eset | bezpečne na nete

Ransomvér, čo sa skrýva za týmto zlovestne znejúcim názvom?

Malvér, ktorý dokáže uzamknúť zariadenie alebo zašifrovať jeho obsah s cieľom vymôcť od majiteľa daného zariadenia peniaze. Na oplátku autori škodlivého kódu sľubujú, samozrejme bez akýchkoľvek záruk, obnovenie prístupu k zablokovanému zariadeniu alebo dátam.

Najčastejšie používané techniky:

1.

Diskcoder ransomvér

Zašifruje celý disk a zamedzí používateľovi prístup k operačnému systému.

2.

Screen locker

Zablokuje prístup k obrazovke zariadenia.

3.

Crypto-ransomvér

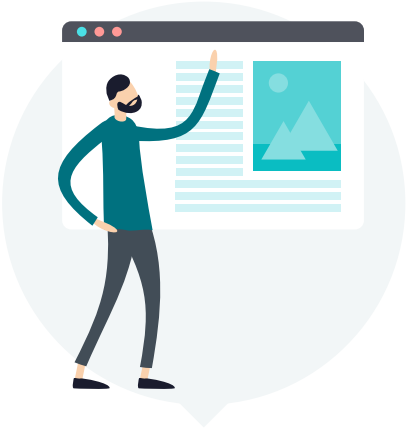
Zašifruje dáta uložené na disku obete.

4.

PIN locker

Zameriava sa na zariadenia so systémom Android a mení prístupové kódy s cieľom „vymknúť“ používateľov z ich zariadení.

Spôsoby infikovania:



Škodlivé webové stránky

E-mailové prílohy

Skrátené odkazy v e-mailoch

Nástroje, ktoré slúžia na sťahovanie rôzneho obsahu

Príspevky na sociálnych sieťach a četovacie služby

Máte podozrenie, že sa váš počítač nainfikoval ransomvérom?

- okamžite odpojte zariadenie z domácej siete, vypnite pripojenie WiFi (alebo mobilné dáta) a hibernujte počítač,
- ak hibernácia nie je možná, počítač vypnite a vyhľadajte odborníka alebo dodávateľa svojho bezpečnostného softvéru,
- po vyčistení počítača nasaďte zálohu (pokiaľ si sami netrúfate, obráťte sa na profesionála),
- v prípade, ak bolo vaše zariadenie napadnuté ransomvérom s podmienkou zaplatenia výkupneho, určite nič neplaťte.