Facebook ads used to steal 615000+ credentials in a phishing campaign

Cybercriminals are abusing Facebook ads in a large-scale phishing scam aimed at stealing victims' login credentials.

Researchers from security firm ThreatNix spotted a new large-scale campaign abusing Facebook ads. Threat actors are using Facebook ads to redirect users to Github accounts hosting phishing pages used to steal victims' login credentials.

The campaign targeted more than 615,000 users in multiple countries including Egypt, the Philippines, Pakistan, and Nepal.

The landing pages are phishing pages that impersonate legitimate companies. Once the victims provided the credentials, they will be sent to the attackers through a Firestore database and a domain hosted on GoDaddy.

"Our researchers first came across the campaign through a sponsored Facebook post that was offering 3 GB mobile data from Nepal Telecom and redirecting to a phishing site hosted on GitHub pages." reads the post published Threatnix.

Facebook phishing

The campaign appears well orchestrated, threat actors used localized Facebook posts and pages that mimic legitimate organizations and targeted ads for specific countries. The scammers used an intriguing trick to avoid detection, the used shortened URL that initially points to a benign page that is modified after the approval of the ads.

"While Facebook takes measures to make sure that such phishing pages are not approved for ads, in this case the scammers were using Bitly link's which initially must have pointed to a benign page and once the ad was approved, was modified to point to the phishing domain." continues the post.

Attackers behind this campaign used at least 500 Github repositories hosting phishing pages, some of which are already inactive. The first phishing page was created in GitHub 5 months ago.

"Following some digging we were able to gain access to those phished credentials. At the time of writing this post there appears to be more than 615,000+ entries and the list is growing at a rapid pace of more than a 100 entries per minute." concludes the post.

Experts are working with relevant authorities to take down the phishing infrastructure used in this campaign.

In October, Facebook detailed an ad-fraud cyberattack that's been ongoing since 2016, crooks are using a malware tracked as SilentFade (short for "Silently running Facebook Ads with Exploits") to steal Facebook credentials and browser cookies.

The social network giant revealed that malware has a Chinese origin and allowed hackers to siphon $4 million from users' advertising accounts. Threat actors initially compromised Facebook accounts, then used them to steal browser cookies and carry out malicious activities, including the promotion of malicious ads.

References:

- https://securityaffairs.co/wordpress/112882/hacking/facebook-phishing-campaign-2.html?web_view=true
- https://www.google.com/amp/s/techdator.net/facebook-ads-and-github-abused-for-stealing-account-credentials/amp/
- https://latesthackingnews.com/2020/12/30/facebook-ads-phishing-campaign-stole-facebook-credentials-of-615k-users/