V únoru se v Česku objevil škodlivý kód, který nahrává záznamy přes mikrofon a webkameru

15.3.2024 - Rita Gabrielová, Lucie Mudráková | ESET software

V únoru se v Česku vedle spywaru Agent Tesla a spywaru Formbook nově objevil škodlivý kód Rescoms.

Tento malware se podobně jako spyware zaměřuje na odcizení našich dat a nabízí útočníkům řadu špionážních funkcí – kromě zaznamenávání stisků kláves, pořizování snímků obrazovky a ovládání klávesnice a myši dokáže vytvářet také audio a video nahrávky prostřednictvím mikrofonu a webkamery v napadeném zařízení. Bezpečnostní experti proto uživatelům doporučují, aby byli obezřetní v případě nevyžádaných příchozích e-mailů a nepodceňovali ochranu kvalitním bezpečnostním řešením. Vyplývá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET.

Spyware Agent Tesla se od začátku nového roku zatím stále drží zhruba na pětině všech detekovaných případů pro operační systém Windows. Podle bezpečnostních expertů byl únor měsícem, kdy se na Česko zaměřovaly především celosvětové útoky a přílohy s českými překlady se tak ve větším množství neobjevovaly. V případě spywaru Agent Tesla se jednalo především o přílohu s názvem „ESTADO DE CUENT…HL - 695026972.exe“, spyware Formbook se poté nejvíce šířil prostřednictvím příloh s názvy „0053_PO29000224.exe“ a „Účtenka.exe“.

V únorové statistice se nově objevil také škodlivý kód Rescoms. Šířil se stejně jako oba zástupci spywaru e-mailovými přílohami s podezřelými názvy „x.exe“ a „459120568.exe“.

„Ačkoli byla České republika v únoru mezi pěti zeměmi, na které cílil spyware Agent Tesla nejčastěji, česky pojmenované přílohy byly tentokrát zastoupeny pouze okrajově. Dalšími cílovými zeměmi bylo Japonsko, Turecko, Polsko a Španělsko, a spyware nejčastěji ukrývala právě příloha se španělským názvem. Česká příloha, kterou útočníci vydávali za domnělou účtenku, se tentokrát objevila pouze v případě útoků spywaru Formbook,“ říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

„Trojský kůň Rescoms, který je známý i pod názvem Remcos, je dalším typem škodlivého kódu, který útočníci využívají k narušení našeho soukromí a odcizení osobních údajů. Útočníci ho šíří většinou prostřednictvím spamových kampaní, ale může být součástí i složitějších útoků. Ačkoli je na internetu ke stažení jako komerční nástroj, který útočníci vydávají za software ke vzdálené správě systému Windows, je to malware s celou řadou funkcí k odcizení dat a odposlechu obětí,“ dodává Jirkal.

Spyware je dlouhodobě jednou z největších hrozeb pro české uživatele. Jeho prostřednictvím se útočníci zaměřují na odcizení přihlašovacích údajů, především uživatelských hesel. Malware Rescoms má také řadu funkcionalit, které útočníkům v okamžiku, kdy škodlivým kódem infikují počítač, otevřou dveře k našemu soukromí.

„Trojský kůň Rescoms umožní útočníkovi vzdáleně ovládat a monitorovat systém oběti. Mezi jeho funkcionality patří zaznamenávání stisků kláves, pořizování snímků obrazovky nebo ovládání klávesnice a myši. Útočníci ho využívají také na krádeže uložených hesel a obsahu historie prohlížení. Není to ale vše, Rescoms dokáže vytvářet i audio a video nahrávky prostřednictvím mikrofonu a webkamery nebo stahovat a spouštět libovolné soubory,“ vysvětluje Jirkal.

Bezpečnostní experti uživatelům proto doporučují maximální obezřetnost při práci s elektronickou poštou, nereagovat na e-maily, které přijdou bez vyžádání z neznámé adresy, a rozhodně v nich neklikat na odkazy ani neotvírat žádné přílohy.

Kromě bezpečnostního softwaru, který uživatele dokáže před zmíněnými hrozbami účinně ochránit, patří ke správnému přístupu ke kybernetické bezpečnosti také nutnost uvědomit si, že každý z nás může být cílem útočníků. Jedním z největších omylů, před kterými bezpečnostní specialisté opakovaně varují, je falešný pocit bezpečí plynoucí z toho, že si uživatelé myslí, že nejsou jako terč pro kybernetické útočníky dostatečně zajímaví.

„V našich doporučeních se vždy snažíme upozorňovat na to, že útočník si nehledá konkrétní oběti, ale pomocí automatizovaných procesů dnes dokáže zacílit na velké množství náhodně vybraných lidí. Je to jeho cíl – čím víc z nás obdrží e-mail s nebezpečnými přílohami obsahujícími spyware nebo jiný malware, tím se zvýší pravděpodobnost, že někdo přílohu skutečně otevře a vpustí škodlivý kód do počítače. Motivem pro útočníky je samozřejmě vysoká prodejní cena našich dat a údajů na černém trhu," dodává Jirkal z ESETu.

Před nebezpečnými e-mailovými přílohami uživatele ochrání dobře nastavená antispamová ochrana, která je součástí moderních a komplexních bezpečnostních řešení. Ta nabízejí navíc řadu dalších funkcí, jako je například správce hesel nebo virtuální privátní síť VPN.

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost najdete například v online magazínu Dvojklik.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide. Nejčastějším rizikům pro děti na internetu se věnuje iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

Společnost ESET ve spolupráci s kyberbezpečnostními odborníky dále připravuje podcast True Positive. Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio řešení od ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-v-unoru-se-v-cesku-objevil-skodlivy-kod-ktery-nahrava-zaznamy-pres-mikrofon-a-webkameru