Godra Ransomware

Early Alert Report

INTRODUZIONE

In data 16 Dicembre 2017 è stato identificato un nuovo Ransomware denominato Godra. Il Ransomware esegue la crittografia dei file offrendo poi la chiave di decodifica attraverso il pagamento di un riscatto pari a €2000 in BTC. Godra è compatibile solo con le versioni di Windows x64.

DESCRIZIONE

MD5:

df5f6dd725fc67b25dde32946f8a2930

E-mail legata al Ransomware:

godra@protonmail.ch

Indirizzo Bitcoin:

13srq1SP93mEs7asR2UxWBUts3x9oUcuac

FUNZIONAMENTO

Il Ransomware esegue la crittografia di numerosi file e ne modifica l'estensione in .godra.

ES: <File_name>.<extension>.godra

Successivamente viene creato il file della nota di riscatto che presenta il seguente testo:

YOUR personal data is encrypted! ATTENTION! Do not try to decrypt the files. ANY CHANGE encrypted files to destroy them! THE ONLY WAY to decrypt your files - follow the instructions EXACTLY !!! What's wrong with my computer? All your important files are encrypted. All your documents, photos, videos, databases, and other files are no longer available because they are encrypted. Do not try and do not waste time on decryption or repair your files, because no one will be able to decrypt your files without decryption of our service. Can I restore files? Of course. We guarantee return of your files after the payment: 2.000,00 EUR (two thousand euros) in the BTC (BitCoin) equivalent You have 48 hours to send the payment, otherwise the price will double. Also, if you do not make payment within 72 hours, your files will be permanently lost. After payment please send us a "User ID" and the number of purse from which the payment was made on godra@protonmail.ch the User ID: (Personal ID)

Godra Ransomware

Early Alert Report

and we will send you a decryption program that will recover your files. Please note that * ANY WAY * do not change theirencrypted files, because the recovery will be impossible.
You can send us the file on godra@protonmail.ch (100 KB), to prove that the decoding is possible.
HOW TO PAY?
We accept payments only in BTC-currency (BitCoin). Payment should be done at the following address:
13srq1SP93mEs7asR2UxWBUts3x9oUcuac
Do not use the "deep web" wallets, such as Tor Wallet, Onion Wallet, Shad's Wallet, Hidden Wallet , etc.
Buy BTC (BitCoin) only from the official BitCoin Exchange!
Official exchange rates and prices: https://howtobuybitcoins.info/
Best Practices for Buying: https://bit4coin.net/ or https://www.coinbase.com/ or https://xcoins.io/
On Bit4Net not need registering! On xcoins.io BitCoin can buy through PayPal!
Email-address for communication: godra@protonmail.ch
Send us an email with your "User ID" and a purse, from which the payment was made!
ATTENTION!
Do not try to decrypt the files. ANY CHANGE encrypted files to destroy them! THE ONLY WAY to decrypt your files - follow the instructions EXACTLY !!!