Vzestup quishingu je alarmující, bijí na poplach bezpečnostní experti

novinky.cz/clanek/internet-a-pc-bezpecnost-vzestup-quishingu-je-alarmujici-biji-na-poplach-bezpecnostni-experti-40455557

Barbora Růžičková

Internetoví podvodníci neustále hledají cesty, jak napálit důvěřivce. Často k tomu využívají phishing – 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.

Malware StripedFly má na kontě přes milion obětí. V tichosti útočil roky

Nárůst o 578 procent

Prakticky na stejném principu funguje také quishing, základem takového phishingového útoku je však QR kód. Bezpečnostní experti Check Pointu varovali, že jen na přelomu léta a podzimu došlo k nárůstu podvodů využívajících QR kódy o rekordních 578 procent.

Plnovousem dnes už nikoho nepřekvapíte, na scénu se vrací knír

Seznam Native

Útočníci zneužívají toho, že se QR kódy staly v dnešní rychlé době velmi populární. „QR kód sám o sobě vypadá neškodně a snadno se za něj skryje škodlivý úmysl. Pokud není původní obrázek naskenován, bude vypadat jen jako obyčejný obrázek. Navíc vytvořit QR kód je velmi snadné, existuje spousta bezplatných stránek, které s tím pomohou," konstatoval Petr Kadrmas, bezpečnostní expert Check Pointu.

„Za QR kódy se většinou skrývá odkaz. Hackeři, nebo kdokoli jiný, mohou tímto odkazem uživatele přesměrovat například na stránku, jejímž cílem jsou krádeže přihlašovacích údajů," podotkl Kadrmas.

Zároveň popsal i jeden ze zachycených případů, který zneužívá značku Microsoft. „Záminkou může být, že vypršela platnost vícefaktorového ověřování společnosti Microsoft a je třeba vše znovu ověřit. Ačkoli je ve zprávě uvedeno, že pochází od oddělení zabezpečení společnosti Microsoft, adresa odesílatele je jiná," popsal průběh podvodu bezpečnostní expert.

„Jakmile však uživatel naskenuje QR kód, bude přesměrován na stránku, která vypadá jako stránka společnosti Microsoft, ale ve skutečnosti je to jen stránka pro sběr přihlašovacích údajů," doplnil Kadrmas.

Co je QR kód?

QR kódy se na první pohled výrazně neliší od obyčejného čárového kódu. Obsahuje ale daleko více informací, které mohou využít především mobilní telefony při přístupu na internet. Všechny informace z kódu získáte velice jednoduše pouhým přiložením fotoaparátu ke QR značce. Za QR kódy se většinou skrývá odkaz na webové stránky.

Nové taktiky a techniky

Podle něj budou hackeři vždy zkoušet „nové taktiky a techniky a budou se snažit zneužívat i běžně používané věci“, jako jsou například i QR kódy. Rozšířenost QR kódů je v dnešní době masivní a málokoho by patrně napadlo, jak snadno zneužitelné mohou být.

Kyberšmejdi se s quishingem zaměřovali prozatím především na zahraniční uživatele. S ohledem na množství zachycených podvodů je ale patrně jen otázkou času, než budou stejné phishingové podvody zkoušet i v tuzemsku. Uživatelé by se tedy měli mít při používání QR kódů na pozoru.

Podvodníci si hrají na novináře

Uživatelé by se měli mít na pozoru před různými investičními podvody, ve kterých útočníci zneužívají jméno zpravodajského serveru Novinky.cz. Na snadné výdělky lákají podvodníci zpravidla v souvislosti se známými osobnostmi. V posledních měsících se objevily například falešné články s prezidentem Petrem Pavlem či moderátorem Janem Krausem.

Jde nicméně o typický phishingový podvod, kdy se útočníci snaží pod vidinou snadného zisku ve skutečnosti z lidí vylákat peníze. Podvod je to ale poměrně propracovaný, všechny odkazy ve falešném článku vedou na další podvodný web.

Aby důvěřivce kyberzločinci co nejvíce zmátli, nechtějí po něm v některých případech vyplňovat okamžitě čísla kreditních karet ani odesílat žádné peníze. Vše začíná registrací na dané platformě, načež uživatele bude kontaktovat správce platformy. Teprve s jeho pomocí jsou pak z důvěřivců vylákány peníze. Nemusí ho přitom kontaktovat pouze e-mailem, ale klidně i telefonicky.

Poradíme, na co si dát pozor a jak nesednout podvodníkům na lep, a to v dříve uveřejněném článku.

Foto: Novinky

+4

Vishing, smishing a phishing. Podvodů přibylo, varují bezpečnostní experti