Black Ruby Ransomware Skips Victims in Iran and Adds a Miner for Good Measure

bleepingcomputer.com/news/security/black-ruby-ransomware-skips-victims-in-iran-and-adds-a-miner-for-good-measure

By
Lawrence Abrams

- February 9, 2018
- 06:10 PM
- 2

A new ransomware was discovered this week by MalwareHunterTeam called Black Ruby. This ransomware will encrypt the files on a computer, scramble the file name, and then append the BlackRuby extension. To make matters worse, Black Ruby will also install a Monero miner on the computer that utilizes as much of the CPU as it can.

Unfortunately, this ransomware is not decryptable at this time. If you wish to discuss or receive help, you can use our dedicated Black Ruby Help & Support topic.

Black Ruby won't run if a victim is from Iran

Black Ruby will only encrypt a computer if the victim is not from Iran. When started, the ransomware will query http://freegeoip.net/json/ and check if the response contains **"country_code":"IR"**.

If the site does indicate that the user is from Iran, the process will terminate and will not perform any malicious activity on the computer.

Black Ruby may be installed via Remote Desktop Services

While it is not 100% confirmed, there is a good chance that Black Ruby is being installed via Remote Desktop Services. In a Reddit post, a user asked for help with a server that was encrypted by Black Ruby over the weekend when no one was in the office.

The first thing people thought, including myself, was if they had remote desktop services enabled. While the user has not confirmed if the remote desktop services was open to the public, this was most likely the method the attacker used to gain access to their network.

Black Ruby Drops a Monero Miner

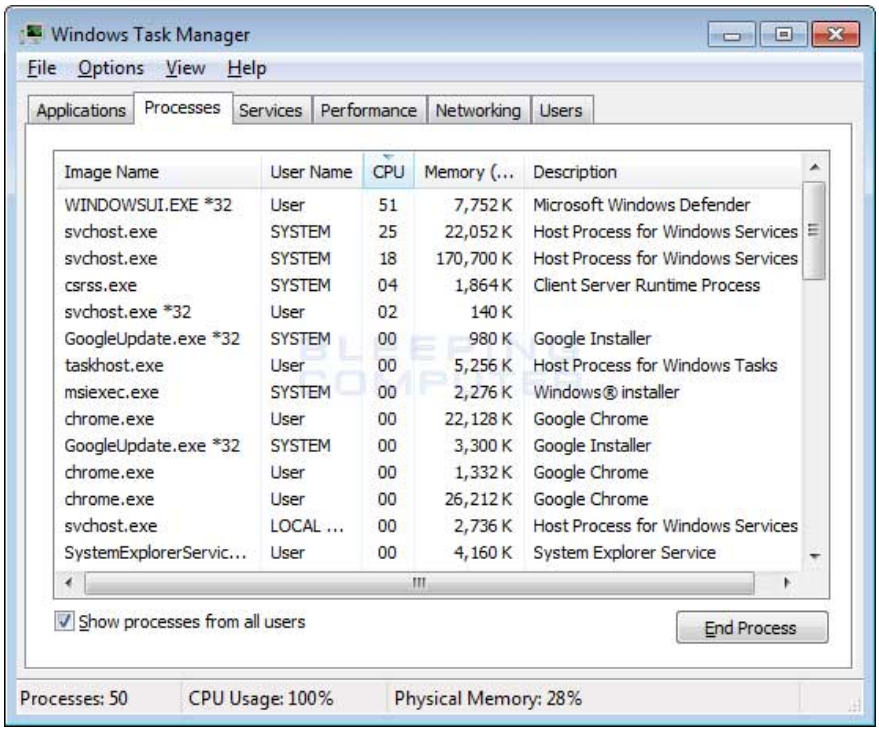
To make matters worse, the developers decided to install a Monero miner on the computer before encrypting it. This way if the victim does not pay the ransom, the attackers can at least generate digital currency from them.

When a user logs in, Black Ruby will extract a miner executable to C:\Windows\System32\BlackRuby\svchost.exe.

```
public static bool smethod_0()
{
    try
    {
        DirectoryInfo expr_0B = new DirectoryInfo(Class6.string_3);
        expr_0B.Create();
        expr_0B.Attributes = FileAttributes.Hidden;
        File.Copy(Application.ExecutablePath, Class6.string_3 + "\\WindowsUI.exe");
        File.WriteAllBytes(Class6.string_3 + "\\Svchost.exe", Class5.smethod_0(Resources.Byte_0, Class3.byte_0));
        Thread.Sleep(10000);
        if (File.Exists(Class6.string_3 + "\\Svchost.exe"))
        {
            bool result = true;
            return result;
        }
    }
    catch (Exception)
    {
        bool result = false;
        return result;
    }
    return false;
}
```

Extract Embedded Miner

When the miner is executed, it will connect to the pool at de01.supportxmr.com:3333 where it will begin mining for the Monero currency.



