UNC5537

Date: 17th June 2024 | Severity: Medium

Summary

The UNC5537 threat group was first reported by Mandiant in June 2024. The financially motivated group, likely composed of hackers based in North America, was linked to an attack against the cloud computing company, Snowflake, that impacted over 150 organizations around the world.

Attack Vectors

UNC5537 gains initial system access using stolen credentials that were compromised in other attacks by information-stealing malware (for example, Vidar, RisePro, Redline, Racoon, Lumma, and Metastealer). Once inside the system, the threat actors deploy the FROSTBITE reconnaissance utility (AKA rapeflake) that launches various SQL queries to collect general user and system information (for example, user roles, IP addresses, and session IDs). In addition, the attackers use DBeaver Ultimate to connect and run SQL queries across the victim's instances. Finally, UNC5537 executes commands to exfiltrate data from the compromised servers, which is then sold on underground cybercrime forums.

Indicator of compromise

INDICATOR TYPE	INDICATORS
URLS	• 45[.]155[.]91[.]99 • 93[.]115[.]0[.]49 • 104[.]129[.]24[.]124 • 198[.]54[.]131[.]152 • 146[.]70[.]119[.]24 • 176[.]123[.]6[.]193 • 45[.]86[.]221[.]146 • 198[.]44[.]136[.]82 • 198[.]44[.]129[.]82 • 154[.]47[.]30[.]150 • 194[.]230[.]160[.]237 • 146[.]70[.]171[.]112 • 102[.]165[.]16[.]161 • 66[.]115[.]18[.]247 • 206[.]217[.]205[.]49 • 194[.]230[.]148[.]99 • 154[.]47[.]30[.]137 • 19[.]44[.]136[.]56 • 5[.]47[.]87[.]202 • 146[.]70[.]117[.]56 • 185[.]248[.]85[.]59 • 184[.]147[.]100[.]29 • 176[.]220[.]186[.]152 • 194[.]230[.]147[.]127 • 96[.]44[.]191[.]140 • 146[.]70[.]166[.]176 • 146[.]70[.]165[.]227 • 194[.]230[.]144[.]50 • 146[.]70[.]171[.]99 • 194[.]230[.]144[.]126 • 87[.]249[.]134[.]11 • 185[.]213[.]155[.]241 • 37[.]19[.]210[.]21 • 79[.]127[.]217[.]44 • 194[.]230[.]158[.]107 • 169[.]150[.]223[.]208

Recommendation

- Regular Software Updates and Patching
  Ensure all systems, applications, and firmware are up to date with the latest security patches. Implement automated patch management solutions to streamline this process.
- Network Security
  Use firewalls and intrusion detection/prevention systems (IDS/IPS) to monitor and control incoming and outgoing network traffic. Segment networks to limit the lateral movement of attackers. Employ virtual private networks (VPNs) for secure remote access.
- Endpoint Protection
  Deploy endpoint detection and response (EDR) solutions to monitor and respond to threats on individual devices. Use antivirus and anti-malware software to detect and remove malicious software.
- User Training and Awareness
  Conduct regular security awareness training for employees to recognize phishing attempts, social engineering, and other common attack vectors. Implement policies for strong, unique passwords and multi-factor authentication (MFA).
- Access Control
  Implement the principle of least privilege, ensuring users have only the access necessary to perform their job functions. Use role-based access control (RBAC) to manage user permissions.
- Data Encryption
  Encrypt sensitive data both at rest and in transit to protect it from unauthorized access. Use secure encryption standards and manage encryption keys properly.
- Backup and Recovery
  Maintain regular backups of critical data and ensure they are stored securely. Test backup and recovery procedures to ensure data can be restored in the event of an incident.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Link

- https://dashboard.ti.insight.rapid7.com/#/tip/cyber-term/666aa84f6a68e62fff39e3b1