Context Identifies new AVIVORE threat group

03 Oct 2019

The Threat Intelligence and Incident Response Team at Context Information Security has identified a new threat group behind a series of incidents targeted at the aerospace and defence industries in the UK and Europe. Named by Context as AVIVORE, the group is not previously publicly known or reported and Context believes it is responsible for the recently reported attacks within the aerospace and defence supply chain.

Context has been investigating attacks against large multinational firms that compromise smaller engineering services and consultancy companies in the supply chain for more than 12 months. The attackers use legitimate remote connectivity or other collaborative working solutions to bypass the generally well-defended perimeters and gain access to the target. This technique, referred to as 'Island Hopping', has also seen the adversary leverage chains of activity or connections across multiple business units or geographical locations within victim environments.

As a result of its discoveries, Context has been working closely with victims, security organisations and law enforcement agencies across Europe, including the UK's National Cyber Security Centre (NCSC), in order to reduce the impact and prevent further compromises. In addition to aerospace and defence engineering victims, Context has seen AVIVORE target assets related to other verticals including automotive, consultancy, energy/nuclear and space and satellite technology. Context also assesses with moderate confidence that the objective of the campaign is intellectual property theft.

"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.

Whilst AVIVORE has been observed operating in the UTC+8 timezone and makes use of the PlugX Remote Access Trojan shared with APT10 and other actors, the Tactics, Techniques and Procedures (TTPs), infrastructure and other tooling differ significantly. This

leads Context to believe that this activity is attributed to a previously untracked nation-state level adversary.

AVIVORE has shown itself to be a highly capable threat actor, adept at both 'living-off-the-land' and masquerading its activity within the 'business as usual' activities of employees in its victim organisations. It has also shown a high degree of operational security awareness, including routinely clearing forensic artefacts as it progresses, making detection and investigation difficult.

"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."

To mitigate against these attacks, Context recommends the following measures:

- Impose access limitations on supplier connections over VPNs, such as preventing their use outside of the supplier's business hours or from IP addresses and locations other than those pre-agreed and restrict access only to data and assets they require to perform their actions.

- Ensure that security measures, such as multifactor authentication and enhanced auditing/logging are deployed to hosts and services into which suppliers are required to connect, in order to prevent or support the investigation of any suspicious user behaviour.

- Ensure that external remote access services implement appropriate log retention, including sources of inbound connections and that identification of concurrent or adjacent geographically-impossible connections is possible.

- Ensure that credentials for highly privileged accounts and remote services are stored securely and their use is appropriately monitored. Hosts such as domain controllers, sensitive file shares and Public Key Infrastructure servers, should also be subject to additional scrutiny and monitoring.

- Where possible, applications, documentation and technical information related to network infrastructure and configuration of remote access services should be made available only to engineers, IT support staff and other individuals with legitimate business needs.

For a more detailed blog on AVIVORE, please go to:
https://www.contextis.com/en/blog/avivore

Learn more about AVIVORE with our Webinar: Defending against new AVIVORE threat group. Register now