New Mamba 2FA bypass service targets Microsoft 365 accounts

By
Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)

October 8, 2024 04:27 PM **0**

An emerging phishing-as-a-service (PhaaS) platform called Mamba 2FA has been observed targeting Microsoft 365 accounts in AiTM attacks using well-crafted login pages.

Additionally, Mamba 2FA offers threat actors an adversary-in-the-middle (AiTM) mechanism to capture the victim's authentication tokens and bypass multi-factor authentication (MFA) protections on their accounts.

Mamba 2FA is currently sold to cybercriminals for $250/month, which is a competitive price that positions it among the most alluring and fastest-growing phishing platforms in the space.

Discovery and evolution

Mamba 2FA was first documented by Any.Run (https://any.run/cybersecurity-blog/analysis-of-the-phishing-campaign/) analysts in late June 2024, but Sekoia reports (https://blog.sekoia.io/mamba-2fa-a-new-contender-in-the-aitm-phishing-ecosystem/) that it has been tracking activity linked to the phishing platform since May 2024.

Additional evidence shows that Mamba 2FA has been supporting phishing campaigns since November 2023, with the kit being sold on ICQ and later on Telegram.

Following Any.Run's report of a campaign backed by Mamba 2FA, the operators of the phishing kit made several changes to their infrastructure and methods to increase the stealthiness and longevity of the phishing campaigns.

For example, starting in October, Mamba 2FA introduced proxy servers sourced from IPRoyal, a commercial provider, to mask the IP addresses of relay servers on authentication logs.

Previously, relay servers connected directly to Microsoft Entra ID servers, exposing the IP addresses and making blocks easier.

Link domains used in phishing URLs are now very short-lived and typically rotated weekly to avoid blocklisting by security solutions.

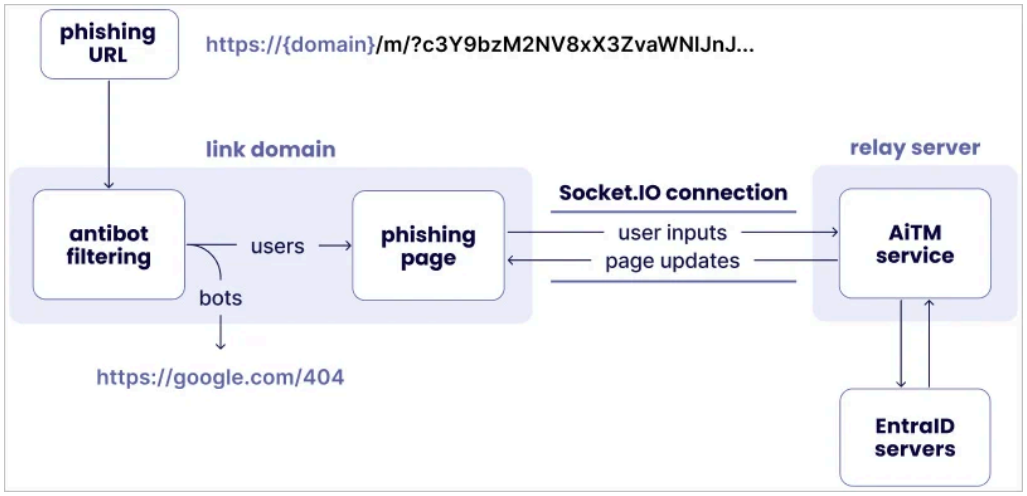
Another change was enhancing HTML attachments used in phishing campaigns with benign filler content to hide a small snippet of JavaScript that triggers the attack, making it harder for security tools to detect.

"Biting" Microsoft 365 users

Mamba 2FA is specifically designed to target users of Microsoft 365 services, including corporate and consumer accounts.

Like other similar PhaaS platforms, it uses proxy relays to conduct AiTM phishing attacks, allowing the threat actors to access one-time passcodes and authentication cookies.

The AiTM mechanism uses the Socket.IO JavaScript library to establish communication between the phishing page and the relay servers at the backend, which in turn communicate with Microsoft's servers using the stolen data.

