AUTOCONT

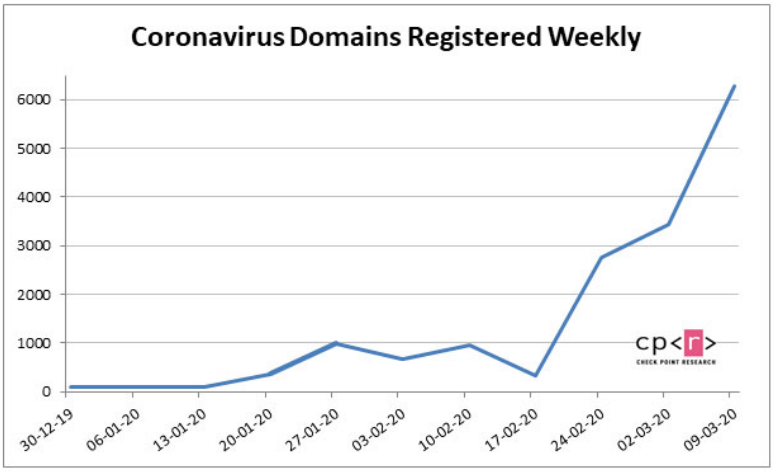
Covid 19 útočí i na kybersystémy

Nezapomeňte uživatelům připomínat, že jsou pod ofenzívou kyberzločinců

V současné době kriminálníci neváhají zneužívat potřebu informací, kterou má celá populace. Ani tato doba neodradí tyto skupiny k útokům na kybernetické systémy, útokům na účty, hesla, bankovní účty a kreditní karty. Skutečně je potřebné být v této době ostražitými i na této „frontě“ a nezapomenout, že třeba pracovníci v Home Office jsou statisticky zranitelnější ohledně sociálních manipulací.

Nový report zveřejněný společnosti Check Point (18. 3. 2020) si všímá mj. prudkého nárůstu domén (webových stránek) se vztahem ke Covid 19 a také „mimořádných sezónních slev“ u nabídek na prodej hackerských nástrojů a škodlivých kódů (na DarkWebu).

Nově registrovaných domén s tématikou Covid19 je za poslední období 10x více! Dá se očekávat, že spousta těchto stránek (domén) slouží jako návnada, jako past na uživatele!



Nově registrovaných domén s tématikou Covid19 je za poslední období 10x více! Dá se očekávat, že spousta těchto stránek (domén) slouží jako návnada, jako past na uživatele, jako prostředek pro sociální manipulaci!

Jsou nabízeny hackerské služby se slevou, což znamená, že se dostanou do rukou (nástroje pro hacking) a k dispozici (pronájem hacking aktivit) **větší skupině lidí a dá se tedy očekávat jejich větší aktivita!**

Přestože někteří operátoři ransomware (kriminální gangy) přislíbily zastavit útoky na zdravotní zařízení a medicinské organizace po dobu COVID19 pandemie, jedná se o DoppelPaymer a Maze, není možné na to spoléhat. Buďme proto opatrní.

Lidský článek je vždy ten nejslabší a tak upozorněte své uživatele na sociální manipulace, na nebezpečí, které představují. Většinou stačí dát si vteřinu, dvě na rozmyšlenou a situace vypadá jinak a možná ty dvě vteřiny zachrání Vaše data. Buďte opatrní, dávejte pozor a hlídejte si i své emoce a pudy, protože vše se dá zneužít.

Co tedy nedělat zvláště v dnešní době:

- Nestahovat z Internetu a všech „store“ soubory a aplikace (opravdu to potřebujete?)
- Neotvírat nečekané emaily, email od neznámých lidí a organizací, řetězové emaily atd. (přemozte svoji zvědavost v emailech, které jste nečekali)
- Neklikat na vložené linky a to ať v mailech nebo na sociálních sítích (linky v emailech a odkazy včetně sociálních sítí obecně, podívejte se, kam opravdu vedou)
- Nebrouzdejte bezmyšlenkovitě po všech stránkách s danou tématikou, nevěřte výběru vyhledávačů (i ty mohou být zmanipulovány). Nezapomeňte, že spousta stránek je nástrahou.

Luděk Mandok, CISA, CISM, CRISC

V Ostravě 20. 3. 2020