Svchost.exe Miner in Task Manager

When mining it will use the maximum amount of CPU it can, which will cause a computer to become extremely slow and for a victim's CPU to become very hot for an extended period of time.

How Black Ruby encrypts a computer

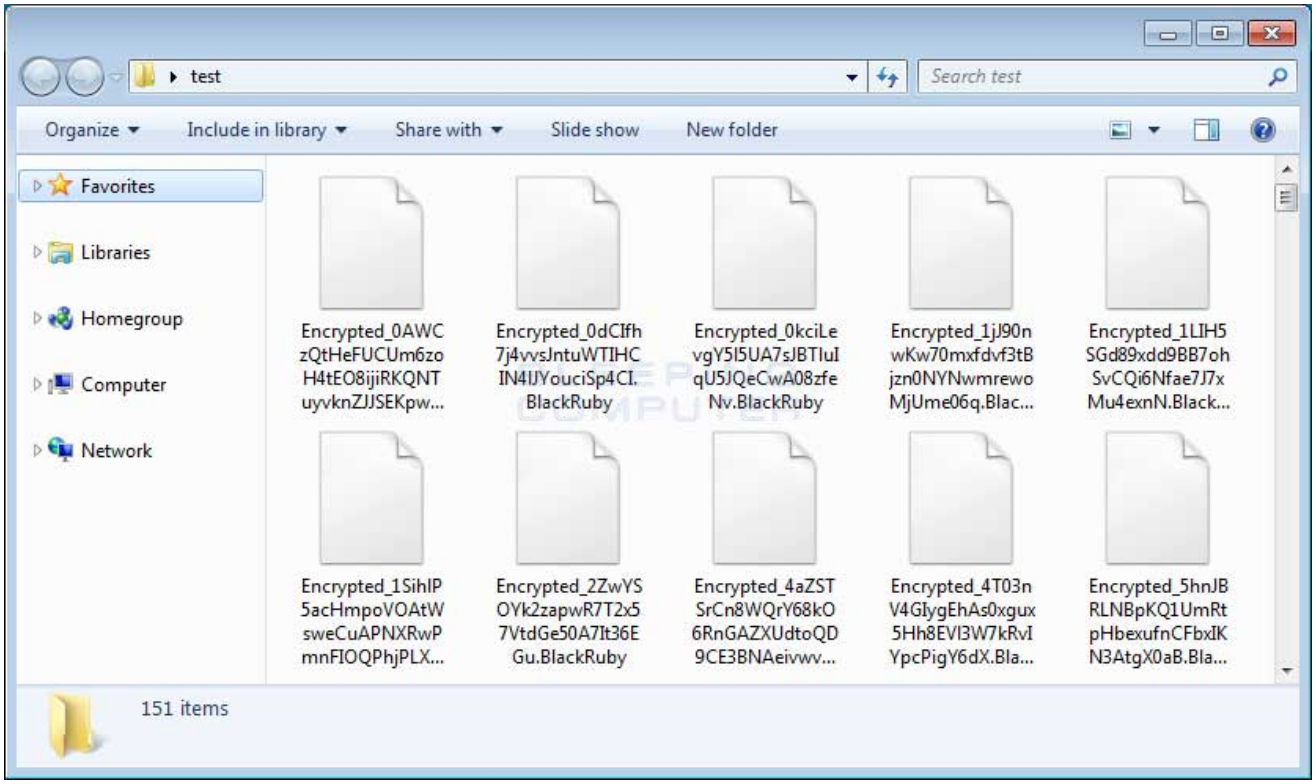
When Back Ruby is installed it will check to see if your IP address is in Iran. If it is, it will terminate the program. If not, it will first extract a Monero miner as described above. After it extracts and executes the miner it will terminate the sql.exe process and execute the following commands:

```
cmd.exe /C vssadmin.exe delete shadows /all /Quiet
cmd.exe /C WMIC.exe shadowcopy delete
cmd.exe /C Bcdedit.exe /set {default} recoveryenabled no
cmd.exe /C Bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
cmd.exe /C wevtutil.exe cl Application
cmd.exe /C wevtutil.exe cl Security
cmd.exe /C wevtutil.exe cl System
```

