BlackRuby Ransomware

Early Alert Report

INTRODUZIONE

In data 8 Febbraio 2018 è stato identificato un nuovo Ransomware denominato BlackRuby. Il Ransomware esegue la crittografia dei file offrendo poi la chiave di decodifica attraverso il pagamento di un riscatto pari a $650 in BTC.

DESCRIZIONE

MD5:

81e9036aed5502446654c8e5a1770935

E-mail legata al Ransomware:

TheBlackRuby@Protonmail.com

Indirizzo Bitcoin:

19S7k3zHphKiYr85T25FnqdxizHcgmjoj1

FUNZIONAMENTO

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

ES: <File_name>.<extension>.BlackRuby

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

Black Ruby === Identification Key === [redacted] === Identification Key === [Can not access your files?] Congratulations, you are now part of our family #BlackRuby Ransomware. The range of this family is wider and bigger every day. Our hosts welcome our presence because we will give them a scant souvenir from the heart of Earth. This time, we are guest with a new souvenir called "Black Ruby". A ruby in black, different, beautiful, and brilliant, which has been bothered to extract those years and you must also endure this hard work to keep it. If you do not have the patience of this difficulty or you hate some of this precious stone, we are willing to receive the price years of mining and finding rubies for your relief and other people of the world who are guests of the black ruby. So let's talk a little bit with you without a metaphor and literary terms to understand the importance of the subject.

BlackRuby Ransomware

Early Alert Report

It does not matter if you're a small business or you manage a large organization, no matter whether you are a regular user or a committed employee, it's important that you have a black ruby and to get rid of it, you need to get back to previous situation and we need a next step.
The breadth of this family is not supposed to stop, because we have enough knowledge and you also trust our knowledge.
We are always your backers and guardian of your information at this multi-day banquet and be sure that no one in the world can take it from you except for us who extracts this precious stone.
We need a two-sided cooperation in developing cybersecurity knowledge. The background to this cooperation is a mutual trust, which will result in peace and tranquility, you must pay $650 (USD) worth of Bitcoins for restore your system to the previous state and you are free to choose to stay in this situation or return to the normal.
Do not forget that your opportunity is limited. From these limits you can create golden situations. Be sure we will help you in this way and to know that having a black ruby does not always mean riches. You and your system are poor, poor knowledge of cybersecurity and lack of security on your system!.
===
[HOW TO DECRYPT FILES]
1. Copy "Identification Key".
2. Send this key with two encrypted files (less than 5 MB) for trust us to email address "TheBlackRuby@Protonmail.com".
3. We decrypt your two files and send them to your email.
4. After ensuring the integrity of the files, you must pay $650 (USD) with bitcoin and send transaction code to our email, our bitcoin address is "19S7k3zHphKiYr85T25FnqdxizHcgmjoj1".
5. You get "Black Ruby Decryptor" Along with the private key of your system.
6. Everything returns to the normal ana your files will be released.
===
[What is encryption?]
Encryption is a reversible modification of information for security reasons but providing full access to it for authorised users.
To become an authorised user and keep the modification absolutely reversible (in other words to have a possibility to decrypt your files) you should have an "Personal identification Key". But not only it. It is required also to have the special decryption software (in your case "Black Ruby Decryptor" software) for safe and complete decryption of all your files and data.
[Everything is clear for me but what should I do?]
The first step is reading these instructions to the end. Your files have been encrypted with the "Black Ruby Ransomware" software; the instructions ("how-to-decrypt-files.txt") in the folders with your encrypted files are not viruses, they will help you. After reading this text the most part of people start searching in the internet the words the "Black Ruby Ransomware" where they find a lot of ideas, recommendation and instructions, it is necessary to realise that we are the ones who closed the lock on your files and we are the only ones who have this secret key to open them.
[Have you got advice?]
[*** Any attempts to get back you files with the third-party tools can be fatal for your encrypted files ***]
The most part of the tried-party software change data with the encrypted files to restore it but this cases damage to the files.
Finally it will be impossible to decrypt your files, when you make a puzzle but some items are lost, broken or not put in its place - the puzzle items will never match, the same way the third-party software will ruin your files completely and irreversibly. You should realise that any intervention of the third-party software to restore files encrypted with the Black Ruby Ransomware" software may be fatal for your files.
If you look through this text in the internet and realise that something is wrong with your files but you do not have any instructions to restore your files, please contact your antivirus support.