K logix
Be confident.

JULY 2024 | THREAT INTEL NEWSLETTER

SaaS Security: UNC5537 and Scattered Spider

C-Suite level threat review by applicable business area addressing active threats.

The two threat actors highlighted in this report, UNC5537 and Scattered Spider, are targeting Software-as-a-Service (SaaS) applications. Targeting a widely used SaaS application enables threat actors to compromise a broad range of organizations. Additionally, SaaS applications often host large amounts of sensitive data, amplifying the impact of a compromise. Moreover, some organizations may not fully understand the SaaS shared security model, leading to inadequate security controls. As threat actors increasingly target SaaS applications, it is important for organizations to counter this threat by developing strong third-party risk management practices. The importance of SaaS security is reflected in the recent publication of National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) version 2.0 which puts a greater emphasis on third-party risk management.

UNC5537:

UNC5537 is a financially motivated threat actor tracked by Mandiant. This adversary is known to conduct extortion attacks, exfiltrating and then threatening to publicize confidential data. Mandiant assesses with moderate confidence that UNC5537 members are based in North America and Turkey. While this threat actor has been linked to cyberattacks worldwide, it caught public attention with its recent campaign targeting Snowflake customers. Snowflake is a data storage and analytics SaaS solution.

Scattered Spider:

Scattered Spider, previously covered in two K logix newsletters, warrants renewed attention due to an evolution in its tactics and targets. Forgoing its use of ransomware, Scattered Spider is shifting to data theft with an eye towards SaaS applications. This adversary is a threat to all industries with its most recent victims being in finance, telecommunication, and entertainment.

UNC5537

Threat Level: Low

Attack:

UNC5537 used compromised credentials on Snowflake instances and successfully compromised instances that did not have multi-factor authentication (MFA) enabled (MITRE T1078). Researchers believe that the compromised credentials were acquired from infostealer malware on non-Snowflake owned systems. In some cases, the infostealer malware infected contractor systems. Once access is obtained, the threat actors conduct reconnaissance such as identifying existing users and roles (MITRE T1087). UNC5537 then creates temporary stages (i.e., location where data is stored for loading and unloading) to store and subsequently exfiltrate data (MITRE T1074 and MITRE TA0010).

Remediation:

- Implement MFA
- Consider putting in place a policy that requires users to reset their passwords annually.
- Ensure network allow lists are in place to guard access to critical resources.
- Require contractors with access to critical resources to undergo security awareness training.

Scattered Spider

Threat Level: High

Attack:

Scattered Spider commonly infiltrates organizations through sophisticated social engineering techniques. For example, Scattered Spider personnel have impersonated highly privileged users to the IT Help Desk, resetting MFA and thus, taking over the account (MITRE T1566). To avoid detection, Scattered Spider utilizes various techniques including creating a new virtual machine to bypass security protections (MITRE T15578.002) and disable Endpoint, Detection and Response (EDR) tools (MITRE T1562.001). In recent incursions, this adversary has shifted from conducting double extortion ransomware attacks to conducting just data exfiltration, targeting SaaS applications. For exfiltration, this threat actor leverages cloud synchronization tools such as Airbyte and Fivetran (MITRE T1567.002). Moreover, Scattered Spider is extracting Active Directory Federated Services certificates for Golden SAML attacks, further demonstrating a focus on cloud environments and services.

Remediation:

- Assess the risk-level of SaaS applications. The risk-level should guide what security controls are put in place to protect the SaaS application. Factors to consider during the risk assessment: 1) the type of data that will be stored on the application and 2) the role the application will have in maintaining critical functions.
- Conduct third-party monitoring periodically based on risk to the organization.
- Ensure a comprehensive third-party risk management program is in place.
- Ensure logging and monitoring is in place for SaaS applications.

