Sneaky 2FA

PREVALENCE	IMPLEMENTATION
Medium	Synchronous relay

ALIASES Sneaky Log, WikiKit

LICENSING	Phishing-as-a-Service
TARGET	Microsoft 365
FIRST SEEN	September 2024

CONTEXT

- PhaaS since at least October 2024, sold on Telegram
- Quickly emerged at the end of 2024 and the beginning of 2025

ANTI-BOT PAGES

- Cloudflare Turnstile challenge impersonating Microsoft
- Cloudflare Turnstile with a blurred background

INFRASTRUCTURE

- Affiliate's infrastructure:
  - Phishing domain

URL PATTERNS

- Autograb URL:
  - `https://<domain>/<uri>/#<email-address>` or `https://<domain>/<uri>/?a=<base64(email-address)>`
- Phishing pages:
  - `https://<domain>/<uri>/[a-zA-Z0-9]{120,170}/(index|verify|validate)`

MAIN STEPS

Benign HTML page — Phishing domain

- HTML page with food-related content not visible to user
- Loading the next-stage using `window.location.reload()`
- Obfuscated using HTML tags

Cloudflare Turnstile page — Phishing domain

- HTML page with food-related content not visible to user
- Embed JavaScript code loading the Turnstile challenge

Redirection steps — Phishing domain

- HTML page with food-related content not visible to user
- Loading the next-stage using window.location.reload()
- Obfuscated JavaScript code managing the redirection

Fake Microsoft authentication page — Phishing domain

- HTML page embedding all the Microsoft authentication pages
- Base64-encoded images and obfuscation using HTML tags
- Obfuscated JavaScript code managing the authentication process

Redirection — Microsoft domain

- Redirection to a legitimate Office365 URL

AUTHENTICATION WITH MICROSOFT SERVICES

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

TOP ASNS

AS14061
AS14956
AS36352
AS58329
AS39378

OTHER CHARACTERISTICS

Redirection to Wikipedia webpages (Microsoft themed) using href links, *e.g.* `https://href[.]li/?https://en.wikipedia[.]org/wiki/`

INDICATORS IN CODE

- HTML tags, such as `<!-- Food Section -->`
- HTML title, *e.g.* "Verify your account", "Verify your identity", "Confirm your login", "Signin to your account", etc.

TRAC Labs	WikiKit AiTM Phishing Kit: Where Links Tell Lies	Dec 2024
Sekoia.io	Sneaky 2FA: exposing a new AiTM Phishing-as-a-Service	Jan 2025