

# KoreanLocker Ransomware

Early Alert Report

## INTRODUZIONE

In data 10 Gennaio 2018 è stato identificato un nuovo Ransomware denominato KoreanLocker. Il Ransomware esegue la crittografia dei file offrendo poi la chiave di decodifica attraverso il pagamento di un riscatto pari a 1 BTC.

## DESCRIZIONE

### MD5:

b067635d568f7abaa51d5251dd378d25

### E-mail legata al Ransomware:

powerhacker03@hotmail.com

### Indirizzo Bitcoin:

1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v

## FUNZIONAMENTO

KoreanLocker esegue la crittografia di grandi quantità di file e ne modifica l'estensione in .locked.

**ES:** <File\_name>.<extension>.locked

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

----- koreanLocker ransomware ----- Your computer is infected with ransomware your personal files such as photos, documents, videos and other important documents zashifrovyvays using strong encryption algorithm, called RSA-2048 is your private key is created and stored on our server no one can decrypt your files ever. And I guarantee that you will never be able to decipher without the private key. Again, there is no way to pay for a small coin, and decode it Be sure to check your assigned Bitcoin address. If you make a mistake, it will not be restored and your Bitcoin disappear

You must pay within 24 hours,  
if you do not pay within this time, your private key will be automatically deleted from our servers  
, please keep in mind  
Be sure to check your personal ID  
Bitcoin address: 1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v  
Create a little coin purse and send us a small coin ( 1BTC) to our bit.  
Follow the three steps to recover files  
not waste your time.

# KoreanLocker Ransomware

## Early Alert Report

Explanatory document (.txt) in the folder that contains encrypted files, not a virus. Explanatory document (.txt) will help you decrypt the files.

You can see the document (.txt) for the restoration of files in the folder where the files are encrypted

We are not good people. But only in part,

Please note that the worst has already happened, and the fate of the file will depend on your decisions and fast action.

1) Payment is only possible in Bitcoins. Therefore purchase 1 Bitcoin (1BTC) through BTC. Then move Bitcoin 1 (1BTC) on Bitcoin address on the screen.

2). Send your personal ID to the official email-address below.

3). Please make the payment and send us an email, and we will send your decrypting tool, and the private key via email throughout the day

4) Please send a little coin and send your personal identifier on the official e-mail address in Korea.

Additional Information:

The private key - the key to deciphering and restoring files

The public key used to encrypt your file

Official address: [www.bithumb.com](http://www.bithumb.com)

official address: [www.coinone.com](http://www.coinone.com)

official address: [www.localbitcoins.com](http://www.localbitcoins.com)

Official E-mail: [powerhacker03@hotmail.com](mailto:powerhacker03@hotmail.com)

\*\*\*

Best wishes

Team ransomware Korean

----- koreanLocker ransomware -----