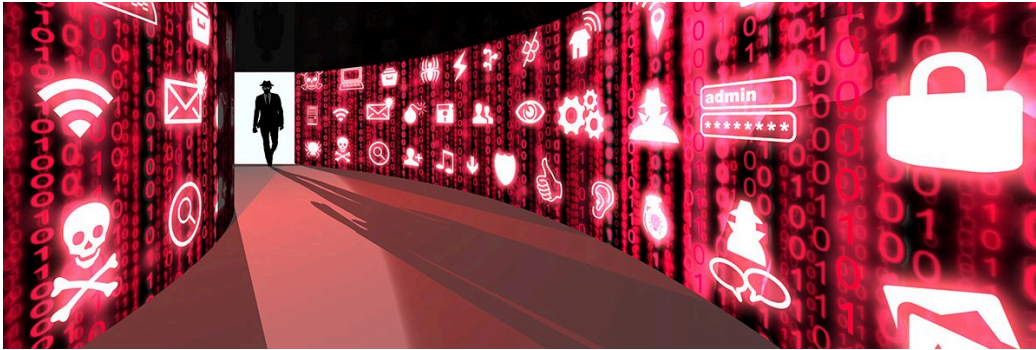


New threat group behind Airbus cyber attacks, claim researchers

By Alex Scroxton

Published: 2019-10-03 · Archived: 2026-04-02 12:05:00 UTC



beebright - stock.adobe.com

beebright - stock.adobe.com

Context Information Security’s threat intel and response teams says it has evidence that the recent supply chain attacks on Airbus are the work of a newly identified group called Avivore

-
-

A number of [high-profile cyber attacks on Airbus](#) in the past 12 months, which exploited [virtual private networks](#) (VPNs) used by some of its supply chain partners to access the aerospace firm’s systems, is likely to have been the work of a previously unidentified threat group, according to [Context Information Security’s](#) researchers.

Dubbed Avivore, the group’s existence came to light during Context’s investigation of a number of attacks against multinational enterprises that compromise smaller engineering services and consultancies working in their supply chains.

In such supply chain attacks – also known as [Island Hopping](#) – the adversary uses legitimate connectivity or collaboration tools to bypass the target’s perimeters. These attacks will often see criminals using chains of activity or connections spanning multiple business and geographical locations in the victim environment.

The Avivore group, which has not been identified or tracked before, seems to have targeted assets related to a number of verticals besides aerospace and defence, including automotive, energy, and space and satellite technology.

“Previous reporting into recent incidents affecting aerospace and defence have linked this activity to [APT10](#) and JSSD (Jiangsu Province Ministry of State Security). Though the nature of the activity makes attribution

challenging, our experience of the campaign suggests a new group that we have codenamed Avivore,” said Oliver Fay, principal threat intelligence analyst at Context.

The group appears to operate in the UTC +8 timezone and exploits [the PlugX remote access Trojan](#), which has been used extensively by APT10.

However, its tactics, techniques and procedures (TTPs), infrastructure and other tooling is significantly different to known Chinese-state actors. It is this that has led Context to the conclusion that Avivore is a previously untracked nation state-level adversary.

According to Context, the group is a “highly capable” actor, skilled at living-off-the-land and obfuscating its activity in the day-to-day business activities of its victims’ employees. It also appears to have a high degree of operational security awareness – for example, it clears forensic artefacts as it progresses to make detection harder.

“The capability of the threat actor makes detecting these incidents challenging, however the complex nature of the supplier relationship makes investigation, co-operation and remediation a significant issue,” said James Allman-Talbot, head of cyber incident response at Context.

“When the organisation that has enabled the intrusion forms a critical part of your value chain, the operational business risk increases dramatically and difficult decisions need to be made in a short space of time.”

Context set out a number of recommendations for enterprises to consider adopting whether they are likely to be a target of a supply chain attack or not.

These include imposing access limitations on supplier and partner connections using VPNs, such as preventing use outside business hours, agreeing specific locations and IP addresses for access, and imposing restrictions on access to data and other assets.

Other useful steps could include introducing multifactor authentication and enhancing auditing and logging at hosts and services into which suppliers connect.

Steps should also be taken to ensure that remote access services implement appropriate log retention; to ensure that credentials for remote services are stored securely and their use monitored; and where possible, to make applications, documents and technical information relating to enterprise networks and remote access services available only to engineers and IT support staff.

Read more on Hackers and cybercrime prevention



[Cyber attack that downed airport systems confirmed as ransomware](#)



[By: Alex Scroxton](#)



[TCS to inject AI and quantum computing into aerospace through French delivery centre](#)



[By: Karl Flinders](#)



[GenAI provides future for connected engineering](#)



[By: Joe O'Halloran](#)



[Dassault Systèmes, Cranfield collaborate on 3DEXperience centre of excellence](#)



[By: Joe O'Halloran](#)

Source: <https://www.computerweekly.com/news/252471769/New-threat-group-behind-Airbus-cyber-attacks-claim-researchers>