Ongoing Malicious Campaign Impacting Azure Cloud Environments

Date: 26th February 2024 | Severity: High

Summary

The cyberattack, which has affected multiple environments, targeted top executives of large companies.

Hundreds of Azure accounts, Microsoft's cloud service, would have been compromised in a security breach that has exposed critical user data.

According to the cybersecurity company Proofpoint, the hacking uses the same malicious campaign detected in November 2023, which integrates credential theft through phishing methods and cloud account takeover (CTO). This would help attackers gain access to OfficeHome and, at the same time, to Microsoft 365 applications.

The hackers allegedly used proxy services to bypass geographical restrictions and mask their true location. To carry out the attack, the cybercriminals embedded links in the documents that redirected users to phishing websites. These links often had the anchor text "View document," which did not raise suspicions.

Attack Vectors

The attack was meticulously planned and targeted both mid-level and senior employees, although more accounts belonging to the former were compromised. According to Proofpoint, positions such as sales directors, account managers, financial directors, operations vice presidents, financial directors, presidents, and CEOs were the most common targets. This allowed the attackers to access information across the organization's levels and domains.

In this type of attacks, once the account is compromised, cybercriminals deploy their own MFA (multifactor authentication) to prolong access, for example by adding an alternate mobile number or setting up an authentication app so that the user cannot regain access. In addition, attackers remove all evidence of suspicious activity to erase their tracks.

The objective of these cyber-attacks is data theft and the commission of financial fraud. Although there is currently no clear evidence to identify the authors of the attacks, it is believed that they originated in Russia and Nigeria, based on the use of local fixed-line ISPs in these regions.

Following the attack's behavioral patterns and techniques, our threat analysts identified specific indicators of compromise (IOCs) associated with this campaign. Namely, the use of a specific Linux user-agent utilized by attackers during the access phase of the attack chain:

Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36

Attackers predominantly utilize this user-agent to access the 'OfficeHome' sign-in application along with unauthorized access to additional native Microsoft365 apps, such as:

- 'Office365 Shell WCSS-Client' (indicative of browser access to Office365 applications)
- 'Office 365 Exchange Online' (indicative of post-compromise mailbox abuse, data exfiltration and email threats proliferation)
- 'My Signins' (used by attackers for MFA manipulation; for more info about this technique, see our recent Cybersecurity Stop of the Month blog)
- 'My Apps'
- 'My Profile'

Indicator of Compromise

INDICATOR TYPE	INDICATORS
Domian	sachacel.ru lobnya.com makeapp.today alexhost.com mol.ru smartape.net airtel.com mtnonline.com acedatacenter.com
User agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
ISP	Sokolov Dmitry Nikolaevich Dom Tehniki Ltd Selena Telecom LLC

Recommendation

Submit the Domain to the Network team to update their database with the file hashes.

Monitor for the specific user agent string and source domains in your organization's logs to detect and mitigate potential threats.

Enforce immediate change of credentials for targeted users, and enforce periodic password change for all users.

Identify initial threat vectors, including email threats (e.g. phishing, malware, impersonation, etc.), brute-force attacks, and password spraying attempts.

Employ auto-remediation policies to reduce attackers' dwell time and minimize potential damages.

Make regular backups of important and critical files.

Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.

Update and Patch operating system, applications, and security software's up to date with latest patches.

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 Links

https://en.softonic.com/articles/microsoft-azure-suffers-the-biggest-security-breach-in-its-history

Community Alert: Ongoing Malicious Campaign Impacting Azure Cloud Environments | Proofpoint US

Copyright © Mphasis Corporation. All rights reserved.