Národní úřad pro kybernetickou bezpečnost varuje před zneužitím aplikace OneNote, stahují malware

- CZ24 News | 16. února 2023

ČESKO: Národní úřad pro kybernetickou bezpečnost (NÚKIB) varuje před zneužíváním e-mailových příloh aplikace OneNote společnosti Microsoft. Roste počet případů, kdy útočníci těmito přílohami maskují škodlivý soubor, takzvaný malware, který útočníkovi umožní vzdálený přístup do napadeného počítače. NÚKIB o tom informoval v tiskové zprávě.

“K úspěšnému zneužití potřebuje útočník interakci oběti: po otevření e-mailu a přílohy OneNote je zobrazen rozostřený dokument s velkým nápisem ‘Double Click To View File’, který vizuálně překrývá škodlivé soubory,” uvedl úřad. Poté, co příjemce na oznámení dvakrát klikne, zobrazí se varování, které ale většina lidí ignoruje a potvrdí, že chce pokračovat. Tímto potvrzením jsou soubory spuštěny.

“Společnost Proofpoint zabývající se kybernetickou bezpečností eviduje za leden letošního roku více než 50 různých útočných kampaní. Tyto kampaně zahrnují tisíce e-mailů bez specifičtějších cílů v Evropě a Severní Americe, které zpravidla zneužívají běžná témata jako jsou daně, vyzvednutí zásilky, faktury a podobně. K nejčastěji staženým malware patří AsyncRAT, Quasar RAT, Redline a Xworm,” doplnil úřad.

Microsoft už loni snahy o zneužití své aplikace řešil, nyní ale útočníci přišli s novým typem útoku. Podle NÚKIB je pravděpodobné, že nový postup zneužití příloh OneNote si bude postupně osvojovat stále více útočníků. Aby uspěli a ovládali napadený počítač, potřebují ale součinnost příjemce počítače. Ten se tak napadení může bránit tím, že bude maximálně opatrný při otevírání jakýchkoliv příloh na svých zařízeních.

ZDROJ: NÚKIB / ČTK /