ESET: Útočníci si výrazně zlepšili češtinu, přesvědčivými e maily v červnu opět nejvíc šířili infostealer Formbook

7.7.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Také v červnu bezpečnostní experti sledovali provázané spamové kampaně v Česku. Jejich cílem bylo pravděpodobně opět šířit především nechvalně známý infostealer Formbook, který se v červnu s více než pětinou všech zachycených detekcí vyšplhal do čela pravidelné statistiky pro operační systém Windows v Česku. S téměř shodným podílem detekcí ho však následoval i malware Agent.CLE, který útočníkům pomáhá připravit počítače k následné infekci. Bezpečnostní experti se proto domnívají, že spolu útoky opět souvisely. S ohledem na velmi dobrou úroveň češtiny ve škodlivých e-mailech apelují na co nejopatrnější zacházení s příchozí poštou. Vyplývá to z pravidelné analýzy detekčních dat společnosti ESET.

Infostealer Formbook a malware Agent.CLE měly v červnové statistice téměř shodný podíl detekcí v rámci všech zachycených škodlivých kódů pro operační systém Windows v Česku. Již v květnu bezpečnostní experti upozornili na to, že útočné kampaně těchto dvou škodlivých kódů spolu mohou souviset a vyloučené to podle nich není ani tentokrát.

„Nemáme sice přímý důkaz, že útočníci v červnu využili malware Agent.CLE k tomu, aby připravili napadený počítač pro infekci infostealerem Formbook, jisté ukazatele tomu ale nasvědčují. Nejsilnější aktivita malwaru Agent.CLE připadla na 12. a 19. června. V dané dny jsme pozorovali zároveň také zvýšenou aktivitu škodlivého kódu Formbook. Útočníci si navíc opět dali mezi jednotlivými kampaněmi týden přestávku. Předpokládáme proto, že se znovu opakoval stejný vzorec z letošního května," vysvětluje vývoj kyberhrozeb Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET.

Zatímco spamové kampaně malwaru Agent.CLE byly přeložené do češtiny, přímé útoky infostealeru Formbook byly vedeny v angličtině. Malware Agent.CLE útočníci schovávali pod přílohy, které se tvářily jako objednávky – „Objednavka_2928.bat" či „Gufero-612025_pdf.cmd". Na infostealer Formbook mohli pak uživatelé a uživatelky narazit především v příloze s názvem „MT103-17463829584.exe".

„Útoky v češtině byly tentokrát opravdu velmi dobře připravené. V minulosti, když se kyberútočníci rozhodli komunikovat česky, nás často na něco nekalého upozornila špatná úroveň češtiny, hrubky a stylistické přešlapy. V červnových útocích jsme ale na nic takového nenarazili. Je tak možné, že stále zlepšující se úroveň nástrojů umělé inteligence v tomto směru útočníkům s přípravou spamových kampaní pomáhá. Vyzval bych proto k co největší opatrnosti. Infostealery jsou velkým rizikem pro naše hesla k řadě důležitých účtů a v hledáčku útočníků jsou jak jednotlivci, tak zaměstnanci firem. Rozhodně je proto důležité neklikat bez rozmyslu na odkazy ani neotevírat soubory v předem nevyžádaných zprávách. Právě v letních měsících, kdy se lidé po dovolené vrátí do kanceláře a budou procházet doručené e-maily, může být riziko vyšší," dodává Jirkal.

Spamové kampaně v Česku jsou dlouhodobě specifické tím, jak útočníci maskují škodlivý kód za různé přílohy e-mailů. Při bližším pohledu lze vidět, že příloha může mít rovnou příponu, která označuje spustitelný soubor (například .exe nebo .bat). Dokumenty v přílohách mohou mít ale také dvě koncovky, přičemž tu druhou z nich, která by na škodlivou aktivitu upozornila, uživatelé nemusí

vždy vidět.

„Příloha se ve velkém počtu případů může jevit jako dokument v programu MS Word, ve formátu PDF nebo jako obrázek. Uživatelé pak nemusí mít vůbec podezření, že otevírají soubor, se kterým je něco špatně. 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. Infostealery jsou již pokročilou kybernetickou hrozbou a rozhodně bych je nepodceňoval. S našimi odcizenými daty a přihlašovacími údaji pak mohou útočníci obchodovat na dark webu nebo je využít k přípravě nových útoků," dodává Jirkal z ESETu.

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.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-utocnici-si-vyrazne-zlepsili-cestinu-presvedcivymi-e-maily-v-cervnu-opet-nejvic-sirili-infostealer-formbook