مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Threat Actors Targeting Azure Cloud Environments with Account Takeover Tactics

Tracking #:432315626

Date:19-02-2024

EXECUTIVE SUMMARY:

The UAE The Cyber Security Council has observed an ongoing malicious campaign targeting Microsoft Azure cloud environments, compromising hundreds of user accounts, including senior executives.

TECHNICAL DETAILS:

An ongoing malicious campaign targeting Microsoft Azure environments, resulting in the compromise of hundreds of user accounts, including senior executives. This campaign, first detected in late November 2023, employs credential phishing and cloud account takeover (ATO) techniques.

Attack Overview
The attackers use spear-phishing emails with individualized phishing lures within shared documents. These documents contain embedded links that redirect users to malicious phishing webpages upon clicking the URL. The attackers' focus spans a wide range of positions, including Sales Directors, Account Managers, Finance Managers, and executives such as Vice Presidents, Chief Financial Officers, and Presidents.

Techniques and Tools
The attackers use a Linux user-agent (Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36) to access the OfficeHome sign-in application, indicating a departure from traditional methods. This user-agent choice, combined with the targeted sign-in application, potentially exposes the attackers' geographical locations.

Post-compromise activity includes downloading sensitive data, abusing mailbox access to launch internal and external phishing attacks with personalized content, and initiating financial fraud schemes through emails sent to human resources and finance departments.

Mailbox rules: Attackers create dedicated obfuscation rules, intended to cover their tracks and erase all evidence of malicious activity from victims' mailboxes.

INDICATORS OF COMPROMISE(IoCs):

Refer to this link **here** for IOCs and more information

RECOMMENDATIONS:

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Enable multi-factor authentication (MFA) for all users and service accounts.
- Monitor and investigate suspicious logins and access attempts.
- Implement a strong password policy and enforce regular password changes.
- Educate users on how to identify and report phishing attempts.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings (e.g. IOCs, TTPs...etc).

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

1. https://www.proofpoint.com/us/blog/cloud-security/community-alert-ongoing-malicious-campaign-impacting-azure-cloud-environments