After those commands are executed, it will scan the computer for certain file types that it will encrypt. The files types encrypted by Black Ruby are:

```
.gif, .apk, .groups, .hdd, .hpp, .log, .m2ts, .m4p, .mkv, .mpeg, .epub, .yuv, .ndf, .nvram, .ogg, .ost, .pab,
.pdb, .pif, .png, .qed, .qcow, .otp, .s3db, .qcow2, .rvt, .st7, .stm, .vbox, .vdi, .vhd, .vhdx, .vmdk, .vmsd,
.psafe3, .vmx, .vmxf, .3fr, .3pr, .ab4, .accde, .accdr, .accdt, .ach, .acr, .sd0, .sxw, .adb, .advertisements,
.agdl, .ait, .apj, .asm, .awg, .back, .backup, .sti, .oil, .backupdb, .bay, .bdb, .bgt, .bik, .bpw, .cdr3,
.cdr4, .cdr5, .cdr6, .ycbcra, .cdrw, .ce1, .ce2, .cib, .craw, .crw, .csh, .csl, .db_journal, .dc2, .pptm,
.dcs, .ddoc, .ddrw, .der, .des, .dgc, .djvu, .dng, .drf, .dxg, .eml, .ppt, .erbsql, .erf, .exf, .ffd, .fh,
.fhd, .gray, .grey, .gry, .hbk, .ibd, .7z, .ibz, .iiq, .incpas, .jpe, .kc2, .kdbx, .kdc, .kpdx, .lua, .mdc,
.mef, .config, .mfw, .mmw, .mny, .mrw, .myd, .ndd, .nef, .nk2, .nop, .nrw, .ns2, .ns3, .ldf, .ns4, .nwb, .nx2,
.nxl, .nyf, .odb, .odf, .odg, .odm, .orf, .otg, .oth, .py, .ots, .ott, .p12, .p7b, .p7c, .pdd, .pem,
.plus_muhd, .plc, .pot, .pptx, .py, .qba, .qbr, .qbw, .qbx, .qby, .raf, .rat, .raw, .rdb, .rwl, .rwz, .conf ,
.sda, .sdf, .sqlite, .sqlite3, .sqlitedb, .sr2, .srf, .srw, .st5, .st8, .std, .stx, .sxd, .sxg, .sxi, .sxm,
.tex, .wallet, .wb2, .wpd, .x11, .x3f, .xis, .ARC, .contact, .dbx, .doc, .docx, .jnt, .jpg, .msg, .oab, .ods,
.pdf, .pps, .ppsm, .prf, .pst, .rar, .rtf, .txt, .wab, .xls, .xlsx, .xml, .zip, .1cd, .3ds, .3g2, .7zip,
.accdb, .aoi, .asf, .asp, .aspx, .asx, .avi, .bak, .cer, .cfg, .class, .cs , .css, .csv, .db, .dds, .dwg,
.dxf, .flf, .flv, .html, .idx, .js, .key, .kwm, .laccdb, .lit, .m3u, .mbx, .md, .mdf, .mid, .mlb, .mov, .mp3,
.mp4, .mpg, .obj, .odt, .pages, .php, .psd, .pwm, .rm, .safe, .sav, .save, .sql, .srt, .swf, .thm, .vob, .wav,
.wma, .wmv, .xlsb, 3dm, .aac, .ai, .arw, .c, .cdr, .cls, .cpi, .cpp, .cs, .db3, .docm, .dot, .dotm, .dotx,
.drw, .dxb, .eps, .fla, .flac, .fxg, .java, .m, .m4v, .max, .mdb, .pcd, .pct, .pl, .potm, .potx, .ppam, .ppsm,
.ppsx, .pptm, .ps, .r3d, .rw2, .sldm, .sldx, .svg, .tga, .wps, .xla, .xlam, .xlm, .xlr, .xlsm, .xlt, .xltm,
.xltx, .xlw, .act, .adp, .al, .1, .bkp, .blend, .cdf, .cdx, .cgm, .cr2, .crt, .dac, .dbf, .dcr, .ddd, .design,
.dtd, .fdb, .fff, .fpx, .h, .iif, .indd, .jpeg, .mos, .nd, .nsd, .nsf, .nsg, .nsh, .odc, .odp, .pas, .pat,
.pef, .pfx, .ptx, .qbb, .qbm, .sas7bdat, .say, .st4, .st6, .stc, .sxc, .tlg, .wad, .xlk, .aiff, .bmp, .cmt,
.dat, .dit, .edb, .flvv, .avhd , .back , .c , .ctl , .dbf , .disk , .dwg , .gz, .mail, .nrg, .ora , .ova,
.ovf, .pmf, .ppt , .pptx, .pst, .pvi, .pyc, .sln, .tar, .vbs, .vcb, .vfd, .vmc, .vsd, .vsdx, .vsv, .work,
.xvd, .123, .3dm, .602, .aes, .asc, .brd, .bz2, .cmd, .dch, .dif, .dip, .docb, .frm, .gpg, .jsp, .lay, .lay6,
.m4u, .mml, .myi, onetoc2, .PAQ, .ps1, .sch, .slk, .snt, .suo, .tgz, .tif, .tiff, .uop, .uot, .vcd, .wk1,
.wks, .xlc",
```

