NÚKIB a české zpravodajské služby spolu s NSA a FBI upozorňují na ruskou kybernetickou kampaň proti subjektům podporujícím Ukrajinu

21.5.2025 - | Národní úřad pro kybernetickou a informační bezpečnost

Za kampaní stojí jednotka ruské vojenské rozvědky GRU č. 26165, známá pod označením APT28 (též Fancy Bear, Forrest Blizzard aj.). Tato skupina již více než dva roky vede špionážní operace proti subjektům z obranného a dopravního sektoru, zahrnující leteckou, námořní a železniční dopravu. Zasahují také vládní instituce a komerční společnosti v členských státech NATO, na Ukrajině i v sousedních zemích.

Útočníci využívají známé taktiky jako password spraying, cílené phishingové e-maily, změny nastavení e-mailových schránek v prostředí Microsoft Exchange a zneužívání zranitelností v softwaru, jako je Outlook (NTLM) nebo WinRAR. Získávají tak přístup do systémů, kde následně instalují malware sloužící k udržení přítomnosti a odcizování dat.

Jednotka 26165 rovněž aktivně monitorovala přepravu pomoci na Ukrajinu prostřednictvím přístupu k IP kamerám umístěným na hraničních přechodech, železničních uzlech a dalších strategických bodech. V rámci sledované kampaně se zaměřili především na IP kamery využívající protokol RTSP, přičemž použili veřejně známé výchozí přihlašovací údaje nebo techniky brute force pro prolomení přístupu. Získaná data zahrnovala statické snímky a metadata z kamer. Z analýzy více než 10 000 cílených kamer vyplývá, že většina z nich (81 %) se nacházela na Ukrajině. Další se vyskytovaly v Rumunsku, Polsku, Maďarsku a na Slovensku.

Aktéři GRU se dále zaměřovali na jednotlivce odpovědné za koordinaci dopravy a společnosti spolupracující s napadenými organizacemi. Zneužívali důvěryhodné obchodní vztahy k dalšímu šíření v cílových sítích. Identifikovali také subjekty zapojené do výroby komponent pro systémy průmyslového řízení (ICS), které se používají např. v železniční dopravě.

Ve zprávě upozorňujeme, že tyto aktivity budou pravděpodobně pokračovat. Technologické a logistické společnosti, stejně jako organizace v oblasti dopravy, by proto měly posílit monitorování, aktivně vyhledávat známky kompromitace (threat hunting) a zavést odpovídající ochranná opatření proti těmto sofistikovaným hrozbám. Indikátory kompromitace a taktiky a techniky útočníků naleznete v plném znění dokumentu zde.

https://nukib.gov.cz/cs/infoservis/aktuality/2253-nukib-a-ceske-zpravodajske-sluzby-spolu-s-nsa-a-fbi-upozornuji-na-ruskou-kybernetickou-kampan-proti-subjektum-podporujicim-ukrajinu