Evilginx - ywnjb

PREVALENCE	IMPLEMENTATION
Medium	Reverse proxy

ALIASES

LICENSING Open source
TARGET Microsoft 365
FIRST SEEN December 2022

CONTEXT

- Open-source AitM phishing kit maintained by *kgretzky*, available on GitHub since 2017
- Configuration file (phishlet) required for the phishing kit, most attackers use a variant of the phishlet named "o365" with the configured subdomain "YWNjb" to harvest Microsoft 365 credentials. This phishlet was first observed in December 2022.

ANTI-BOT PAGES

Not provided by Evilginx
Custom pages used by attackers

INFRASTRUCTURE

Clustering:

- Phishing clusters based on the subdomains used by the kit, which depend on the phishlet (configuration)
- Main phishing cluster "YWNjb" uses the characteristic subdomain "YWNjb"

URL PATTERNS

Identical to Microsoft ones, but using a malicious domain names, *e.g.*:

- `<phishing-domain>/common/oauth2/v2.0/authorize`
- `<phishing-domain>/common/GetCredentialType`
- `<phishing-domain>/common/SAS/BeginAuth`

MAIN STEPS (FOR YWNJB PHISHLETS)

Fake Microsoft authentication page	Phishing subdomain "office." or "login."
• HTML page containing the fake Microsoft authentication page and obfuscated heavy JavaScript code	
Script handling authentication steps	Phishing subdomain "ywnjb."
• Legitimate Microsoft code injected with the phishing subdomain	
Exfiltration	Phishing subdomain "office." or "login."
• Phishing server operating as a reverse proxy, relaying all requests to Microsoft API	
Redirection	Microsoft domain
• Redirection to a Microsoft URL using the HTTP Location header from the request to the subdomain "react."	

AUTHENTICATION WITH MICROSOFT SERVICES

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

TOP ASNS

AS16509
AS14061
AS22612
AS47583
AS14956

OTHER CHARACTERISTICS

Unwanted traffic (incorrect path, or else) redirecting to Rick Astley song on YouTube

INDICATORS IN CODE

Malicious URLs included in legitimate Microsoft code

Kuba Gretzky	*evilginx2* repository on GitHub	Jul 2018
Microsoft	From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fr…	Jul 2022