K logix

BE CONFIDENT.

VOL 3 | FEBRUARY 2023 | THREAT INTEL NEWSLETTER

Scattered Spider, UNC3944 and Vice Society

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

The adversaries identified in this report utilize credential theft to gain initial access to their victims' networks, which is a commonly employed technique. IBM found that the most common initial attack vector in 2021 and 2022 was compromised credentials. Moreover, Scattered Spider / UNC3944 are linked to recent attacks where the goal is to uncover information to facilitate credential theft, specifically SIM swapping. SIM swapping is when a malicious actor steals identifying information to impersonate individuals to their mobile carrier, stealing phone numbers and thereby compromising credentials.

Scattered Spider / UNC3944:

Threat analysts have recently observed attacks targeting telecommunications and business process outsourcing companies with the objective of stealing information to perform SIM swapping attacks. Scattered Spider, a threat actor tracked by CrowdStrike, and UNC3944, a threat actor tracked by Mandiant, have been observed employing this strategy. In addition to a shared objective, they also share several techniques, suggesting a connection. Both appear to be financially motivated.

Vice Society Ransomware:

Vice Society, a financially motivated ransomware group, targets a range of industries with its top target being the education sector followed by healthcare and local governments. This adversary does not appear to limit attacks to a specific country or region. Most recently, it has attacked organizations in the United States, Europe, and Australia. Vice Society is known to employ the double extortion technique, encrypting and exfiltrating data to place additional pressure on victims to pay the ransom.

Scattered Spider

Threat Level: High

Attack:

To gain initial access to an organization, Scattered Spider leverages social engineering techniques such as impersonating IT individuals via phone calls and SMS messages and creating phishing pages. CrowdStrike observed this threat actor using the Bring-Your-Own-Vulnerable-Driver (BYOVD) technique to escalate privileges. To bypass security detection products, the threat actor used drivers that were signed by different stolen certificates (T1553.002). To successfully employ the BYOVD attack, Scattered Spider attempted to exploit CVE-2015-2291, which is a persistent Microsoft windows vulnerability.

Remediation:

- To prevent an adversary from exploiting CVE-2015-2291, Windows users should enable the recommended driver block rules. Microsoft provides information for how to do this here.
- To prevent malicious actors from gaining initial access, ensure comprehensive Identity and Access Management controls are in place, such as MFA and conditional access policies.
- Invest in anti-phishing solutions that can identify and flag phishing emails.
- Patching should be automated, conducted at a defined cadence. The process should also be documented in policy and procedure.
- Ensure a robust third-party risk management program is in place. Vendors' cybersecurity programs should be reviewed and audited periodically, and this should be required in policy.

Vice Society

Threat Level: High

Attack:

Vice Society has been observed gaining initial access into an organization via compromised credentials [T1078] or exploiting vulnerabilities in internet-facing systems [T1190]. The adversary will then conduct reconnaissance, exploring the network and identifying opportunities to escalate privileges. Historically, Vice Society has deployed third-party ransomware encryptors such as Hello Kitty / Five Hands and Zeppelin. However, Sentinel One recently observed Vice Society using a new, custom-branded encryptor that combines asymmetric and symmetric encryption. Vice Society likely acquired this capability from a third-party vendor that supplies tools to ransomware groups.

Remediation:

- Conduct automated access recertifications on a quarterly basis to prevent access creep.
- Implement a PAM solution that supports just-in-time access.
- Follow the National Institute of Standards and Technology (NIST) guidelines for managing password policies.
- Response and recovery plans should be in place and tested on a quarterly basis.

Scattered Spider / UNC3944 Details:

- **Examination of Scattered Spider:** https://www.crowdstrike.com/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic/
- **Examination of UNC3944:** https://www.mandiant.com/resources/blog/hunting-attestation-signed-malware

Vice Society Details:

- **Joint Advisory released by the FBI, CISA, and MS-ISAC:** https://www.cisa.gov/uscert/ncas/alerts/aa22-249a
- **Examination of new encryption scheme:** https://www.sentinelone.com/labs/custom-branded-ransomware-the-vice-society-group-and-the-threat-of-outsourced-development/

How K logix Can Help

- Technology Advisory
  - Endpoint Detection and Protection
  - Identity and Access Management
  - Managed Security Service Provider
  - Security Information and Event Management
  - Email Security
- Programmatic Advisory
  - Identity and Access Management Program Maturity
  - Threat Intelligence Program Maturity
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI)
  - Tabletop exercises
  - Penetration testing

Vice Society Attacks by Industry Since Starting Operations in the Summer of 2021

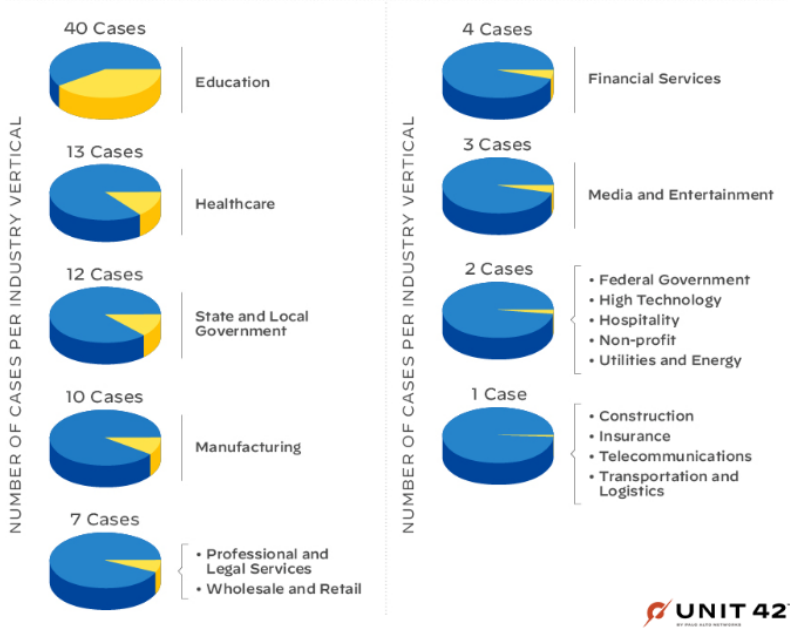

Image from: https://unit42.paloaltonetworks.com/vice-society-targets-education-sector/

ABOUT K LOGIX
Cybersecurity Advisory and Consulting Services
Our white-glove approach empowers leaders to advance their security programs to strategically align with the business to reduce risk.