

Covid-19 ve phishingu již netáhne. Hackeři hledají nová témata.

Brno, 25.8.2020 – Ze srpnového Cloud Security Reportu, který vydala společnost Wandera vyplývá, že v období mezi březnem a červnem vzrostl počet phishingových útoků na více než dvojnásobek oproti průměrným hodnotám. Hlavním tématem těchto útoků byl Covid-19.

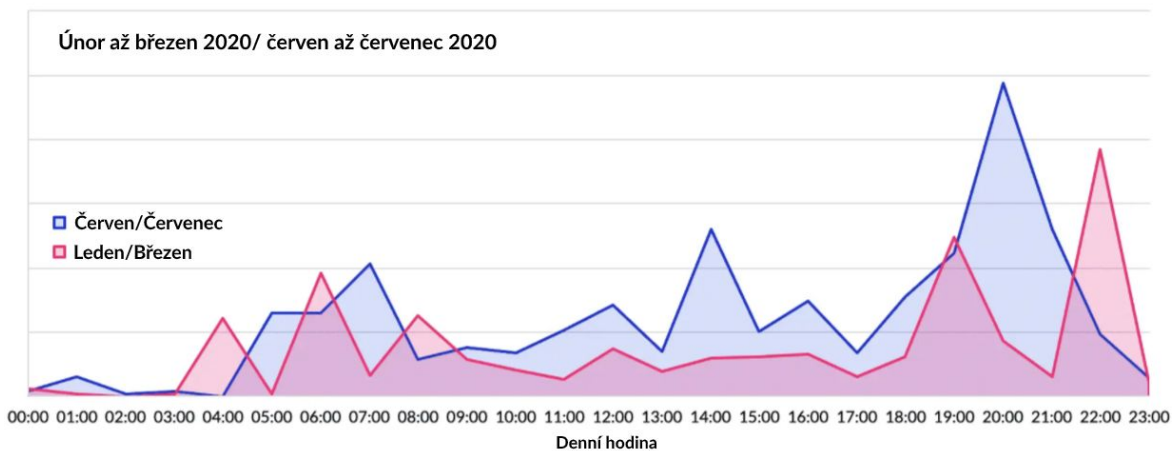
Při phishingovém útoku se obvykle podvodník snaží přimět svou oběť k návštěvě podvržené stránky, tzv. návnady, za účelem získání důvěrných informací (např. hesla). Phishing se primárně zaměřuje na obecně známé značky nebo témata, které mají vysokou šanci, že koncový uživatel klikne na odkaz vedoucí oběť k návnadě. Covid-19 byl tedy v posledních měsících velmi vděčným tématem pro mnoho útočníků. Na grafu č.1 můžeme pozorovat, že pomyslného vrcholu dosáhly phishingové útoky 28. Června. Od tohoto data počet útoků pozvolně klesá, což poukazuje na to, že téma koronaviru již není tak účinné. Útočníci se nyní začnou zaměřovat na jiná, více aktuální témata.



Graf č.1 Počet phishingových útoků

Nejvíce obětí útoků je mezi 20 a 22 hodinou

Na grafu č.2 vidíme, jak se změnil denní čas, kdy se uživatelé stávají oběťmi phishingu. Křivky porovnávají období od února do března a od června do července tohoto roku. Obecný vzorec zůstává relativně podobný. Vrcholy můžeme pozorovat ráno, kolem poledne a nejvyšší vrchol ve večerních hodinách mezi 20:00 a 22:00.



Graf č.2 Denní hodina phishingových útoků

Tyto vrcholy korelují s volným časem zaměstnanců, což značí, že se pracovníci častěji stanou obětí když nejsou dostatečně ostražiti, tedy mimo hlavní pracovní dobu. Při školení kybernetické bezpečnosti je tedy důležité zdůrazňovat, že pravidla musí být uplatňována 24 hodin denně, jinak se stávají neúčinná.

Report také ukazuje, že bez nastavení pravidel pro používání pracovních telefonů mimo pracovní dobu nebo využití softwaru pro ochranu mobilních zařízení se firmy vystavují riziku phishingu, instalaci malwaru a dalším bezpečnostním hrozbám. To může vést ke ztrátě cenných dat nebo ochromení fungování firemních systémů.

Celý report najdete ke stažení zde:

<https://www.wandera.com/cloud-security-report-august-2020/>

O Wandere

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.