When encrypting files it will rename them to the format Encrypted_[scrambled_file_name.BlackRuby. For example, a file called test.jpg would be encrypted and renamed as Encrypted_zIX2dFXFt9qNfifBu1mqkNVYTX79ZS48TWWU5BRm3Q.BlackRuby.



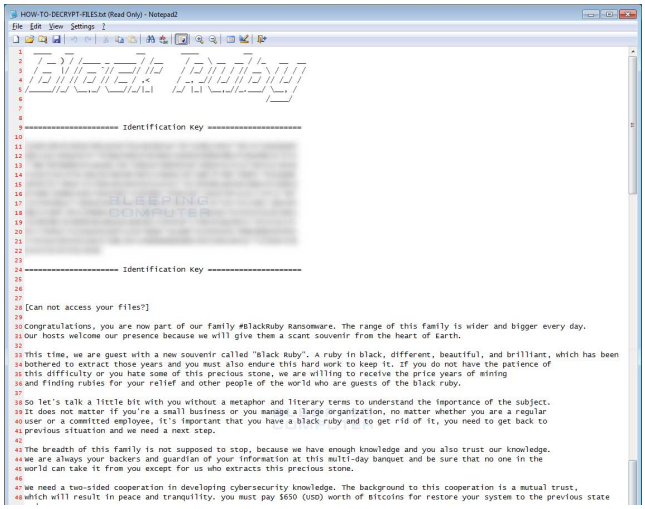
Encrypted BlackRuby Files

When the ransomware has finished encrypting a computer, it will drop a ransom note named **HOW-TO-DECRYPT-FILES.txt** to the Windows desktop. This ransom note is quite bizarre and doesn't quite make sense. For example, it opens with the following statement and gets more bizarre as you continue to read it.

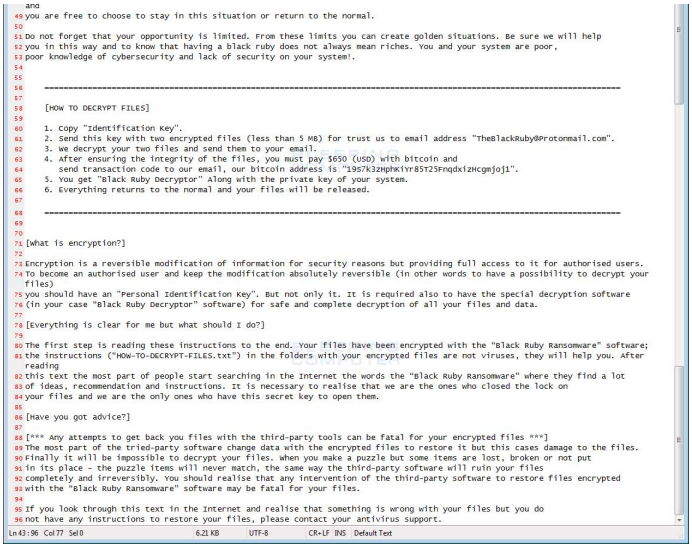
Congratulations, you are now part of our family #BlackRuby Ransomware. The range of this family is wider and bigger every day.
Our hosts welcome our presence because we will give them a scant souvenir from the heart of Earth.

