Kyberzločinci zneužívají elektronický podpis: jak nenaletět podvodným e-mailům

17.10.2024 - | PROTEXT

Útok začíná e-mailem, který je obvykle vytvořen tak, aby se podobal legitimní komunikaci služby Docusign. V tomto konkrétním schématu se podvodníci obvykle neobtěžují pečlivě falšovat nebo maskovat adresu odesílatele, protože díky možnostem přizpůsobení služby mohou pravé e-maily Docusign pocházet z jakékoli adresy.

Jak funguje phishing napodobující Docusign

Ve většině případů je oběť upozorněna, že musí elektronicky podepsat nějaký dokument, obvykle finanční, jehož přesný účel není z textu e-mailu zcela zřejmý.

V některých případech používají phisheři další trik, o kterém jsme psali už dříve v samostatném příspěvku – e-mail obsahuje PDF přílohu s QR kódem.

Oběť je vyzvána k naskenování tohoto QR kódu, který má údajně zpřístupnit dokument k podpisu. QR kód však vede ve skutečnosti na podvodnou webovou stránku. Tato metoda má přimět uživatele, aby škodlivý odkaz neotevřeli na počítači, ale na chytrém telefonu, kde jsou phishingové adresy URL hůře odhalitelné a kde nemusí být nainstalován bezpečnostní software.

Někdy se e-mail o službě Docusign vůbec nezmiňuje. V jedné z verzí podvodu s PDF obsahujícím QR kód, který jsme nedávno probírali v článku zaměřeném na techniky spearphishingu v hromadných e-mailech, je služba Docusign zmíněna pouze v připojeném PDF dokumentu.

Někdy si kyberzločinci dají záležet na tom, aby napodobili vzhled legitimního e-mailu služby Docusign, doplněného bezpečnostním kódem v zápatí e-mailu.

V některých případech podvodníci napodobují integraci služby Docusign se službou Microsoft SharePoint.

Stručně řečeno, taktiky a kvalita provedení se mohou e-mail od e-mailu lišit. Základní princip však zůstává stejný – podvodníci spoléhají na to, že příjemce neví, jak elektronické podepisování pomocí služby Docusign vlastně funguje.

Nepozorná oběť přejde přes odkaz (nebo QR kód) na phishingovou stránku a zadá svoje přihlašovací údaje zaměstnance, které se tak dostanou přímo k útočníkům.

Uživatelská jména a hesla získaná při úspěšných phishingových útocích se často shromažďují v databázích, prodávána na nelegálních tržištích dark webu a později využívána k útokům na organizace.

Jak e-podpis pomocí služby Docusign skutečně funguje

Samotný proces podepisování dokumentu pomocí služby Docusign je pro běžného uživatele velmi jednoduchý. Od strany, která žádá o podpis, obdržíte e-mail s velkým žlutým tlačítkem **Review Document**, které nelze přehlédnout.

Kliknutím na toto tlačítko budete přesměrováni prostřednictvím jedinečného odkazu na webové

stránky Docusign (na doméně docusign.net). Na stránce, která se otevře, se zobrazí krátká zpráva od iniciující strany a vedle ní tlačítko Continue, stejně velké a žluté.

Dokument k podpisu je k dispozici okamžitě, bez zadávání hesel. Jednoduše si jej prohlédnete, případně doplníte některé údaje (například jméno, datum a podobně) do příslušných polí, připojíte svůj podpis a kliknete na tlačítko Finish (které je, hádáte správně, také velké a žluté). To je vše. Nic jiného není zapotřebí.

Co Docusign NIKDY nedělá:

Pamatujte, že smyslem služby Docusign je co nejvíce usnadnit firmám i jednotlivcům výměnu elektronicky podepsaných dokumentů.

Jakékoli další kroky nebo omezení, například vytváření účtu, zadávání přihlašovacích údajů, otevírání příloh nebo nutnost používat k podepisování chytrý telefon, jsou v rozporu s touto zásadou. Proto Docusign nic z toho nevyžaduje a snaží se, aby byl proces podepisování co nejrychlejší a nejjednodušší.

Jak se chránit před phishingem

Chcete-li svoji organizaci chránit před phishingovými útoky, které napodobují Docusign a další populární služby, zvažte následující opatření:

ČTK Connect ke zprávě vydává obrazovou přílohu, která je k dispozici na adrese https://www.protext.cz.

https://www.ceskenoviny.cz/tiskove/zpravy/kyberzlocinci-zneuzivaji-elektronicky-podpis-jak-nenaletet-podvodnym-e-mailum/2583480