Client Threat Advisory:
Financially Motived Criminal Group Uses Advanced Social Engineering Tactics and Reconnaissance to Target Telecom, Technology & Manufacturing

This client advisory provides an overview of techniques and tactics attributed to a financially motivated criminal group that is actively targeting organizations across various industries. Aon's Stroz Friedberg Incident Response and the Threat Intelligence team has investigated multiple related incidents in recent months. This advisory details observations from the initial attack phase to the impacted network infrastructure as well as suggested security mitigation recommendations.

Overview

Aon has observed currently active and persistent targeting of organizations across telecommunications, technology, manufacturing, and other related sectors by a financially motivated criminal group. This threat actor is known as Scattered Spider, UNC3944, 0ktapus, and other variations of these names due to different naming conventions used by security companies.

This threat actor group was first observed by security researchers in May 2022[1] and has established itself as using advanced social engineering tactics to gain initial access, conducting reconnaissance within victim organizations' networks, and exfiltrating sensitive data from Cloud environments. In some instances, the group has been observed deploying ransomware with a focus on ESXi servers. These targeted campaigns have led to financial and reputational damage to impacted organizations across telecom, technology, manufacturing, logistics and outsourcing, and cryptocurrency industries.

[1] https://thehackernews.com/2023/05/threat-group-unc3944-abusing-azure.html

This threat actor's attacks are characterized by tactics, techniques, and procedures (TTPs) such as SIM swapping, social engineering, and quick lateral movement across a victim's environment. The main TTPs observed are as follows:

- Conducting large-scale SIM swapping attacks.
- Carrying out coordinated phishing attacks. Uses Telegram or SMS messages to redirect to phishing sites.
- Using social engineering tactics such as calling Help Desk employees and impersonating IT staff.
- Focusing on MFA fatigue to bypass MFA.
- Demonstrating a robust understanding of Azure, AWS, and Microsoft 365 environments.
- Exfiltrating large volumes of sensitive data from both on-premise and cloud environments.

Tactics Techniques & Procedures (TTPs)

This threat actor has been observed deploying a variety of tactics, typically using existing technologies within a victim's environment. Common tactics identified across Aon engagements attributed to this threat actor include the following TTPs during the initial access and reconnaissance phases of the attack.

Initial Access

- This threat actor may attempt to gain access to a privileged account through social engineering of an organization's password and Multi Factor Authentication (MFA) reset process. Tactics can include calling into the Help Desk.
    - If an organization's password reset procedures require that a newly reset password is conveyed only through a user's manager, this threat actor may try to compromise another account via phishing or through an access broker.
    - With this compromised account, this threat actor may target a privileged account through the helpdesk by stating the target account has a new manager and the password should instead be sent to a new number.
- Common aspects of phishing calls to Help Desks can include the following TTPs:
    - Targeted accounts are often privileged domain accounts or Microsoft Azure administration accounts.
    - Frequent use of VoIP voice phone numbers to call Help Desks.

- When a phishing attempt is detected by the Help Desk and the call is ended, the threat actor calls back using a fake accent to speak with a different Help Desk staff member.
- The threat actor claims to have lost their MFA device.
- The treat actor confirms new password and MFA enrollment was successful in real-time.
- The threat actor is often able to provide the targeted user's employee ID, manager's name, and date of birth.
- Recordings of calls indicate English speakers who may be native or near native speakers.

Reconnaissance

Immediately after initial access, this threat actor has been observed collecting information about the victim organization's environment using the following search terms across backup locations, cloud storage (Azure Blob, AWS S3, etc), CyberArk, database backup locations, ESXi, internal code repositories, SAP, and other applications.

Search Terms Used by Threat Actors in SharePoint / File Repository:

- Administrator Backup
- Code Signing
- Confidential
- CyberArk
- Digicert
- EV Code Signing
- HSM
- Logistics
- Privileged
- Privileged and Confidential
- Recovery Plan
- Third Party Logistics
- Vendor
- Vendor management

Cloud Infrastructure Activities

This threat actor has demonstrated a significant level of knowledge and skillset when operating within an organizations Azure and AWS environments. They are persistent and able to pivot rapidly based on the organization's response actions regardless of the cloud provider. Typically, the threat actor gains access to accounts with tenant-level credentials in the targeted organization's cloud environment. Common attack processes include the following tactics:

- Spinning up rogue VMs to use as an attack base of operations.
- Spinning up clones of legitimate VMs to use as an attack base of operations.
- Exporting entire VMs, focusing on systems with sensitive data content.
- Re-configuring firewall ACLs to enable Internet access to cloud-hosted systems, followed by using the systems for remote access into the victim environment.
- Exporting sensitive data from company cloud storage to threat actor-controlled cloud storage.

On-Premise Operations

This threat actor has been observed executing the following on-premise activities in a victim organization's environment:

- Targeting virtualization infrastructure (VMWare ESXi) and occasionally deploying ransomware (see below).
- Enabling SSH into ESXi servers to lock organization out of consoles.
- Leveraging vCenter CLI to access high value VMs.

Continued Access & Deployment Methods

This threat actor has been observed using the following tools and techniques to gain and maintain persistent access to a victim organization's environment:

- Azure Intune

- PDQ Deploy
- Rust Desktop
- Spashtop
- SSH Tunnels
- VPN (Site-to-Site Links, Client VPN, RDP)
- Threat actor-deployed AWS Lambda functions
- Infrequent use of IPMI, iDRAC and iLO in certain situations

Connections to Ransomware

In some instances, this threat actor has been observed deploying ransomware on ESXi servers after data exfiltration occurs or security teams attempt to evict the threat actor from the environment. This threat actor has loosely affiliated itself with the ALPHV/Blackcat ransomware group in some instances and has used the ransomware group's negotiations and leak site infrastructure to post information about victim organizations.

Threat Actor Communications

This threat actor has been observed sending personalized and threatening messages over email, phone, and SMS to gain attention from victim organizations. In some instances, they have contacted media to add pressure and extract payment from companies. Techniques include:

- Identifying contact information for executive leadership and sending personalized threats over email, by phone, or via SMS .
- If the threat actor does not receive a response to initial messages, they may identify the contact information of family members for executive leadership, clients, or vendors and send threats via email, phone or SMS.
- Leveraging compromised accounts to join internal security calls hosted on video conferencing platforms.
- Contacting the media or security blogs to provide information related to data breaches.

Recommendations and Countermeasures

Aon recommends organizations consider taking the following steps to help focus on prevention and detection:

- Provide enhanced training to employees and Help Desks to detect phishing, social engineering, and account takeover attempts.
- Use security features provided by telecom providers to lock SIM cards to prevent SIM swapping attempts. Create an account PIN or password to lock phone number from unauthorized porting attempts.
- Harden ESXi to prevent execution of unsigned code.
- Monitor or limit use of Remote Management (RMM) tools on systems.
- Consider use of AppLocker on critical systems.
- Use hardware tokens such as YubiKey for M365/Azure admin roles.
- Use conditional access policies (CAP) to limit where M365 admins can sign in from.
- Actively patch for known CVEs such as CVE-2021-35464 and CVE-2015-2291.
- Limit remote access to cloud administration consoles and monitor alerts using resources such as Azure AD Identity Protection for token theft and anomalous access.

About Aon

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Our colleagues provide our clients in over 120 countries and sovereignties with advice and solutions that give them the clarity and confidence to make better decisions to protect and grow their business.

Follow Aon on LinkedIn, Twitter, Facebook and Instagram. Stay up-to-date by visiting the Aon Newsroom and sign up for News Alerts here.