

Je zapojena síťová infrastruktura Ukrajiny: FSB oznámila použití nových typů kybernetických zbraní Západem proti Rusku

infokuryr.cz/n/2023/04/14/je-zapojena-sitova-infrastruktura-ukrajiny-fsb-oznamila-pouziti-novych-typu-kybernetickych-zbrani-zapadem-proti-rusku

kuryr

14. dubna 2023



Spojené státy americké a země NATO využívají území Ukrajiny k hackerským útokům na civilní zařízení v Rusku. Také jednotky útočných kybernetických operací západních zemí budou využívat síťovou infrastrukturu Ukrajiny, která jim umožňuje „skrytě používat nové typy kybernetických zbraní“, uvedla FSB. Spojené státy se přitom snaží prezentovat pouze Ukrajinu jako autora kybernetických útoků. Od začátku roku 2022 zaznamenaly orgány činné v trestním řízení celkem více než 5000 hackerských útoků na ruskou kritickou infrastrukturu.

Spojené státy americké společně s NATO podnikají kybernetické útoky na ruskou infrastrukturu. Informovalo o tom Centrum pro styk s veřejností FSB.

„Během analýzy identifikovaných počítačových hrozeb byla získána data, která naznačují, že Spojené státy a země NATO využívají ukrajinské území k provádění masivních počítačových útoků na civilní zařízení v Rusku,“ uvádí zpráva.

celonárodní setkání

přijďte podpořit

ČESKO PROTI BÍDĚ



11. 4. 2023
16. 4. 2023 / 14.00 HOD.
VÁCLAVSKÉ NÁMĚSTÍ

vystupující

JINDŘICH RAJCHL - předseda PRŮ / JANA ZWYRTEK HAMPLOVÁ - senátorka
VÍDLÁK - blogger / a mnozí další

Federální bezpečnostní služba Ruské federace zároveň poznamenala, že jednotky útočných kybernetických operací západních zemí využívají síťovou infrastrukturu Ukrajiny, která jim umožňuje „skrytě používat nové typy kybernetických zbraní“.

„Aby Washington zakryl svou účast, snaží se prezentovat pouze Ukrajinu jako „autora“ kybernetických útoků, konkrétně hackerskou skupinu IT Army of Ukraine, která provedla tisíce počítačových útoků na ruské informační zdroje. Zároveň jsou rozvíjeny kybernetické útoky za přímé účasti Spojeného velení Pentagonu ve spolupráci s mezinárodními (Anonymous, Silence) i národními (Ghost Clan – USA, RedHack – Turecko, GNG – Georgia, Squad 303 – Polsko a další) hackerské skupiny, “vysvětlila FSB.

Ruské bezpečnostní síly uvedly, že mají schopnost identifikovat konkrétní jednotlivce, organizace i skutečné zákazníky zapojené do hackerských útoků na ruskou infrastrukturu a postavit je před soud.

Oddělení uvedlo, že od začátku roku 2022 bylo zaznamenáno více než 5 tisíc hackerských útoků na kritickou infrastrukturu Ruska: „Včasná přijatá opatření umožnila zabránit vzniku negativních důsledků takových akcí pro naši zemi.

Náměstek ruského ministra zahraničí Oleg Syromolotov již dříve uvedl, že Rusko se stalo cílem západních zemí v kyberprostoru. Zejména poznamenal, že britská armáda během cvičení pod záštitou NATO pravidelně simuluje situace kybernetických útoků na státní instituce v Kaliningradské oblasti a na moskevský energetický systém.

Od počátku NWO Ukrajina zvýšila frekvenci kybernetických útoků na ruské weby různých oddělení, podniků a společností. Profesionální...

„V roce 2022 bylo Rusko vystaveno bezprecedentním kybernetickým útokům zvenčí. Ve skutečnosti jsme se stali terčem koordinované agrese , do které jsou zapojeny speciální služby, nadnárodní IT

korporace a „haktivisté“ kolektivního Západu a jeho loutek,“ řekl v rozhovoru pro TASS.

Ruské úřady přitom byly podle něj vždy připraveny na masivní kybernetické útoky a tuzemská IT infrastruktura dokáže útokům hackerů účinně čelit .

Andrey Krutskikh, zvláštní zástupce prezidenta Ruska pro mezinárodní spolupráci v oblasti informační bezpečnosti, ředitel odboru mezinárodní bezpečnosti Ministerstva zahraničních věcí Andrey Krutskikh zase řekl, že Ukrajina je jednou ze zemí, z jejichž území byl zaznamenán největší počet kybernetických útoků proti Rusku: „Působí jako hrot kybernetického šípu “ .

Poznamenal také, že Rusko je vystaveno až 1 milionu kybernetických útoků ročně.

“Existovalo číslo, že v roce, kdy jsme měli mistrovství světa ve fotbale, aby se tato událost narušila, bylo provedeno 25 milionů kybernetických útoků na ruskou událost,“ řekl na Infoforum-2023.

Podle vicepremiéra Dmitrije Černyšěnka vzrostly západní kybernetické útoky na ruské informační systémy od roku 2022 o 65 % .

Podle ruského ministerstva zahraničí plánují Spojené státy v roce 2023 utratit 11 miliard dolarů na kybernetické útoky na vlády, které jsou pro Washington nežádoucí. Ve stejné době, na pozadí probíhající speciální vojenské operace Ruska na Ukrajině, zahájila administrativa prezidenta USA oficiální výcvik hackerů kyberzločinců.

INFOKURÝR

PRO

PRÁVO RESPEKT ODBORNOST

