ESET: Nejoblíbenější zbraní kyberútočníků byl v únoru keylogger, zaznamenává stisky kláves na klávesnici

13.3.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Nejčastějším škodlivým kódem pro operační systém Windows v Česku byl v únoru infostealer Agent.AES. Bezpečnostní experti jej detekovali ve čtvrtině všech zachycených případů. V bezpečnostní komunitě je tento malware známý také jako Snake Keylogger, který zaznamenává stisky kláves na klávesnici napadeného počítače. Jak však bezpečnostní experti varují, Snake Keylogger dokáže také odcizit přihlašovací údaje, hesla a uživatelská data stejně jako řada dalších infostealerů. Posilování tohoto škodlivého kódu potvrzuje očekávání expertů, kteří jej označují za jednoho z možných nástupců slábnoucího spywaru Agent Tesla. Vyplývá to z pravidelné statistiky kybernetických hrozeb pro operační systém Windows v České republice od společnosti ESET.

Zatímco ještě v lednu na prvním místě pravidelné statistiky pro operační systém Windows v Česku figuroval infostealer Formbook, v únoru už tuto pozici obsadil škodlivý kód Agent.AES. Podobně jako infostealer Formbook je i tento škodlivý kód označován za potenciálního nástupce spywaru Agent Tesla, který začal slábnout a postupně ustupovat z čela statistiky na konci loňského roku.

„Malware Agent.AES řadíme opět mezi infostealery, jejichž prostřednictvím se útočníci již několik let pravidelně zaměřují na české uživatele a uživatelky. Tento škodlivý kód lze najít i pod názvem Snake Keylogger. Typickým chováním keyloggeru je zaznamenávání stisků kláves na klávesnici, dokáže ale odcizit data dalšími způsoby, které jsou typické pro tento typ škodlivých kódů. Útočníci jej neustále vyvíjejí – řetězí jeho kód s odkazem na slovo had v jeho názvu – a stále úspěšněji jej ukrývají před odhalením," vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

Keylogger byl nejvíce aktivní 14. a 20. února. Jako ostatní škodlivé kódy pro operační systém Windows jej útočníci šířili v infikovaných e-mailových přílohách. Nejčastěji se jednalo o přílohy s anglickými názvy „Payment Erro.exe" a „Bank Transfer Form.exe". Třetí nejčastěji zastoupenou škodlivou přílohou byl spustitelný soubor se slovenským názvem „Potvrdenie platby.exe".

„Během několika měsíců se nám na předních příčkách statistiky střídají možní nástupci spywaru Agent Tesla. Lze očekávat, že budeme ještě nějaký čas oscilovat mezi infostealery Formbook a Agent.AES jako největší kybernetickou hrozbou pro uživatele operačního systému Windows v Česku. Ať už jeden, nebo druhý – v hledáčku útočníků nadále zůstávají naše přihlašovací údaje, hesla a další velmi cenná data. Útočníci dokážou s využitím keyloggeru odcizit hesla z komunikačních platforem nebo e-mailových klientů, z FTP, webových prohlížečů nebo bezdrátových sítí. Odcizená data mohou následně díky keyloggeru odesílat přes e-mail, FTP nebo dokonce prostřednictvím komunikační platformy Telegram. Naše doporučení tak zůstávají stejná – nepodceňovat hrozby šířící se elektronickou komunikací, tvořit silná a unikátní hesla pro své online účty a spravovat je pomocí šifrovaných správců hesel," říká Jirkal.

Ještě v lednu představovaly detekce infostealeru Formbook více než 40 procent všech zachycených případů v Česku. V únoru se však tento škodlivý kód propadl na hodnotu necelých deseti procent všech zachycených případů. Škodlivý kód Agent Tesla se nadále drží na hodnotě okolo tří procent případů v Česku.

„Infostealer Formbook, jak také naznačuje propad počtu případů z února, nestál tentokrát za žádnou výraznější útočnou kampaní. V případě škodlivého kódu Agent Tesla se opět objevily e-mailové přílohy s českými názvy, které uživatelé a uživatelky pravidelně vídali v minulých letech. Domníváme se, že se jedná o starší kampaně, které mohou být ale nadále funkční. Přestože vývoj tohoto škodlivého kódu jeho autor ukončil, starší verze mohou vlastnit útočníci, kteří jej v minulosti koupili na černém trhu. Tyto staré verze mohou dál bez omezení využívat a škodlivý kód pouze schovávat do nových verzí příloh. Proto je zatím příliš brzy mluvit o tom, že škodlivý kód Agent Tesla již nepředstavuje pro uživatele a uživatelky v Česku žádnou hrozbu," uzavírá Martin Jirkal z ESETu.

Spolehlivou obranou před infostealery, které se řadí již k pokročilému škodlivému kódu, je moderní bezpečnostní software. Škodlivý e-mail dokáže včas rozpoznat a přesune jej do bezpečné složky, kterou za tímto účelem vytvoří. V předmětu e-mailu pak uživatelé uvidí, že se jedná o hrozbu. Zprávu si mohou následně ve vytvořené složce prohlédnout a smazat. Moderní bezpečnostní programy kromě obrany před kybernetickými hrozbami poskytují i praktické nástroje k ochraně našeho soukromí. Zabezpečená složka ESET Folder Guard chrání cenná data uživatelů před malwarem, který se je snaží poškodit. Uživatelé mohou vytvořit až několik zabezpečených složek, ke kterým budou mít přístup jen důvěryhodné a uživatelem povolené aplikace. Funkce Ochrana identity pak monitoruje černý trh s prodejem osobních údajů a upozorní uživatele, pokud se s jeho údaji obchoduje na dark webu.

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.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET, v podcastu TruePositive a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

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 výzkumná a 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-nejoblibenejsi-zbrani-kyberutocniku-byl-v-unoru-keylogger-zaznamenava-stisky-klaves-na-klavesnici