened in 2021 when Calypso, LuckyMouse, Tick and Winnti Group, among others, exploited Microsoft Exchange vulnerabilities to compromise email servers all around the globe. Several large and influential organizations, such as the Swedish supermarket chain Coop, suffered at the hands of the attackers. The nature of the vulnerabilities allowed the installation of a web shell to the server, which was then used to serve as an entry point for further malware installation.

Staying locked up and secure

The NIST Cybersecurity Framework from the U.S. federal government provides a valuable starting point for anyone wanting to ensure that his or her supply chain remains locked up and secure. It recommends that *"The practice of communicating and verifying cybersecurity requirements among stakeholders is one aspect of cyber supply chain risk management (SCRM). A primary objective of cyber SCRM is to identify, assess and mitigate products and services that may contain potentially malicious functionality, are counterfeit or are vulnerable due to poor manufacturing and development practices within the cyber supply chain."*

The importance of patch management

The propensity for supply chain attacks also highlights the importance of **adequate patch management processes**. This helps ensure that any potential back doors to your organization are shut as soon as they are discovered. Software companies watch closely for new vulnerabilities in their applications and regularly release security updates that eliminate potential threats. Prevention is always better than protection. It is, therefore, **important to download these security updates as soon as they are released.** If you are running Windows, you can learn more about automatic updates from Microsoft here.