CEPHAS

PREVALENCE	Low
IMPLEMENTATION	Synchronous relay
ALIASES	W3LL Panel, OV6
LICENSING	Phishing-as-a-Service
TARGET	Microsoft 365
FIRST SEEN	August 2024

CONTEXT

- PhaaS used since August 2024
- Kit formerly known as W3LL Panel since at least February 2019
- W3LL Panel has AitM capabilities since March 2022

ANTI-BOT PAGES

- Custom Cloudflare Turnstile (optional)

INFRASTRUCTURE

Affiliate-controlled:

- Initial domain, can be object storage service
- Phishing domain

Operator's infrastructure:

- Central server interacting with Microsoft API (AS202015)

URL PATTERNS

- Phishing page: `https://<phishing-server>/<UUID>/`
- Encoded phishing page content: `GET <folder>/p5Qw9X8rN3.php`
- Turnstile verification: `POST <folder>/bR7sD9kJ2m.php`
- Credentials exfiltration: `POST <folder>/khL9kO2fV1.php`

MAIN STEPS

Static HTML document • Obfuscated HTML and JavaScript • Optional Cloudflare Turnstile • JavaScript fetching, decoding and rendering the fake Microsoft page from the phishing server	Local file or attachment URL
Anti-bot checks • The fake Microsoft page is not returned (404) if checks on the source IP and User-Agent suggest automated scanning	Phishing domain
JavaScript code implementing authentication steps • Sending user inputs to the phishing server and updating the fake Microsoft page for each authentication step	Phishing domain
Exfiltration • Send data in HTTP POST parameters	Phishing domain
Redirection • Redirection to a configurable decoy URL	Often Microsoft domain

AUTHENTICATION WITH MICROSOFT SERVICES	TOP ASNS
APP ID 4765445b-32c6-49b0-83e6-1d93765276ca (OfficeHome)	AS202015 AS14061 AS399629 AS36352 AS20473 AS14956

INDICATORS IN CODE

- Default Turnstile text: `Online safety check underway.`
- Hard-coded HTML element ids: `JKDfIUfjdsnf`, `KlwiHWjdk`, `UuejjerBHDdhEHE`
- Attachment / Landing page :
  - long comments about events happening at specific locations (*e.g.* "wine tasting on Riverside Avenue ...", "Anime Convention at the golf course ...")
  - `class="cloudflare_security_text"`
- Phishing page
  - two-words comments about astronomy concepts (*e.g.* "Stellar Vortex", "Spectral Quasar")
  - `localStorage.getItem('ov-cf')`

Group-IB	W3LL done: uncovering hidden phishing ecosystem driving BEC attacks	Sep 2023
Group-IB	W3LL phishing kit – the tools, the criminal ecosystem, and the market impact	Oct 2023

TLP:CLEAR