Saiga 2FA

PREVALENCE	IMPLEMENTATION
Low	Synchronous relay

ALIASES SAIGA Page

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

CONTEXT
- Phishing kit used by the threat group "SAIGA Group", allegedly offered as-a-service
- Actively used in the wild in early 2025, and discovered by Sekoia in February 2025
- Relative low level of sophistication

ANTI-BOT PAGES
- Custom Cloudflare Turnstile pages, possibly not used by default by the kit

INFRASTRUCTURE
- Affiliate's infrastructure:
  - Phishing domain names

URL PATTERNS
- Autograb URL:
  - `https://<domain>/?S=<email-address>`
- Exfiltration endpoints:
  - `/api/(config|check-bot|check-ip|deets|email|login|notice|auth|poll|process|kmsi)/`

MAIN STEPS

JavaScript pages implementing phishing functions — Phishing domain
- Initial HTML page fetching several JavaScript scripts
- Obfuscated JavaScript of a Next.js application
- JavaScript code communicating with the phishing server, parsing data, and dynamically displaying fake Microsoft authentication pages

Exfiltration — Phishing domain
- POST requests to multiple endpoints exfiltrating victim's data and fetching server's data

Redirection — Custom domain
- Redirection to a URL received by the phishing server

AUTHENTICATION WITH MICROSOFT SERVICES

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

TOP ASNS
AS36352
AS9009
AS47583
AS23470
AS16276

OTHER CHARACTERISTICS
- Design of the fake Microsoft authentication pages does not exactly copy the legitimate ones (different font, different boxes)

INDICATORS IN CODE
- Next.js JavaScript code
- HTML title using Latin words, *e.g.* `Dolor et culpa ut culpa nulla occaecat esse eiusmod velit nisi aliquip irure eu ad.`
- Characteristic JSON files received from `/api/` endpoints containing configuration settings

Sekoia.io	Saiga 2FA malware object in Sekoia.io CTI (Customer access only)	Feb 2025
Red Piranha	Suspected SAIGA Threat Actors Exploit Australian Legal Sector with EDR Bypass	Mar 2025

TLP:CLEAR