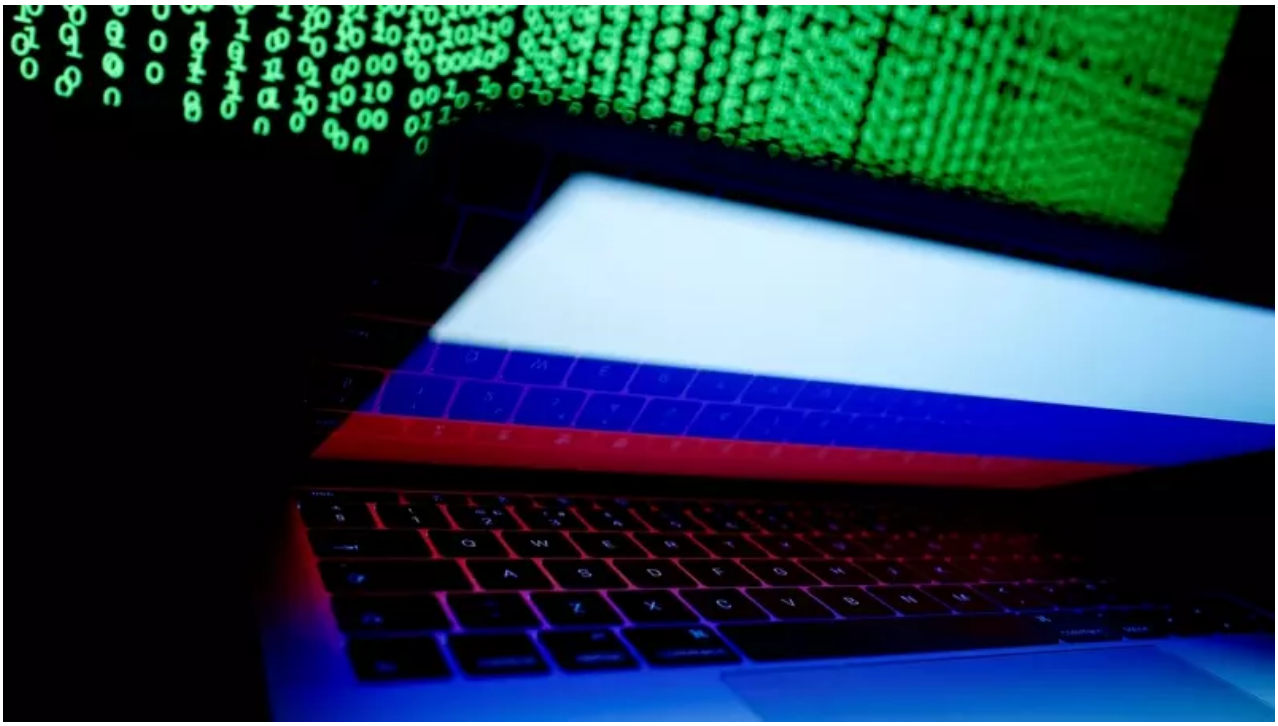
Na české banky útočili proruští hackeři. K útokům verbují za úplatu kohokoliv

novinky.cz/clanek/internet-a-pc-bezpecnost-na-ceske-banky-utocili-prorusti-hackeri-k-utokum-verbuji-za-uplatu-kohokoliv-40442064

Miloslav Fišer



Hackerská skupina NoName057(16) je aktivní již od března loňského roku, bezpečnostní experti dávají její vznik do souvislosti s válkou na Ukrajině. Proruští hackeři totiž vedou útoky typu DDoS proti zemím, které Ukrajinu podporují opakovaně.

„Proruská skupina NoName057(16) útočila na Českou republiku už mnohokrát. Snažila se například ovlivnit české prezidentské volby a napadala i společnosti z výrobního sektoru nebo banky. Nová vlna útoků se zaměřila znovu právě na banky," prohlásil Miloslav Lujka, bezpečnostní expert Check Pointu.

Zdůraznil přitom, že kromě bank byl středeční útok směřován na pražskou burzu cenných papírů. V minulosti útočila skupina NoName057(16) také na cíle v Polsku, Lotyšsku a Litvě.

Pět bank postihly technické problémy s přihlašováním do bankovnictví

Útok DDoS (Distributed Denial of Service) má vždy stejný scénář. Stovky tisíc počítačů – v některých případech klidně i miliony – začnou přistupovat v jeden okamžik na konkrétní server. Ten zpravidla nezvládne tak vysoké množství požadavků zpracovat a spadne. Pro běžné uživatele se pak takto napadená webová stránka tváří jako nedostupná.

„DDoS útoky mají sice dopad na uživatele, kteří se na stránku nebo službu nemohou dostat, ale nejedná se o sofistikovaný útok. Může jej provést kdokoli s dostatečnou výpočetní silou. K podobným útokům si lze často pronajmout nějaký výkonný botnet. Například ruská hackerská skupina Killnet ovládá jeden z největších aktivních botnetů složený ze 4,5 milionu infikovaných zařízení," konstatoval Lujka.

Odměna až 25 000 Kč za útok

Bezpečnostní experti již dříve upozornili, že podobné útoky jsou i finančně motivované. Skupina dává různé finanční pobídky, aby nalákala další členy k zapojení do útočných operací. „Někteří uživatelé ze zemí, jako je Kanada a Německo, se chtěli připojit k hackerské skupině NoName(057)16 a pokusili se stáhnout spustitelný soubor DDosia, jehož prostřednictvím by mohli provádět DDoS útoky," varoval Martin Chlumecký, analytik malwaru z Avast Threat Labs.

„Tento soubor je dostupný pouze ověřeným členům příslušné skupiny na Telegramu a někteří uživatelé Avastu jej aktivně zařadili na seznam výjimek v antiviru. Ten tak soubor neoznačí jako malware, a lze jej tudíž spustit," popsal Chlumecký aktuální praxi.

I bez větších technických znalostí si za každý úspěšný DDoS útok mohou podle analýzy Avastu členové hackerské skupiny přijít až na 80 000 rublů, tedy 25 000 korun v kryptoměnách. Získané peníze se dělí mezi členy. Útočníci tak milionové částky vydělávají doslova korunku po koruně, respektive v tomto konkrétním případě rubl po rublu.

„Motivace se tak mění z politické na finanční. Skupina NoName(057)16 používá tuto finanční pobídku, aby zvýšila svou úspěšnost a vybudovala si tak jméno v hackerské komunitě. Politická motivace může pro mnohé hrát pouze druhotnou roli jak u vedoucích projektů, tak i mezi hackery-dobrovolníky," zamyslel se Chlumecký.

Česko mohou ochromit DDoS útoky, varoval NÚKIB