Mamba 2FA

PREVALENCE	IMPLEMENTATION
Medium	Synchronous relay

ALIASES

LICENSING Phishing-as-a-Service
TARGET Microsoft 365
FIRST SEEN November 2023

CONTEXT
- PhaaS since at least November 2023, sold on Telegram

ANTI-BOT PAGES
Blank page
Use of Adspect anti-bot service

INFRASTRUCTURE
Operator's infrastructure
- Phishing domain names
  - three groups: `/o/`, `/r/` or `/s/` phishing URLs
  - including some compromised legitimate domains (*e.g.* WordPress)
- Exfiltration domain names
  - usually 3 active at a time (one for each of the groups of phishing URLs)
  - behind Cloudflare
  - hosting Node.js code (Express, Socket.IO)

URL PATTERNS
- Autograb URL:
  - `https?://<phishing-domain>/(o|r|s)/?(c3Y9bzM2NV|aXBkYXRhP)<base64>N0123N<email>`
- Exfiltration URL:
  - `(https|wss)://<exfiltration-domain>/socket.io/?EIO=4&transport=...`

MAIN STEPS

Anti-bot check	Phishing domain

- Obfuscated HTML and JavaScript
- JavaScript fingerprinting of the web browser

Fake Microsoft authentication page	Phishing domain

- Obfuscated JavaScript code implementing all the variations in a Microsoft 365 authentication

Exfiltration	Exfiltration domain

- Send data using Socket[.]IO JavaScript library (WebSocket with HTTP fallback)

Redirection	Microsoft domain

- Redirection to a legitimate Office URL

AUTHENTICATION WITH MICROSOFT SERVICES

APP ID 4765445b-32c6-49b0-83e6-1d93765276ca (OfficeHome)

TOP ASNS
IPRoyal proxies in ASs
Simoresta UAB and Karolio IT

OTHER CHARACTERISTICS
- Anti-bot check redirection to `https://google.com/404/`
- Final redirection to `https://outlook.office365.com/error/`

INDICATORS IN CODE
- Anti-bot page:
  - `<img src="/files/images/Logo.png" data-digest="<base64>" onerror="(new Function(atob(this.dataset.digest)))();" style="visibility: hidden;">`
- Phishing page:
  - `<html id='html' sti='<base64>' vic='<autograb>' lang='en'>`
  - `const pointLink = "<base64>";`

AnyRun	Analysis of the Phishing Campaign: Behind the Incident	Jun 2024
Sekoia.io	Mamba 2FA: A new contender in the AiTM phishing ecosystem	Oct 2024
Randy McEoin	Anti-bot services used by PhaaS - Part 1	Dec 2024