

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **27** ze dne **9.2.2023**

Infostealery zůstanou rizikem pro uživatelská hesla také v letošním roce

V prosincových datech společnosti ESET pro Českou republiku zůstaly na předních místech hlavní škodlivé kódy pro operační systém Windows, se kterými se uživatelé mohli setkávat celý uplynulý rok – spyware Agent Tesla a spyware Formbook. Ačkoli počet detekcí u obou škodlivých kódů jen mírně překročil desetinu všech případů, podle bezpečnostních expertů potvrdil a nastínil vývoj i v letošním roce, kdy se podle jejich očekávání útočníci zaměří na úroveň používané češtiny a stabilní škodlivé kódy doplní zcela nové útoky dosud spíše okrajových rodin malwaru. Vyplývá to z pravidelné statistiky společnosti ESET.

Poslední data společnosti ESET z prosince loňského roku potvrdila stávající převahu všech dlouhodobě přítomných škodlivých kódů pro operační systém Windows v Česku. Ačkoli u spywaru Agent Tesla počet detekcí oproti listopadu v prosinci klesl, bezpečnostní specialisté považují situaci i pro následující rok za stabilní a nepředpokládají, že by nějaký typ dlouhodobě detekované malwaru z českého prostředí zcela vymizel.

„Zhruba v posledním půl roce se situace v České republice stabilizovala na třech rodinách malwaru a pro příští rok očekáváme, že se situace nebude výrazně měnit. Výjimkou může být samozřejmě nástup nových rodin. Již v tuto chvíli ve statistice pozorujeme například rodinu malwaru RedLine Stealer, která aktuálně získává na popularitě na černém trhu. Počítáme také s tím, že se během roku 2023 objeví měsíce, kdy se útočníci i v rámci celosvětových kampaní zaměří na Česko s do češtiny lokalizovaným spamem. Infostealery, kam spadají právě spywary a password stealery, zkrátka zůstanou pro české uživatele primárním rizikem,“ říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Nebezpečné e-maily s přílohami budou útočníci stále zlepšovat

Spyware Agent Tesla a spyware Formbook se v prosinci objevily v téměř shodném počtu detekcí, který přesahoval desetinu všech zachycených případů. Spyware Agent Tesla se objevoval spíše v rámci celosvětových kampaní, útoky v češtině byly ale v prosinci také poměrně silné. Nebezpečné přílohy v e-mailech se tentokrát jmenovaly NPO-2212-000016.pdf.exe, Zpusob_platby, jpg.exe a Poptavka 00413_pdf.exe. U spywaru Formbook poté útočníci vsadili na sezónu mezi svátky a spyware šířili prostřednictvím příloh, které vydávali za dokumenty k platbám dovolených. Zde se však útoky v češtině neobjevily.

„Jedním z důvěryhodných ukazatelů, že by s příchozí komunikací nemuselo být vše v pořádku, stále zůstává čeština. Pro útočníky, kteří zpravidla nejsou rodilými mluvčími, je zkrátka komplikovaná a ani různé překladače vždy nepřeloží text správně,“ vysvětluje Jirkal. „Přesto můžeme počítat s tím, že jak se škodlivé kódy neustále vyvíjejí do propracovanějších verzí, mohou útočníci investovat také do věrohodnějších jazykových překladů. V posledních týdnech se velmi zvedla diskuze také o generování spamu za pomoci algoritmů umělé inteligence. Tam ale předpokládáme, že bude v následujících letech převažovat hlavně angličtina a do češtiny bude text překládán spíše strojově,“ doplňuje Jirkal.

Zhruba v pěti procentech všech případů byl v prosinci detekován také backdoor Agent.AES, který se v počtu detekcí s mírným nárůstem dostal před password stealer Fareit. V jeho případě se uživatelé mohli nejčastěji setkat s přílohami Drawing & Specifications____JPG.exe nebo kopie platby09886673.exe.

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **27** ze dne **9.2.2023**

Spam prozradí gramatické chyby

Uživatelé před útoky infostealerů spolehlivě ochrání moderní bezpečnostní řešení. Premiové verze bezpečnostních softwarů navíc často obsahují i tzv. správce hesel, specializované programy, které ukládají hesla v zašifrované podobě a automaticky heslo doplní v případě přihlášení do konkrétního online účtu. Uživatelé si pak pamatují jen jedno heslo, a to právě pro přihlášení do této služby. Správci hesel jsou bezpečnější alternativou k ukládání hesel do internetových prohlížečů, které nejsou před útoky infostealerů dostatečně chráněné.

Vedle kvalitního antivirového řešení pak bezpečností experti apelují na opatrnost uživatelů při práci s příchozí elektronickou komunikací. E-mailové účty totiž stále patří mezi přední cíle různých podvodných nabídek a výzev.

„Na podvodných e-mailových přílohách, které šíří spyware, jasně vidíme záměr útočníků – snaží se v uživateli vyvolat dojem, že příloha je legitimním dokumentem k jeho platbám a objednávkám. Využívají tak i v případě šíření spywaru manipulaci, kterou dobře známe z phishingových útoků, jejichž objem stále roste také v Česku a vyrovnají se pomalu útokům škodlivým kódem,“ říká Jirkal z ESETu a dodává: „Uživatelé by v příchozí komunikaci, a to nejen v e-mailu, měli věnovat pozornost adrese odesílatele, správnosti češtiny a nikdy by v takové zprávě neměli otevírat soubory nebo klikat na odkazy.“

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

- Win32/Formbook trojan (13,13 %)
- MSIL/Spy.AgentTesla trojan (11,15 %)
- MSIL/Spy.Agent.AES trojan (4,62 %)
- Win32/PSW.Fareit trojan (2,89 %)
- Win32/Rescoms trojan (1,98 %)
- VBS/Agent.QMG trojan (1,73 %)
- MSIL/Spy.RedLine trojan (1,49 %)
- Win32/PSW.Agent.ONW trojan (0,93 %)
- Java/Adwind trojan (0,87 %)
- Win32/Spy.VB.OLN trojan (0,85 %)

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

Zdroj: ESET