BREAKING CYBERSECURITY NEWS: BOTNET TARGETS BASIC AUTH IN MICROSOFT 365 PASSWORD SPRAY ATTACKS

Vairav Cyber Security News Report

Date: 2025-02-25

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

EXECUTIVE SUMMARY

A recent cybersecurity incident has unveiled a massive botnet comprising over 130,000 compromised devices conducting password-spray attacks against Microsoft 365 (M365) accounts globally. Attackers are exploiting Basic Authentication (Basic Auth) to bypass Multi-Factor Authentication (MFA), leading to unauthorized access without triggering security alerts. This development underscores the critical need for organizations to transition to more secure authentication methods to protect sensitive data and maintain operational integrity.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: The botnet executes password-spray attacks targeting M365 accounts by leveraging Basic Auth, an outdated authentication method where user credentials are transmitted in plaintext or base64 encoded form. This approach allows attackers to bypass MFA protections and gain unauthorized access without triggering security alerts. The botnet operates through command and control (C2) servers hosted by U.S. provider SharkTech, with traffic proxied through Hong Kong-based UCLOUD HK and China-linked CDS Global Cloud. The C2 servers run Apache Zookeeper and use Kafka to manage botnet operations. The system timezone on the C2 servers is set to Asia/Shanghai, and their uptimes indicate the botnet has been active since at least December 2024. The attacks utilized Basic Auth methods, with the user agent "fasthttp" appearing in authentication logs. This discovery highlights the importance of monitoring non-interactive sign-ins, which are often overlooked by security teams.

Identification: Security researchers at SecurityScorecard identified the botnet's activity while investigating numerous failed sign-in attempts in the non-interactive sign-in logs of a Microsoft 365 tenant.

Threat Actor: The botnet's infrastructure and tactics suggest possible links to Chinese-affiliated threat actors. However, definitive attribution has not been established.

Affected Entities/Industries: The attack has implications across various industries, particularly those heavily reliant on Microsoft 365 for email, document storage, and collaboration. Key affected sectors include financial services, healthcare, government and defense, technology and SaaS providers, and education and research institutions.

Potential Impact: The attack poses significant risks, including unauthorized access to sensitive information, potential data breaches, operational disruptions, financial losses, and reputational damage. The exploitation of Basic Auth allows attackers to bypass MFA and Conditional Access Policies, increasing the likelihood of account compromise.

Exploitation Methods: Attackers employed password-spray attacks using credentials stolen by infostealer malware. By targeting non-interactive sign-ins through Basic Auth, they evaded MFA protections and security alerts, enabling unauthorized access to M365 accounts.

RELATED THREAT INTELLIGENCE & IOCs

Malicious IPs

- 168[.]232[.]198[.]140
- 186[.]84[.]88[.]65
- 157[.]100[.]136[.]29
- 182[.]48[.]71[.]9
- 75[.]31[.]61[.]38
- 176[.]63[.]24[.]12
- 45[.]181[.]131[.]193
- 138[.]117[.]178[.]208
- 115[.]72[.]28[.]107
- 212[.]47[.]134[.]161
- 187[.]190[.]63[.]60
- 103[.]134[.]127[.]6
- 181[.]80[.]212[.]44

- 190[.]236[.]203[.]231
- 187[.]17[.]132[.]99
- 112[.]206[.]110[.]5
- 190[.]12[.]151[.]92
- 38[.]41[.]0[.]115
- 187[.]246[.]226[.]42
- 70[.]39[.]115[.]74
- 70[.]39[.]120[.]10
- 204[.]188[.]218[.]178
- 204[.]188[.]218[.]179
- 204[.]188[.]210[.]226
- 204[.]188[.]210[.]227

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- **Disable Basic Authentication**: Organizations should promptly disable Basic Auth in their Microsoft 365 environments to prevent attackers from exploiting this outdated protocol.
- **Monitor Non-Interactive Sign-Ins**: Regularly review non-interactive sign-in logs for unauthorized access attempts, focusing on anomalies such as increased login attempts or unfamiliar user agents.
- **Rotate Credentials**: Immediately change passwords for accounts flagged during recent sign-in attempts to prevent unauthorized access.

Security Best Practices

- **Implement Multi-Factor Authentication (MFA)**: Ensure MFA is enabled for all user accounts to add an extra layer of security against unauthorized access.
- **Restrict Legacy Protocols**: Disable legacy authentication protocols like POP, IMAP, and SMTP that do not support MFA and are susceptible to attacks.

- **Enhance Conditional Access Policies**: Develop and enforce Conditional Access Policies to restrict login attempts based on factors such as location, device compliance, and risk level.

For Advanced Security Teams

- **Deploy Advanced Threat Protection**: Utilize tools like Microsoft Defender for Identity and Microsoft Sentinel to detect and respond to suspicious activities in real-time.
- **Conduct Threat Hunting**: Proactively search for signs of compromise within the network, focusing on unusual authentication patterns and potential lateral movement.
- **Engage in Continuous Monitoring**: Implement continuous monitoring solutions to detect and respond to security incidents promptly, minimizing potential damage.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://www.bleepingcomputer.com/news/security/botnet-targets-basic-auth-in-microsoft-365-password-spray-attacks/
- https://securityscorecard.com/wp-content/uploads/2025/02/MassiveBotnet-Report_022125_03.pdf

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