IMPORTANT CYBERSECURITY NEWS: HACKERS USE MICROSOFT TEAMS CHATS TO DELIVER MALWARE TO WINDOWS PCS

Vairav Cyber Security News Report

Date: April 16, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Thirbam Sadak 148
Baluwatar, Kathmandu

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

ReliaQuest has identified a sophisticated cyberattack targeting organizations in the finance and professional services sectors. The attackers initiated the breach through a Microsoft Teams phishing campaign, leading to the deployment of a previously unknown PowerShell-based backdoor. This incident underscores the continuous evolution of threat actors and the importance of proactive cybersecurity measures such as basic cybersecurity awareness among all employees.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: The attack commenced with a targeted phishing campaign delivered via Microsoft Teams, exploiting the platform's communication features to deceive recipients. Upon successful phishing, the attackers deployed a novel PowerShell-based backdoor, enabling remote control over the infected systems. A distinctive aspect of this attack was the use of COM TypeLib hijacking for persistence—a technique not previously observed in the wild. By manipulating the Windows registry to point to a malicious TypeLib, the attackers ensured their backdoor would execute whenever the associated COM object was instantiated, thereby maintaining persistent access without detection.

Identification: ReliaQuest detected the intrusion while investigating multiple customer incidents in March 2025. The combination of familiar initial access methods with novel persistence techniques prompted a deeper analysis, leading to the discovery of the new backdoor and the COM TypeLib hijacking method.

Threat Actor: The initial tactics align with those of "Storm-1811" (also known as "STAC5777"), a threat group associated with Black Basta ransomware deployments. However, the introduction of new techniques suggests possible evolution within the group or the formation of a new subgroup.

Affected Entities/Industries:

- Finance sector organizations
- Professional, scientific, and technical services firms

Potential Impact:

- Unauthorized access to sensitive data
- Potential deployment of ransomware
- Operational disruptions
- Reputational damage

Exploitation Methods:

- Phishing via Microsoft Teams
- Deployment of a novel PowerShell-based backdoor
- Persistence through COM TypeLib hijacking

RELATED THREAT INTELLIGENCE & IOCs

Microsoft Teams Phishing Tenant

- techsupport[at]sma5smg.sch[.]id

Malicious IPs

- 181.174.164[.]180
- 130.195.221[.]182
- 98.158.100[.]22
- 181.174.164[.]107
- 181.174.164[.]140
- 181.174.164[.]2
- 181.174.164[.]240
- 181.174.164[.]4
- 181.174.164[.]41
- 181.174.164[.]47
- 5.252.153[.]15
- 5.252.153[.]241

Malware Hashes (SHA256)

- f74fac3e5f7ebb092668dc16a9542799ccacc55412cfc6750d0f100b44eef898
- 08b6bfc9a75a6bf94994936a4c3e6d6946a2437b31d8f6e8841a52df76397237
- ff707131ff8cb4779afa66addd6efce3ce165e115806570cc3c2ed6df6be8de0
- 074124df8f60cef79577cad43a3adef39a4f773c2f4b5e33e292992d410cc012
- 41c3c83a0b39d91d2c35398113788eabcad2de36138304c812dce0282941b152
- f74fac3e5f7ebb092668dc16a9542799ccacc55412cfc6750d0f100b44eef898
- ef9456ada1d93e7cfc1750be1afd68807d532b6e893edd5ad79f016affd29dd0
- ecfcca6de9fb12c2989f0a46a235f3de2c7b6f0be0a4822af9848ee21e3b541d
- 7ddbf961dfbb78daee07b04111b8dedf693bb8807406cd2c442480c551d247e1
- 2df636a9ebdc6799d494151915656dc302deeade7e7ddca2e2e414869777e740
- 62faba34d0439b74ec716e62eb990063f3a03a5516de3976bfdd80cb0e39a76a
- 9c13fbdbc450474d4477c397497c9b40be7b89a1b4f9dfc57d764c7405301bb9
- 1821e33b7355d857fe3af5b67cb651260fa010a12d5ebd8d30ad110b647b2e6b
- f560e95fd233a8441c5195a3864c78d9ef5d3b9033a383c555d7c1e3c30fca0a
- e68084a7eb869ef88cd61ec26537c7ca0433124cebfbd20aebc8b4330952c653
- b59e9d53ab73464e14d81f5a00e1c7580a99eed078a8dff448b926de3f0df0e6
- bbd1afa9d0b142a0cc0ef7f1487eed512d538c79cd225e6ca9ca77e0a85f1f60
- e7dd0d24a511cf8170840f8ebac3df3787ba3bfd97d136f4a18a115700d137ff
- 3d0a09ba259d5f4b1e8d261fe05fef56b8611ba30edf46b7d927f8f0808b9c53
- 6395a9b7be56159dc8d2fc2858b6f0fdcf63a1623ea426a49625195123f5166f
- 2b21d0a08fce188885520e610a68f06766729ea935631afc843747f1cee387ab
- 291700be999ed8d361e9418a3375353c384999afc42271affa7ecc395f137fc0
- ec513db1dcd045444fb7282f382786d91ed3357d254797afacec8b7bab1f5070
- 4dbd1bf6a07b97cb14cd4e2d78d09bc3561f225b64f99dc40774959e6bd9de21
- 7a0dea548c6cd0259ffb339865add2b739ab6441b1b5263e3787120b8622d286
- c09dffd32f233b9d65fe73432cfa29c1de9ea56cfd2f42b985f5e0cccfc0aa4f
- 3c2c2d10650b98a7121c9d76e206fa1ffe81374e0594d226c0bf56eb17423825
- 287e85989b76b8b395311575fc20cd18efa38571ccf94cec2a3d3d0683862d79
- 7b89423831873906aa3f28507d1adbcca92b37dbb8a9be4f2d753ebc31467f33

- abfb7c3c3ea828bf85874c596cac17770668abb28734cbeec67dc8c958afd340
- 3448da03808f24568e6181011f8521c0713ea6160efd05bff20c43b091ff59f7

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Restrict external communication capabilities in Microsoft Teams to prevent phishing attempts.
- Monitor for unusual registry modifications, particularly those related to COM TypeLib entries.
- Implement detection rules for anomalous PowerShell activity indicative of backdoor deployment.

Security Best Practices

- Conduct regular security awareness training focusing on phishing threats via collaboration platforms.
- Enforce the principle of least privilege to minimize potential impact from compromised accounts.
- Maintain up-to-date antivirus and endpoint detection solutions capable of identifying novel threats.

For Advanced Security Teams

- Develop and deploy custom detection signatures for COM TypeLib hijacking attempts.
- Perform threat hunting activities focusing on registry anomalies and PowerShell execution patterns.
- Collaborate with threat intelligence providers to stay informed about emerging tactics and threat actors.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://gbhackers.com/hackers-use-microsoft-teams-to-deliver-malware/
- https://reliaquest.com/blog/threat-spotlight-hijacked-and-hidden-new-backdoor-and-persistence-technique/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com