

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **16** ze dne **23.8.2022**

Ukládání hesel do prohlížečů

Password stealer Fareit, který dokáže odcizit uživatelská hesla, se v červenci šířil přes nové verze škodlivých e-mailových příloh. V pravidelném měsíčním přehledu kybernetických hrozeb pro operační systém Windows v Česku se objevil mezi třemi nejčastějšími riziky.

V téměř pětina všech případů kybernetických hrozeb pro operační systém Windows v Česku se v červenci objevil spyware Agent Tesla. Útoky opět probíhaly především v angličtině a nejčastější škodlivá příloha byla tentokrát pojmenovaná Payment Advice OIS641PF RO_PDF.exe.

Bezpečnostní specialisté zaznamenali útočné kampaně s využitím spywaru Agent Tesla především ve dnech 7. a 11. července. Útočníci opět zneužili škodlivé přílohy s příponou .exe a v e-mailech komunikovali se svými oběťmi anglicky.

Přípona .exe

Přípona .exe označuje spustitelný soubor, který ale v případě kybernetického útoku obsahuje také škodlivý kód. Pokud uživatel takovou přílohu ze svého e-mailu otevře a spustí, spyware napadne jeho zařízení. Výsledkem je pak odcizení přístupových údajů k různým službám.

Největším rizikem je spyware pro hesla, která ukládáme do internetových prohlížečů. Webové prohlížeče totiž nejsou před těmito útoky dostatečně zabezpečené. Motivem je pro útočníky ukradená data zpeněžit – prodávají samotné přihlašovací údaje na černém trhu nebo požadují výkupné za opětovné zpřístupnění služeb.

SPYWARE FORMBOOK SE SNAŽÍ OBEJÍT BEZPEČNOSTNÍ PROGRAMY

V desetině všech případů se v červenci opět objevil spyware Formbook. Šířil se tentokrát prostřednictvím přílohy, která měla název IUMh2If0uRXe0K7.exe. Nezvykle pojmenovaná příloha na sebe upozornila také bezpečnostní specialisty.

Útočníci se nás ve svých kampaních prozatím vždy snažili přesvědčit, že sdělení e-mailu je opravdové a týká se nějaké reálné situace. To také potvrzovaly názvy příloh jako objednávka, účtenka nebo faktura. Varovat nás poté mohla právě angličtina, nebo když útočníci nepoužili správně češtinu. Červencová příloha ale ukazuje na to, že útočníci pravděpodobně mění strategii. Už nás primárně nepřesvědčují k tomu, abychom škodlivou přílohu otevřeli. Snaží se spíše obejít antivirové programy.

FAREIT NEÚTOČÍ VE VELKÉM, V ČESKU JE ALE NEJVĚTŠÍM RIZIKEM

Password stealer Fareit byl v červenci detekován jen v necelých pěti procentech případů, jako jediný se však cíleně zaměřil na české uživatele.

Největší útočné kampaně měl Fareit tentokrát 7. a 11. července. Během těchto útoků se objevily nové mutace škodlivých příloh v češtině s názvy Produkty_objednany_P.O_4704526-doc.exe nebo Objednávka_P.O.52204962_EXIM-TECH.exe. I když se password stealer Fareit objevuje v menším počtu případů, počet e-mailů v češtině zatím každý měsíc roste.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **16** ze dne **23.8.2022**

Password stealer Fareit dokáže odcizit hesla nejen z internetových prohlížečů, ale také z chatovacích aplikací, e-mailu nebo služeb jako VPN či FTP.

Nebezpečné e-mailové přílohy v červenci 2022:

- Spyware Agent Tesla
- Payment Advice OIS641PF RO_PDF.exe
- Spyware Formbook
- IUMh2If0uRXeOK7.exe
- Password stealer Fareit
- Produkty_objednany_P.O_4704526-doc.exe
- Objednávka_P.O.52204962_EXIM-TECH.exe

JAK ÚČINNĚ CHRÁNIT SVÉ PŘIHLAŠOVACÍ ÚDAJE?

Bezpečnostní specialisté opakovaně doporučují věnovat pozornost jak tvorbě silných hesel, tak jejich bezpečné správě.

Každé heslo bychom měli využívat pouze pro jednu konkrétní online službu, měli bychom mít tedy unikátní heslo pro svůj e-mail, internetové bankovníctví nebo pro každý účet na sociálních sítích. Heslo by také mělo být dostatečně složité a obsahovat nejméně deset různých znaků, jako jsou malá a velká písmena, číslice a speciální znaky, pokud to služba, ke které heslo vytváříme, umožňuje. Svá hesla bychom neměli nikam zapisovat. Pokud si je nepamatujeme, je vhodným nástrojem pro jejich ukládání správce hesel.

Správce hesel je specializovaný program, který ukládá hesla v zašifrované podobě a automaticky dané heslo vyplní při našem přihlašování do zvoleného online účtu. Musíme si tak pamatovat pouze jediné heslo, a to pro přístup do něj. Správce hesel lze pořídit samostatně nebo jako součást kvalitního bezpečnostního programu.

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

1. MSIL/Spy.AgentTesla trojan (18,65 %)
2. Win32/Formbook trojan (9,33 %)
3. Win32/PSW.Fareit trojan (4,71 %)
4. MSIL/Spy.Agent.AES trojan (3,22 %)
5. Win32/Agent.TJS trojan (2,43 %)

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **16** ze dne **23.8.2022**

6. VBS/Agent.QDF trojan (2,42 %)
7. VBS/Agent.QEG trojan (2,30 %)
8. MSIL/Spy.Agent.DFY trojan (1,44 %)
9. BAT/CoinMiner.AUB trojan (1,03 %)
10. VBS/Agent.QEN trojan (0,89 %)

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

Zdroj: ESET