AVIVORE – Hunting Global Aerospace through the Supply Chain

contextis.com/en/blog/avivore

Until now, most prominent supply chain intrusions have been "vertical"; initial victims are typically Managed Services Providers or software vendors leveraged by attackers to move up or down the supply chain. However, since summer 2018, Context Information Security has been investigating a series of incidents targeting UK and European Aerospace and Defence that are best described as "horizontal". Advanced attackers have been leveraging direct connectivity between suppliers and partners who are integrated into each other's value chains. We have been tracking this activity under the codename AVIVORE.

Affected victims include large multinational firms (Primes) and smaller engineering or consultancy firms within their supply chain (Secondaries). Context has worked closely with victims, the National Cyber Security Centre (NCSC), security organisations, and law enforcement agencies across Europe to reduce impact and prevent further compromise.

Who is AVIVORE?

Context categorises AVIVORE as a previously unknown and untracked nation-state level adversary, whose operators' working hours appear to correlate to a time zone of UTC +8. The primary objective for their intrusions is believed to be espionage, as well as access enablement through supply chain partners.

Recent reporting into incidents affecting Aerospace and Defence Primes has speculated that either APT10 or JSSD (Jiangsu Province Ministry of State Security) may be responsible for this activity. Whilst certain similarities between these adversaries' campaigns and those investigated by Context exist, the Tactics, Techniques and Procedures (TTPs), infrastructure

and tooling observed differ significantly. Whilst involvement of these named adversaries cannot be ruled out, available evidence suggests this campaign is the work of a separate adversary group.

Capable and Adaptable

AVIVORE showed themselves to be highly capable; adept at both “living-off-the-land” (masquerading as legitimate users) and in their operational security awareness; including forensically covering their tracks. They demonstrated detailed knowledge of key individuals associated with projects of interest, and were able to successfully mirror working times and patterns of these users to avoid arousing suspicions. They were also able to manipulate victim environments and security controls to facilitate and obfuscate their activities (e.g. modifying firewall rules to accept RDP over alternate ports; establishing hosts within the victim environment as remote access proxies). AVIVORE’s attack methodology for the linked intrusions followed a relatively set-format:

- Access into victim through leverage of compromised user credentials and legitimate external remote access services;
- Escalate privileges within victim environment via abuse of legitimate tools and/or highly privileged service and enterprise administrator accounts;
- Conduct account and host enumeration using 'net' commands;
- Schedule execution of scripts and tooling run in the context of the ‘SYSTEM’ user;
- Remove forensic artefacts of scripts & tooling, and clearing of event logs following execution;
- Use of RDP for lateral movement around the victim environment.

Infrastructure and Tooling

AVIVORE made extensive use of infrastructure providing interconnectivity between victims; affected Secondaries are often suppliers to multiple Primes and frequently maintain direct network connectivity via Virtual Private Networks (VPNs) or other remote and collaborative working solutions. AVIVORE exploited this relationship to bypass the (generally well-defended) perimeters of the Primes, evading critical controls and taking advantage of the challenges many organisations face in cross-boundary coordination.

This technique, referred to as "Island Hopping", allowed AVIVORE to chain activity across multiple business units (with local IT and security teams operating independently) or geographical locales within victim environments. Where Context had visibility of victim-facing network infrastructure employed by AVIVORE, it primarily consisted of commercial VPN infrastructure located in Singapore and Japan, as well as Tor. This all served to obfuscate the origin of AVIVORE’s connections into victim networks and made investigation challenging.

AVIVORE demonstrated a preference for in-built system tooling and abuse of legitimate software. They introduced network scanning and certificate extractions tools, as well as Windows SysInternals tools such as ProcDump, across multiple victim environments. These binaries were renamed to imitate Windows DLLs and staged in file system locations associated with compatibility and performance logging. Such tools were typically executed on remote systems using scheduled tasks and then removed, together with their output, following execution.

Multiple instances of the PlugX Remote Access Trojan were discovered on compromised hosts. Evidence suggested these implants were deployed between October 2015 and October 2016. File system artefacts indicated that attackers may have interacted with them between deployment and the 2018 intrusions. Although direct interaction with these implants was not observed during the investigation period, Context assess with low-moderate confidence that they may be associated to the AVIVORE intrusions. Evidence indicated that some of the implants were patched in-memory, with modified configuration blocks injected post-execution to provide new C2 domains during times AVIVORE operators were active inside victim environments.

Future Recommendations and Mitigations

Though the majority of activity investigated by Context has taken place since Jan/Feb 2018, artefacts from some victim environments indicate that AVIVORE likely maintained persistent access since October 2015, and potentially even earlier. Therefore, it is possible that this is a small portion of a broader campaign. In addition to Aerospace and Defence engineering victims, Context has seen AVIVORE target assets related to a number of other verticals including:

- Automotive
- Consultancy
- Energy/Nuclear
- Space and Satellite Technology

Based on the information and assets sought by AVIVORE, Context assesses with moderate confidence that the objective of the recent campaign was intellectual property theft from victim organisations. Although defence against advanced nation-state level actors can be challenging, Context recommend the following mitigations to disrupt future AVIVORE activity:

- 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. Logs should contain enough information on the sources of inbound connections to enable identification of anomalies, such as concurrent log-ins with impossible geography.
- 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 particular 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 need.