ESET: V září se na scénu vrátil trojský kůň, který útočníci vydávají za nástroj vzdálené správy pro Windows

20.10.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Ačkoli infostealer Formbook v září nezopakoval své kampaně z předchozího měsíce, stále se drží v čele pravidelné statistiky jako největší hrozba pro české uživatele a uživatelky počítačů s operačním systémem Windows. Ve větším počtu detekcí se tentokrát neobjevil ani nechvalně proslulý malware Agent Tesla, zato jsme mohli narazit na škodlivé kódy Agent.DIC a Rescoms. Právě druhý jmenovaný malware vzbudil pozornost svou zvýšenou přítomností v Česku – jedná se o škodlivý kód s celou řadou funkcí k odcizení dat a odposlechu obětí. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET.

V září bezpečnostní experti z ESETu sledovali změny v pravidelné statistice kyberhrozeb pro operační systém Windows v Česku. Zatímco ještě v srpnu výrazně vzrostla aktivita nechvalně proslulého infostealeru Agent Tesla, poslední analýza opět potvrzuje, že se jednalo pravděpodobně jen o jednorázovou kampaň díky stále dostupným starším verzím tohoto škodlivého kódu.

Ačkoli kyberhrozbám nadále kraluje infostealer Formbook, v září nezopakoval silnější kampaně z konce letošního léta. Nejvíce se objevoval maskovaný za downloader Win64/Agent.ECK a ukrytý v nebezpečné e-mailové příloze s anglickým názvem „shipping documents.exe“. Útočníci jej tak nadále šíří pomocí dalších škodlivých kódů.

„Infostealer Formbook v září tentokrát doplnily dva typy malwaru, které u nás tak často nepotkáme. Prvním z nich byl škodlivý kód, který označujeme jako Agent.DIC a jehož funkcí je stahovat do zařízení další malware. Na konci sledovaného měsíce jsme zachytili velmi silný útok na Česko. Útočníci posílali na své oběti e-mail s předmětem ‚Žádost o cenovou nabídku‘ a škodlivý kód byl jako vždy ukrytý v přiloženém dokumentu, jehož název byl poskládaný ze znaků české abecedy,“ říká Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

Po delší pauze se ve větším zastoupení objevil také škodlivý kód Rescoms. Útočníci jej šířili prostřednictvím downloaderu s názvem BAT/Agent.RMJ. Na potenciální oběti opět vyslali škodlivé e-maily a nebezpečný kód nastražili pod přílohu „OBJEDNAVKA_34002174.bat“.

„V posledních týdnech pozorujeme u malwaru Rescoms nárůst případů. V České republice je to konkrétně zhruba od poloviny září. Stále provádíme detailnější analýzy, nicméně může za tím být i změna nákupního chování útočníků na černém trhu. I díky zásahu proti malware rodině Lumma Stealer klesla poptávka po této hrozbě a útočníci mohou zkrátka hledat nové, vhodnější nástroje,“ říká Jirkal a dodává: „Trojský kůň Rescoms, který je známý i pod názvem Remcos, je aplikace pro vzdálenou správu počítače, kterou útočníci již řadu let otevřeně zneužívají. Je to malware s celou řadou funkcí k odcizení dat a odposlechu obětí. S ohledem na tuto přítomnost infostealerů, downloaderů a trojských koní v našem prostoru je na místě opět připomenout, aby uživatelé a uživatelky kyberútočníky nepodceňovali, i když se může na první pohled zdát, že je situace stále stejná.“

Škodlivý kód zaměřený na krádež dat je bohužel jednou z nevětších hrozeb, které v současnosti lidé v Česku čelí. Na náš region se střídavě zaměřují globální i cílené spamové kampaně, ve kterých útočníci šíří malware v e-mailech s nebezpečnými přílohami odkazujícími na domnělé doklady

objednávek, účtenky a faktury. Podle bezpečnostních expertů jsou v ohrožení jak uživatelé a uživatelky z řad široké veřejnosti, tak lidé z firem, kteří s podobnými dokumenty každý den pracují a ve spěchu si nebezpečí nemusí hned všimnout.

