

Globální shrnutí přehledu hrozeb za Q1/2020

Kybernetická rizika u nás i ve světě definovala na počátku roku pandemie COVID-19. Útočníci se na nouzovou situaci rychle adaptovali a výrazně tak přibýlo podvodných kampaní, které tématu koronaviru zneužívaly. Naopak útoky cílené na firmy v globálním pohledu slábly. Vyplývá to ze zprávy společnosti ESET za první čtvrtletí roku 2020.

Vládl Malware těžící z obav z COVID-19

V porovnání s koncem roku 2019 **narostl letos počet podvodných webových stránek o 21 %**. Značná část z nich obsahuje různé formy phishingu. **V první polovině března zaznamenali analytici šedesátinásobný nárůst webů související s virem COVID-19**. Nejčastěji se s těmito hrozbami setkávali uživatelé v Rusku, Peru, Japonsku, USA a Francii. Odkazy na takovéto stránky se šířily především spamem.



Wannacry je stále nejrozšířenějším ransomwarem

V prvním kvartálu roku 2020 zaznamenali analytici z ESETu celosvětový pokles v detekcích ransomware. Výjimku představuje přelom ledna a února, kdy v regionu jižní Afriky operovaly dvě výrazné kampaně: CrYSIS a Sodinokibi.

Nejvýraznějším ransomwarem zůstává

WannaCryptor, ten je široké veřejnosti spíše známý jako WannaCry z roku 2017. **Stojí za 40 % detekcí veškerého ransomware**, a to navzdory tomu, že zneužívá zranitelnost, na kterou byla aktualizace vydána již před třemi lety.



Doxing jako nový bezpečnostní trend

Přelom roku 2019 a 2020 byl ve znamení nového trendu. Tvůrci ransomware začali krást citlivé informace (například bydliště, telefonní čísla, fotografie, politické názory či sexuální orientaci) uživatelů a vyhrožovat jejich zveřejněním, pokud oběť nezplatí výkupné. Tato technika se nazývá také doxing. **Slouží namísto klasického zašifrování dat, případně se obě metody kombinují**. V případě firem mohou například útočníci začít zveřejňovat ukradené dokumenty s návrhy nových výrobků a další cenné obchodní informace.



Klesla cena Bitcoinu, klesaly i počty detekcí těžebních malware

S nástupem koronakrizy **klesla burzovní hodnota kryptoměn**, především Bitcoinu. **Útoky**, jejichž cílem je těžit kryptoměny, **byly proto na počátku roku na ústupu**. Na konci března byly v porovnání s prosincem 2019 na **poloviční hodnotě detekcí**.

↓
50% pokles

Důvodem poklesu ale může být také operace Interpolu, díky které se v lednu podařilo identifikovat útočníky, kteří stáli za pětinou nelegálních kampaní těžících kryptoměny po celém světě.

