canopius

Scattered Spider

A Case Study to Predict Future Threats

Scattered Spider

Aliases

Muddled Libra, Roasted 0ktapus, Starfraud, Scatter Swine, UNC3944.

First Seen

April 2022

Targeted Industries

- Telecommunications
- Travel & Tourism
- Financial Services
- Community & Lifestyle
- Energy & Utilities

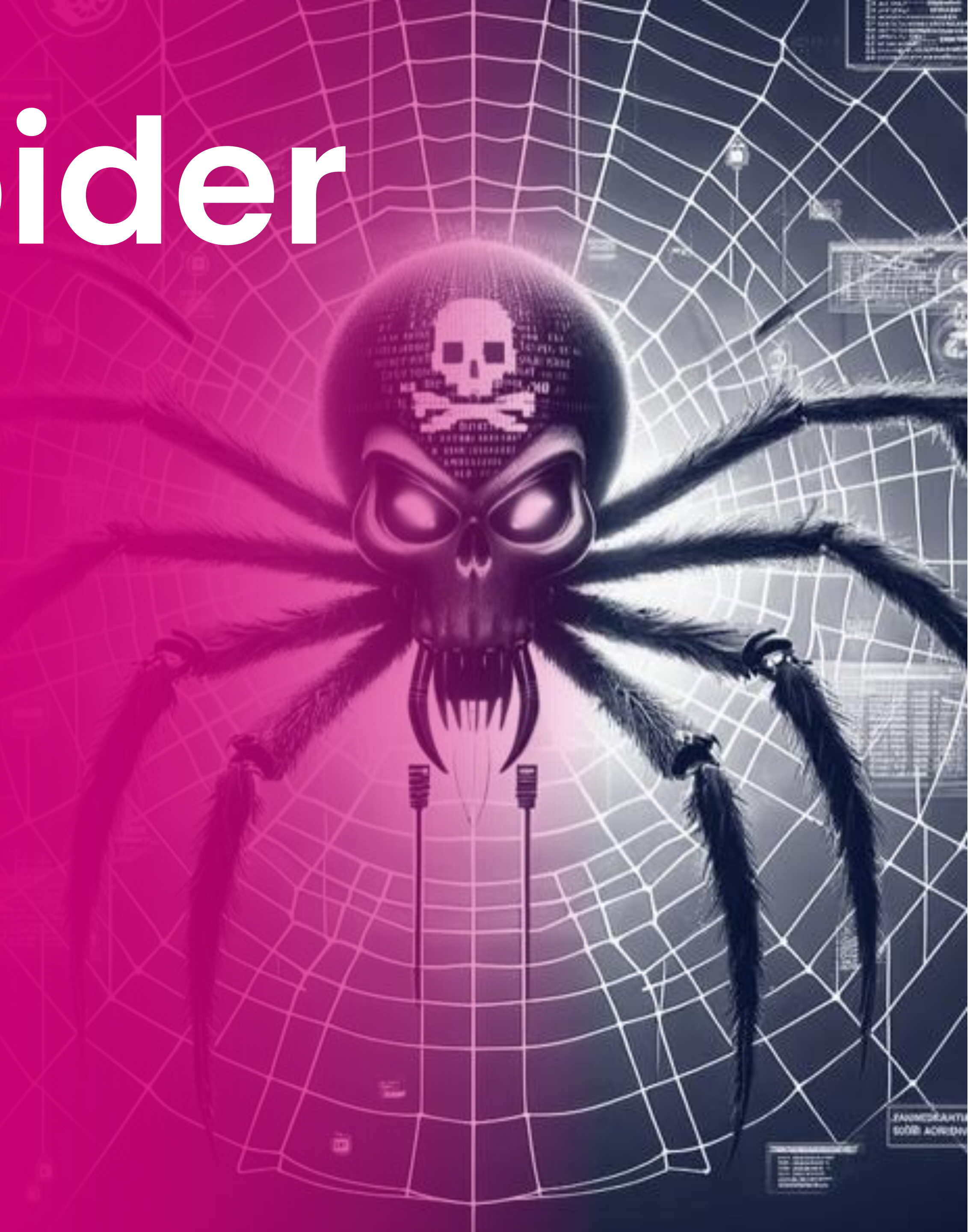
Targeted Regions

- United States of America
- Canada
- Australia
- Singapore

Scattered Spider

Scattered Spider was 2023's most searched for and queried threat actor. The group has swiftly gained attention in the cybersecurity landscape following their strategic attacks on Vegas casinos, and they now stand at the forefront of threat intelligence discussions, representing a new wave of cyber threats.

