Obrovský úspěch na mezinárodní úrovni. Bezpečnostní informační služba společně s NSA, FBI a dalšími organizacemi popsala ruskou kyberšpionáž.

28.5.2025 - Ladislav Šticha | Bezpečnostní informační služba

Bezpečnostní informační služba (BIS) se podílela na analýze a popsání více než dva roky trvajících špionážních aktivit ruské tajné služby GRU. BIS se konkrétně v rámci mezinárodní spolupráce koordinované americkou NSA podílela na přípravě technické analýzy, takzvaného Joint Cyber Security Advisory (JCSA) popisující techniky a taktiky, které ruský kybernetický aktér APT28 (jednotka 26165 GRU) využil při útocích v letech 2022 až 2024. Část škodlivých aktivit ruské APT28 popsaných v JCSA se týkala i České republiky. Na přípravě zprávy JCSA se podílely v ČR ještě Národní úřad pro kybernetickou a informační bezpečnost a Vojenské zpravodajství a další bezpečnostní organizace z USA, Velké Británie, Německa a dalších zemí.

GRU vedla více než dva roky špionážní operace proti subjektům z obranného a dopravního sektoru, zahrnující leteckou, námořní a železniční dopravu. Aktivity zasahovaly také vládní instituce a soukromé firmy v členských státech NATO, na Ukrajině a v dalších státech. Jednalo se například o phishingové útoky na e-mailové schránky v prostředí Microsoft Exchange a zneužívání zranitelností v softwaru, jako je Microsoft Outlook nebo WinRAR.

Jednotka GRU 26165 také prolomila přístup k IP kamerám, aby mohla aktivně monitorovat provoz na hraničních přechodech, železničních uzlech a dalších strategických bodech. Získaná data zahrnovala statické snímky a metadata z kamer.

Analýza více než 10 000 bezpečnostních kamer ukázala, že většina z nich (81 %) se nacházela na Ukrajině, další v Rumunsku, Polsku, Maďarsku a na Slovensku. V ČR nebyla kompromitace IP kamer zjištěna.

Zpráva JCSA upozorňuje mimo jiné, že popsané aktivity budou zřejmě pokračovat. Technologické a logistické společnosti, stejně jako organizace v oblasti dopravy, by proto měly posílit monitorování, aktivně vyhledávat známky kompromitace (provádět threat hunting) a zavést účinná ochranná opatření proti těmto sofistikovaným hrozbám. Informační podporu jim nabízí 33 stran dnes vydané zprávy.