ESET: Česko bylo v květnu terčem organizované skupiny útočníků, škodlivé kódy nakoupili na dark webu

12.6.2025 - Lucie Mudráková | ESET software

Praha, 12. června 2025 – Do popředí pravidelné statistiky malwaru pro operační systém Windows v Česku se v květnu vyšplhaly tři škodlivé kódy, které podle bezpečnostních expertů útočníci využili v organizovaném spamovém útoku na české uživatele a uživatelky. Cílem útočníků bylo pravděpodobně podpořit šíření infostealeru Formbook, který je využívaný ke krádežím přihlašovacích údajů, především hesel. Útočníci škodlivé kódy nakoupili podle bezpečnostních expertů na dark webu. Šířili je prostřednictvím podvodných e-mailů v češtině a jednotlivé vlny útoku mezi sebou různě provazovali. Jakmile oběti otevřely škodlivou přílohu e-mailu, spustily malware, který do jejich počítače stáhl další hrozbu. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET.

Na základě analýzy škodlivých kódů pro operační systém Windows došli bezpečnostní experti k závěru, že Česká republika byla v květnu pod organizovaným útokem. V čele pravidelné statistiky se tentokrát objevily v současnosti spíše okrajové škodlivé kódy. Podle bezpečnostních expertů je útočníci nakoupili na dark webu. Jedná se ve všech případech o malware, který dokáže stáhnout do zařízení další škodlivý kód – v případě České republiky především nechvalně proslulý infostealer Formbook, který je určený ke krádežím uživatelských dat, především hesel k našim účtům.

„Není to poprvé, kdy všechny důkazy svědčí tom, že se Česká republika stala cílem promyšlené spamové kampaně z dílny menšího počtu útočníků. Letošní květen byl ale unikátní tím, že zachycené útoky na sebe přesně navazovaly, byly vedeny v češtině a vykazují jasné známky vzájemného propojení," říká Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET. „Všechny nejčastěji zastoupené škodlivé kódy mohou útočníci sehnat na černém trhu, tedy na dark webu. Jejich úkolem je stahovat do zařízení další malware. Ke stahování dalšího škodlivého obsahu docházelo v květnu ze serveru, odkud útočníci šíří také obávaný infostealer Formbook. Ten v květnu navíc vykazoval zvýšenou aktivitu přesně v časech zachycených spamových kampaní. S velkou pravděpodobností se proto domníváme, že hlavní snahou útočníků bylo právě nasazení tohoto infostealeru," říká Jirkal.

Že jde o konkrétní útok na Česku republiku, dokazují i e-maily v češtině včetně českých překladů příloh, které obsahovaly zmíněné škodlivé kódy. Uživatelé a uživatelky je v domnění, že otevírají přílohu s podrobnostmi o nějaké objednávce, vpustili do svých počítačů.

„Již v dubnu jsme zaznamenali desítky tisíc škodlivých e-mailů, které doslova zasypaly Česko. S ohledem na to, že se útočníkům evidentně vyplatí své útoky inovovat a věnovat jim další čas na vylepšení, by měli být čeští uživatelé a uživatelky nanejvýš opatrní při práci s e-maily a neklikat na odkazy ani neotevírat soubory přiložené v přílohách, pokud se jedná o nevyžádanou komunikaci. Spolehlivou ochranou před infostealery je pak vždy především bezpečnostní software," dodává Jirkal.

Zmíněné útoky začaly 12. května. Útočníci použili škodlivý kód Agent.QMG a šířili jej podvodným e-mailem ve škodlivé příloze s názvem Objednavka_250197.vbs.

„Malware Agent.QMG sledujeme v Česku dlouhodobě a v minulosti se již objevil na předních místech naší statistiky. Jeho úkolem je především stahovat z internetové adresy do zařízení další škodlivý

kód. Podobně pak funguje malware Agent.CLE, který převzal pomyslnou štafetu už 13. května. I v tomto případě útočníci zvolili prověřenou strategii a malware schovali do souboru, který vydávali za objednávku," vysvětluje Jirkal.

Po kratší přestávce, kterou pravděpodobně využili k přípravě, se útočníci vrátili 19. května, a to opět v útoku, který byl provázaný s těmi předešlými. Tentokrát použili škodlivý kód Agent.TAY. I tento malware měl shodné funkcionality se škodlivým kódem Agent.QMG. Podvodné e-mailové zprávy útočníci rozesílali stále v češtině, příloha však měla už jen obecnější označení POĠ_. 40715CZ25.vbs. Spolu s ním byl v tomto balíčku ukrytý i již zmíněný škodlivý kód Agent.CLE. Na závěr této série útočných kampaní, 20. května, pak útočníci ještě jednou přes e-mail rozšířili samotný malware Agent.CLE v příloze s názvem Objednávka_omni-x05140001_pdf.bat.

„Infostealer Formbook, kvůli kterému útočníci všechny výše popsané manévry uskutečnili, je považovaný za nástupce v Česku dlouhodobě přítomného škodlivého kódu Agent Tesla. Ten začal slábnout na konci loňského roku a nyní se ve statistice objevuje v několika procentech případů. Infostealery nejsou rizikem jen pro Česko, proto byl květnový organizovaný útok na naše prostředí tak neobvyklý. Potvrzuje se, že i když Česká republika není zemí s vysokým počtem potenciálních obětí, přesto útočníkům stojí za to připravit útok přímo nám na míru. Situaci nadále monitorujeme," dodává Jirkal z ESETu.

Ačkoli je e-mail dnes jen jedním ze způsobů elektronické komunikace, nadále zůstává jedním z nejrozšířenějších, především ve firemním prostředí. Společnost ESET právě pro firemní zákazníky v březnu aktualizovala svou platformu ESET PROTECT. Součástí této aktualizace byla také nová ochrana proti spoofingu a útokům využívajících homoglyfy. ESET Cloud Office Security nyní také obsahuje funkci zpětného stažení e-mailů, která umožňuje rychle odvolat a umístit do karantény jakékoli doručené e-maily, které vyhodnotí jako podezřelé.

Uživatelé produktů 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 digitální 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 TruePositive 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