

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **18** ze dne **20.9.2022**

V srpnu rostl počet útoků na uživatelská hesla

Bezpečnostní specialisté z ESETu zaznamenali v srpnu růst detekcí u všech nejčastějších typů spywaru, které dlouhodobě představují riziko pro operační systém Windows v Česku. Nejčastěji detekovaným škodlivým kódem byl opět spyware Agent Tesla, který se stejně jako po celé léto objevil ve zhruba pětině všech případů. Spyware Formbook a password stealer Fareit v srpnu posílily výrazněji, neobjevily se ale v žádném větším útoku. Doménou srpna byly především útočné kampaně v angličtině, přesto se nadále objevovaly nebezpečné e-mailové přílohy také v češtině. Vyplývá to z pravidelné statistiky společnosti ESET.

Srpnová statistika nejčastějších kybernetických hrozeb pro uživatele operačního systému Windows opět potvrdila stabilní počet detekcí spywaru v Česku. Bezpečnostní specialisté zaznamenali spyware Agent Tesla téměř v pětině všech případů.

„Spyware Agent Tesla se v počtu detekcí držel celé léto na stabilních hodnotách a v srpnu počet zachycených případů mírně vzrostl. Nejsilnější útočné kampaně proběhly tentokrát v první polovině měsíce, 12. a 15. srpna. Zbytek měsíce byl ale spíše klidný,“ shrnuje vývoj kybernetických hrozeb Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Spyware je jedním z nejčastěji detekovaných škodlivých kódů v České republice. Útočníci jeho prostřednictvím cílí především na uživatelská hesla, která dále využívají k přípravě nových útoků, nebo je prodávají na černém trhu. Seznam odcizených přihlašovacích údajů může útočníkům pomoci s přípravou tzv. slovníkových útoků, při kterých používají objemné seznamy hesel ve snaze prolomit přístupy k našim online účtům.

Vstupní branou do zařízení je pro spyware e-mail. K jeho šíření využívají útočníci nebezpečné e-mailové přílohy, které svým názvem často odkazují na proplacení nějaké faktury nebo potvrzení objednávky. Útočníci se tak snaží uživatele přimět k tomu, aby ve chvíli nepozornosti přílohu spustili v domnění, že zpráva je adresována opravdu jim a obsahuje nějaké důležité informace.

„V srpnu tentokrát převládaly především e-mailové přílohy v angličtině. U spywaru Agent Tesla jsme nejčastěji detekovali přílohu s názvem Contract Agreement.exe. Spyware Formbook, který měl největší útočnou kampaň 24. srpna, se zase nejvíce šířil prostřednictvím přílohy s názvem Booking Specification.exe,“ říká Jirkal.

Zatímco u anglicky pojmenovaných příloh existuje větší šance, že uživatelé při otevření takového e-mailu zpozorní a budou mít pochyby, zda je zpráva adresována právě jim, u příloh v češtině je riziko otevření nebo spuštění mnohonásobně vyšší.

„Český název přílohy používali útočníci v srpnu u spywaru Formbook. Příloha byla označena názvem OBJEDNAT.scr. Password stealer Fareit, který je také typem spywaru a který se přes prázdniny šířil právě prostřednictvím česky označených příloh, se tentokrát nejčastěji ukrýval v příloze FQ-PO#09488378.exe. Počet případů, ve kterých jsme ho detekovali, přitom v srpnu opět vzrostl a není vyloučené, že se v dalším období opět vrátí v nějaké silnější kampani, kterou útočníci připraví na míru českým uživatelům,“ dodává Jirkal.

Útočníci využívají spyware především k odcizení hesel, která ukládáme do internetových prohlížečů. Právě internetové prohlížeče nejsou před těmito útoky řádně zabezpečené.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **18** ze dne **20.9.2022**

„Heslo stále patří mezi nejspolehlivější bezpečnostní prvek v online světě. Uživatelé přitom jejich tvorbě a správě vždy nevěnují takovou pozornost, jakou by měli,“ říká Jirkal. „Ke každému online účtu bychom měli mít unikátní heslo, které nebudeme používat nikde jinde. Mělo by být také dostatečně silné, tedy složené nejméně z deseti různých znaků nebo tvořené heslovou frází z několika různých slov. Hesla bychom neměli nikam zapisovat a k jejich ukládání využívat specializované správce hesel, které je uloží v zašifrované podobě. Pro případ, že se útočníci dostanou k našemu heslu a pokusí se prolomit přístup do našeho účtu, doporučuji využívat vícefaktorové přihlašování zasláním kódu do SMS nebo do aplikace.“

Správce hesel, specializovaný program, který bezpečně uloží naše hesla k online účtům, mohou uživatelé pořídit samostatně, i jako součást moderního bezpečnostního řešení. To také celkově chrání zařízení před spywarem v případě, kdy uživatelé stále propracovanější útoky včas sami nerozpoznají.

Nejčastější kybernetické hrozby pro operační systém Windows v České republice za srpen 2022:

1. MSIL/Spy.AgentTesla trojan (19,24 %)
2. Win32/Formbook trojan (15,80 %)
3. Win32/PSW.Fareit trojan (13,45 %)
4. MSIL/Spy.Agent.AES trojan (2,92 %)
5. Win32/Agent.TJS trojan (2,83 %)
6. MSIL/Spy.Agent.DFY trojan (1,14 %)
7. Java/Adwind trojan (0,63 %)
8. BAT/CoinMiner.AUB trojan (0,59 %)
9. Win32/Qhost trojan (0,52 %)
10. MSIL/Agent.VQU trojan (0,50 %)

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

Zdroj: ESET