E-Bezpečí 2024, 9(1): Page 70-72. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=3999

NEVIDITELNÝ ÚTOK: HOMOGLYFY A HOMOGRAFY JAKO ZBRANĚ KYBERZLOČINCŮ

Kamil KOPECKÝ

Použití homoglyfů a homografů pro kybernetické útoky (především různé druhy online podvodů) je technika, která je záludná a může oklamat i zkušené uživatele. V našem článku popisujeme, jak tato taktika funguje, jak ji útočníci využívají a jak se lze proti ní bránit.

Jak útoky fungují:

Homoglyfy: Tyto znaky vypadají téměř stejně jako jiné znaky, například "a" (cyrilice) místo "a" (latinka). Útočník vytvoří doménu, která vizuálně odpovídá skutečnému webu, ale využívá podobné znaky z jiného písma. Uživatel si rozdílu nemusí všimnout, a po přihlášení předá své přihlašovací údaje útočníkovi.

ZNAKY A JEJICH ASCII KÓD V LATINCE

ČERVENĚ OZNAČENÉ ZNAKY JSOU ZAPSÁNY CYRILICÍ
(LIŠÍ SE KÓDEM ZNAKU)

Homografy: Technika homografů využívá více znaků s podobným zápisem. Například „paypal.com“ a „paypal.com“ mohou vypadat stejně, ale druhá varianta používá jiné znaky z cyrilice. Při kliknutí na tuto verzi webové adresy je uživatel přesměrován na falešnou stránku, která sbírá citlivé informace.

ZNAKY A JEJICH ASCII KÓD V LATINCE

ZNAKY A JEJICH ASCII KÓD V LATINCE

Možností, jak lze zneužít tyto záměny znaků či slov, je skutečně mnoho - od phishingového útoku odkazujícího na podvodné stránky, přes sociální inženýrství apod.

Závěr

Útoky využívající homoglyfy a homografy dokazují, že kybernetická

bezpečnost je velmi komplexní a dynamickou oblastí, ve které musí být jednotlivci i organizace neustále ve střehu. Útočníci neustále vylepšují své taktiky, aby oklamali i ty nejzkušenější uživatele. Proto je klíčové pochopit, že ochrana před takovými hrozbami vyžaduje víceúrovňový přístup. Jedinci i společnosti mohou účinně snížit riziko úspěšného phishingového útoku kombinací několika strategií.

Povědomí: Uživatelé by měli být informováni o hrozbách a způsobech útoků, aby mohli být lépe připraveni rozpoznat podezřelé aktivity. Školení zaměstnanců v oblasti kybernetické bezpečnosti nebo vedení osvětových kampaní pro veřejnost zvyšuje obecnou úroveň bdělosti a umožňuje identifikovat potenciální útoky.

Technická opatření: Organizace by měly implementovat vhodné technologie, jako jsou antiphishingové filtry, šifrování dat a vícefaktorové ověřování, aby se snížila pravděpodobnost, že budou útočníci úspěšní. Důležité je také používat pravidelně aktualizovaný antivirový software a udržovat software obecně aktuální.

Bezpečnostní návyky: V neposlední řadě by měli uživatelé zavést do praxe bezpečnostní návyky, jako je ruční zadávání URL adres, kontrola certifikátů na webových stránkách nebo nedůvěra k podezřelým e-mailům od neznámých odesílatelů. Zároveň je důležité vždy ověřovat autenticitu zpráv od známých institucí.

Kombinací těchto tří složek lze výrazně zlepšit obranu před hrozbami homoglyfových a homografových útoků a posílit celkovou úroveň kybernetické bezpečnosti.

Pro E-Bezpečí
Kamil Kopecký
Univerzita Palackého v Olomouci