Storm-1167

PREVALENCE	IMPLEMENTATION
High	Synchronous relay

ALIASES FlowerStorm

LICENSING	Phishing-as-a-Service
TARGET	Microsoft 365
FIRST SEEN	April 2023

CONTEXT

- Major AitM PhaaS since
- Similarities with Rockstar 2FA, which disappeared in Q4 of 2024

ANTI-BOT PAGES

- Custom Cloudflare Turnstile with Microsoft logo

INFRASTRUCTURE

Operator's infrastructure

- Phishing domain: mostly `.it.com` FQDNs since mid-February 2025, and `.com` or `.de` domain names related to business, technology, finance or legal themes
- FQDN from Tencent cloud platform - hosting the main JavaScript code
- Exfiltration domain: most likely a single `.cfd`, `.sbs`, or `.xyz` domain name per affiliate until mid-March 2025, since FQDNs of the phishing domain

URL PATTERNS

FQDN from Tencent cloud platform:

- Pattern of Tecent domain names: `<BucketName-APPID>.cos.ap-<REGION>.myqcloud.com`, *e.g.* `5425043750-1317754460.cos.ap-tokyo.myqcloud[.]com`

Exfiltration domain:

- URL: `/google.php`
- Domain name: `[0-9]{9,10}\.(cfd|my\.id|sbs|xyz)`, *e.g.* `5425043750[.]sbs`

MAIN STEPS

Cloudflare Turnstile page	Phishing domain

Two templates:

- White page embedding the Turnstile challenge with instructions generated randomly
- Dark page embedding the Turnstile challenge, a Microsoft logo and fake Microsoft instructions

JavaScript code implementing authentication steps	FQDN from Tencent cloud platform

- Obfuscated JavaScript
- JavaScript code implementing all the variations in a Microsoft 365 authentication, and rendering fake Microsoft pages

Exfiltration	Exfiltration domain

- Send data to "/google.php" into POST parameters using the "do" field to indicate the step

Redirection	Microsoft domain

- Redirection to a legitimate Office365 URL

AUTHENTICATION WITH MICROSOFT SERVICES		TOP ASNS
APP ID	4765445b-32c6-49b0-83e6-1d93765276ca (OfficeHome)	AS132203 AS19871

INDICATORS IN CODE

- Pseudo-randomly generated HTML title for anti-bot and phishing pages (lowercase)
- HTML comments in various languages (English, French, German, Arabic, Spanish), formerly using nature theme (flowers or fruits)

Microsoft TI	Detecting and mitigating a multi-stage AiTM phishing and BEC campaign	Jun 2023
Sophos X-Ops	Phishing platform Rockstar 2FA trips, and "FlowerStorm" picks up the pieces	Dec 2024

TLP:CLEAR