In summary, it will contain instructions to contact the developer at TheBlackRuby@Protonmail.com and to make a payment of $650 USD in bitcoin to the address 19S7k3zHphKiYr85T25FnqdxizHcgmjoj1. This address is static and has one payment made to it so far.

The full contents of the ransom note are below.



Ransom Note Part 1



Ransom Note Part 2

Unfortunately, at this time there is no way to decrypt files encrypted by Black Ruby for free. Furthermore, if you do not plan on paying the ransom, be sure to remove the Monero miner or your computer will become unusable due to the high CPU utilization.

If you wish to discuss this ransomware, you can use our BlackRuby Ransomware Help & Support topic.

How to protect yourself from the Black Ruby Ransomware

To protect yourself from the Black Ruby Ransomware, it is particularly important that you do not have any computers running remote desktop services connected directly to the Internet. Instead place computers running remote desktop behind VPNs so that they are only accessible to those who have VPN accounts on your network.

In order to protect yourself from ransomware in general, it is important that you use good computing habits and security software. First and foremost, you should always have a reliable and tested backup of your data that can be restored in the case of an emergency, such as a ransomware attack.

You should also have security software that incorporates behavioral detections to combat ransomware and not just signature detections or heuristics. For example, Emsisoft Anti-Malware and Malwarebytes Anti-Malware both contain behavioral detection that can prevent many, if not most, ransomware infections from encrypting a computer.

Last, but not least, make sure you practice the following security habits, which in many cases are the most important steps of all:

- Backup, Backup, Backup!
- Do not open attachments if you do not know who sent them.
- Do not open attachments until you confirm that the person actually sent you them,
- Scan attachments with tools like VirusTotal.
- Make sure all Windows updates are installed as soon as they come out! Also make sure you update all programs, especially Java, Flash, and Adobe Reader. Older programs contain security vulnerabilities that are commonly exploited by malware distributors. Therefore it is important to keep them updated.
- Make sure you use have some sort of security software installed that uses behavioral detections or white list technology. White listing can be a pain to train, but if your willing to stock with it, could have the biggest payoffs.
- Use hard passwords and never reuse the same password at multiple sites.

For a complete guide on ransomware protection, you visit our How to Protect and Harden a Computer against Ransomware article.

Related Articles:

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

New RansomHouse group sets up extortion market, adds first victims

Ransomware attack exposes data of 500,000 Chicago students

IOCs

Hashes:

```
daea4b5ea119786d996f33895996396892fa0bdbb8f9e9fcc184a89d0d0cb85e
```

Files:

```
C:\Windows\system32\BlackRuby\WindowsUI.exe
C:\Windows\system32\BlackRuby\Svchost.exe
```

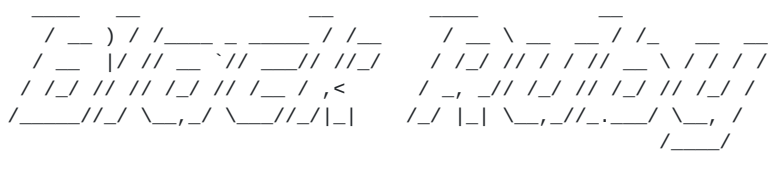
Registry Keys:

```
HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\BlackRuby
HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run "Windows Defender" =
"C:\Windows\system32\BlackRuby\WindowsUI.exe"
```

Email Addresses::

```
TheBlackRuby@Protonmail.com
```

Ransom Note Text:



========== Identification Key ==========

[id]

========== 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.
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 and 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.
```

Bitcoin Address:

```
19S7k3zHphKiYr85T25FnqdxizHcgmjoj1
```

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

- 

  Alexanderks29 - 4 years ago

  I'm infected what do now

- 

TheBlackRuby - 4 years ago

The "Black Ruby" is still alive and active and we are the creators of it. We are still pleased to be able to help our friends. Recently, our email service has been blocked and we have been forced to launch mail on other services for communication with users because all users are respected. Here's a very important point: If Black ruby is guest your system, be sure to send the two files as a test to one of the email addresses described here, because a potential opportunist and fraudsters may want to ask you for receive funds if they do not have any key and decryption. we would like to remind you that sending two files as a test to decrypt a file is important and will prevent misuse. If you use the TOR network, you can send your request to the address TheBlackRuby@torbox3uiot6wchz.onion (register in torbox3uiot6wchz.onion and after send email) and if you are connected to the Internet without a connection to the network, you can send an email to blackruby@tutanota.com

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: