

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **34** ze dne **18.4.2023**

Útočníci zkouší v Česku šířit spyware přes poznámkové soubory programu OneNote

Kromě osvědčené strategie v podobě nebezpečných e-mailových příloh, kterými byla v únoru také domnělá potvrzení k dovozeným, zkouší útočníci obcházet zabezpečení novými metodami.

Ačkoli se počet detekcí všech dlouhodobě přítomných škodlivých kódů pro operační systém Windows v Česku zatím nemění, bezpečnostní experti zachytili v únoru nebývale silný útok na české uživatele. Detekovanými škodlivými kódy byly tentokrát kromě spywaru Agent Tesla také spyware Formbook a downloader Agent.PLI, který útočníci šířili prostřednictvím škodlivých skriptů v poznámkových souborech programu OneNote. Vyplyvá to z pravidelné statistiky kybernetických hrozeb od společnosti ESET.

Spyware Agent Tesla se v únoru ve statistice společnosti ESET objevil opět ve zhruba 15 procentech všech případů. Tentokrát byl aktivní především závěrem měsíce a nejrozšířenější škodlivá e-mailová příloha, jejíž prostřednictvím se šířil, se jmenovala "IMG_Evaluate_AWB_HBL & CHECKLIST Docs..exe". Na rozdíl od spywaru Agent Tesla ale bezpečnostní specialisté zaznamenali silné útoky 21. února, a to v případě obou dalších nejčastěji detekovaných škodlivých kódů.

"Spyware Formbook, jeden z malwarů, které jsme v rámci silného únorového útoku objevili, se šířil přes e-mailovou přílohu s názvem Booking Details!!..exe. Předpokládáme tak, že cílem spywaru byli uživatelé, kteří již v těchto měsících začali objednávat dovolené. Dalším typem útočícího malwaru byl Agent.PLI. Zde vidíme nový trend v útočných kampaních – zasílání poznámkových dokumentů programu OneNote, které obsahují škodlivé skripty. Agent.PLI se nejčastěji objevoval jako sdílený dokument s názvem Invoice 575367.bat. Tuto metodu útočníci zkouší pravděpodobně kvůli zpřísňujícím se pravidlům pro posílání e-mailových příloh, a hledají možnosti, jak toto omezení obejít," vysvětluje Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Přílohy a dokumenty s příponami .exe. nebo .bat označují typy spustitelných programů v operačním systému Windows. Bezpečnostní experti upozorňují uživatele, aby takové programy nikdy nespouštěli, pokud si nejsou jisti jejich původem, obsahem a funkcionalitami.

Místo přílohy v e-mailu sdílené poznámky OneNote

Bezpečnostní specialisté opakovaně upozorňují, že útočníci budou mít letos velký zájem přehodnocovat současné strategie a investovat do nových typů útoků.

"Přestože útoky s použitím programu OneNote aktuálně slábnou a zdá se tedy, že úspěšné nebyly, princip této strategie se určitě může znovu objevit," říká Jirkal. *"Celkově byl útok velmi jednoduchý. V poznámkovém dokumentu s příponou .one bylo vloženo několik škodlivých .bat skriptů, které byly překryty obrázkem. Obrázek nabádal uživatele ke kliknutí a otevření dokumentu. Kliknutím na tento obrázek se spustil jeden ze škodlivých skriptů, který začal stahovat do zařízení další malware, nejčastěji z rodin Qbot, Icel, AgentTesla nebo RedLine,"* dodává Jirkal z ESETu.

Infostealery, mezi které nejčastěji detekované škodlivé kódy v operačním systému Windows spadají, jsou aktuálně jednou z největších hrozeb v Česku. Kybernetičtí útočníci je používají ke krádeži osobních dat uživatelů, a to nejčastěji uživatelských hesel. Nejvíce zranitelná jsou pak hesla ukládaná do internetových

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **34** ze dne **18.4.2023**

prohlížečů, které nejsou před útoky spywaru dostatečně zabezpečené. Bezpečnostní specialisté tak uživatelům doporučují využívat tzv. správce hesel, programy, které hesla ukládají v zašifrované podobě. Správce hesel bývají také součástí kvalitních bezpečnostních programů, které uživatele před spywarem spolehlivě ochrání.

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

- MSIL/Spy.AgentTesla trojan (15,14 %)
- Win32/Formbook trojan (9,61 %)
- BAT/Agent.PLI trojan (3,54 %)
- Win32/PSW.Fareit trojan (1,96 %)
- MSIL/Spy.Agent.AES trojan (1,95 %)
- Win32/Shafmia trojan (1,43 %)
- BAT/Runner trojan (1,22 %)
- MSIL/Disdroth trojan (1,17 %)
- MSIL/Spy.RedLine trojan (1,15 %)
- Win32/Warzone trojan (1,01 %)

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

Zdroj: ESET