ESET: Česko v dubnu zasypaly desítky tisíc škodlivých e-mailů

2.6.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Praha, 14. 5. 2025 – V dubnu opět vzrostly detekce infostealeru Formbook, který tak stále stojí v čele pravidelné statistiky kybernetických hrozeb pro operační systém Windows v Česku. Útočníci jej tentokrát šířili v neobvykle silné kampani zaměřené na Českou republiku a Slovensko. Útoky načasovali na Velikonoce. Bezpečnostní experti zachytili nejvíce případů škodlivého kódu na Zelený čtvrtek a v úterý po Velikonočním pondělí, kdy se lidé vraceli do práce a otevírali své e-maily. K šíření infostealeru využili škodlivý program ModiLoader, který poté, co infikuje počítač, stahuje další malware a spouští ho podle pokynů útočníků. Vyplývá to z pravidelné statistiky detekčních dat společnosti ESET.

Počet případů infostealeru Formbook vzrostl v dubnu na více než třetinu všech zachycených detekcí. Velké kampaně připravili útočníci v první polovině měsíce, kdy šířili škodlivý kód globálně prostřednictvím e-mailů v angličtině. Během velikonočních svátků pak na Česko zacílila silná kampaň, ve které útočníci využili škodlivý program ModiLoader. Ten jim slouží k dalšímu šíření malwaru určenému ke krádežím informací či k získání vzdáleného přístupu k počítači – škodlivých kódů Rescoms a Agent.AES nebo již zmíněného infostealeru Formbook.

„Škodlivý program ModiLoader je známou a stálou hrozbou nejen v České republice, většinou jej ale neevidujeme v tak masivní kampani, jaké jsme byli svědky letos v dubnu. Útočníci si pro české uživatele a uživatelky tentokrát připravili promyšlenou strategii," říká Martin Jirkal, vedoucí analytického týmu v pražské výzkumné pobočce společnosti ESET. „Útok začal na Zelený čtvrtek. O tom, jak byla tato kampaň silná, svědčí i množství škodlivých e-mailů, které jsme monitorovali – jejich počet se vyšplhal na desítky tisíc. Na Slovensko mířilo v tento den podle našich dat 41 % všech celosvětových útoků tohoto programu, na Českou republiku to bylo 30 %. Velký skok v detekčních datech jsme pozorovali i v úterý po Velikonocích. Pravděpodobným vysvětlením je to, že lidé, kteří se vraceli ze svátků zpět do práce k počítačům, otevírali mezi pracovními e-maily bohužel i ty škodlivé," vysvětluje Jirkal.

E-mailové zprávy, které obsahovaly škodlivý program ModiLoader, informovaly příjemce o tom, že obdržel dokument se shrnutím objednávky, spolu s požadavkem na její potvrzení. Text zprávy byl napsaný v češtině bez gramatických a stylistických chyb, což opět potvrzuje, že byl útok cílený a pečlivě připravený. V příloze těchto e-mailů byl ModiLoader „schovaný" v dokumentu s názvem „Objednavka.iso". Pokud oběť soubor otevřela, zobrazil se soubor „Obejdnavka.cmd", který po spuštění nakazil dané zařízení.

„Zachycený dubnový útok je názornou ukázkou toho, jak dnes útočníci podobné kampaně připravují. Svátky a období volna jsou pro ně dobrou příležitostí. Mohou zneužít toho, že máme naši pozornost nasměrovanou jinam – k našim dovoleným a volnočasovým aktivitám. Zasílání škodlivých kódů v e-mailech se jim bohužel stále velmi vyplácí a potvrzují to i naše dubnová čísla," říká Jirkal a dodává: „V případě takto připravených útoků neexistuje obrana, která by byla úplně snadná a jednoduchá, přesto se ale uživatelé mohou bránit velice efektivně. Vždy v případě nevyžádané e-mailové komunikace doporučujeme skepsi a obezřetnost spolu s využíváním profesionálního bezpečnostního softwaru, který dokáže spolehlivě reagovat na širokou škálu různých útoků, a to i v případě, kdy se jedná o zcela nové typy kybernetických hrozeb."

Škodlivý program ModiLoader se obvykle šíří prostřednictvím phishingových kampaní. Ty mají v

případě operačního systému Windows v Česku podobu zpráv o objednávkách s nebezpečnými přílohami, které útočníci vydávají za různé související dokumenty – faktury nebo shrnutí objednávek. ModiLoader po spuštění stáhne další škodlivé kódy (například infostealer Formbook) ze serveru útočníků, nebo jsou již distribuovány spolu s ním jako jeho součást. Následně škodlivý obsah dešifruje a poté spustí přímo z paměti napadeného počítače.

„Kromě velké velikonoční kampaně jsme ModiLoader detekovali i v následujících dnech v jednom menším útoku. V obou případech útočníci využili tento program pro šíření infostealeru Formbook, který byl také již součástí škodlivé přílohy. Jejich cílem tedy byla jako vždy naše uživatelská data, především hesla," vysvětluje Jirkal.

Spolehlivou pojistkou před nechtěným 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. Pokud bezpečnostní program rozpozná škodlivý kód v nějakém souboru, dokáže jeho spuštění zablokovat a přesunout ho do tzv. karantény, o čemž jsou uživatelé vždy informováni. Společnost ESET v březnu aktualizovala svou platformu ESET PROTECT, která je součástí řešení pro firemní zákazníky. Součástí aktualizace je také nová ochrana proti spoofingu a útokům využívajícím homoglyfy – nově jako součást stávajícího řešení ESET Cloud Office Security (ECOS). ESET Cloud Office Security navíc 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.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-cesko-v-dubnu-zasypaly-desitky-tisic-skodlivych-e-mailu