Scattered Spider's cadre of young threat actors, some as young as 19, are showcasing a fresh approach to cyber operations: finessed attacks on cloud-based infrastructure, and sophisticated and targeted social engineering tactics to gain access. These tactics position Scattered Spider as a prime example of the innovative strategies shaping the cybersecurity landscape and guide us in fortifying defences against the threats of tomorrow.



Campaigns & Themes

Scattered Spider has shown inconsistencies across their campaign history: First targeting telecommunications companies, then broadening their industry scope; Initially monetizing through Dark Web marketplaces, then pivoting to ransomware-as-a-service. But can we identify any commonalities?

Threat Actor Timeline

Q3-Q4 2022
Silent SIM Swaps

Series of attacks targeting the Telecommunications sector, attempting to gain access to mobile carrier networks and occasionally performing SIM Swapping attacks.

In each incident, initial access is achieved through targeted social engineering, involving phone calls and text messages that impersonate IT staff.

Deep & Dark Web monitoring has indicated that Scattered Spider profited from these operations by performing SIM Swapping operations as a service.

Q4 2022 – Q2 2023
Azure Strikes

Suspected Scattered Spider attacks on Azure-native organisations, characterized by SIM swaps for initial access and resulting in manipulated and exfiltrated data.

Q3 – Q4 2023
Expanding & Extorting

Scattered Spider starts monetizing their operations through ransomware-as-a-service operators (ALPHV) and diversifies their victim base.

Campaigns & Themes

Since their first confirmed appearance in April 2022, Scattered Spider's targets and monetization methods have fluctuated.

However, their attack methods remain consistent. There are 3 common characteristics to each of their campaigns:

Cloud-Confident

Scattered Spider are highly competent at crawling and exploiting **cloud-based infrastructure**, particularly Microsoft Azure.

Coercive & Manipulative

Scattered Spider gains access to credentials and secrets through targeted social **engineering** attempts and through impersonation of employees.

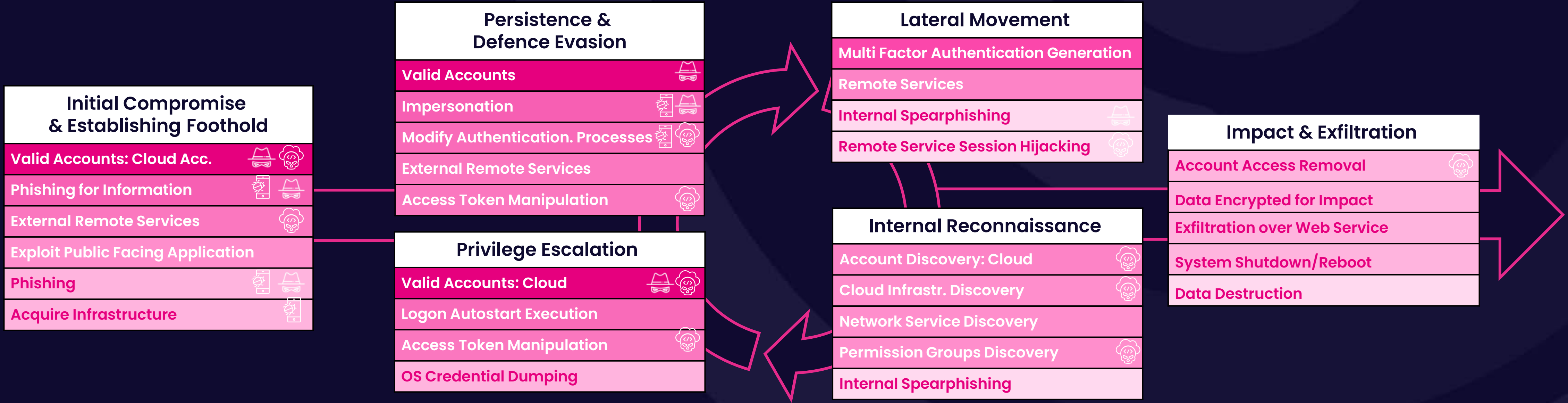
Mobile Infiltration

Scattered Spider exploits **mobile devices**, leveraging them either as conduits for coercing targets or as critical instruments for circumventing multi-factor authentication systems.

