Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

BRNO • 1. LISTOPADU 2022
ANALÝZA HROZBY

UPOZORNĚNÍ NA ZVÝŠENÉ RIZIKO DDOS ÚTOKŮ PROTI ČESKÝM SUBJEKTŮM V KONTEXTU GEOPOLITICKÉ SITUACE A INCIDENTŮ PROBĚHLÝCH V POSLEDNÍM MĚSÍCI

SHRNUTÍ

- **KONTEXT: Dané upozornění je distribuováno v návaznosti na nedávno proběhlé či stále probíhající geopolitické události a s nimi spojené riziko kyberútoků typu Distributed Denial of Service (DDoS). Možným spouštěčem je v tuzemském případě hlavně společné zasedání vlád ČR a Ukrajiny, jež se uskutečnilo dne 31. října 2022 v Kyjevě. Během zasedání se dle mediálních výstupů diskutovala témata, která mohou být aktéry s nepřátelskými úmysly považována jako provokativní.**
- **PROBĚHLÉ ÚTOKY: NÚKIB na základě interních dat registruje během října neobvykle vysoký počet DDoS útoků (celkem 13 incidentů). Jejich počet téměř dorovnal souhrnné hodnoty za prvních devět měsíců letošního roku. K části říjnových útoků se na svém telegramovém kanále přihlásila skupina Anonymous Russia. Zvýšený počet útoků byl evidován také letos v dubnu, kdy se české organizace staly obětí útoků ruskojazyčné skupiny Killnet.**
- **SITUACE V ZAHRANIČÍ: V minulém týdnu proběhly DDoS útoky také v Polsku, ještě o týden dříve pak v Bulharsku. Horní komora polského parlamentu se stala obětí útoku po schválení rezoluce označující Rusko za teroristický stát.**
- **HACKTIVISMUS PRORUSKÝCH SKUPIN: V návaznosti na politická rozhodnutí států EU/NATO již od začátku ruské invaze na Ukrajinu evidujeme DDoS útoky ruskojazyčných hacktivistů. Většinou tyto aktivity reagují na kroky, které jsou považovány za „proukrajinské“ (např. oznámení oprav ukrajinské těžké techniky v ČR). Podle dostupných informací nelze vyhodnotit, zda a případně nakolik jsou dané skupiny zaštítěné státem.**
- **MITIGACE / DETEKCE: Využít lze primárně doporučení z varování ze dne 25. února 2022. Ta se týkají přímo hrozby DDoS útoků. Opatření zmíněná v tomto varování v bodech 3.1 a 3.2 jsou použitelná jakoukoliv organizací, na rozdíl od bodů 3.3 a 3.4, které jsou určeny specificky poskytovatelům internetového připojení.**
- **ZHODNOCENÍ: DDoS útoky obvykle nemají dlouhodobý dopad a primárně znamenají krátkodobý výpadek webových stránek či navazujících služeb. Přesto může dojít k dočasným výpadkům, a to včetně kritických služeb (např. portály veřejné správy či finanční služby). Na základě extrapolace trendu a v kontextu nynější situace NÚKIB vyhodnocuje, že existuje zvýšené riziko DDoS útoků vůči českým subjektům. Doporučujeme ostražitost a implementaci příslušných mitigací.**

UPOZORNĚNÍ: Předložené informace vycházejí z otevřených informací, interních dat NÚKIB nebo od jeho partnerských organizací.