Hackers target Airbus suppliers in quest for commercial secrets

September 26 2019, by Daphne Benoit, Fabien Zamora, Laurent Barthelemy and Mathieu Rabechault

This picture shows an Airbus A-320 of the Iberia airline during take-off on September 24, 2019 at the airport in Duesseldorf, western Germany.

European aerospace giant Airbus has been hit by a series of attacks by hackers targeting its suppliers in search of commercial secrets, sources told AFP, adding they suspected a Chinese link.

AFP spoke to seven security and industry sources, all of whom confirmed a spate of attacks in the past 12 months but asked for anonymity because of the sensitive nature of the information they were sharing.

Two security sources involved in investigating the hacking said there had been four major attacks.

Airbus has long been considered a tempting target because of the cutting-edge technologies that have made it one of the world's biggest commercial plane manufacturers, as well as a strategic military supplier.

In January, it admitted to a security incident that "resulted in unauthorised access to data", but people with knowledge of the attacks outlined a concerted and far bigger operation over the last year.

AFP's sources said the hackers targeted British engine-maker Rolls-Royce and the French technology consultancy and supplier Expleo, as well as two other French contractors working for Airbus that AFP was unable to identify.

Airbus did not immediately reply to a request for comment.

A spokesperson for Rolls-Royce declined to comment on the specifics of any attack but said: "We have experience of attempts to gain access to our network and we have a team of experts who work closely with the relevant authorities to ensure that we combat these attempts and minimise any potential impact."

Expleo said it would neither "confirm nor deny" that it had been targeted.

Romain Bottan of the aerospace security specialist BoostAerospace said the intrusions as described by sources to AFP showed that hackers were seeking out weak links in the chain to compromise Airbus's systems.

"Very large companies are very well protected, it's hard to pirate them, so smaller companies are a better target," he said.

VPN entry point

The attack against Expleo was discovered at the end of last year but the group's system had been compromised long before, one of the sources told AFP on condition of anonymity.

"It was very sophisticated and targeted the VPN which connected the company to Airbus," the source said.

A VPN, or virtual private network, is an encrypted network that enables employees to access company systems remotely.

Airbus suppliers sometimes operate in a VPN linking them with colleagues at the plane-maker.

The other attacks used the same methods, with the first of them detected at a British subsidiary of Expleo, formerly known as Assystem, as well as Rolls-Royce, which provides engines for Airbus planes.

According to several of the sources, the hackers appeared to be interested in technical documents linked to the certification process for different parts of Airbus aircraft.

They also said that several stolen documents were related to the innovative turbo-prop engines used on the Airbus military transport plane A400M.

One of the sources said the hackers were also interested in the propulsion systems for the Airbus A350 passenger jet, as well as its avionics systems controlling the plane.

Who to blame?

None of the sources who spoke to AFP could formally identify the perpetrators of the attacks, pointing to the extreme difficulty in obtaining evidence and identification.

Many state-backed and independent hackers are known to disguise their tracks, or they may leave clues intended to confuse investigators or lead them to blame someone else.

But the sources said they suspected Chinese hackers were responsible, given their record of trying to steal sensitive commercial information and the fact that Beijing has just launched a plane designed to compete with Airbus and US rival Boeing.

State-owned plane-maker Comac has already launched manufacturing of its first mid-range airliner but has struggled to get it certified.

Engines and avionics are "areas in which Chinese research and development is weak," one of the sources said.

In its quest to break the stranglehold of Airbus and Boeing on the global aircraft market, Beijing also has ambitions to build a long-haul jet called the C929, which will be developed in partnership with Russia.

Several sources said they believed a group of hackers linked to the Chinese Communist Party, known as APT10, could be behind the attacks.

The United States considers APT10 to be state-backed hackers linked to the Chinese intelligence services and military.

But another source pointed to another group of Chinese hackers known as JSSD, which are believed to operate under the regional security ministry in the coastal province of Jiangsu.

"The JSSD is focused on the aerospace industry," one source said, explaining that they employ people "familiar with the language, the software and aerospace codes."

In October 2018, the US Justice department named several JSSD officers as being responsible for a hacking operation targeting an engine being developed by US-based General Electric and French aerospace group Safran.

"At the time of the intrusions, a Chinese state-owned aerospace company was working to develop a comparable engine for use in commercial aircraft manufactured in China and elsewhere," a US statement said.

France and Airbus have been left in a delicate position by the discovery of the hacking attacks, sources told AFP, with the country and company needing to take into account their commercial ties with China.

Achilles' heel

The attacks show up the vulnerability of Airbus to intrusions via its global supplier network, and the value of its technology to foreign countries.

"The aerospace sector is the one that suffers most from cyberattacks, mostly through spying or people seeking to make money from this industry," said Bottan of BoostAerospace.

There is also a major industrial risk for Airbus, with hackers potentially able to knock out production for strategic suppliers which would have a knock-on effect on production.

"If someone wanted to slow down production, they can quickly identify the critical supplier, the single sources, which are unique in their role," one expert said.

Belgian aerospace design and manufacturing firm ASCO had an IT meltdown earlier this year caused by malware, and it took a month to restore its systems, one source said.

That incident hit Airbus production.

Citation: Hackers target Airbus suppliers in quest for commercial secrets (2019, September 26) retrieved 2 May 2024 from https://techxplore.com/news/2019-09-hackers-airbus-suppliers-quest-commercial.html