NakedPages

PREVALENCE	IMPLEMENTATION
High	Reverse proxy

ALIASES Storm-1101, SakaiPages, ironsentry

LICENSING Phishing-as-a-Service

TARGET Microsoft 365, allegedly 5+ others

FIRST SEEN May 2022

CONTEXT

- Major AitM PhaaS between 2023 and 2025
- Rebranded multiple time (NakedPages, SakaiPages, IronSentry) and remains widespread

ANTI-BOT PAGES

- Custom Cloudflare Turnstile with black footer
- Default Cloudflare Turnstile webpage, with or without custom text

INFRASTRUCTURE

- Initial domain:
  - either Cloudflare Workers, subdomains from `workers.dev`
  - affiliate-controlled domain names
- Phishing domain:
  - affiliate-controlled domain names

URL PATTERNS

Initial Clouflare Turnstile and redirection URLs:

- mostly `https://<initial-domain>/?(qrc|email)=<email-address>`
- or `https://<initial-domain>/?(qrc|email)=<base64(email-address)>`
- sometimes additional query fields, such as `?cfg`

Additional redirection steps:

- `https://<phishing-domain>/?dataXX0=.*`
- `https://<phishing-domain>/owa/?login_hint=<email-address>`

Default Microsoft endpoints (reverse proxy), *e.g.*:

- `https://<phishing-domain>/aadcdn.msftauth.net/~/shared/1.0/content/.*`

Final redirection step:

- `https://<phishing-domain>/ping/v5767687`

MAIN STEPS

Cloudflare Turnstile webpage — Initial domain

- Cloudflare Turnstile HTML page displaying the malicious domain name

Previous versions used a custom page to hide the malicious domain, which contained a typo: "We needs to review…".

Anti-bot checks and redirection step — Initial domain

- Anti-bot checks performed on server-side
- HTML page embedding JavaScript to redirect to the phishing domain including the victim's email address in the phishing URL and using an iframe

Fake Microsoft authentication page — Phishing domain

- Phishing server operating as a reverse proxy, relaying all requests to Microsoft API

Redirection — Mosty Microsoft domain

- Redirection to another URL using the HTTP Location returned by the server

AUTHENTICATION WITH MICROSOFT SERVICES

APP ID

- 00000002-0000-0ff1-ce00-000000000000 (Office 365 Exchange Online)
- 72782ba9-4490-4f03-8d82-562370ea3566 (Office365)
- 4765445b-32c6-49b0-83e6-1d93765276ca (OfficeHome)

TOP ASNS

AS36352
AS215540
AS401120
AS149440
AS14061

INDICATORS IN CODE

For previous versions of custom Cloudflare Turnstile webpages:

- `We needs to review the security of your connection before proceeding.`
- `We need to review the security of your connection before proceeding.`

Microsoft login page:

- `rickorigin=`

CloudSEK	Sophisticated Phishing Toolkit Dubbed "NakedPages" for Sale on Cybercrime Forums	Jun 2022
Microsoft	DEV-1101 enables high-volume AiTM campaigns with open-source phishing kit	Mar 2023