Operace SECURE: Kaspersky pomáhá INTERPOLu chránit data uživatelů

20.6.2025 - | PROTEXT

Infostealer je typ malwaru, který je navržen tak, aby extrahoval cenná uživatelská data, včetně finančních informací, přihlašovacích údajů nebo souborů cookie. Získaná data se ukládají do záznamových souborů a kyberzločinci je poté distribuují v rámci undergroundové komunity dark webu. Podle údajů týmu Kaspersky Digital Footprint Intelligence bylo v letech 2023–2024 infikováno různými typy infostealerů téměř 26 milionů zařízení se systémem Windows. V průměru každá čtrnáctá infekce infostealerem vede ke krádeži informací o kreditní kartě.

Záměrem operace, která probíhala od ledna 2025 do dubna 2025, bylo přesně určit a narušit škodlivé kybernetické aktivity související s infostealery pomocí lokalizace serverů, mapování fyzických sítí a provádění cíleného odstraňování hrozeb. Operace byla podporována privátními partnery INTERPOLu, mezi něž patří i společnost Kaspersky, kteří sdíleli data o škodlivých infrastrukturách zapojených do ovládání nebo distribuce infostealerů, včetně informací o řídicích (C&C) serverech pro šíření malwaru.

V rámci operace bylo prozkoumáno téměř 70 variant infostealerů a 26.000 souvisejících IP adres a domén, přičemž policisté zabavili přes 40 serverů. Po provedení operace úřady informovaly přes 216.000 zjištěných i potenciálních obětí, aby mohly okamžitě podniknout příslušné nápravné kroky, například změnit hesla, zmrazit účty nebo zablokovat neoprávněný přístup.

Hlavní úspěchy operace SECURE:

• Ve Vietnamu policie zatkla 18 podezřelých a zabavila jim zařízení v jejich domovech a na pracovištích. U vůdce skupiny našla přes 300 milionů VND (11.500 USD) v hotovosti, SIM karty a firemní registrační dokumenty, což naznačuje používání schématu otevírání a prodeje firemních účtů.

• Na Srí Lance a na Nauru provedly úřady domovní razie, při nichž bylo zatčeno 14 osob (12 na Srí Lance a 2 na Nauru) a identifikováno 40 obětí.

• V Hongkongu policie analyzovala přes 1700 zpravodajských informací poskytnutých INTERPOLem a identifikovala 117 C&C serverů hostovaných u 89 poskytovatelů internetových služeb. Tyto servery byly používány kyberzločinci jako centrály pro spouštění a řízení škodlivých kampaní, včetně phishingu, online krádeží peněz a podvodů na sociálních sítích.

„INTERPOL nadále podporuje účinné společné akce proti globálním kybernetickým hrozbám. Operace SECURE opět ukázala sílu sdílení informací při narušování škodlivé infrastruktury a prevenci rozsáhlých škod působených jednotlivcům i firmám,“ říká **Neal Jetton**, ředitel oddělení kybernetické kriminality INTERPOLu.

„Kybernetické hrozby neznají hranice, a proto by je neměla mít ani mezinárodní spolupráce na jejich potlačení. Soukromé společnosti, které bojují jako obránci v první linii, shromažďují data o reálných kybernetických hrozbách a sdílení těchto dat s orgány činnými v trestním řízení pomáhá zastavovat šíření zjištěných hrozeb. Globální kybernetická bezpečnost je sdílenou odpovědností a společnost Kaspersky chválí roli INTERPOLu jako prostředníka při sdružování zúčastněných stran, jejichž

příspěvek je nezbytný pro vytváření bezpečnějšího digitálního světa,“ komentuje **Julija Šlyčkovová**, viceprezidentka pro globální veřejné záležitosti ze společnosti Kaspersky.

Hrozba krádeže informací nabírá v poslední době na síle. Služba Kaspersky Digital Footprint Intelligence neustále monitoruje dark web, aby odhalila ukradené přihlašovací údaje, zvýšila povědomí o nebezpečí a sdílela strategie pro zmírnění souvisejících rizik.

Pokud je zjištěn únik dat způsobený infostealery, je třeba okamžitě podniknout následující kroky:

• Máte-li podezření, že došlo k úniku údajů o vaší bankovní kartě, okamžitě jednejte: sledujte oznámení z banky, zablokujte kartu a nechejte si vystavit novou a změňte heslo k aplikaci nebo webovým stránkám banky. Použijte dvoufaktorové ověřování a další metody kontroly totožnosti. Pokud dojde k úniku údajů o účtu a zůstatku, buďte obzvláště ostražití vůči phishingovým e-mailům, podvodným SMS a hovorům. Kyberzločinci si vás na základě těchto informací mohou vybrat za oběť cílených útoků. Pokud máte pochybnosti, obraťte se přímo na svoji banku.

• Změňte hesla k ohroženým účtům a sledujte podezřelé aktivity spojené s těmito účty.

• Proveďte na všech zařízeních kompletní bezpečnostní kontroly a odstraňte veškerý zjištěný malware.

• Jelikož se infostealery zaměřují na osobní i firemní zařízení, doporučuje se firmám proaktivně monitorovat trhy na dark webu a odhalit napadené účty dříve, než začnou představovat riziko pro zákazníky nebo zaměstnance. Podrobného průvodce pro nastavení monitorování najdete zde.

Zdroj: Kaspersky

https://www.ceskenoviny.cz/tiskove/zpravy/operace-secure-kaspersky-pomaha-interpolu-chranit-data-uzivatelu/2689004