

Mahdollisten kiristysohjelmien poistaminen

Kehittyneessä kiristysohjelmassa käytetään tekniikkaa, jossa se salaa käyttäjän tiedostot, jolloin ne eivät ole käytettävissä, ja vaatii lunastusmaksun salauksen purkamiseksi.

Muista, että edes lunnaiden maksamisen jälkeen ei ole takeita siitä, että tiedostojesi salaus puretaan.



Poista salaus henkilökohtaisista tiedostoista

Tietuille tunnetuille kiristysohjelmille on mahdollista palauttaa tiedostot ilmaisten ohjelmistojen avulla. Valitettavasti yksikään ilmaisista ohjelmistoista ei pysty tarjoamaan palautusratkaisuja kaikille tunnetuille kiristysohjelmille. Itse asiassa sinun on löydettävä salauksenpurkuohjelma, joka on suunniteltu erityisesti tietyn tyyppiselle kiristysohjelmalle.

Aluksi sinun on selvitettävä, mikä kiristysohjelma on salannut tiedostosi.



Seuraavat palvelut voivat auttaa tässä:

ID-Ransomware: Voit ladata verkkosivustolle tiedoston, jolla hyökkääjät ovat toimittaneet viestinsä. Lisäksi tarjolla on latauspainike salatuille tiedostoille. Voit myös syöttää kiristäjän sähköpostiosoitteen, jos olet saanut sellaisen rikollisilta heihin yhteyden ottamiseksi.

Palvelu käyttää näitä tietoja hyökkäyksessä käytetyn kiristysohjelman tunnistamiseen. Se tunnistaa jo yli 1100 haittaohjelmanäytettä.

NO MORE RANSOM: Palvelu ei ainoastaan auta tunnistamaan tarkkaa kiristysvirusta, vaan tarjoaa lisäksi oikean salaustyökalun – jos sellainen on olemassa.

Verkkosivusto tarjoaa kiristysohjelmaneuvonnan sekä **"Crypto Sheriff"** -työkalun. Siellä voit täyttää lomakkeen bitcoin- tai TOR-sipuliverkko-osoitteille, verkkosivustojen osoitteille ja lunastusvaatimusten sähköposteille sekä mahdollisuuden ladata sivulle salattuja tiedostoja.

Seuraavaksi verkkosivusto tarkistaa, tunnetaanko tämäntyyppinen kiristysohjelma ja onko olemassa ratkaisua. Jos on, he tarjoavat sinulle linkin salauksenpurkuratkaisun ratkaisun lataamiseen.

Seuraavat muut toimittajat tarjoavat ilmaisia salauksenpurkutyökaluja tietyn tyyppisille kiristysohjelmille.

- **Avast-kiristysohjelmatyökalut osoitteessa avast.com/c-topic-ransomware** tarjoavat lisätietoja kiristysohjelmista ja siitä, kuinka poistaa kiristysohjelmat Mac- ja Windows-tietokoneista.

Löydät tällä hetkellä saatavilla olevat salauksenpurkajat osoitteesta:

avast.com/ransomware-decryption-tools. Nämä työkalut voivat auttaa purkamaan

Mahdollisten kiristysohjelmien poistaminen

tiedostoja, jotka on salattu yli 20 eri kiristysohjelmalla. Klikkaa nimeä nähdäksesi merkkejä infektiosta ja saadaksesi ilmaisen korjauksen.

➤ **AVG-kiristysohjelmien salauksenpurkutyökalut** avg.com/en-gb/ransomware-decryption-tools#apocalypse tarjoaa salauksenpurkutyökaluja tiedostoille, jotka on salattu seuraavilla kiristyshaittaohjelmilla:

- Apocalypse
- BadBlock
- Bart
- Crypt888
- Legion
- SZFLocker
- TeslaCrypt

➤ **Kaspersky Labin salauksenpurkajat** noransom.kaspersky.com/ on suunniteltu pienille ja keskisuurille yrityksille. Kaspersky Lab isännöi laajaa joukkoa salauksenpurkutyökaluja, joiden avulla voidaan purkaa monia haitallisia kiristysohjelmatyyppejä.

Kiristysohjelmatyyppi	Purkaa salauksen tiedostoista, joihin vaikutus kohdistuu
Rakhni Decryptor	Rakhni, Agent.iih, Aura, Autoit, Pletor, Rotor, Lamer, Cryptokluchen, Lortok, Democry, Bitman (TeslaCrypt) versio 3 ja 4, Chimera, Crysis (versiot 2 ja 3), Jaff, Dharma, uudet versiot seuraavista: Cryakl kiristysohjelma, Yatron, FortuneCrypt
Rannah Decryptor	Rannah, AutoIt, Fury, Cryakl, Crybola, CryptXXX (versiot 1, 2 ja 3), Polyglot aka Marsjoke
Wildfire Decryptor	Wildfire kiristysohjelma
CoinVault decryptor	CoinVault ja Bitcryptor kiristysohjelma
Shade Decryptor	Shade versio 1 ja 2
Xorist Decryptor	Xorist ja Vandev
Rector Decryptor	Purkaa tiedostojen salauksen, joihin Rector vaikuttaa

Jos et ole löytänyt ratkaisua täältä, etsi verkosta laitteellesi joutunutta kiristysohjelmaa.