Kliknutí, které se nevyplácí. Takto se v počítači zabydlí malware

novinky.cz/clanek/internet-a-pc-bezpecnost-kliknuti-ktere-se-nevyplaci-takhle-se-v-pocitaci-zabydli-malware-40422950

„Poté, co v červenci 2022 Microsoft zablokoval v základním nastavení spuštění tzv. maker a učinil tím metodu spuštění kódu přes makra neefektivní, přišli nyní útočníci s novým typem útoku," varovali bezpečnostní experti z NÚKIB.

Podle nich k úspěšné infiltraci škodlivého kódu útočníkům stačí, aby otevřeli přílohu v e-mailu, na které je vyobrazen rozostřený dokument v aplikaci OneNote s velkým nápisem „Double Click To View File", tedy dvakrát klikněte pro zobrazení dokumentu.

Tento vizuál ale ve skutečnosti překrývá škodlivé soubory. Pokud tedy důvěřivci v podobných zprávách skutečně kliknou, vpustí si tím do svého počítače nezvané návštěvníky.

Podvody na internetu tvoří téměř dvě třetiny kyberzločinů

Internet a PC

Co je phishing?

Internetoví podvodníci často rozesílají e-maily, které vyvolávají dojem, že pocházejí od důvěryhodné firmy, banky, úřadu nebo webové stránky.

Pomocí těchto zpráv se útočníci snaží vylákat citlivé informace, které se týkají například bankovních kont. Tato data následně využívají k odčerpání financí z účtu postiženého.

Více než 50 různých útočných kampaní

„Útočníci tímto způsobem zneužívají funkcionality OneNote, která po spuštění souboru dovolí aktivovat skript, který stáhne malware zajišťující vzdálený přístup útočníka," popsali scénář útoku bezpečnostní experti.

Kyberbezpečnostní společnost Proofpoint zachytila jen v uplynulém měsíci 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 apod. K nejčastěji staženým malware patří AsyncRAT, Quasar RAT, Redline a Xworm.

„Je pravděpodobné, že trend zneužití OneNote příloh si bude osvojovat stále více útočníků. Jelikož je k úspěšnému útoku zapotřebí zapojení příjemce e-mailu, nejúčinnějším způsobem boje je, stejně jako u jiných podobných kampaní, informovat a poučit uživatele o probíhající kampani a vyzvat je k hlášení podezřelých příloh správci systému. Také v tomto případě platí, že uživatelé by měli být opatrní a maximálně obezřetní na to, jaké přílohy stahují či otevírají ve svých zařízeních," varovali pracovníci úřadu.

Desatero bezpečného internetu

1. Důležité jsou pravidelné aktualizace celého počítače. Ty je nutné stahovat pro operační systém, bezpečnostní bránu (firewall), antivirus i další programy.

2. Některé viry dokážou bezpečnostní software v PC zablokovat. Proto je vhodné pravidelně kontrolovat, zdali funguje.

3. Škodlivé programy se často šíří prostřednictvím nevyžádané pošty. Pokud nevíte, od koho e-mail je, nikdy nestahujte jeho přílohu a neklikejte na žádné odkazy.

4. Pozor je nutné dávat na e-maily, v nichž odesílatel požaduje, abyste se přihlásili na nějakou webovou stránku a aktualizovali informace o vašem účtu.

5. Při zadávání přístupových hesel na internetových stránkách je nutné kontrolovat, zda je web zabezpečený. To poznáte například podle ikonky zámečku na liště internetového prohlížeče nebo tak, že adresa webové stránky začíná zkratkou https, kde „s“ znamená bezpečná.

6. Citlivé osobní informace zadávejte vždy pouze na internetových stránkách, které bezpečně znáte.

7. Do e-mailů nepatří důvěrné informace, jako je například číslo kreditní karty nebo heslo k bankovnímu účtu. Elektronickou poštu totiž může zachytit útočník.

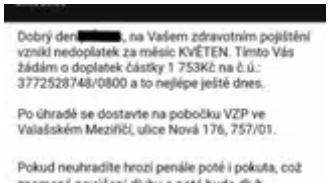
8. Firewall dovoluje lépe zabezpečit operační systém. Méně zkušení uživatelé by jej rozhodně neměli vypínat. Při nedostatečných znalostech je vhodné jej nechat pracovat v automatickém režimu.

9. V internetových kavárnách a na cizích počítačích se nepřihlašujte do internetového bankovnictví. V počítači mohou být nainstalované keyloggery.

10. Obezřetnost je nutná při připojení k nezašifrovaným bezdrátovým sítím. Ty totiž může kdokoliv odposlouchávat a získat tak přístup ke všem datům v cizím počítači.

Splaťte dluh na pojistném, zkoušejí to podvodníci v e-mailech na klienty VZP

Domácí


Dobrý den [redacted], na Vašem zdravotním pojištění vznikl nedoplatek za měsíc KVĚTEN. Tímto Vás žádám o doplatek částky 1 753Kč na č.ú.: 3772528748/0800 a to nejlépe ještě dnes.

Po úhradě se dostavte na pobočku VZP ve Valašském Meziříčí, ulice Nová 176, 757/01.

Pokud neuhradíte hrozí penále poté i pokuta, což