January 22, 2025

Sophos X-Ops Reports Sophisticated Threats Exploiting Microsoft Office 365

Overview: Sophos X-Ops' Managed Detection and Response (MDR) team is actively mitigating incidents linked to two distinct threat actor groups exploiting Microsoft Office 365 features to infiltrate targeted organizations. These adversaries aim to exfiltrate data and deploy ransomware, leveraging vulnerabilities in configurations such as external Teams communications. Sophos has identified these groups as STAC5143 and STAC5777, with STAC5777 overlapping with Microsoft-recognized Storm-1811 and STAC5143 resembling FIN7-linked operations. Both groups exploit email-bombing and fake tech support schemes, posing significant risks to organizations relying on Office 365.

CTI Analysis: Sophos' investigations, initiated in November and December 2024, revealed coordinated tactics such as overwhelming employees with spam emails, followed by malicious Teams communications posing as technical support. The observed activities from the threat clusters STAC5143 and STAC5777 indicate highly sophisticated, multi-stage attacks that leverage advanced social engineering and exploitation of legitimate tools. Both groups initiate their attacks with email bombing and fake IT support messages via Microsoft Teams, aiming to trick victims into providing remote access.

STAC5143 employs tools like RPivot and JAR files to gain persistent access, with the goal of credential theft and data exfiltration, while utilizing techniques like PowerShell commands and obfuscation to avoid detection. STAC5777, on the other hand, uses Microsoft Quick Assist and side-loaded malware to capture keystrokes, harvest credentials, and scan the network for potential pivot points, reflecting a trend of ransomware groups adopting publicly available attack techniques.

Impact Analysis

The impact of these campaigns is substantial, as they involve a combination of credential theft, data exfiltration, and ransomware deployment. The adversaries' use of techniques like keylogging, credential harvesting, and network scanning increases the risk of unauthorized access to sensitive information, potentially enabling further lateral movement within the organization. In one case, Black Basta ransomware was deployed,

which, if successful, could lead to operational disruptions, financial loss, and extensive data encryption. The attackers' ability to manipulate system settings, disable security tools, and gain remote control through utilities like WMIC and Quick Assist allows them to compromise multiple systems, putting the entire network at risk. Although the attacks were blocked in this instance, the potential for reputational damage, legal risks from data breaches, and increased future attack risks highlight the importance of reinforcing defenses against these sophisticated tactics.

Mitigation

- Disable external Teams communication by default.
- Implement multi-factor authentication (MFA) for all Office 365 accounts.
- Conduct regular employee awareness training on phishing and impersonation tactics.
- Monitor and restrict the use of remote-control tools like Quick Assist.
- Deploy endpoint protection solutions with behavioral detections.
- Regularly review and update Office 365 configurations to mitigate potential vulnerabilities.

Conclusion: The threat clusters STAC5143 and STAC5777 emphasize the persistent risks posed by advanced threat actors leveraging legitimate tools for malicious purposes. Organizations must remain vigilant and proactive, adopting robust security protocols and employee training to mitigate these threats effectively. As adversaries refine their methods, collaboration and information sharing among security teams are paramount to safeguarding critical assets.

Source:

https://news.sophos.com/en-us/2025/01/21/sophos-mdr-tracks-two-ransomware-campaigns-using-email-bombing-microsoft-teams-vishing/

https://github.com/sophoslabs/IoCs/blob/master/MAILBOMB-TEAMS-RANSOMWARE.csv

https://www.bleepingcomputer.com/news/security/ransomware-gangs-pose-as-it-support-in-microsoft-teams-phishing-attacks/