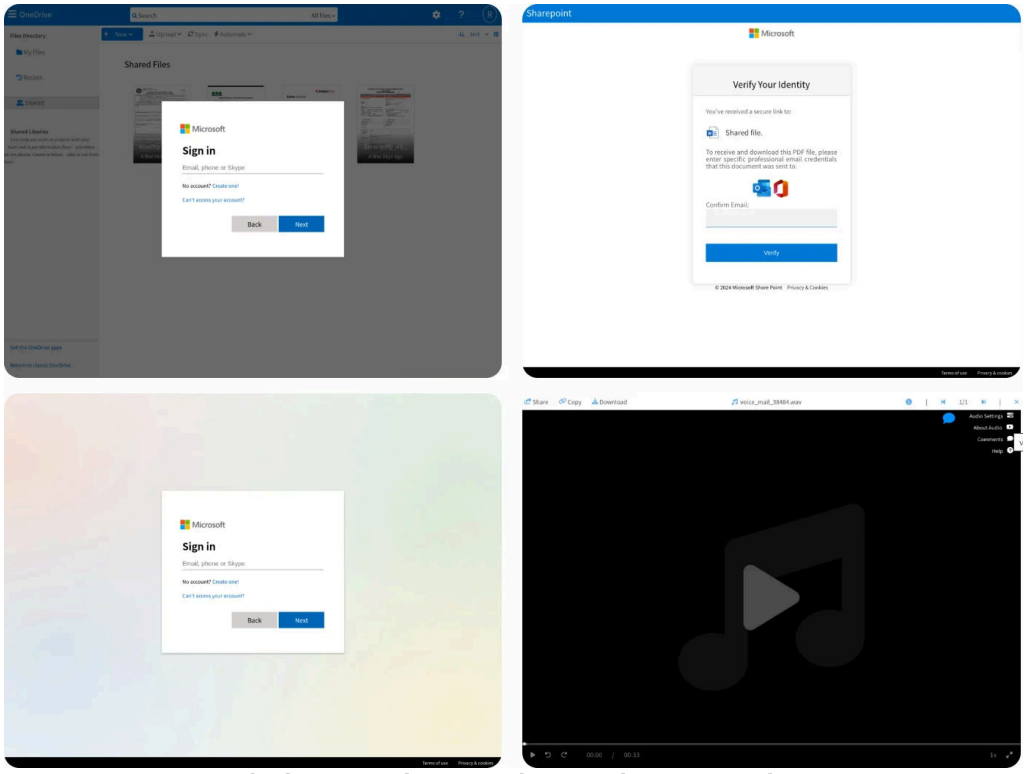


Mamba 2FA operational overview

Source: Sekoia

Mamba 2FA offers phishing templates for various Microsoft 365 services, including OneDrive, SharePoint Online, generic Microsoft sign-in pages, and fake voicemail notifications that redirect to a Microsoft login page.

For enterprise accounts, the phishing pages dynamically assume the targeted organization's custom login branding, including logos and background images, making the attempt appear more authentic.



Phishing templates used in Mamba 2FA attacks

Source: Sekoia

Captured credentials and authentication cookies are transmitted to the attacker through a Telegram bot, enabling them to initiate a session immediately.

Mamba 2FA also features sandbox detection, redirecting users to Google 404 webpages when it deduces it's being under analysis.

Overall, the Mamba 2FA platform is yet another threat to organizations, allowing low-skilled actors to perform highly effective phishing attacks.

To protect against PhaaS operations using AiTM tactics, consider using hardware security keys, certificate-based authentication, geo-blocking, IP allowlisting, device allowlisting, and token lifespan shortening.

Related Articles:

Police dismantles phone unlocking ring linked to 483,000 victims (https://www.bleepingcomputer.com/news/security/police-dismantles-iserver-phone-unlocking-network-linked-to-483-000-victims/)

Microsoft Sway abused in massive QR code phishing campaign (https://www.bleepingcomputer.com/news/security/microsoft-sway-abused-in-massive-qr-code-phishing-campaign/)

Microsoft Outlook bug blocks email logins, causes app crashes (https://www.bleepingcomputer.com/news/microsoft/microsoft-outlook-bug-blocks-email-logins-causes-app-crashes/)

Microsoft fixes Word bug that deleted documents when saving (https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-word-bug-that-deleted-documents-when-saving/)

Microsoft: Word deletes some documents instead of saving them (https://www.bleepingcomputer.com/news/microsoft/microsoft-word-for-microsoft-365-deletes-some-documents-instead-of-saving-them/)

MAMBA 2FA (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MAMBA-2FA/)

MICROSOFT 365 (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MICROSOFT-365/)

PHISHING (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PHISHING/)

PHISHING KIT (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PHISHING-KIT/)

PHISHING-AS-A-SERVICE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PHISHING-AS-A-SERVICE/)