EvilProxy

PREVALENCE	IMPLEMENTATION
Medium	Reverse proxy

ALIASES Storm-0835

LICENSING Phishing-as-a-Service

TARGET Microsoft 365, Google, allegedly 20+ others

FIRST SEEN August 2020

CONTEXT

- Phishing kit sold on cybercrime forums (Exploit and XSS) since at least August 2020, as well as on Telegram
- Major AitM PhaaS from 2020 to early 2025
- Reverse proxy

ANTI-BOT PAGES

- Custom reCAPTCHA pages

INFRASTRUCTURE

Affiliate's infrastructure

URL PATTERNS

- Initial URLs:
  - `https://<phishing-subdomain-1>/?[a-zA-Z0-9]{2,6}=[a-zA-Z0-9]{2,6}`
  - `https://<phishing-subdomain-1>/?username=<email-address>`
- Authentication URL:
  - `https://[a-f0-9]{32}\.<phishing-domain>/.*`
- Authentication URL (older versions):
  - `https://[a-f0-9]{8}-[a-f0-9]{8}\.<phishing-domain>/.*`
  - `https://(accounts|0ffice|0nline1|l1ve)\.<phishing-domain>/.*`

MAIN STEPS

reCAPTCHA webpage (optional)	Phishing subdomain 1

- HTML page containing a reCAPTCHA challenge and obfuscated JavaScript code

Fake Microsoft authentication page	Phishing subdomain 1

- HTML page containing the fake Microsoft authentication page and obfuscated heavy JavaScript code

Authentication steps	Phishing subdomains 2 and 3

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

Redirection	Phishing subdomains 2 and 3

- Redirection to a Microsoft URL fetched using a WebSocket

AUTHENTICATION WITH MICROSOFT SERVICES

APP ID 72782ba9-4490-4f03-8d82-562370ea3566 (Office365)

TOP ASNS

AS14061
AS63949
AS14956
AS401120
AS399629

OTHER CHARACTERISTICS

- WebSockets communicating ping-pong, command and redirection URL data
- Automatically authorise the KMSI (Keep me signed in)
- Authentication request every 6 hours to keep the compromised session active (`RequestType=OrgIdWsFederation:federation`)

INDICATORS IN CODE

- HTML title of the reCAPTCHA webpage: `reCAPTCHA: Click Allow to verify that you are not a robot`

Resecurity EvilProxy Phishing-as-a-Service with MFA Bypass Emerged in Dark Web Sep 2022