Attack Pattern Deep-Dive

We have now identified 3 key characteristics of a Scattered Spider attack: cloud (IaaS) exploitation, sophisticated social engineering, and mobiles. **But what should we expect to see based upon these characteristics?** Here, we explore the nature of these attacks and draw out these key themes across Scattered Spider's typical attack kill-chain.

Identifying an Attack Path The Figure Below Illustrates the most common MITRE ATT&CK techniques used by Scattered Spider throughout the attack lifecycle. The depth of colour indicates the frequency of technique usage. These techniques demonstrate their competency in the cloud, using mobiles, and performing social engineering.



Initial Compromise & Establishing Foothold	
Valid Accounts: Cloud Acc.	🕵 ☁
Phishing for Information	📱 🕵
External Remote Services	☁
Exploit Public Facing Application	
Phishing	📱 🕵
Acquire Infrastructure	📱

Persistence & Defence Evasion	
Valid Accounts	🕵
Impersonation	📱 🕵
Modify Authentication. Processes	📱 ☁
External Remote Services	
Access Token Manipulation	☁

Privilege Escalation	
Valid Accounts: Cloud	🕵 ☁
Logon Autostart Execution	
Access Token Manipulation	☁
OS Credential Dumping	

Lateral Movement	
Multi Factor Authentication Generation	
Remote Services	
Internal Spearphishing	🕵
Remote Service Session Hijacking	☁

Internal Reconnaissance	
Account Discovery: Cloud	☁
Cloud Infrastr. Discovery	☁
Network Service Discovery	
Permission Groups Discovery	☁
Internal Spearphishing	

Impact & Exfiltration	
Account Access Removal	☁
Data Encrypted for Impact	
Exfiltration over Web Service	
System Shutdown/Reboot	
Data Destruction	

☁ Cloud Attacks   🕵 Social Engineering   📱 Mobile Devices (Affected)

Threat Landscape Predictions

Scattered Spider are a new, and young threat group. How do they compare to the rest of the threat landscape? And **can we use Scattered Spider's characteristics to predict the nature of future cyber threats?**

	Scattered Spider's Behaviour & Characteristics	Threat Landscape Trends	What Should We Expect Going Forward?
Cloud Attacks	Scattered Spider is highly proficient in Microsoft Azure, and is known to: • Use open-source attack tooling to gather Azure secrets & other sensitive information • Execute "golden SAML" attacks by adding rogue federated identity providers to victim's Azure AD • Create Azure virtual machines & modify Azure's firewalls to maintain persistence • Use Azure Data Factory to modify pipelines and exfiltrate data to attacker-controlled servers.	Attack techniques targeting Infrastructure-as-a-Service (IaaS) operations have increased by **60%** between 2022 and 2023.	The number of large organizations with a multi-cloud strategy is predicted to rise from 76% to 85% during 2024. [1] And the cybersecurity skills gap is widening, especially with respect to cloud security. The number of attacks targeting virtualized infrastructure will likely grow as the cloud adoption increases and the knowledge gap widens.
Social Engineering	Scattered Spider relies heavily on social engineering and impersonation throughout the attack kill-chain. They conduct SMS phishing campaigns to gain initial access, and once inside will impersonate employees in an attempt to maintain or extend their access.	Employees remain an organisations' weakest link. **33.2%** of poorly trained users will fail a phishing test. [2]	Deep-fake and generative AI technologies play into the hands of the threat actors and with these technologies we should expect to see increasingly convincing and coercive social engineering attempts.
Mobile Devices	Scattered Spider conducts credential theft through SMS phishing campaigns. And occasionally, they will conduct SIM swapping attacks to further embellish & improve their impersonation attempts during calls to service desks, or to receive MFA codes.	**17%** of enterprise users encountered phishing links on their mobile devices. [3]	As baseline security levels improve amongst organisations, threat actors will look to find gaps in control coverage by targeting difficult-to-manage and sometimes forgotten assets, such as mobile devices.

Mitigating the Threat

So what do we do to protect ourselves? Scattered Spider has a vast toolkit of techniques they may use in an attack. At Canopius, we've performed an analysis of these techniques to identify the controls that offer the best breadth of protection against their most common techniques.

