ESET: Kybernetičtí útočníci před koncem roku zintenzivňují své aktivity v Česku

19.11.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Praha, 19. listopadu 2025 – Zatímco ještě v září kyberbezpečnostní experti z ESETu sledovali pokles detekcí, v říjnu se infostealer Formbook opět přiblížil k 30 procentům všech zachycených případů škodlivého kódu v Česku. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET. Nárůst aktivity se však týkal i trojského koně Rescoms či infostealeru Agent Tesla, dalších dvou nejčastějších typů malwaru. V říjnu bezpečnostní specialisté opět zachytili větší množství škodlivých e-mailů a příloh s českými překlady. Cílem byli pravděpodobně především zaměstnanci a zaměstnankyně českých firem.

V říjnu oproti předchozímu měsíci opět vzrostl počet případů infostealeru Formbook v Česku. Rostla však také aktivita ostatních škodlivých kódů, které bezpečnostní specialisté v České republice dlouhodobě pozorují. Říjen tak byl podle jejich analýzy měsícem, ve kterém opět převládaly cílené útoky na české uživatele a uživatelky.

„V říjnu jsme u infostealeru Formbook pozorovali následující vzorec – nejvíce škodlivé aktivity jsme monitorovali vždy v pondělí, což naznačuje, že útočníci posílali škodlivé e-maily s infikovanými přílohami vždy o víkendu a zaměřili se tak především na lidi pracující s počítačem," vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET. „Nejedná se přitom o nijak novou strategii. S blížícím se koncem roku útočníci počítají s tím, že zaměstnanci budou dostávat větší objem elektronické pošty a v okamžiku nepozornosti či ve spěchu mohou nechtěně otevřít infikovaný soubor. A i tentokrát se snažili své oběti napálit tím, že e-maily vydávali za poptávky po produktech firmy."

Útočníci škodlivý kód Formbook schovávali nejčastěji pod soubor s názvem „msedge_elf.dll". V těle e-mailu, kde se tentokrát často objevovala čeština, se dle bezpečnostních analytiků objevovaly gramatické chyby. Právě chyby a nestandardní tón komunikace je spolehlivým ukazatelem toho, že s komunikací nemusí být vše v pořádku.

Také v případě dalších nejčastěji detekovaných škodlivých kódů – trojského koně Rescoms či infostealeru Agent Tesla – nebyla čeština výjimkou. Malware Rescoms se kromě přílohy s názvem „SDC34108.75.bat" objevil také v příloze „OBJEDNAVKA_34002174.bat". Ještě výmluvnější pak byl předmět e-mailu „OBJEDNÁVKA K FAKTUŘE".

„Ani v případě trojského koně Rescoms nenechali útočníci tentokrát nic náhodě a vsadili na češtinu. Jak jsme již upozorňovali minulý měsíc, aktuálně v Česku sledujeme nárůst případů tohoto škodlivého kódu a platilo to rozhodně i pro říjen. Účel trojského koně Rescoms je podobný jako v případě infostealerů – útočníci jej využívají k narušení našeho soukromí a odcizení osobních údajů. Může být ale součástí i složitějších útoků. Jedná se o aplikaci určenou ke vzdálené správě počítače, kterou v současných kampaních útočníci vydávají za software ke vzdálené správě systému Windows," vysvětluje Jirkal.

V případě infostealeru Agent Tesla pak bezpečnostní experti mluví o opětovném využívání starých kampaní z minulosti. Aktivní vývoj tohoto škodlivého kódu jeho autor totiž ukončil. Nejčastěji se v říjnu objevoval v e-mailových přílohách „RFQ - U1058 New Materials Order B13D60.scr" či pro Česko určených verzích „Poptavka 00413_pdf.exe" nebo „Zpusob_platby,jpg.exe".

Jak bezpečnostní specialisté upozorňují, závěr roku bývá vždy s ohledem na všudypřítomný shon pro kyberzločince ideální. Jako vždy doporučují především kombinovat ostražitost a zdravou podezíravost s profesionální kyberbezpečnostní ochranou.

„Na říjnových případech útoků infostealeru Formbook jsme mohli vidět, že i v době, kdy už mají útočníci k ruce řadu nástrojů generativní umělé inteligence, mohou stále připravit komunikaci, která bude obsahovat řadu chyb. Může se to stávat v případech, kdy nechtějí trávit přípravou útoků příliš mnoho času a rychle zacílit na co nejširší skupinu lidí. I přes to bych obecně doporučoval se na chyby příliš nespoléhat a všímat si dalších ukazatelů – kdo je odesílatelem zprávy, zda e-mail přišel bez vyžádání nebo v návaznosti na předchozí komunikaci či zda sedí e-mailová adresa s oficiální doménou webu, pokud se jedná například o nějakou známou instituci či firmu. Víme, že se tato rada může zdát málo platná s ohledem na to, jak býváme na konci roku všichni vytížení, opravdu se ale vyplácí zpomalit a věnovat příchozí e-mailové komunikaci dost času na kontrolu," doporučuje Jirkal z ESETu.

Spolehlivou pojistkou před nechtěným otevřením škodlivé přílohy a vpuštěním škodlivého kódu do zařízení je bezpečnostní software. Dokáže vytvořit bezpečnou složku, do které zjištěnou hrozbu přesune. Uživatelé si poté mohou e-mail ve složce v případě zájmu prohlédnout a pak jej smazat. Součástí aktualizované platformy ESET PROTECT pro firemní zákazníky z letošního jara je proto také nová ochrana proti spoofingu a útokům využívajícím homoglyfy. Nově je součástí stávajícího řešení ESET Cloud Office Security (ECOS). To navíc také obsahuje funkci zpětného stažení e-mailů, která umožňuje rychle odvolat a umístit do karantény jakékoli doručené e-maily, které vyhodnotí jako podezřelé.

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-kyberneticti-utocnici-pred-koncem-roku-zintenzivnuji-sve-aktivity-v-cesku