cyberSuite

Cyber Threat Intelligence

Scattered Spider Targets Insurance Industry

Threat Advice-25-0040

1300 829 237 | info@cybersuite.com.au | Level 3, 4-6 Bligh St, Sydney NSW 2000 | cybersuite.com.au

Scattered Spider

Threat Advice	TA-25-40	**Date**	23-06-25
Severity	Critical	**Threat Type**	Threat Actor

EXECUTIVE SUMMARY

Scattered Spider (also known as UNC3944, Octo Tempest, and Muddled Libra) is a financially motivated cybercriminal group known for targeted social engineering and identity-focused attacks.

Recently, Scattered Spider has turned its focus to insurance and financial service providers, leveraging tactics such as Phishing, SIM swaps, multi-factor authentication (MFA) spamming attacks, and manipulation of help desk personnel to gain initial access to systems.

Once inside, they gain increased access to the systems and extract sensitive customer data while deploying ransomware to extort their victims.

Australian and New Zealand insurers, brokers, and financial institutions are specifically at heightened risk due to the sensitive personal and financial data they manage.

This group's tactics exploit human vulnerabilities more than technical weaknesses, emphasising the need for strengthened identity management, vigilant employees, and robust IT/help desk procedures.

KEY RISKS TO INSURANCE INDUSTRY

Data Breach: Theft of sensitive customer data, resulting in severe reputational damage, regulatory penalties, and potential litigation.

Operational Disruption: Deployment of ransomware and sabotage of critical systems leading to significant business interruptions and customer dissatisfaction.

Financial Losses: Substantial ransom demands, incident response costs, system rebuild or repair costs, and long-term impacts on customer trust and revenue.

Secondary Attacks: Leveraging initial access to target insurers' clients and vendors, creating broader industry disruptions and potential further reputational damages.

RECOMMENDATIONS AND MITIGATIONS

Low Effort Mitigations

Security Awareness Training	Educate staff on social engineering and impersonation techniques aimed at resetting user passwords and MFA tokens.
Use Positive Identity Verification	Define processes to ensure the verification of individuals happens over a separate channel when required, especially when they request access to systems, password changes, or financial transfers are involved.
Enable Strong MFA	Use app-based or hardware tokens; avoid SMS-based MFA, due to sim swap risks.
Block Malicious Domains	See appendix B.
Monitor your organisation's Remote Monitoring and Management (RMM) Tools	Alert on installations of software in appendix C.

Medium Effort Mitigations

Conditional Access Policies	Restrict access based on device health, location, enterprise enrolment status, and user risk.
Cloud Identity and Access Management (IAM) Hardening	Audit and restrict IAM roles; enforce least privilege and role-based access control.
Endpoint Detection & Response (EDR)	Deploy EDR tools to detect lateral movement and credential dumping.
SIM Swap Monitoring	Work with telecom providers to detect and alert on SIM changes.

High Effort Mitigations

Zero Trust Architecture	Implement identity-based access controls and continuous trust verification.
Threat Hunting Program	Proactively search for adversary tactics, techniques, and procedures (TTPs), and behavioural anomalies.
Red Team Exercises	Simulate Scattered Spider's TTPs to test defences, including social engineering and cloud exploitation.
Incident Response Playbooks	Develop and rehearse playbooks for ransomware, cloud compromise, and identity theft scenarios.

Appendix

APPENDIX A - TACTICS, TECHNIQUES AND PROCEDURES USED BY THE THREAT ACTOR

1. Reconnaissance & Resource Development

- Identifies targets using cloud identity platforms (e.g. Okta, Microsoft Entra).
- Registers phishing domains and prepares remote access tools.
- Gathers malware and infrastructure for future use.

2. Initial Access

- Launches phishing, smishing, and vishing campaigns.
- Performs SIM swapping to intercept MFA codes.
- Uses attacker-in-the-middle (AiTM) phishing kits to bypass MFA.

3. Execution & Persistence

- Installs legitimate remote access tools (e.g. AnyDesk, TeamViewer).
- Adds attacker-controlled MFA tokens to compromised accounts.
- Abuses federated identity systems to impersonate users.

4. Privilege Escalation

- Exploits SSO configurations to gain admin access.
- Uses "living off the land" techniques to avoid detection.
- Manipulates cloud IAM roles for elevated privileges.

5. Discovery & Lateral Movement

- Enumerates Active Directory and extracts credential stores.
- Maps cloud infrastructure and identifies sensitive systems.

6. Data Exfiltration & Impact

- Uses SaaS tools and ETL platforms to extract data.
- Deploys ransomware (e.g. DragonForce, BlackCat) to encrypt systems.
- Engages in extortion via encrypted communication channels.

7. Detection Evasion & Persistence

- Monitors internal communications (e.g. Slack, Teams).
- Rotates phishing domains frequently to avoid blacklisting.
- Maintains access through cloud identity manipulation.

APPENDIX B - MALICIOUS DOMAINS USED BY THE THREAT ACTOR

- victimname-sso[.]com
- victimname-servicedesk[.]com
- victimname-okta[.]com

APPENDIX C - LEGITIMATE TOOLS USED BY THE THREAT ACTOR

Tool Name	Intended Use Case
Fleetdeck.io	Enables remote monitoring and management of systems.
Level.io	Enables remote monitoring and management of systems.
Pulseway	Enables remote monitoring and management of systems.
Tactical.RMM	Enables remote monitoring and management of systems.
Screenconnect	Enables remote connections to network devices for management.
Splashtop	Enables remote connections to network devices for management.
Ngrok	Enables remote access to a local web server by tunnelling over the internet.
TeamViewer	Enables remote connections to network devices for management.
Mimikatz	Extracts credentials from a system.
Tailscale	Provides virtual private networks (VPNs) to secure network communications.

APPENDIX D - MALICIOUS TOOLS USED BY THE THREAT ACTOR

Tool Name	Use Case
AveMaria (also known as WarZone)	Enables remote access to a victim's systems.
Raccoon Stealer	Steals information including login credentials, browser history, cookies, and other data.
VIDAR Stealer	Steals information including login credentials, browser history, cookies, and other data.

APPENDIX E - FURTHER READING

Defending Against UNC3944: Cybercrime Hardening Guidance from the Frontlines | Google Cloud Blog

Scattered Spider | CISA