Mezinárodní operace TALPA

24.10.2023 - Ondřej Moravčík | Policie ČR

Úspěšný zátah proti tvůrcům známého ransomware Ragnar Locker.

Minulý týden se příslušníci Národní centrály proti terorismu, extremismu a kybernetické kriminalitě služby kriminální policie a vyšetřování Policie České republiky (NCTEKK) podíleli na završení několikaleté mezinárodně koordinované operace proti tvůrcům známého ransomware Ragnar Locker. Operace TALPA, proběhla ve spolupráci s jednotkami Francie, Itálie, Japonska, Lotyšska, Nizozemí, Španělska, Švédska, Ukrajiny a USA a byla aktivně podporována Europolem a Interpolem.

Ransomware Ragnar Locker se prvně objevil v prosinci 2019. Tato skupina byla zodpovědná za řadu významných útoků na kritickou infrastrukturu po celém světě, např. i vůči nemocnicím (skupina neútočila na cíle v České republice). Organizovaná kriminální skupina, která tímto způsobem útočila, využívala tzv. dvojího vydírání – požadovala zaplacení výkupného za odblokování systému a zároveň i za nezveřejnění ukradených dat. Hlavní pachatel, který pobýval i v ČR, byl zadržen v Paříži. Na základě evropského vyšetřovacího příkazu byla provedena domovní prohlídka v místě jeho pobytu v Praze. Tento případ je ukázkou fungující zahraniční spolupráce nejen napříč Evropou.

V rámci akce provedené mezi 16. a 20. říjnem byly provedeny domovní prohlídky a prohlídky jiných prostor v Česku, Španělsku a Lotyšsku. Hlavní tvůrce tohoto škodlivého kmene ransomwaru byl 16. října zatčen v Paříži ve Francii a v Praze byla provedena domovní prohlídka jeho bydliště. V následujících dnech bylo ve Španělsku a Lotyšsku vyslechnuto pět podezřelých. Na konci akčního týdne byl hlavní pachatel, podezřelý z toho, že je vývojářem skupiny Ragnar, předveden před vyšetřující soudce pařížského soudního dvora.

Infrastruktura ransomwaru byla zabavena také v Nizozemsku, Německu a Švédsku, kde byla také zrušena související webová stránka pro prezentaci odcizených dat na serveru Tor.

Tato mezinárodní operace následovala po komplexním vyšetřování vedeném francouzským národním četnictvem spolu s orgány činnými v trestním řízení z Česka, Německa, Itálie, Japonska, Lotyšska, Nizozemska, Španělska, Švédska, Ukrajiny a Spojených států amerických.

Jaký druh malwaru je Ragnar Locker?

Ragnar Locker, který je aktivní od prosince 2019, je název kmene ransomwaru a zločinecké skupiny, která jej vyvinula a provozuje. Tento škodlivý aktér se proslavil útoky na kritickou infrastrukturu po celém světě, naposledy se přihlásil k útokům na portugalského národního dopravce a nemocnici v Izraeli. Tento kmen ransomwaru se zaměřoval na zařízení s operačním systémem Microsoft Windows a k získání přístupu do systému obvykle využíval odhalené služby, jako je Remote Desktop Protocol. Skupina Ragnar Locker byla známá tím, že používala dvojí vyděračskou taktiku, kdy požadovala vyděračské platby za dešifrovací nástroje a také za nevydání ukradených citlivých dat. Úroveň ohrožení skupiny Ragnar Locker byla považována za vysokou vzhledem k tomu, že skupina měla sklon útočit na kritickou infrastrukturu.

Již v říjnu 2021 byli na Ukrajinu vysláni vyšetřovatelé z francouzského četnictva a americké FBI spolu se specialisty z Europolu a INTERPOLu, aby společně s ukrajinskou národní policií provedli vyšetřovací opatření, která vedla k zatčení dvou významných provozovatelů programu Ragnar Locker. Od té doby vyšetřování pokračovalo a tento týden vedlo k vlně zatčení a dalších procesních úkonů.

Toto vyšetřování opět ukazuje, že mezinárodní spolupráce je klíčem k likvidaci organizovaných zločineckých skupin útočících páchajících útoky proti kritické informační infrastruktuře prostřednictvím ransomware.

Více informací naleznete pod tímto linkem:

https://www.europol.europa.eu/media-press/newsroom/news/ragnar-locker-ransomware-gang-taken-down-international-police-swoop

https://www.policie.cz/clanek/mezinarodni-operace-talpa.aspx