Threat Intelligence Report

Workplace Collaboration Tools: An Overlooked Attack Vector

Cyber criminals are increasingly exploiting widely used workplace tools, such as office suites, collaboration platforms, and business messaging applications, as initial attack vectors due to their widespread adoptions and the valuable data they contain. These applications, integral to everyday business operations, are trusted communications channels and data repositories for employees and are deeply embedded in corporate workflows. This makes them prime targets for social engineering attacks by threat actors seeking to gain access to corporate networks, exfiltrate data, and deploy ransomware. By taking advantage of users' familiarity and reliance on these tools, cyber criminals can bypass traditional security measures that are often more focused on external threats. Common tactics include posing as help desk or IT personnel over corporate chat channels, distributing malware via trusted document-sharing platforms, and impersonating employees to solicit credentials or other sensitive information.

THREAT ACTIVITY

- In August 2024, threat actors leveraged a widely used web-based collaborative platform to steal credentials. The threat actors compromised a supplier's account, and uploaded a seemingly legitimate document that had been weaponized with a malicious payload. The threat actors then exploited the platform's ability to share documents, sending the document to identified employees using the legitimate infrastructure. Once the recipient opened the document, they were prompted to enter their credentials, which were then stolen by the attackers.
- In May 2024, the Black Basta ransomware group and Storm-1811, operator of Black Basta ransomware, were observed conducting mass e-mail spam attacks to enable social engineer campaigns. After flooding victim inboxes with spam e-mails, the threat actors contacted victims over the phone, posing as IT or help desk staff, and tricked target users into downloading remote monitoring and management (RMM) tools to "fix" the spam e-mail issue. In October 2024, Black Basta ransomware group escalated their social engineering tactics by posing as IT support on internal company communication platforms, eliminating the need for threat actors to communicate with victims via phone and lending legitimacy to their social engineering efforts.
- In September 2024, security researchers observed threat actors abusing two trusted collaboration platforms to bypass traditional e-mail security solutions and socially engineer victims into surrendering network credentials. In the first phase of the campaign, threat actors sent legitimate-appearing PDF documents to victims. Rather than containing malicious code, which could be easily caught by e-mail security features, the documents contained QR codes with instructions to scan in order to view the full document content. The QR code directed victims to a real page on a well-known collaboration platform, where the victim was prompted to click on a shared file link matching the name of the e-mailed document. From there, the victim was directed to a spoofed login page for a second collaboration tool, widely used for cloud document storage, which harvested the victim's credentials.

THREAT ASSESSMENT

FTI Cybersecurity assesses that cyber criminals will continue to exploit workplace tools as key vectors for social engineering attacks. Traditional security measures and training have primarily focused on identifying and defending against external threats, leaving employees more vulnerable to social engineering attacks originating from within internal workplace tools. FTI Cybersecurity further assesses the rise of remote work has expanded the attack surface, as employees increasingly rely on internal workplace tools to communicate and collaborate, often with no ability to validate communications in-person. The real-time nature of some of these social engineering attacks enables cyber criminals to adapt their tactics based on immediate target user responses, increasing the chances of success compared to one-off phishing attempts.

RECOMMENDED ACTIONS

- Restrict communication from external users in workplace communication platforms, when possible; if not, allowlist trusted domains.
- Conduct regular phishing simulation exercises to reinforce security best practices, remind employees of established IT support procedures, and provide resources on how to recognize suspicious behaviors and verify requests from external entities.
- Uninstall or block RMM tools when they are not in use.
- Strengthen access authentication policies to harden systems against phishing threats.
- Implement application control policies to restrict RMM tool usage to authorized software only.
- Ensure that logging is enabled for internal communication platforms and regularly review sign-in logs to identify and flag suspicious sign-in activity.

SOURCES

- New Black Basta Social Engineering Scheme
- Black Basta ransomware poses as IT support on Microsoft Teams to breach networks
- Threat actors misusing Quick Assist in social engineering attacks leading to ransomware
- Quishing 2.0: QR Code Phishing Evolves with Two-Step Attacks and SharePoint Abuse
- Phishing in Style: Microsoft Sway Abused to Deliver Quishing Attacks
- Hackers Exploit Microsoft Teams In New Ransomware Scam
- A Surge in Credential Hijacking Attacks Exploits Microsoft SharePoint: A User and Defender's Nightmare

Why FTI Cybersecurity

MULTIDISCIPLINARY EXPERTISE

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, prosecuting offices, and global private sector institutions

GLOBALLY POSITIONED

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

INTEGRATED & COMPREHENSIVE

Comprehensive services include crisis communications, e-discovery, forensic investigations, and more

Seamless integration of FTI Consulting's expertise across service offerings

FTI Cybersecurity Global Offices

AMERICAS

Atlanta
Boston
Chicago
Houston
Irvine
Los Angeles
Mexico City
Miami
New York
San Francisco
São Paulo
Seattle
Toronto
Washington, DC
Wayne

EMEA

Berlin
Brussels
Cape Town
Dubai
Dublin
Düsseldorf
Frankfurt
Johannesburg
London
Madrid
Mumbai
Munich
Paris
Zurich

APAC

Brisbane
Hong Kong
Melbourne
Perth
Shanghai
Singapore
Sydney
Tokyo

CONTACT FTI CYBERSECURITY

Email: #fticybersecurity@fticonsulting.com