„Trojského koně Rescoms útočníci využívají k narušení našeho soukromí a odcizení osobních údajů – podobně, jako například infostealer Formbook. Mimo spamové kampaně může být součástí i složitějších útoků. Na internetu jej můžeme potkat jako komerční nástroj, který útočníci vydávají za software ke vzdálené správě systému Windows," říká Jirkal. „Dobře víme, že útočníci investují do přípravy svých kampaní nemalé prostředky a věnují čas strategii. V posledních týdnech je velkým tématem konec podpory pro verzi operačního systému Windows 10 a jak ukázal náš nejnovější průzkum, někteří uživatelé nemusí být v tomto tématu tak dobře zorientovaní a informovaní. Může tak být snadné je oklamat lživou komunikací zneužívající známou službu. V celkové situaci tak můžeme ve spěchu a nepozornosti kliknout na soubory, které působí věrohodně a na první pohled nám obdržená zpráva slibuje pomoc s nějakým procesem či úkolem. Ve skutečnosti je to ale malware, který nás má poškodit," dodává Jirkal.

I přes veškerou opatrnost můžeme sami vpustit škodlivý kód do našeho zařízení. Proto bezpečnostní experti doporučují zvážit pořízení profesionální ochrany našich počítačů, která slouží jako spolehlivá pojistka v případech, kdy se útočníkům podaří nás oklamat. Společnost ESET svá řešení nyní nabízí v akci 3za2 – od 1. září do 31. prosince 2025 mají zákazníci z řad domácností i firem možnost získat tříleté předplatné za cenu dvou let. Více informací o kampani, včetně seznamu konkrétních řešení a podrobných podmínek, najdete na webových stránkách společnosti ESET.

Uživatelé řešení ESET jsou před těmito hrozbami chráněni.

Společnost ESET®, která byla založena v Evropě, je předním dodavatelem řešení kybernetické bezpečnosti s pobočkami po celém světě. Poskytuje špičková řešení kybernetické bezpečnosti, která pomáhají předcházet útokům ještě před jejich vznikem. ESET kombinuje technologie umělé inteligence (AI) a lidskou odbornost, čímž pomáhá předejít nově vznikajícím globálním kybernetickým hrozbám, ať již známým či dosud neznámým. Poskytuje zabezpečení pro firmy, kritickou infrastrukturu a jednotlivce. Ať už jde o ochranu koncových zařízení, cloudu nebo mobilních zařízení, řešení a služby společnosti ESET, které využívají technologie umělé inteligence a kladou důraz na cloudové prostředí, zůstávají vysoce efektivní s minimálními nároky na uživatele.

Technologie ESET jsou vyvíjeny v EU a zahrnují robustní systém detekce a reakce, ultra-bezpečné šifrování a multifaktorovou autentizaci. S nepřetržitou obranou v reálném čase a silnou místní podporou udržuje ESET uživatele v bezpečí a firmy v chodu bez narušení jejich provozu. Neustále se vyvíjející digitální prostředí vyžaduje progresivní přístup k bezpečnosti. Jen v České republice nalezneme tři výzkumná a vývojová centra společnosti, a to v Praze, Jablonci nad Nisou a Brně. Výzkumné pobočky po celém světě podporují aktivity společnosti v rámci Threat Intelligence, stejně jako její silná globální síť partnerů.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost naleznete 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 RESET a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

Lucie Mudráková
Specialistka PR a komunikace
ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.com

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.
tel: +420 720 829 561
vitezslav.pelc@eset.com

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-v-zari-se-na-scenu-vratil-trojsky-kun-ktery-utocnici-vydavaji-za-nastroj-vzdalene-spravy-pro-windows