Útočníci zacílili se spywarem na Česko

18.9.2023 - Lucie Mudráková | ESET software

S téměř pětinou všech detekcí zůstává hlavním kybernetickým rizikem pro české uživatele operačního systému Windows spyware Agent Tesla. Bezpečnostní experti upozornili, že v srpnu byla Česká republika mezi hlavními cílovými zeměmi, a to hned po Japonsku a Turecku. Nebezpečná e-mailová příloha měla tentokrát český název děkovný dopis.docx.exe. Vyplývá to z pravidelné statistiky kybernetických hrozeb pro operační systém Windows v Česku od společnosti ESET.

Zatímco na základě červencových dat byl spyware Agent Tesla detekován v téměř třetině všech zachycených případů, v srpnu jeho detekce klesly na necelou pětinu. I přesto byla Česká republika hned po Japonsku a Turecku zemí, které byly v srpnu nejvíce vystaveny útokům tohoto malwaru.

„Nejsilnější útoky jsme zachytili 14. srpna a na konci měsíce, 29. a 30. srpna. A zatímco v červenci se e-mailové přílohy, přes které se infostealery šíří mezi uživateli, neobjevovaly v českém jazyce, v srpnu byla jedna z nejčastějších příloh pojmenována děkovný dopis.docx.exe. Jednoznačně tak vidíme, že tentokrát bylo Česko cílovou zemí," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Další přílohou, jejímž prostřednictvím útočníci spyware v srpnu distribuovali, byl soubor s anglickým názvem AMENDED PURCHASE ORDER.exe. Podobně i v případě spywaru Formbook mohli uživatelé v srpnu narazit na přílohu Repeat Order #0828.exe.

„Zatímco u e-mailových příloh v cizích jazycích mohou uživatelé zpozornět a více se zamyslet nad tím, kdo by jim takovou zprávu mohl odeslat, u česky pojmenovaných příloh je vždy riziko, že ji ve spěchu otevřou. Spyware je pak rizikem hlavně pro ta zařízení, která nejsou chráněna žádným bezpečnostním softwarem," dodává Jirkal.

Ve druhé polovině srpna bezpečnostní experti zaznamenali také pokles detekcí v případě malwaru Agent.QMG. Podle nich je ale možné, že útočníci ještě změní způsob jeho šíření, aby zajistili větší úspěšnost kampaní. V srpnu se tento škodlivý kód nejčastěji objevoval v přílohách SALES-CONTRACT.vbs nebo Produkt nové objednávky.vbe.

„Detekce v případě operačního systému Windows jsou v Česku poměrně stabilní, nepozorujeme zde tak velké výkyvy, jako například u platformy Android, kde útočníci daleko častěji mění strategie a způsoby šíření škodlivých kódů," říká Jirkal a dále vysvětluje: „I když se například může zdát, že na základě poklesu detekcí ztrácí škodlivý kód svou schopnost útočit na uživatele, může se jednat pouze o přechodné období, během kterého útočníci škodlivý kód aktualizují a vylepšují."

Spyware je malware, který se v Česku vyskytuje dlouhodobě. Cílem infostealerů, kam se také tento škodlivý kód řadí, jsou především naše uživatelská data, která mají stále větší cenu na černých trzích. Nejvíce cenná jsou pak především hesla, která mohou otevřít dveře k celé řadě našich účtů, včetně těch, ze kterých mohou útočníci odcizit naše peníze.

„Spyware rozhodně není typem malwaru, který by měli uživatelé podceňovat. Spolehlivou obranou před ním je tak vždy především bezpečnostní software. Ten je nezbytnou pojistkou právě pro případy, kdy ve chvíli nepozornosti spustíme přiloženou přílohou v e-mailu nebo v jiných komunikačních platformách. Kvalitní bezpečnostní programy obsahují dnes i správce hesel, které uživatelům pomohou se správou jejich přihlašovacích údajů," říká Jirkal z ESETu.

Především správné nakládání s dostatečně silnými hesly, která by uživatelé neměli nikdy používat pro více svých účtů, je přístup, který může zamezit větším škodám v případě napadení spywaru. Zabezpečení svých účtů uživatelé posílí také využíváním dalšího faktoru – například potvrzením ve spárované aplikaci nebo SMS kódem – při přihlášení.

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio produktů ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-utocnici-zacilili-se-spywarem-na-cesko