Tycoon 2FA

PREVALENCE	IMPLEMENTATION
High	Synchronous relay

ALIASES Storm-1747

LICENSING	Phishing-a-a-Service
TARGET	Microsoft 365, Google
FIRST SEEN	August 2023

CONTEXT

- PhaaS since at least August 2023, sold on Telegram
- Major AitM PhaaS in 2024 and early 2025
- Includes source code from Dadsec at the origin

ANTI-BOT PAGES

- Custom CAPTCHA pages
- Fake Cloudflare Turnstile pages
- Fake hCaptcha pages
- Fake reCAPTCHA pages

INFRASTRUCTURE

Operator's infrastructure

- Phishing domain names
- Central servers:
  - Verification domain names (returning 1 or 0)
  - Exfiltration domain names

URL PATTERNS

- Domain names, mostly matching this pattern `[a-z0-9]{2,6}\.[a-z]{5,15}\.(ru|com|es)` (also .cc, .info, .su, .vip and other TLDs)
- Autograb URL mostly matching these patterns:
  - `https://<domain>/[a-zA-Z0-9@!]{4,15}/($|*|?em=|)<email-address>`
  - `https://<domain>/[a-zA-Z0-9]{0,15}@[a-zA-Z0-9]{0,15}/`
  - `https://<domain>/[a-zA-Z0-9]{0,15}@[a-zA-Z0-9]{0,15}/($|*)<username-email-address>`
- Others URLs (resources, exfiltration, check): pseudo-randomly generated

MAIN STEPS

HTML pages (Anti-bot, redirection, and fake Microsoft authentication pages) — Phishing domain

- HTML page loading a custom CATCHA challenge
- Obfuscated JavaScript code using AES encryption and base64 encoding (crypto-js library)

Check with central server — Verification domain

- Receive 1 or 0 from central server, likely to continue or not

JavaScript code implementing authentication steps — Phishing domain

- Obfuscated JavaScript code using AES encryption and base64 encoding(crypto-js library)
- JavaScript implementing user's browser fingerprint and anti-debugging functions and all the variations in a Microsoft 365 authentication

Fingerprinting — Phishing domain

- Send obfuscated information on the host and the authentication

Exfiltration — Exfiltration domain

- Send obfuscated data

AUTHENTICATION WITH MICROSOFT SERVICES		TOP ASNS
APP ID	4765445b-32c6-49b0-83e6-1d93765276ca (OfficeHome)	AS9009 AS29802

OTHER CHARACTERISTICS

- Unwanted traffic redirection to various eCommerce websites

INDICATORS IN CODE

- Code deobfuscation by using libraries fetched from:
  - `https://code.jquery.com/jquery-3.6.0.min.js`
  - `https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.1.1/crypto-js.min.js`
- Invisible character (unicode U+200B) in HTML title

Sekoia.io	@sekoia_io analysts uncovered a new emerging Adversary-in-the-Middle (AiTM) Phishing-...	Oct 2023
Sekoia.io	Tycoon 2FA: an in-depth analysis of the latest version of the AiTM phishing kit	Mar 2024
Randy McEoin	Tycoon2FA Deobfuscation	Nov 2024
Randy McEoin	Anti-bot services used by PhaaS - Part 2	Dec 2024

TLP:CLEAR