Beat: Miscellaneous

Experts: Thailand`s largest internet service provider `compromised`

-, 13.01.2014, 16:11 Time

USPA News - Some customers of True Internet, Thailand`s largest internet service provider, have been served popups with advertisements for months after a hacker allegedly compromised the company`s transparent proxy, potentially allowing hackers to spy on users. Internet service providers (ISPs) in Thailand use transparent proxies to act as an intermediary when customers request access to websites, allowing censorship and the caching of frequently used objects to reduce bandwidth.

The exploit is believed to have affected the transparent proxy used by True Internet since late last year, according to two computer security experts who studied the exploit. "This particular exploit is used to send unsuspecting users to a website with the goal of some of them signing up, allowing the attacker to collect affiliate commissions," said one of the experts, speaking on the condition of anonymity. He said there was no evidence to suggest the exploit was also used for other purposes, but indicated the attacker would have been able to spy on users or manipulate their actions online. "True - and all other ISPs in Thailand - run a transparent proxy. When a user tries to access a website from outside Thailand, the ISP intercepts it, fetches the content if it is not already cached, and then serves it to the user," the expert explained. "In this case, someone figured out how to poison the cache and put in a spoofed JavaScript file in the cache entry for a link that is used by websites to serve ads from Google." The way the exploit works is through a spoofed JavaScript file, sending Internet users to a website that was first created on October 30 and registered with a Panama address and Peru phone number. The site has become the 905th `most-visited` website in Thailand, indicating the exploit affected many web users, according to Alexa.com, which showed 98.8 percent of visitors to the website were from Thailand. The affected file has an expiry date of one year in the future, meaning users will continue seeing popups and redirects for a year unless they clear their temporary Internet files and access a valid version of the JavaScript file. Jacob Fish, who also studied the issue, said it appeared the exploit was being turned on at certain times, possibly to avoid detection. "When you have the power of loading spoofed JavaScript files for any website, you can show users popups, send them to other websites or modify a website to display other advertisements," one of the experts said. "Although we have not seen it in this case, the attacker could have exploited the same method to monitor a user`s Internet activity, hijack a session after a user logged in to a website, and submit forms." Postings on various Internet forums showed True users complaining about the popups as early as October, with some of them reporting the issue was resolved after deleting their temporary Internet files. True Internet did not immediately return requests for comment on this story.

Article online:
https://www.uspa24.com/bericht-1781/experts-thailands-largest-internet-service-provider-compromised.html

Editorial office and responsibility:
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement):

Editorial program service of General News Agency:
UPA United Press Agency LTD
483 Green Lanes
UK, London N13NV 4BS
contact (at) unitedpressagency.com

Official Federal Reg. No. 7442619