Kyberútočníci nám v únoru posílali ke kontrole smlouvy a pracovní nabídky, v e-mailech ale ukrývali malware

19.3.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Kyberútočníci v únoru manipulovali české uživatele a uživatelky nebezpečnými e-maily s žádostmi o kontrolu smluv či pracovních nabídek. Jednalo se však jen o zastírací strategii pro šíření škodlivého kódu CloudEyE. Jednou z jeho hlavních funkcí je stahovat do počítače další škodlivé kódy, což útočníkům pomáhá s jejich šířením. Spolu s tímto malwarem se v Česku objevily dále také škodlivé kódy Aotera a Formbook. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET.

V únoru zůstal v čele pravidelné statistiky pro Českou republiku škodlivý kód CloudEyE. Bezpečnostní experti v jeho případě zaznamenali nejsilnější útoky v období od 5. do 7. února.

„Minulý měsíc jsme mohli v našem regionu sledovat pokračující aktivitu malwaru CloudEyE, i když už se nejednalo o takový nárůst případů, jako tomu bylo v lednu. Podvodné e-maily, kterými útočníci tento škodlivý kód šíří, obsahovaly jako přílohu nebezpečný skript. Jakmile oběti této kampaně přílohu stáhly a spustily, škodlivý kód CloudEyE začal do počítače stahovat další malware, což je ostatně jeden z jeho hlavních úkolů. V únoru byly tyto útoky připravené na míru českým uživatelům a uživatelkám – útočníci je ve zprávách vyzývali ke kontrole smluv nebo pracovních nabídek, za které škodlivé přílohy vydávali," vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

V závěsu za malwarem CloudEyE se v únoru objevil škodlivý kód s názvem Aotera. Na české uživatele a uživatelky i v tomto případě cílila rozsáhlá phishingová kampaň, přičemž bezpečnostní experti zachytili nejsilnější útoky 11. února. Předmět škodlivého e-mailu byl „RE: REQUEST FOR QUOTATION – URGENT". Příloha ukrývala právě zmíněný malware.

„Aotera je škodlivý kód typu loader. Útočníci ho šíří jako samostatný spustitelný soubor a vydávají ho za relevantní přílohu v e-mailové zprávě. Jakmile oběť soubor spustí, malware Aotera v paměti rozbalí a aktivuje další schovaný škodlivý kód. Podle naší analýzy se v únoru tímto způsobem šířil například škodlivý kód SnakeStealer anebo infostealer Formbook," říká Jirkal.

Infostealery jsou škodlivé kódy, které se v rámci operačního systému Windows objevují dlouhodobě a s přetrvávající intenzitou, a to nejen v Česku. Útočníci k jejich šíření využívají stále rafinovanější způsoby, včetně zprostředkujícího malwaru, který tomuto šíření pomáhá – ať už je to CloudEyE nebo Aotera. Bezpečnostní experti proto doporučují hlavně opatrnost při čtení elektronické pošty. V případě předně nevyžádané zprávy by uživatelé a uživatelky neměli nikdy klikat na odkazy v e-mailu ani stahovat a spouštět přiložené soubory. Pokud zpráva působí dojmem, že je odesílatelem nějaká známá instituce, například banka nebo státní správa, vždy doporučují si její pravdivost s danou institucí nejdříve ověřit.

Dvojici výše zmíněných škodlivých kódů doplnil také infostealer Formbook. Výrazněji aktivní byl především ve druhé polovině února. V jeho případě se pak mohli uživatelé a uživatelky setkat s celou přehlídkou podvodných zpráv na různá témata. Většina e-mailů byla v angličtině, přestože je útočníci odesílali z Česka.

„Podvodná komunikace je sice velmi často spjata se šířením škodlivého kódu v rámci operačního systému Windows, přesto byl únor v tomto ohledu výjimečný co do pestrosti smyšlených scénářů. V případě infostealeru Formbook se objevovaly nejrůznější náměty – faktury, pracovní smlouvy nebo informace o zásilkách. Zprávy přitom kladly velký důraz na naléhavé řešení situace. Právě naléhavost je jedním z ukazatelů phishingové komunikace. Techniky sociálního inženýrství jsou zákeřné svým zneužíváním lidských emocí. Jakmile v nás nějaká zpráva vyvolává nervozitu, strach, ale třeba i zvědavost, je vždy potřeba v první řadě zbystřit a uvědomit si, že jsme možná někým manipulovaní. Jakmile máme takové podezření, je důležité začít si všímat dalších podezřelých věcí – v jaké podobě je adresa odesílatele, zda se jedná například o oficiální podobu nějaké známé služby, za kterou by se mohli útočníci vydávat. I v případě phishingu bych uživatelům a uživatelkám doporučoval pořídit si moderní bezpečnostní software neboli antivir, byť v dnešní podobě tyto programy nabízejí už více nástrojů a funkcí, než jen ochranu před počítačovými škodlivými kódy," dodává Jirkal z ESETu.

Moderní bezpečnostní software umí zamezit přístupu škodlivého kódu do našeho zařízení. 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.

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-kyberutocnici-nam-v-unoru-posilali-ke-kontrole-smlouvy-a-pracovni-nabidky-v-e-mailech-ale-ukryvali-malware