Ivan Štubňa: OVLIVNÍ CIA - MISTR SVĚTOVÝCH KYBERÚTOKŮ - PŘEDČASNÉ VOLBY V ČR?

cz24.news/ivan-stubna-ovplyvni-cia-majster-svetovych-kyberutokov-predcasne-volby-v-sr

29. června 2023

Stáhnout PDF

Sledujte nás na Telegramu: @cz24news

USA/SLOVENSKO: CIA se podílela na svržení nebo pokusu o svržení více než 50 zákonných vlád jiných zemí – prostřednictvím kyberútoků, což způsobilo nepokoje v příslušných zemích.

V květnu tr byla zveřejněna zpráva o vyšetřování CIA, která odhaluje „impérium amerických hackerů“ a jejich podíl na organizaci převratů po celém světě.

CIA po dlouhou dobu tajně organizovala „barevné revoluce“ a nepřetržitě vykonávala špionážní aktivity, uvádí se ve zprávě čínského Národního centra pro nouzovou reakci na počítačové viry a internetové bezpečnostní společnosti. Rychlý rozvoj internetu v tomto století přinesl CIA nové příležitosti k provádění jejích infiltrací, rozvracení států a zinscenování politických problémů.

Zpráva odhalila důležité podrobnosti o zbraních, které CIA použila pro kybernetické útoky a podrobnosti o konkrétních případech v oblasti kybernetické bezpečnosti, k nimž došlo v Číně a jiných zemích včetně špionáže. Zpráva uvedla, že jejím cílem bylo poskytnout informace pro oběti kybernetických útoků na celém světě.

Po „Arabském jaru“ (2011) v západní Asii a severní Africe se některé velké nadnárodní internetové společnosti ve Spojených státech zapojily do posílání množství personálu, materiálních a finančních zdrojů konfliktním stranám, podporovaly opoziční strany a veřejně zpochybňovaly zákonné vlády cizích zemí, které nepracovaly pro

zájmy USA. Takové firmy se také podílely na pomoci při dezinformační kampani a rozdmýchávání ohně protestů mezi veřejností.

Zpráva dále citovala několik opatření takových operací, včetně technologie „The Onion Router (TOR)“, která umožňuje anonymní komunikaci, vyvinutou americkou společností s americkým vojenským zázemím. TOR byla bezplatně poskytnuta protivládním pracovníkům v zemích jako Írán, Tunisko a Egypt, aby jim pomohla vyhnout se dohledu ze strany legálních vlád.

Google a Twitter také vyvinuly speciální službu s názvem „Speak2Tweet“, která uživatelům umožňuje komunikovat, když jsou odpojeni od internetu. Tuto technologii používaly protivládní síly v Tunisku a Egyptě, uvádí se ve zprávě. Americká společnost Rand Corporation pracující především pro Pentagon vyvinula technologii, která usnadňuje řízení protestů bez možnosti zjištění kanálů komunikace. Existují i další americké společnosti, které vyvíjely software, umožňující nezávislý širokopásmový přístup, aby se vyhnuli vládnímu monitorování.

V roce 2020 čínská společnost 360 pro kybernetickou bezpečnost odhalila neznámou útočnou organizaci s číslem APT-C-39, která prováděla kybernetické útoky specificky zaměřené na Čínu a její mezinárodní přátele. Zjistilo se, že organizace použila „zbraně“ jako Athena, Fluxwire, Grasshopper, AfterMidnight, HIVE a ChimayRed – všechny spojené s takzvaným únikem Vault 7 – k uskutečnění kybernetických útoků zaměřených na Čínu a další země. Příslušné útoky lze zdokumentovat již od roku 2011.

CIA masivně využívala zranitelnost zero-day ve svých globálních kybernetických útocích, zakládala „zombie botnety“ a „odrazové můstky“ po celém světě k zahájení útoků na síťové servery, síťové terminály, výměníky a směrovače, jakož i obrovské množství průmyslových řídicích zařízení. Čínský technický tým získal vzorek nástroje pro zachycování informací, který výhradně používá

americká Národní bezpečnostní agentura (NSA), což naznačuje, že CIA a NSA mohou společně útočit na stejný cíl, sdílet navzájem útočné kyberzbraně nebo poskytovat technologickou nebo personální pomoc.
Hegemonie kyberprostoru pod americkou manipulací zastiňuje celý svět, přičemž CIA celosvětově spouští automatizované, systematické a inteligentní útoky, uvádí se ve zprávě.

Po analýze relevantních případů technický tým zjistil, že dosah takových útočných kyberzbraní pokryl téměř všechny prostředky internetu, čímž se síť cizí země a důležité a citlivé informace staly náchylné ke kontrole nebo špionáži ze strany USA. Není pochyb, že Spojené státy americké jsou skutečným „impériem hackerů“, kteří útočí všude tam, kde je to pro tzv. „hackery“. zájmy USA nezbytné. Nedělejme si proto iluze, že Slovensko se vyhne pozornosti USA. S nastávajícími volbami budou americké kyberútoky proti SR eskalovat tak, aby se zajistilo vítězství Sorosových progresivních liberálů. Samozřejmě slovenské bezpečnostní síly budou těmto aktivitám pouze nečinně přihlížet a je předpoklad, že je budou jen monitorovat. Nebo prostě dostanou příkaz, aby se do toho nemíchali.

A na závěr jedna perlička. Jistě jste již zaregistrovali, že politicko-ekonomický terorista George Soros udělal oficiálně ze svého mladšího syna Alexe Sorose svého nástupce. Alex jako nováček si nedal pozor na ústa, když vyjádřil obavy, že bývalý prezident Donald Trump se vrátí do Bílého domu a naznačil, že Sorosova organizace bude hrát klíčovou finanční roli v prezidentských volbách v roce 2024. Doslova řekl: „Jakkoli bych rád dostal peníze z politiky, pokud to však bude dělat druhá strana, budeme to muset dělat i my.“

AUTOR: Ivan Štubňa

ZDROJ

Upozornění: Tento článek je výlučně názorem jeho autora. Články, příspěvky a komentáře pod příspěvky se nemusí shodovat s postoji redakce cz24.news. Medicínské a lékařské texty, názory a studie v žádném případě nemají nahradit konzultace a vyšetření lékaři ve zdravotnickém zařízení nebo jinými odborníky.