Co vám řekne délka URL adresy o její bezpečnosti? 5 tipů, jak nebezpečnou URL adresu rozpoznat.

Brno, 22.9. 2020 **– Zářijový Security Cloud report vydaný společností Wandera se věnuje stále aktuálnímu tématu phishingu. Data z reportu ukazují na spojitost mezi délkou URL adres a jejich bezpečností. U odkazů delších než 44 znaků je mnohem vyšší pravděpodobnost, že se jedná o phishing.**

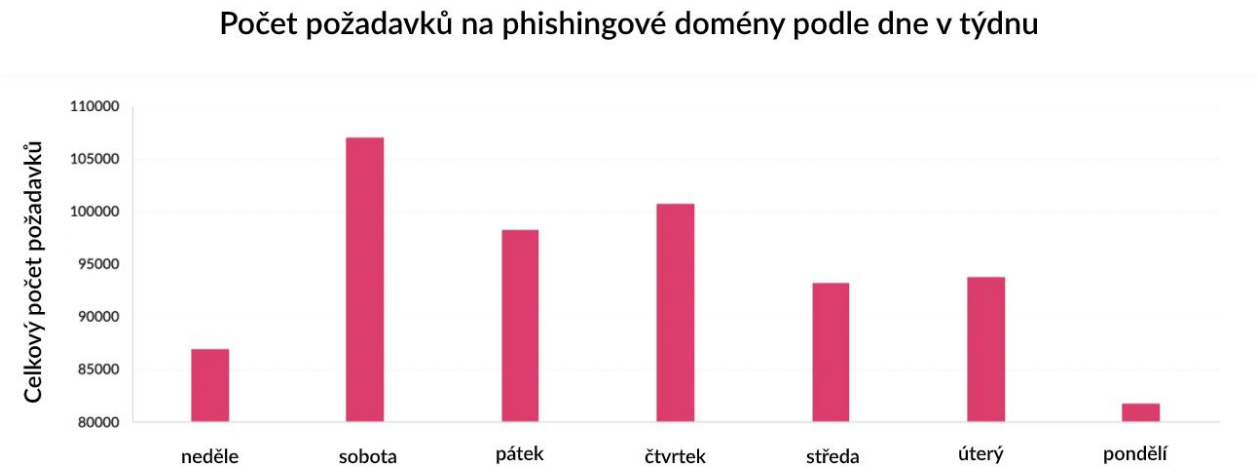
Při phishingovém útoku se obvykle podvodník snaží přimět svou oběť k návštěvě podvržené stránky, tzv. návnady, za účelem získání důvěrných informací (např. hesla). Neobvykle dlouhá URL adresa může být znamením takového útoku. Na grafu č. 1 můžete vidět porovnání délky bezpečných a phishingových adres. Z grafu je patrné, že běžné URL adresy obvykle obsahují 20 až 44 znaků. Adresy delší než 44 znaků mohou indikovat phishingový útok. V průměru byly odkazy nebezpečných domén o 80 % delší než ty bezpečné. U neobvykle dlouhých adres je tedy důležité být více na pozoru a zkontrolovat si i další indikátory, které jsou popsané níže v tomto článku.

Graf č.1 porovnání délek bezpečných a phishingových url adres

Identifikovat takové odkazy bývá problematické na smartphonech a tabletech, kde moderní webové prohlížeče zkracují URL adresy pro elegantnější design. Uživatelé by tedy měli i na mobilních telefonech využívat vyšší úrovně ochrany, zejména vzhledem k nárůstu používání národních znaků ve phishingových adresách. Taková adresa se prezentuje jako známá značka například Starbucks, ovšem do adresy je přidán znak připomínající tvarem běžné písmeno naší abecedy. Výsledná podvodná adresa pak může být například ve tvaru: starβucks.com.

Sobota jako stvořená pro phishing

Počet požadavků na phishingové domény, jak můžeme vidět na grafu č. 2, který zobrazuje výskyt zachycených phishingových domén v jednotlivých dnech v týdnu, je vcelku konstantní. Jediný den, o kterém se dá mluvit jako o relativně klidném je pondělí. Nejvíce kritická je z pohledu phishingu sobota. Společně s daty ze srpnového reportu, ze kterého vyplývá, že uživatelé nejčastěji reagují na phishingové odkazy mezi 20 - 22 hodinou, je i zde možné pozorovat trend, kdy jsou uživatelé nejvíce náchylní k útoku mimo pracovní dobu, když jsou v “uvolněné” náladě.



Graf č.2 Počet požadavků na phishingové domény podle dne v týdnu

5 indikátorů phishingu podle URL adresy

Pomocí umělé inteligence MI:RIAM, která denně zpracovává přes miliardu vstupů, jsme analyzovali i jiné faktory URL adres mimo jejich délku. Sepsali jsme 5 nejkritičtějších indikátorů phishingu nalezených pomocí MI:RIAM:

1) Při napodobování známé značky (např. starβucks.com), má taková URL 1310x větší pravděpodobnost, že se jedná o phishingovou adresu než o bezpečnou.
2) V případech, kdy se v URL adrese vyskytují slova s významem jako účet, podpora nebo ověření, je u odkazu 3,9x větší pravděpodobnost, že se jedná o phishing.
3) Pokud jakákoliv část URL postrádá přirozenost, například místo slov a jmen je použita kombinace znaků a čislic, tak je u odkazu 4,1x vyšší pravděpodobnost, že se jedná phishing.
4) Když jednotlivé části a jejich řazení neodpovídá obvyklému výskytu, např. adresa facebook.com není v tomto případě na konci:

facebook.com_____verifyme_____acc.worldofsteroid.com. U takové adresy je 2,2x větší pravděpodobnost phishingu než u běžné.

5) Při výskytu málo používané domény je 3,7x větší pravděpodobnost, že se jedná o phishing. Například u této url byla použita neobvyklá doména .top: amazon.co.uk.sh320rncspf.top.

Tyto indikátory nemusí být pro nezkušeného uživatele internetu zřejmé, a proto se při identifikaci phishingových útoků stává stále více důležité automatické strojové učení, jakým je například neustále trénovaná MI:RIAM společnosti Wandera.

Celý zářijový report naleznete zde:
https://www.wandera.com/cloud-security-report-september-2020/

O Wandeře

Naše řešení umožňuje firmám mít svá mobilní data pod kontrolou, zajistit bezpečnost samotných zařízení a pomocí vlastního VPN řešení zajistit také bezpečný přístup uživatelů k firemním zdrojům. Díky velkému množství rozmanitých dat, které naše platforma zpracovává, dokážeme zabránit útokům v reálném čase, a předcházet problémům, jakými jsou např. phishing nebo neplánované vysoké útraty za datový roaming. Momentálně má Wandera pobočky v Brně, Londýně a San Franciscu. V roce 2017 získala Wandera. financování 27,5 milionů dolarů od Sapphire Ventures, čímž celkové financování společnosti dosáhlo 53,5 milionu dolarů.