Greatness

PREVALENCE	IMPLEMENTATION
Low	Synchronous relay

ALIASES Storm-1295

LICENSING Phishing-as-a-Service
TARGET Microsoft 365
FIRST SEEN June 2022

CONTEXT
- PhaaS since June 2022
- Significant threat since 2023
- New major version in February 2025, with backend source code rewrite in Python

ANTI-BOT PAGES
- Custom CAPTCHA pages impersonating Microsoft

INFRASTRUCTURE

Operator's infrastructure
- Phishing domain names
- Central server hosted on Amazon AWS (AS16509)

Affiliate's infrastructure (optional)
- Cloud services (Cloudflare R2 or Workers, Linode Object Storage)
- or attacker-controlled domains

URL PATTERNS
- Malicious JavaScript:
  - `https://<phishing-domain>/s/[a-f0-9]{7,12}?[a-f0-9]{7,12}=<email-address>`
  - `https://<phishing-domain>/s/[a-f0-9]{7,12}?[a-f0-9]{7,12}=<base64(email-address)>`
- FingerprintJS library: `https://<phishing-domain>/s/[0-9]{2}?0`
- HTML code: `https://<phishing-domain>/r/[0-9]{2}?session=[a-f0-9]{64}`
- WebSockets: `ws://<phishing-domain>/p/[0-9]{3}?session=[a-f0-9]{64}`

MAIN STEPS

HTML attachment fetching JavaScript	Attachment

- Benign HTML code embedding a JavaScript fetching an external script
- Can also be hosted by the affiliate (cloud service or attacker-controlled domain)

JavaScript and HTML codes	Phishing domain

- JavaScript codes implementing custom CAPTCHA and authentication steps, FingerprintJS library
- HTML code of the fake authentication steps

Exfiltration through WebSockets	Phishing domain

- Encoded data using three XOR keys
- Harvested data in JSON format

Redirection	Microsoft or Google domain

- Redirection to a legitimate domain

AUTHENTICATION WITH MICROSOFT SERVICES

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

TOP ASNS

PacketStream residential proxy
AS16509

OTHER CHARACTERISTICS
- Resources fetched from `upload.wikimedia[.]org` (Microsoft logo), `encrypted-tbn0.gstatic[.]com` (refresh image), `cdn2.iconfinder[.]com` (mail image) and `static.vecteezy[.]com` (CAPTCHA background) by the custom CAPTCHA page
- Some of the authentication requests performed from the central server (AS16509)

INDICATORS IN CODE
- HTML attachment containing such following JavaScript code:
  - `<script> b8527f88086 = ''.replace.call("<obfuscated-url>",/(a2ec21|edd117f1)/g,"");`
    `$.getScript(b8527f88086);</script>`
- Malicious JavaScript code containing characteristic variables and function, *e.g.* `var loader`, `var def_end`, `function docWriter`, `const botdPromise`, `const fpPromise`, *etc.*

Cisco Talos	New phishing-as-a-service tool "Greatness" already seen in the wild	May 2023
Vade	Phishing as a Service: Analyzing "Greatness"	Jun 2023