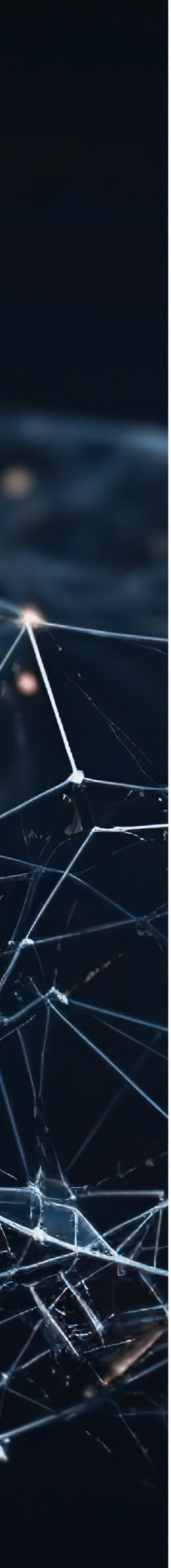


MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

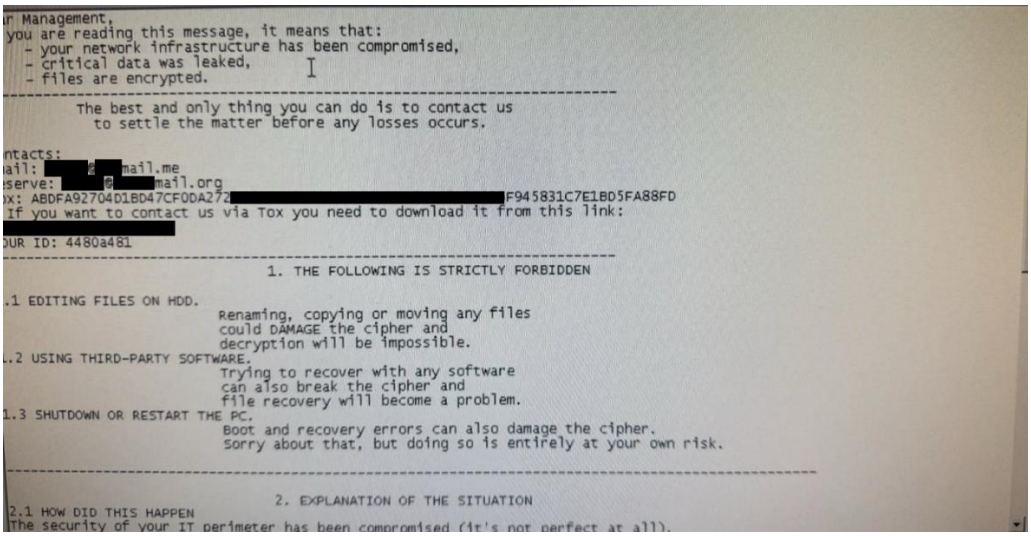
CSIRT.SK

Všeobecné informácie

Ransomvér

Čo je to ransomvér

Jedná sa o typ škodlivého kódu, ktorého úlohou je ukradnúť dáta používateľa, pričom po ich extrakcii tieto dáta v používateľovom zariadení zašifruje, resp. zašifruje/uzamkne celé zariadenie. Následne je používateľ prostredníctvom textovej poznámky na ploche, tzv. ransomnote (Obrázok 1) informovaný o úspešnom útoku. Zároveň je vyzvaný na zaplatenie výkupného výmenou za dešifrovací kľúč, ktorý umožní obnovu zašifrovaných dát, a za prísľub, že útočníci nezverejnia odcudzené údaje. V prípade uzamknutia celého zariadenia je ransomnote zobrazený na obrazovke po načítaní operačného systému.



Obrázok 1 Ransomnote - ukážka

VAROVANIE: Nikdy neplaťte útočníkovi výkupné výmenou za odšifrovanie súborov. Zaplatenie výkupného nezaručuje, že útočník súbory skutočne odšifruje. Zároveň nemožno vylúčiť, že si vo Vašej infraštruktúre vytvoril mechanizmy umožňujúce opätovný neoprávnený prístup alebo opakovanie útoku.

Indikátory ransomvéru vo Vašej infraštruktúre

V nasledujúcich bodoch si môžete skontrolovať jednotlivé indikátory poukazujúce na pravdepodobný výskyt ransomvéru vo Vašej infraštruktúre/vo Vašom zariadení:

☐ nezvyčajná aktivita na zariadení (výrazné zaťaženie a spomalenie, deaktivácia bezpečnostných prvkov, možné odstránenie záloh),

☐ súbory vo Vašom zariadení končia neznámou príponou (napr. mzdy_oktober.docx.xyz),

☐ v zašifrovanom priečinku/na obrazovke sa objaví oznámenie (ransomnote) o vykonaní útoku a o ďalších krokoch, ktoré útočník požaduje od používateľa,

☐ veľké množstvo súborov bolo naraz premenovaných alebo zmenilo dátum poslednej úpravy,

☐ zdieľané sieťové disky alebo priečinky sú nedostupné alebo obsahujú zašifrované súbory.

Ochrana pred ransomvérom

Najúčinnejšou ochranou pred ransomvérovým útokom je prevencia – dostatočné zálohovanie, adekvátne zabezpečenie účtov, ako aj segmentácia siete. Detailný popis zabezpečenia a opatrení môžete nájsť na našom webe.