Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
https://echonetwork.eu/wp-content/uploads/2020/04/20200408-ECHO-WhitePaper-Hackers-Mindset-FINAL.pdf.

15. Jolly, J. 'Huge rise in hacking attacks on home workers during lockdown'. The Guardian, 24 May 2020. Accessed Jul 2020. www.theguardian.com/technology/2020/may/24/hacking-attacks-on-home-workers-see-huge-rise-during-lockdown.

16. Wakefield, J. 'Zoom boss apologises for security issues and promises fixes'. BBC News Online, 2 Apr 2020. Accessed Jul 2020. www.bbc.com/news/technology-52133349.

17. Newhouse, W; Keith, S; Scribner, B; Witte, G. 'National Initiative for Cyber security Education (NICE) Cyber security Workforce Framework'. NIST Special Publication 800-181, National Institute of Standards and Technology, Aug 2017.

18. 'Home working: preparing your organisation and staff'. National Cyber Security Centre, 17 Mar 2020. Accessed Jul 2020. www.ncsc.gov.uk/guidance/home-working.

19. 'Top tips for staying secure online'. National Cyber Security Centre, 17 Dec 2018. Accessed Jul 2020. www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online.

20. ‘Top 5 Steps to Securely Work from Home’. SANS Security Awareness, Mar 2020. Accessed Jul 2020. www.sans.org/sites/default/files/2020-03/02-SSA-WorkingFromHome-FactSheet.pdf.

21. ‘Future impacts of the Coronavirus on Britain’. Ipsos MORI, 1-4 May 2020. Accessed Jul 2020. www.ipsos.com/sites/default/files/ct/news/documents/2020-05/impact_of_coronavirus_-_economy_lives_work.pdf.

A deep dive into Avivore

Oliver Fay, Context Information Security

Until now, most prominent supply chain intrusions have been vertical attacks, with the initial victims typically managed service providers (MSPs) or vendors targeted as a way of getting into and moving up or down the supply chain. However, incidents earlier this year targeting large multi-national firms in the aerospace and defence sectors can best be described as horizontal. Advanced attackers have been leveraging relationships and connectivity between suppliers and partners to get a foothold in each other’s value chains.

While investigating these recent supply chain attacks, Context researchers identified a new threat group that they code-named Avivore. The group was found to be compromising remote connectivity or other collaborative working solutions used by smaller engineering services and consultancy companies in the supply chain to bypass well-defended perimeters and gain access to the main target.

Avivore has been categorised as a previously unknown and untracked nation state-level adversary and the reports into incidents affecting aerospace and defence primes had led to speculation that one of the cyber espionage groups, APT10, the Jiangsu Province Ministry of State Security or JSSD, may be behind them. However, as noted during the investigations, the tools, techniques and processes (TTPs), infrastructure and tooling observed were different from previous campaigns by these groups, so it was possible that it was the work of another, entirely different attacker.

**Capable and adaptable**

This particular threat group showed itself to be highly capable, adept at ‘living off the land’, masquerading as legitimate users, as well as forensically covering its tracks. The group demonstrated detailed knowledge of key individuals associated with projects of interest and mirrored the working times and patterns of those users to avoid arousing any suspicions. The attackers were also able to manipulate their victims’ environments and security controls in order to facilitate and obfuscate their activities. Examples include modifying firewall rules to accept remote desktop protocol (RDP) over alternate ports and establishing hosts within the victim environment as remote access proxies.

**Island hopping**

Avivore makes extensive use of the infrastructure providing interconnectivity between its victims, a technique referred to as ‘Island hopping’. This involves establishing multiple layers of access using compromised credentials, remote access protocols, and establishing communication channels through other hosts to avoid detection.

The group’s attack methodology for the linked intrusions followed a relatively set format. This was firstly gaining access to the victims through compromised user credentials and legitimate external remote access services, then escalating privileges within the victim environment via the abuse of legitimate tools and/or highly privileged service and enterprise administrator accounts. Next was carrying out account and host enumeration using ‘net’ commands; scheduling the execution of scripts and a tooling run in the context of the ‘SYSTEM’ user and then going on to remove forensic artefacts of scripts and tooling; and the clearing of event logs following execution. Finally, the group used RDP for the lateral movement around the victim environment.
to as ‘island hopping’. The secondaries affected are often the suppliers to multiple prime targets and frequently maintain direct network connectivity via VPNs, or other remote and collaborative working solutions. These relationships are exploited by the group in order to bypass the generally well-defended perimeters of the main targets and evade critical controls; as well as take advantage of the challenges many organisations face when it comes to cross-boundary co-ordination.

“Avivore is able to chain activity across multiple business units or geographical areas within victim environments, which serves to obfuscate the origin of the group’s connections into victim networks”

This in turn means that Avivore is able to chain activity across multiple business units or geographical areas within victim environments, which serves to obfuscate the origin of the group’s connections into victim networks and consequently makes investigations challenging.

The group also demonstrates a preference for in-built system tooling and the abuse of legitimate software. It has introduced network scanning and certificate extraction tools, as well as Windows SysInternals tools such as ProcDump, across multiple victim environments. These are renamed to imitate Windows DLLs and staged in file system locations, which are associated with compatibility and performance logging. These are typically executed on remote systems using scheduled tasks and then removed, together with their output, following execution.

