# Kaspersky varuje malé a střední firmy: útočníci maskují malware za ChatGPT i Zoom

**25.6.2025 - | PROTEXT**

**Analytici společnosti Kaspersky zkoumali na vzorku 12 online aplikací pro zvyšování produktivity, jak často je škodlivý a nežádoucí software „přestrojen“ za legitimní aplikace běžně používané malými a středními firmami. V roce 2025 zaznamenali zatím více než 4000 unikátních nebezpečných souborů maskovaných jako populární aplikace. S rostoucí popularitou služeb umělé inteligence kyberzločinci stále častěji maskují malware také jako AI nástroje. Kybernetické hrozby napodobujících ChatGPT vzrostly v prvních čtyřech měsících roku 2025 ve srovnání se stejným obdobím loňského roku o 115 % a dosáhly počtu 177 unikátních nebezpečných souborů. Další populární AI nástroj DeepSeek byl zneužit v 83 souborech. Tento rozsáhlý jazykový model byl spuštěn v roce 2025 a hned se objevil i na seznamu imitovaných nástrojů.**

"*Je zajímavé, že aktéři útoků jsou při výběru AI nástrojů jako návnady dost vybíraví. Nebyly například pozorovány žádné škodlivé soubory napodobující Perplexity. Pravděpodobnost, že útočník použije nějaký nástroj jako krytí pro malware nebo jiné typy nežádoucího softwaru, je přímo závislá na jeho popularitě a hodnocení. Čím více se o něm mluví a čím větší je jeho publicita, tím větší je pravděpodobnost, že uživatel na internetu narazí na falešný balíček. Zaměstnanci malých a středních firem, stejně jako běžní uživatelé, by proto měli být v zájmu bezpečnosti při hledání softwaru opatrní a pečlivě zkoumat nabídky předplatného, které jsou až příliš lákavé na to, aby to byla pravda. Měli by věnovat pozornost například správnosti pravopisu na webových stránek a odkazům v podezřelých e-mailech. V mnoha případech může jít o phishing nebo odkazy, které způsobí stažení škodlivého či potenciálně nežádoucího softwaru*," říká **Vasilij Kolesnikov**, bezpečnostní expert společnosti Kaspersky.

Další taktikou kyberzločinců, na kterou je třeba nyní dávat pozor, je rostoucí zneužívání značek platforem pro usnadnění spolupráce, které má přimět uživatele ke stažení nebo spuštění malwaru. Počet škodlivých a nežádoucích softwarových souborů maskovaných jako aplikace Zoom se v roce 2025 zvýšil o téměř 13 % (1652 výskytů), zatímco názvy jako "Microsoft Teams" a "Google Drive" zaznamenaly nárůst o 100 % (206 výskytů) respektive 12 % (132 výskytů). Tento trend pravděpodobně souvisí s rozšířením práce na dálku a spolupráce geograficky rozptýlených týmů, čímž se tyto platformy staly nedílnou součástí firemních operací napříč odvětvími.

Nejvyšší počet souborů v analyzovaném vzorku byl maskován jako Zoom, což představuje téměř 41 % všech unikátních detekovaných souborů. Častým cílem napodobování jsou nadále aplikace Microsoft Office: na Outlook a PowerPoint připadalo shodně 16 % případů, na Excel téměř 12 %, na Word 9 % a na Teams 5 %.

**Phishing a spam**

Kromě hrozeb ze strany malwaru společnost Kaspersky nadále sleduje širokou škálu phishingových a podvodných schémat zaměřených na malé a střední firmy. Útočníci se snaží ukrást přihlašovací údaje k různým službám - od doručovacích platforem až po bankovní systémy - nebo pomocí podvodných taktik zmanipulovat oběti tak, aby jim poslaly peníze. Jedním z příkladů je pokus o phishing zaměřený na účty služby Google. Útočníci slibují potenciálním obětem zvýšení prodeje pomocí inzerce jejich společnosti na síti X, skutečným cílem je však ukrást jejich přihlašovací údaje. Kromě phishingu jsou malé a střední firmy zaplaveny spamovými e-maily, nově také s tematikou AI,

například s nabídkami na automatizaci různých provozních procesů.

Společnost Kaspersky pozoruje phishingové a spamové nabídky, které odrážejí typické potřeby malých firem. Slibují atraktivní podmínky e-mailového marketingu, půjček nebo služeb, jako je správa reputace, tvorba obsahu, získávání obchodních kontaktů apod.

Další informace o kybernetických hrozbách pro malé a střední firmy najdete na webu Securelist. Pro zmírnění hrozeb namířených proti firmám se jejich majitelům a zaměstnancům doporučuje přijmout následující opatření:

https://www.ceskenoviny.cz/tiskove/zpravy/kaspersky-varuje-male-a-stredni-firmy-utocnici-maskuji-malware-za-chatgpt-i-zoom/2690909