Longitude149

Title: Toyota production to resume after supply chain attack
Published: 01 Mar 2022
Author(s): Alex Scroxton
Original Source: computerweekly.com[1]

# Toyota production to resume after supply chain attack

## Toyota production has been set back by over 10,000 vehicles following a cyber attack on a critical components supplier in Japan

Production of Toyota vehicles, which was temporarily suspended across Japan following a cyber attack on a critical supplier, is to resume on Wednesday 2 March, as the disruption draws warnings about the risks associated with important elements of supply chains.

The attack took place against the systems of Kojima Industries, which is contracted to supply plastics and electronic components to Toyota. According to Reuters, the firm found an error on a file server on Saturday 26 February. Following a reboot, it found malware, and a "threatening message", which may indicate it has fallen victim to a ransomware attack.

The incident has left Kojima unable to ship deliveries to Toyota, which, as a proponent of so-called "just-in-time" manufacturing, does not stockpile parts. It is estimated that production of Toyota vehicles will be set back by about 13,000 units as a result.

A Toyota spokesperson said: "Due to a system failure at a domestic supplier, we suspended our operations on all 28 lines at 14 domestic plants in Japan today, Tuesday 1 March. However, we have decided to resume all operations from the first shift tomorrow, Wednesday 2 March.

"We would like to apologise again to our customers, suppliers and other related parties for any inconvenience caused by today's sudden shutdown," they said.

"Working together with our suppliers, we will make every effort to deliver vehicles to our customers as soon as possible."

It must be stressed that there is no indication that the attack on Kojima has any link to a Russian actor, although in the past few days it is true that Japan has expressed support and offered aid to Ukraine. The Japanese authorities are investigating the possibility, but any further commentary on this point must be treated as pure speculation for now.

[1] https://www.computerweekly.com/news/252514016/Toyota-production-to-resume-after-supply-chain-attack

Bulletproof and Defense.com CEO Oliver Pinson-Roxburgh described the Kojima-Toyota incident as a near-textbook example of a supply chain attack via a supplier.

“Up to 40% of cyber threats are now occurring indirectly through the supply chain,” he said. “It is not enough for businesses to focus on cyber security for just their core corporate network. Every endpoint across an organisation’s technology portfolio needs to be accounted for and protected.

“Research also shows that more than a quarter of organisations do not patch critical vulnerabilities even though they are aware of them,” said Pinson-Roxburgh. “This is a massive threat vector for bad actors to exploit as it can not only impact the company under attack, but as in this case, it can lead to third-party suppliers becoming victims. There needs to be an urgent shift in focus so organisations are not only protecting their own assets but are actively monitoring for threats at every touchpoint they have with other organisations.”

Süleyman Özarslan, co-founder of Istanbul-based Picus Security, said that big game hunting ransomware gangs were known to target the manufacturing sector, and in particular organisations with a similar profile to Kojima.

“Factories will always remain a lucrative target for ransomware,” he said. “Attackers know that manufacturing businesses cannot afford long periods of downtime, such is their importance in the global supply chain. Rightly or wrongly, they are assumed to have the funds required to pay a big ransom, and the inclination to do so as quickly as possible.

“It’s highly disconcerting that a cyber attack can pump the brakes on production at the world’s best-selling car maker,” added Özarslan. “Kojima Industries is a tier-one supplier of Toyota, which may be a significant detail; because of Toyota’s just-in-time production methodology, tier-one suppliers like Kojima may be directly connected to Toyota’s internal networks.

“Naturally, just-in-time production methodologies are more sensitive to cyber attacks. As such, and as a consequence of stories like this one, cyber attacks may play a vital role in shaping production methodologies in the near future.”

###