1. PAM & IAM Tooling

Throughout the attack lifecycle, Scattered Spider relies on the exploitation of valid credentials – coercing them from employees, and discovering them from dumps in systems until they obtain sufficient privileged access. There are a number of arduous steps an organization must take to secure & manage these credentials against each technique, but these tasks are greatly simplified by both Privileged Access Management (PAM) and Identity and Access Management (IAM) tooling. A tool that integrates the two capabilities further closes the gaps of each system.

2. User Training

The workforce are an organisation's weakest link in attacks such as those from Scattered Spider. The workforce needs to be continually trained, and training needs to be updated and informed by threat intelligence to increase awareness of the latest social engineering techniques.

3. Configuration Management & Audit of Azure

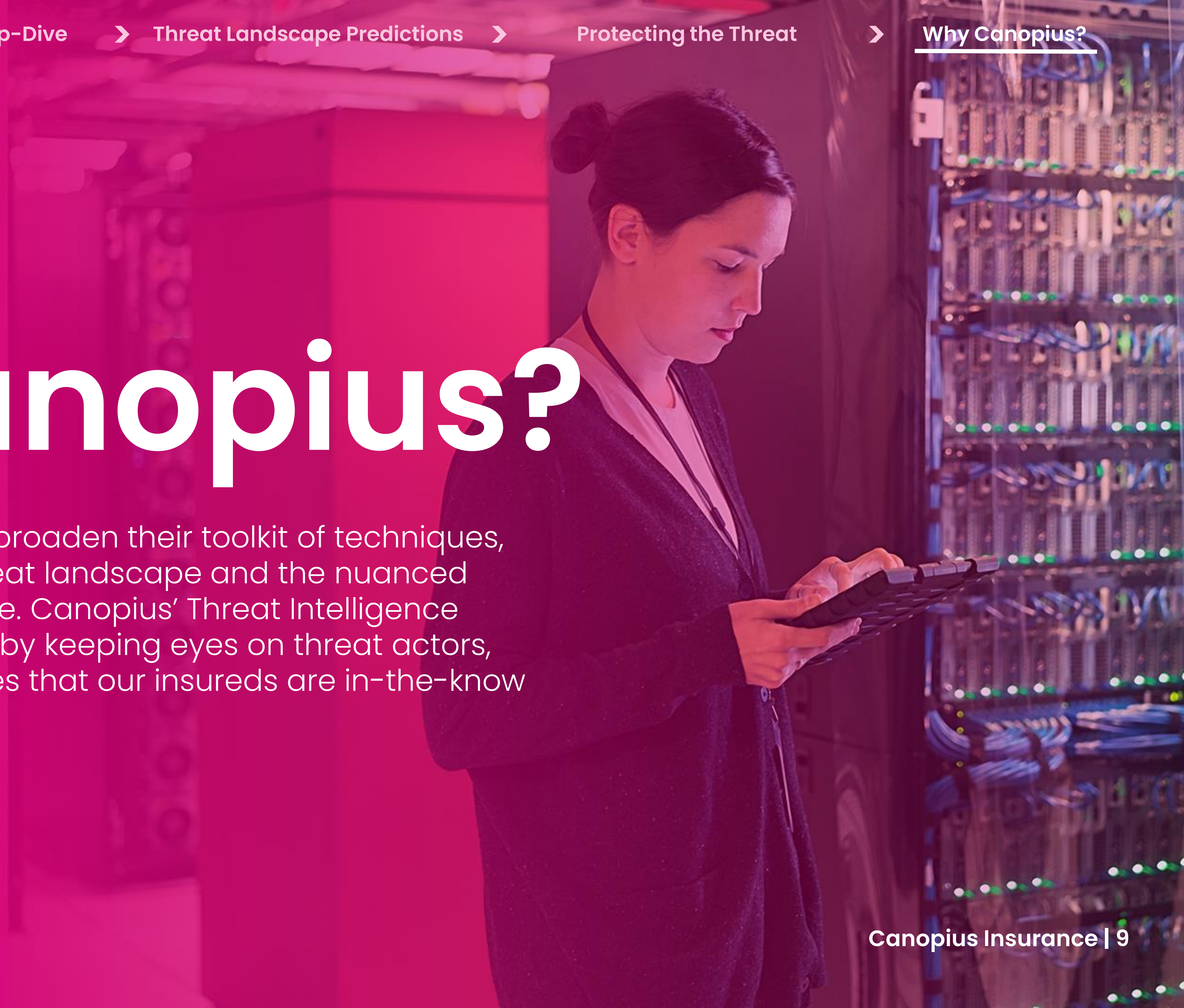
Organisations should leverage tools like Azure Policy for enforcing and auditing resource configurations, Azure Monitor for tracking performance and health, and Azure Security Center for continuous assessment and recommendations. These tools help identify misconfigurations, enforce policies, and provide visibility into the security posture of Azure environments, mitigating risks associated with unauthorized access or data breaches.

