

New automated attack that can break Google reCAPTCHA system

Written by bad_brain

Thursday, 14 April 2016 21:04 -

A group of security researchers has created a new automated attack that can break the CAPTCHA systems hired by Google and Facebook. The result of this experiment were better than they expected.

According to researchers result on Google's reCAPTCHA system, the result was 70.78% success rate over 2,235 CAPTCHA's and the CAPTCHA solving time was 19.2 seconds. On Facebook's CAPTCHA system, the result was 83.5% success rate over 200 CAPTCHAs.

The attackers can rent CAPTCHA-breaking systems that solves CAPTCHA with the use of a human. Any hacker can start their own CAPTCHA-busting business, the whole system would cost around \$110/day with one IP address only, which will solve nearly 63,000 CAPTCHAs in 24 hours from one IP address without being banned or getting detected.

Facebook CAPTCHA system was easy to solve compared to Google CAPTCHA, as Facebook CAPTCHA system use images with higher resolution and Google use low-quality photos, which makes the system harder to solve the CAPTCHAs.

According to researcher said that, "Our completely offline captcha-breaking system is comparable to a professional solving service in both accuracy and attack duration, with the added benefit of not incurring any cost on the attacker."

Before posting their result to the public, the three expert researchers Suphanee Sivakorn, Jason Polakis, and Angelos D. Keromytis, contacted Google and Facebook to submit their result. Google made some changes to harden reCAPTCHA, but Facebook has no replied.

The whitepaper can be downloaded [here](#).