

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **52** ze dne **29.11.2023**

Škodlivý kód se ukrývá v žádostech nebo upozorněních na balíky.

Podle pravidelné měsíční statistiky kybernetických hrozeb pro operační systém Windows v říjnu opět mírně posílil spyware Agent Tesla. Nejsilněji na nás tentokrát útočil ze začátku měsíce. Útočníci k jeho šíření využívají e-mailové přílohy, které záměrně vydávají za různé oficiální dokumenty.

Od září bezpečnostní specialisté upozorňují na větší množství příloh, které útočníci překládají do češtiny. Nejedná se přitom o standardní situaci, protože spyware Agent Tesla je celosvětově rozšířený a útočné kampaně se objevují spíše v angličtině. Aktuálně nicméně můžeme narazit na přílohy, které mají název "děkovný dopis.docx.exe" nebo "Zpusob_platby.jpg.exe".

V říjnu se mezi nejčastějšími škodlivými kódy opět objevil také malware Agent.QMG. Ten se naopak jasně zaměřil na české uživatele. Nejvíce se v Česku objevoval na konci října.

V jeho případě jsme mohli na české překlady narazit již v samotných předmětech e-mailů. Útočníci e-maily zkoušeli vydávat například za žádost o cenovou nabídku nebo za upozornění na balíky od přepravní společnosti DHL. Z podrobnější analýzy bezpečnostní experti také zjistili, že se útočníci primárně specializují na Evropu a cílí postupně na jednotlivé státy. Kromě Česka útočili v říjnu také na Maďarsko, Španělsko, Bulharsko a Itálii.

Nebezpečné e-mailové přílohy v říjnu 2023:

- Spyware Agent Tesla - děkovný dopis.docx.exe, Zpusob_platby.jpg.exe, Inquiry_pdf.exe
- Malware Agent.QMG - 100037779694.vbe

Zdroj: Avcentrum ČR