4. Multi-Factor Authentication (MFA)

Whilst MFA is widely recognised as a critical security control in mitigating against a range of attacks, Scattered Spider has demonstrated a portfolio of techniques that can be used to bypass multi-factor authentication, including SIM Swapping and SMS phishing. It is important for organisations to assess and validate the scope of MFA implementation and the security of the method: hardware-based tokens and software token apps (avoiding use of push notifications) are less susceptible to social engineering.

5. Mobile Device Management (MDM)

Scattered Spider delivers social engineering attacks through mobiles because they have weaker baseline security controls and because mobiles often operate as an authentication key to the network. For organisations that rely on mobile devices for authentication and critical communications, it is important to monitor and manage the security settings & configurations on mobile devices. A mobile device management (MDM) solution can mitigate against Scattered Spider and similar mobile-based attacks by enforcing strong security policies on mobile devices used for accessing corporate resources.



Why Canopius?

As threat actors appear, evolve and broaden their toolkit of techniques, it is critical to keep an eye on the threat landscape and the nuanced changes to the typical attack lifecycle. Canopius' Threat Intelligence team serves our cyber policyholders by keeping eyes on threat actors, such as Scattered Spider, and ensures that our insureds are in-the-know and aren't left behind.

About Canopius' Threat Intelligence Function

Understanding Scattered Spider attacks underscores the importance of a threat intelligence function in identifying, anticipating, and mitigating cyber threats. By analysing patterns associated with such attacks, threat intelligence can guide proactive defences, inform security policies, and enable us to understand your organisation's unique risk profile, which aids us in designing the best insurance policy for your organisation.

Canopius' Threat Intelligence function is built upon the rich data collected by our dedicated cyber incident management team and is supplemented by both premium and open-source threat intelligence feeds and platforms, offering a unique and comprehensive view of the threat landscape. We firmly believe that the fusion of threat intelligence with our claims data provides an unparalleled perspective on cyber risk, enabling us to not only refine our underwriting processes, but also to share invaluable insights with our insureds.

Embracing honesty and transparency, we use our threat intelligence capabilities to work with our clients, aiming to significantly reduce their cyber risk and secure their digital operations. We share our threat intelligence capabilities with our policyholders through threat report, which are part our Proactive Cyber Services offering.

About Canopius' Cyber Incident Management Team

A streamlined cyber incident response to a Scattered Spider attack includes swift detection, system isolation, and containment. An incident response team should be activated immediately to evaluate the attack's extent and prioritize the recovery of essential systems. Strategies should include network segmentation to halt lateral movements, applying patches to vulnerabilities, and bolstering surveillance for new threats. Effective communication with stakeholders and, if needed, law enforcement is crucial, along with a comprehensive post-incident review to refine future response strategies and enhance resilience.

The legal implications of a Scattered Spider cyber-attack are substantial, especially concerning data protection. These incidents could harm an organization's reputation and necessitate notifying affected parties and authorities, inviting further examination and inquiry.

Canopius' in-house Cyber Incident Management team offers expert guidance and vendor selection to effectively navigate and mitigate Scattered Spider incidents, ensuring tailored, top-tier defence solutions for optimal recovery.

References

[1] https://www.datek.co.uk/blog/the-10-biggest-cloud-computing-trends-in-2024-everyone-must-be-ready-for-now

[2] https://blog.knowbe4.com/knowbe4-2023-phishing-by-industry-benchmarking-report

[3] https://keepnetlabs.com/blog/smishing-statistics-2023-the-latest-trends-and-numbers-in-sms-phishing

[4] https://www.crowdstrike.com/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic/

[5] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

[6] https://attack.mitre.org/groups/G1015/

canopius

Smart Actions. Practical Solutions.

THANK YOU