UNC3944 and 0mega Ransomware

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

As more organizations store their critical data in the cloud, adversaries are, in turn, extending their resources to target the cloud environment. As observed by CrowdStrike, in 2022 cloud exploitation cases grew by 95% and "cloud-conscious" actors almost tripled. This rise in cloud threats is predicted to continue in 2023 by CrowdStrike, K logix and various other industry voices. The threats detailed in this report are examples of this larger trend. UNC3944 is targeting Azure environments to steal data. 0mega ransomware group exfiltrated data from a company's SharePoint via compromised Software-as-a-Service (SaaS) credentials.

UNC3944 (other aliases include Scattered Spider):

UNC3944, leveraging its social engineering and technical capabilities, is infiltrating organizations' Azure environments. The threat actor gains full administrative access to Azure Virtual Machines (VMs), establishes remote access to the Azure environment, conducts reconnaissance, deepens its foothold and exfiltrates data. UNC3944 is a financially motivated threat actor that targets a wide range of industries, including telecommunication, cybersecurity, cryptocurrency, and transportation.

0mega Ransomware Group:

The 0mega ransomware group emerged onto the threat landscape about a year ago. In a recent attack linked to them, the threat actor exfiltrated data from a company's SharePoint by exploiting a poorly secured administrator account. The initial access technique is notable; typically, attackers gain access to SaaS environments via the endpoint. Additionally, in this recent attack, 0mega did not encrypt the data, which is indicative of a larger trend among ransomware actors to focus on data exfiltration.

UNC3944

Threat Level: High

Attack:

To hijack organizations' Azure environment, UNC3944 obtains Azure administrative access by combining phishing techniques, including SMS phishing, voice phishing and SIM swapping (MITRE T1566). From here, the attacker has a plethora of options; for example, they can conduct reconnaissance, export information, and create or modify accounts (MITRE T1136.003). The adversary then utilizes the Azure Serial Console to gain an administrative command prompt inside of an Azure Virtual Machine (VM). To maintain persistence, UNC3944 installs multiple remote management tools via PowerShell, all of which are commercially available to evade endpoint detection platforms. The adversary then sets up a direct connection to the VM via Remote Desktop (MITRE T1021). From there, UNC3944 expands its control and steals data.

Remediation:

- Organizations should consider assessing its cloud environment against the Cloud Security Alliance's Cloud Controls Matrix to improve its security and compliance posture.
- It is recommended to periodically review cloud accounts for unused or overly permissive accounts and implement conditional access authentication policies.
- Put in place a Privilege Access Management (PAM) solution that monitors privileged cloud users.
- Consider additional security awareness training that is tailored to privileged users.

0mega Ransomware Group

Threat Level: Low

Attack:

The 0mega group gained initial access to the company's SharePoint by compromising a poorly secured Microsoft Global SaaS admin account (MITRE T1078). The group then elevated its privileges by creating a new Active Directory (AD) (MITRE T1136) user named 0mega that possesses multiple administrator roles, including Global Administrator, SharePoint Administrator, Exchange Administrator, Teams Administrator, and Site Collection Administrator. Within a span of two hours, over 220 of the company's administrators were systematically eliminated (MITRE T1531), hindering incident response and recovery. After exfiltrating data, the attacker uploaded numerous "PREVENT-LEAKAGE.txt" files to inform the victim about the theft and establish a communication channel with the victim.

Remediation:

- Consider acquiring a SaaS Security Posture Management (SaaS) solution to ensure SaaS applications are configured correctly.
- Consider acquiring a Cloud Security Posture Management (CSPM) solution to identify and remediate risks across your organization's cloud environment.
- Enable multi-factor authorization (MFA) for all administrator and service accounts.
- Implement robust monitoring and detection systems in your organization's cloud environment to quickly detect unusual activity.

UNC3944 Details:

- **In-depth overview of how UNC3944's establishes remote access to Azure environments:** https://www.mandiant.com/resources/blog/sim-swapping-abuse-azure-serial
- **Synopsis of UNC3944's attack on Azure environments:** https://www.bleepingcomputer.com/news/security/hackers-use-azure-serial-console-for-stealthy-access-to-vms/

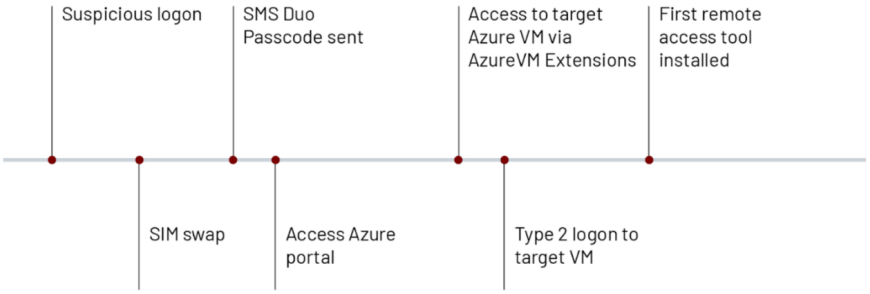
0mega Ransomware Group Details:

- **Overview of recent attack:** https://www.helpnetsecurity.com/2023/06/07/0mega-ransomware-gang-changes-tactics/
- **Additional information on recent attack:** https://cybersecuritynews.com/saas-ransomware-attack/

How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Protection (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
  - Penetration testing
  - Tabletop exercises
  - Threat Intelligence Program Maturity
  - Develop playbooks of adversary TTPs

Example UNC3944 attack path:



Source: https://www.mandiant.com/resources/blog/sim-swapping-abuse-azure-serial

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.