Gabagool

PREVALENCE	IMPLEMENTATION
Low	Synchronous relay

ALIASES Skyw4lker

LICENSING Phishing-as-a-Service
TARGET Microsoft 365
FIRST SEEN October 2024

CONTEXT
- Highly likely a PhaaS, active since at least the end of October 2024
- Possibly the successor of Rockstar 2FA with the backend re-written in Python instead of PHP, based on several technical similarities

ANTI-BOT PAGES
- Custom Cloudflare Turnstile page, containing the text "Browser security check in progress."

INFRASTRUCTURE
Affiliate's infrastructure
- Initial domain name (optional)
- Phishing domain names

Operator's infrastructure
- Central servers: exfiltration domain names

URL PATTERNS
- Credentials exfiltration: `POST <phishing-domain>/<folder>/assets/php/endpoints/accounts.php`

MAIN STEPS

HTML page loading a JavaScript (optional)	Initial domain
• HTML page containing a base64-encoded JavaScript fetching and executing an external JavaScript code	
HTML loading fake Microsoft authentication pages	Phishing domain
• JavaScript performing AES decryption of a base64-encoded HTML • JavaScript downloading additional code • HTML document displaying fake authentication pages	
Fake Microsoft authentication page	Exfiltration domain
• AES-encrypted HTML • HTML code of the fake authentication pages • JavaScript code implementing authentication steps	
Victim IP address	api.ipify[.]org or ipapi[.]co
• Gather the victim IP address using an external service	
Exfiltration	Exfiltration domain, Phishing domain
• Send harvested data	
Redirection	Microsoft domain
• Redirection to another URL set in the JavaScript file	

AUTHENTICATION WITH MICROSOFT SERVICES

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

TOP ASNS

AS174

OTHER CHARACTERISTICS
- Use of landing pages impersonating Sharepoint, and possibly other Microsoft services, in addition to the fake Microsoft authentication page
- Credentials exfiltrated twice: to the operator's central exfiltration domain that implements the AiTM capability, as well as to the affiliate-controlled phishing domain

INDICATORS IN CODE
- Custom Cloudflare Turnstile page and HTML loader containing:
  - CSS comment `/* Your CSS styles */` and car-related HTML comments
  - Characteristic strings, *e.g.* variable `usuuid`, functions `decstr`, `querulous` and `sendMouseData`
- AES-encryption using variables `a`, `b` and `c`, and the JavaScript library `crypto-js.min.js`
- Exfiltration of harvested data using the field `do` (values: `GURI`, `check`, `le`, `ver`, `cV`), `em`, `psk`, and others

TRAC Labs [AiTM Phishing, Hold the Gabagool: Analyzing the Gabagool Phishing Kit] Nov 2024