Kaspersky pomáhá INTERPOLu bojovat proti malwaru Grandoreiro

21.3.2024 - | PROTEXT

Grandoreiro je bankovní trojský kůň původem z Brazílie, který byl podle údajů společnosti Kaspersky aktivní nejméně od roku 2016.

Útoky s jeho použitím často začínají specificky zacíleným phishingovým e-mailem napsaným ve španělštině, portugalštině nebo angličtině. Trojan po instalaci do počítače oběti sleduje vstupy z klávesnice, simuluje činnost myši, sdílí obrazovky a shromažďuje údaje, jako jsou uživatelská jména, informace o operačním systému, době provozu zařízení, a především bankovní identifikátory. Zločinci, kteří tak získají plnou kontrolu nad bankovními účty obětí, pak tyto účty vydrancují a posílají finanční prostředky přes zprostředkovatelskou síť, která pere nelegální zisky.

Výskyt mnoha verzí Grandoreiro mohl naznačovat, že jsou do jeho vývoje zapojeni různí operátoři, přičemž experti společnosti Kaspersky zaznamenali, že je nabízen i jako služba typu „Malware-as-a-Service“ (MaaS). Hojně rozšířený bankovní malware se zaměřuje na minimálně 900 finančních institucí ve více než 40 zemích v Severní a Latinské Americe a Evropě.

V rámci společného úsilí přispěla společnost Kaspersky spolu s dalšími soukromými partnery INTERPOLu k analýze vzorků Grandoreiro, které byly v letech 2020 až 2022 nashromážděny brazilskými a španělskými národními vyšetřovateli kybernetické kriminality. Během tohoto období produkty společnosti Kaspersky odhalily 150 000 útoků s použitím Grandoreiro zacílených na 40 000 uživatelů po celém světě. Nejvíce postiženými zeměmi se ukázaly být Brazílie, Španělsko, Mexiko, Portugalsko, Argentina a USA. Mezi státy, kde malware působil nechyběla ani Česká republika.

Na základě získaných údajů byly do srpna 2023 vypracovány analytické zprávy, které identifikovaly překryvy mezi vzorky, což vyšetřovatelům umožnilo rozkrýt strukturu skupiny organizovaného zločinu.

„Aktivity Grandoreiro sledujeme přinejmenším od roku 2016. V průběhu času útočníci pravidelně zdokonalovali svoje techniky a snažili se zůstat co nejdéle aktivní, aniž by byli odhaleni. Za této situace je nesmírně důležité, aby finanční instituce zůstaly ostražité a zároveň zlepšovaly svoje technologie pro boj proti podvodům a získávaly dostatečné údaje o hrozbách. Pro boj proti této kyberkriminalitě a zajištění bezpečnějšího prostředí pro uživatele a organizace po celém světě je zásadní také větší součinnost mezi soukromými a veřejnými partnery,“ komentuje **Fabio Assolini**, vedoucí latinskoamerického globálního výzkumného a analytického týmu (GReAT) společnosti Kaspersky.

Význam společného přístupu zdůraznil i **Craig Jones**, ředitel oddělení kyberkriminality INTERPOLu: *„Úspěch této operace jasně dokládá důležitost sdílení zpravodajských informací prostřednictvím INTERPOLu a proč jsme odhodláni fungovat jako most mezi veřejným a soukromým sektorem. Zároveň vytváří předpoklady pro další spolupráci v regionu.“*

V souvislosti s aktivním rozšiřováním rodin bankovních trojských koní, jako je Grandoreiro, do zahraničí očekávají odborníci společnosti Kaspersky zvýšené využívání tohoto malwaru i v dalším období. Podle jejich předpovědí o působení crimewaru a finančních hrozeb v roce 2024 bychom se mohli dočkat brazilských bankovních trojských koní, které se budou snažit zaplnit volná místa v oblasti bankovního malwaru pro stolní počítače, přičemž oživení aktivit těchto trojanů se stane

jedním z trendů, které budou v tomto roce na poli finančních hrozeb dominovat.

http://www.ceskenoviny.cz/tiskove/zpravy/kaspersky-pomaha-interpolu-bojovat-proti-malwaru-grandoreiro/2495703