Opakující se DDoS útoky na české instituce

portal.neweb.govcert.cz/informacni-servis/informace/upozorneni-a-hrozby/opakujici-se-ddos-utoky-na-ceske-instituce

Upozorňujeme na opakující se DDoS útoky na české instituce. Za těmito útoky opět stojí ruská hacktivistická skupina NoName057(16), která dle dění ve světě reaguje těmito útoky.

NÚKIB od patrnerů získává v reálném čase seznam domén, na které je prováděn DDoS a proaktivně napadané organizace v případě DDoS útoku kontaktuje.

V případě zasažení DDoS útokem doporučujeme:

- Blokování na základě HTTP hlavičky `User-Agent`: `Go-http-client/1.1`, `Go-http-client/2.0` a prázdného user agenta – touto blokací může dojít k omezení určitých aplikací vytvořených v programovacím jazyce Go
- Blokování provozu z určitých ASN: 199785, 63949, 174, 262287, 212238, 9009, 60068, 39493
- V krajní případ geofencing – blokování komunikace ze zahraničí
- Využít starší doporučení uvedené ve Varování ze dne 25. 2. 2022

Dalším krokem by mělo být kontaktování ISP, který pomůže mitigovat útoky. Častý typ DDoS útoků bývá HTTP flood, SYN flood a zřídka Slowloris.

Od deklarace cílů trvají útoky přibližně 24 hodin.

Obecně nedoporučujeme veřejně zmiňovat aktéry, kteří za tímto útokem stojí. Na svém kanále pak sdílejí své „úspěchy“ a jsou motivováni pokračovat ve svých útocích. Zároveň se jedná o podporu informační války.

V případě otázek se na nás neváhejte obrátit na e-mailové adrese cert@nukib.cz.

Klasifikace

TLP:AMBER

Autor

Národní úřad pro kybernetickou a informační bezpečnost

Datum

24. 10. 2023

Reakce

Zatím žádné reakce na článek