
# Manufacturers should focus on protecting their supply chains

Sep 22, 2021

The manufacturing sector is highly dependent on a secure supply chain. Companies powering this sector are acutely aware of how a cyber attack on any part of a supply chain can bring their business to a screeching halt.

When it comes to cybersecurity protections, this sector must focus on protecting its technological supply chain, as it serves as a juicy target for cybercrminals to attack. In particular, Intel 471 has observed ransomware-as-a-service crews and network access brokers target various manufacturing companies in order to carry out their crimes.

## A Worldwide Problem

Some of the biggest cybersecurity incidents in the past year show how susceptible supply chains can be with regards to a company's IT stack. Here are some of the incidents that have struck third-party IT providers, causing a cascading problem across several industries, including manufacturing:

- In July 2021, affiliates or operators of the REvil ransomware-as-a-service (RaaS) compromised Kaseya, a technology company that provided IT management software to more than 1,000 organizations. The attack was estimated to impact about 1 million downstream systems belonging to managed service providers (MSPs) and customers utilizing Kaseya's remote monitoring and management products. The attackers set a ransom demand of US $70 million, which would allow Kaseya to obtain a decryption key and recover data for all its downstream customers.

- On Dec. 13, 2020, news outlets reported an intrusion campaign by alleged Russian advanced persistent threat (APT) group APT29 that successfully breached IT company SolarWinds and conducted a supply chain attack against SolarWinds customers including the U.S. Treasury, Commerce Department and cybersecurity firm FireEye. According to FireEye, the actors breached numerous private and public victims via trojanized updates to SolarWinds' Orion IT monitoring and management software.

- In March 2021, At least 30,000 organizations across the United States — including a significant number of small businesses, towns, cities and local governments — have over the past few days been hacked by an unusually aggressive Chinese cyber espionage unit that's focused on stealing email from victim organizations, multiple sources tell KrebsOnSecurity. The espionage group is exploiting four newly-discovered flaws in Microsoft Exchange Server email software, and has seeded hundreds of thousands of victim organizations worldwide with tools that give the attackers total, remote control over affected systems.

While Intel 471 does not have exact numbers on how many of these impacted organizations were in the manufacturing or industrial center, the above examples show how ubiquitous software can be. Wildly successful products are pervasive across IT systems of all kinds, which presents huge targets for cybercriminals to go after.

## Ransomware is Everywhere

While ransomware-as-a-service gangs have announced over the past few months that they will stay quiet in the wake of high-profile attacks that have negatively impacted their operations, Intel 471 has observed attacks have continued unabated. Several different RaaS gangs have gone after organizations in the manufacturing industry, including but not limited to:

- BlackMatter
- CLOP
- Conti
- LockBit 2.0
- Prometheus
- REvil
- Ragnar Locker
- Vice Society (aka "FiveHands" or "HelloKitty")

All of these groups and their affiliates go after all shapes and sizes of organizations. We've seen them attack companies with yearly revenue anywhere from thousands to hundreds of millions. The moving financial targets come from attackers doing their research on an organization's finances to tailor a ransom request that an organization

can ultimately pay.

## Credentials are Key

If attackers can't get into an organization through a vulnerability, they will do so through compromised credentials. It's through this credential abuse that attackers can break into organizations' IT systems and launch ransomware attacks. Here are some examples of network access brokers selling compromised credentials on the cybercrime underground:

- In late August, an actor was selling access to 100 different organizations, including a Turkish plastics company, a Turkish machinery fabrication company, and German automotive parts manufacturer

- Also in late August, a prolific access broker advertised a new list of more than 500 organizations that had been compromised, including an Egyptian building materials company, a German electronics manufacturer, and a steel products manufacturer in Singapore

- In July, a Russian-linked actor advertised access to a Turkish automotive component industrial manufacturer via a compromised Citrix account with domain administrator-level privileges that allegedly could be used to edit, modify, add or remove files.

The manufacturing sector is as dependent on technology as any other economic sector. With that trend likely to keep growing, it's imperative that these companies understand where their weak spots are when it comes to cybersecurity and how the cybercrime underground will exploit them if those weaknesses are left unchecked. Keys to a successful business often rely on the internet, just as cybercriminals rely on it to carry out their crimes. By being proactive in assessing risk and closing vulnerabilities, manufacturers will prevent their technology stacks from being a target for the cybercrime underground.