

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **41** ze dne **11.7.2023**

Aktuálním cílem spywaru jsou zaměstnanci firem v Česku

Podle aktuálních dat společnosti ESET doznívá v Česku dubnový útok malwaru Agent.QMG, který do zařízení stahuje celou řadu škodlivých kódů, včetně známých spywarů Agent Tesla a Formbook. V květnu bezpečnostní specialisté zaznamenali celou řadu nebezpečných e-mailových příloh s českými názvy odkazujícími na faktury či objednávky. Cílem kybernetických útočníků tak nyní mohou být především menší firmy, jejichž zaměstnanci s takovými dokumenty frekventovaně pracují. Vyplývá to z pravidelné statistiky kybernetických hrozeb pro Českou republiku.

Bezpečnostní specialisté aktuálně sledují na zařízeních s operačním systémem Windows pokles počtu detekcí u spywaru Agent Tesla. Oproti předchozímu měsíci naopak vzrostly detekce spywaru Formbook a doznívá také útočná kampaň malwaru Agent.QMG. Bezpečnostní experti však varují, že i přes zaznamenaný pokles u některých škodlivých kódů mohou být současné útočné kampaně rizikem jak pro širokou veřejnost, tak především pro zaměstnance různých firem, kteří pracují s počítačem.

"V případě operačního systému Windows aktuálně pozorujeme vyšší zastoupení nebezpečných e-mailových příloh s českými názvy – útočníci spyware ukrývají do přiložených souborů, které vydávají za objednávky či faktury," říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET. "Domnělými odesílateli mají být také různé firmy. To pravděpodobně svědčí o tom, že útočníci v současné době cílí na firmy a organizace, kde se může takový falešný e-mail mezi řadou ostatních zpráv o objednávkách a fakturách dobře ztratit. Zaměstnanci pak mohou přehlédnout varovné signály a přílohu otevřít. Ve chvíli, kdy se škodlivý kód do firmy dostane, může být často doprovázen i dalším malwarem, a to i obávaným ransomwarem, který dokáže zašifrovat důležité firemní soubory a dokumenty. Útočníci následně požadují po napadené firmě výkupné výměnou za to, že zašifrované soubory znovu zpřístupní, nebo pod výhružkou zveřejnění interních dokumentů, které útokem získali," doplňuje Jirkal.

Agent Tesla se v květnu objevoval nejčastěji v příloze s názvem "PURCHASE ORDER.exe" a v menším počtu případů také v přílohách "Kopie oprav účtenky za 11,2021...exe" a "Zpusob_platby.jpg.exe". Spyware Formbook pak útočníci nejčastěji šířili v příloze s názvem "nákupní objednávka pdf.exe".

Nabídka od zahraniční firmy a bezchybná čeština

Malware Agent.QMG, před kterým bezpečnostní experti varovali již v dubnu, postupně ustával v útočných kampaních a v květnu byl detekován v pěti procentech případů. Nejčastěji se ukrýval v příloze s italským názvem "richiesta di offerta Pesci Attrezzature.vbs" či pod českou přílohou "Produkt nové objednávky.vbe". Útočníci e-mail vydávali za obchodní nabídku z italské firmy.

"Agent.QMG ve své útočné kampani šířil také malware GuLoader, který je poměrně obtížné rozpoznat a který má za úkol stahovat do infikovaného zařízení další škodlivé kódy, mimo jiné i spyware. Již v dubnu na sebe upozornil především tím, že útočníci při jeho šíření využívali velmi dobrou úroveň češtiny, takže uživatele již nemusely před malwarem varovat gramatické chyby," vysvětluje Jirkal.

I přestože bezpečnostní specialisté doporučují riziko v podobě malwaru Agent.QMG nepodceňovat, detekce tohoto škodlivého kódu aktuálně klesají a v následujících měsících se teprve ukáže, zda ho útočníci budou v Česku nadále využívat.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo 41 ze dne 11.7.2023

Riziko pro zaměstnance

Bezpečnostní experti opakovaně varují české uživatele před infostealery, mezi které spadá právě spyware Agent Tesla nebo spyware Formbook. Mezi ohrožené uživatele pak patří také zaměstnanci různých firem, kteří na zařízeních s operačním systémem Windows pracují a mohou ve chvílce nepozornosti otevřít nebezpečný e-mail s přílohou, která obsahuje škodlivý kód.

"Kybernetická bezpečnost a její zajištění může být především u menších firem problematická kvůli finančním nákladům. A ačkoli sledujeme, že si celá řada firem již uvědomuje, že by co nejdříve měla svou kyberbezpečnost řešit nákupem odpovídajících technologií, zaměstnanci zůstávají také jednou z oblastí, kterou je potřeba v rámci celkového zabezpečení aktivně řešit, a to bez ohledu na velikost firmy," vysvětluje Jirkal. "I přesto, že firma rizika monitoruje a využívá nějaké softwarové řešení, musí být připravena i na scénář, kdy zaměstnanec ve chvílce nepozornosti zareaguje na manipulativní e-mail, spustí přílohu a vpustí do zařízení malware, který může během několika sekund napáchat dalekosáhlé škody v celé firmě s dopadem na její běžný provoz a tím i na reputaci u zákazníků. Právě vzdělávání zaměstnanců a posilování jejich celkových vědomostí o současných kybernetických rizicích je oblast, na kterou by se měly firmy co nejdříve zaměřit," dodává Jirkal z ESETu.

Kromě používání kvalitního bezpečnostního softwaru by měli uživatelé zůstat ostražití a přistupovat se zdravou skepsí k veškeré komunikaci na internetu, zvláště, pokud je nevyžádaná nebo od neznámého odesílatele. Nezbytnou součástí celkového přístupu ke kybernetické bezpečnosti, ať už firemního či individuálního, je také přístup k informacím o nejnovější hrozbách a vzdělávání.

Nejčastější kybernetické hrozby pro operační systém Windows v České republice za květen 2023:

- MSIL/Spy.AgentTesla trojan (10,18 %)
- Win32/Formbook trojan (9,88 %)
- VBS/Agent.QMG trojan (5,62 %)
- Win32/PSW.Fareit trojan (5,35 %)
- MSIL/Spy.Agent.AES trojan (2,89 %)
- BAT/Runner trojan (2,11 %)
- WinGo/Rozena trojan (1,78 %)
- Win32/Qhost trojan (1,08 %)
- Win32/Delf.NBX virus (0,90 %)
- Java/Adwind trojan (0,90 %)

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

Zdroj: AVcentrum.cz