UNC5537:

- **Overview of UNC5537's targeting of Snowflake instances:** https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion
- **Succinct summary of UNC5537 and Snowflake:** https://www.bleepingcomputer.com/news/security/cylance-confirms-data-breach-linked-to-third-party-platform/#google_vignette

Scattered Spider:

- **Overview of Scattered Spider's techniques:** https://www.bleepingcomputer.com/news/security/scattered-spider-hackers-switch-focus-to-cloud-apps-for-data-theft/
- **Additional look into Scattered Spider's techniques:** https://thecyberexpress.com/unc3944-shifts-focus-to-data-theft-from-saas/

ABOUT K LOGIX

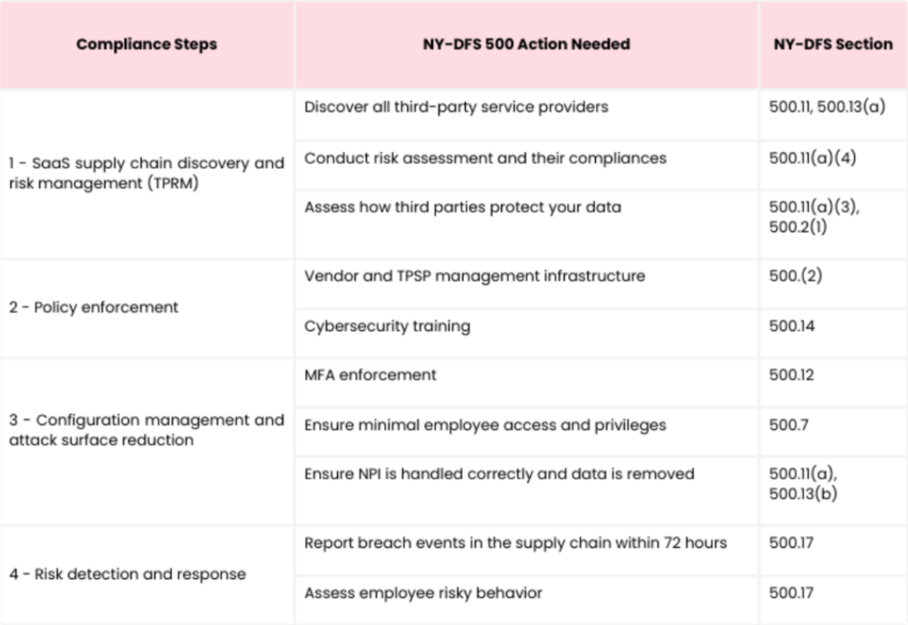
Cybersecurity Advisory and Consulting Services

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.

How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Response (EDR)
  - Identity and Access Management (IAM)
  - Managed Security Service Provider (MSSP)
  - Security Information and Event Management (SIEM)
  - Cloud Security Posture Management (CSPM)
  - SaaS Security Posture Management (SaaS)
- Programmatic Advisory
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
  - Cloud Security Maturity
  - Identity and Access Management Program Maturity
- Threat Intelligence
  - Notification to customers of threats
  - On-demand briefings
  - Threat exposure workshops
  - User awareness training seminars
  - Monthly and quarterly threat intelligence reports

Mapping of NY-DFS Third-Party Risk Management Requirements



Compliance Steps	NY-DFS 500 Action Needed	NY-DFS Section
1 - SaaS supply chain discovery and risk management (TPRM)	Discover all third-party service providers	500.11, 500.13(a)
	Conduct risk assessment and their compliances	500.11(a)(4)
	Assess how third parties protect your data	500.11(a)(3), 500.2(1)
2 - Policy enforcement	Vendor and TPSP management infrastructure	500.(2)
	Cybersecurity training	500.14
3 - Configuration management and attack surface reduction	MFA enforcement	500.12
	Ensure minimal employee access and privileges	500.7
	Ensure NPI is handled correctly and data is removed	500.11(a), 500.13(b)
4 - Risk detection and response	Report breach events in the supply chain within 72 hours	500.17
	Assess employee risky behavior	500.17

Source: https://thehackernews.com/2024/06/why-saas-security-is-suddenly-hot.html