Mitigations for Avivore

Based on the information and assets sought by the attackers, it is thought that the aim of the campaign is intellectual property theft. Although defence against advanced nation-state actors can be challenging, the following is recommended to help disrupt any future Avivore activity:

- Impose access limitations on supplier connections over VPNs – for example, preventing their use outside of suppliers’ business hours or from IP addresses and locations other than those which are pre-agreed, and restrict access only to data and assets required to perform certain actions.
- Ensure that security measures such as multifactor authentication and enhanced auditing and logging are deployed to hosts and services into which suppliers are required to connect.
- Make sure that external remote access services implement the appropriate log retention with enough information on the sources of inbound connections, so anomalies can be identified, such as those with impossible geography.
- Securely store credentials for highly privileged accounts and remote services and make sure their use is appropriately monitored. Domain controllers, sensitive file shares and public key infrastructure (PKI) servers should also be subject to additional scrutiny.
- Where possible, applications, documentation and technical information related to infrastructure and the configuration of remote access services should be made available only to engineers, IT support staff and other individuals with a legitimate business need.

Masquerading as a different threat actor has its advantages to deflect blame and stay under the radar. It can take detailed forensic work to identify a new group. Since originally identifying Avivore, Context has been working closely with the victims, the National Cyber Security Centre (NCSC), security organisations and law enforcement agencies across Europe in order to reduce impact and prevent further compromise by Avivore and any similar new threat actors.

Attack techniques

Below are some examples of methods used by Avivore. The numbers in brackets are the Mitre ATT&CK codes.

External Remote Services: Avivore employs legitimate remote access services including VPN gateways and Citrix Receiver to directly access victim environments (T1133).

Supply Chain Compromise: Avivore has been observed using compromised accounts belonging to managed service providers and conducting intrusions from networks belonging to third-party suppliers to victims (T1195).

Trusted Relationship: By using accounts belonging to legitimate suppliers and other trusted third parties, Avivore abuses trust relationships between its victims and organisations inside their supply chain (T1195).

Valid Accounts: By using compromised accounts belonging to senior engineers, IT staff and suppliers, Avivore is able to access the networks of its victims (T1078).

Tell-tale TTPs

Mitre ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government and in the cyber security product and service community.

ATT&CK is also used to visualise and represent the adversary tactics, techniques and procedures (TTPs) identified at different stages of real-world incidents. The ATT&CK mapping for Avivore has been made available in order to aid network defenders to identify critical controls and areas of visibility which may assist them in mitigating or detecting activity by this adversary.
Sophisticated adversaries such as Avivore are extremely resourceful and will tailor the techniques used to the victim environment. This means that they will rarely use all the capabilities within their arsenal in a single intrusion, nor will they limit themselves to only previously observed techniques.

The future of Avivore

Avivore remains active and the sectors it has targeted remain a high priority for critical networks. However, the current climate created by the arrival of Covid-19 may have had some impact on the level of activity – not least because supply chains are not as active. But it is likely that Avivore and other groups employing similar techniques are turning their attention to other high-priority sectors and regions.

The particular TTPs used by Avivore, along with a growing understanding of its victims’ environments, make it highly likely that it would be able to remain under the radar and retain access to other connected victims, potentially in other sectors, without detection.

Aside from leveraging certain custom capabilities, Avivore’s approach, which is heavily based on ‘living off the land’ and abuse of legitimate/native functionality, is becoming widely used, and therefore it is becoming increasingly difficult to be certain who exactly is conducting intrusions – Avivore or other actors. Attribution has always been a challenge for the cyber security industry and it’s not getting any easier.

About the author

Oliver Fay is a principal consultant in the Response & Advisory team at Context Information Security (www.contextis.com) and leads the company’s Technical Threat Intelligence Services. He manages the delivery of complex analysis and threat intelligence projects and is a CREST Certified Threat Intelligence Manager.

References

1. ‘Context Identifies new AVIVORE threat group’, Context Information Security, 3 Oct 2019. Accessed Jul 2020. www.contextis.com/en/news/context-identifies-new-avivore-threat-group.
2. Mitre ATT&CK, home page. Accessed Jul 2020. https://attack.mitre.org/.

Marc Lueck

Since May 2018, the General Data Protection Regulation (GDPR) has required any organisation doing business with European citizens to make significant changes to its data processes. Over the two years since it came into law, it has ushered in a new level of data hygiene to enterprises.

This was not a painless process, however. Organisations globally went through the often costly exercise of ensuring they had an overview of personal information, as well as implementing tools to be able to process and store that data in a secure manner.

When the GDPR came into force, many organisations quickly deployed best-of-breed security tools to keep their data secure. At that time, the focus was predominantly limited to office boundaries. Now, with current social distancing guidelines forcing huge swathes of the workforce to work remotely, and potentially shifting business focus away from the office environment in the future, organisations are having to revisit their initial efforts and ensure that compliance with GDPR can still be achieved in this new normal. What follows are guidelines as to how organisations can ensure this.

Impact assessments

Businesses that already had processes and policies in place for remote working are in the enviable position of merely having to ensure that those policies and rules are in use by their staff working from home. However, those organisations which have only had an onsite workforce or offered limited flexible working will need to identify if en masse working from home impacts or changes risk levels. This will require opening up their records of processing activities and each of their data protection impact assessments (DPIA).

A DPIA is a process to identify data protection and privacy risk and address them accordingly. Under GDPR, where processing operations present specific risks to individuals’ privacy rights due to their nature, scope or purpose, controllers carry out an assessment of the impact of the proposed processing operations on the protection of personal data.

It’s key to note that a DPIA is an ongoing process, and as any project develops or a new situation arises, new risks might be identified. Means to avoid those risks must also be found. When an organisation is making significant changes to an existing system or process – as might be the case with remote working – it’s necessary to revisit the DPIAs and...