How to delete ransomware creates .bora file extension

If the image, document or file is encrypted with the bora extension, it means that your computer is infected with ransomware STOP (DJVU). And here is how to delete it.

If the image, document or file is encrypted with the bora extension, it means that your computer is infected with ransomware STOP (DJVU).

Ransomware STOP (DJVU) encrypts personal documents on the victim's computer, then displays a message providing the decryption of data if paying with Bitcoin. Instructions for decoding the file are placed in the file _readme.txt on the victim's desktop. This article will guide you how to delete ransomware to create .bora file extension.

Warning: This guide will help you to remove ransomware creating .bora file extension, but not to recover files. You can try ShadowExplorer or free file recovery software to recover data.

1. How to ransomware create .bora file extension to get into computer

Ransomware creates .bore extensions that are distributed via email spam containing ransomware-infected attachments or exploiting holes in installed operating systems and software.

Cyber ??criminals email spam with fake headline information, tricking the recipient into believing it is from a shipping company like DHL or FedEx. The email notifies you that you have an order that you need to receive but cannot send for several reasons. Or sometimes the order confirmation email you bought. Either way it makes the recipient curious and opens the attachment (or click on the link embedded in the email). And by doing this, your computer will be infected with ransomware creating .bora file extension.

Ransomware creates a .bora file extension that attacks victims by hacking the open Remote Desktop Services (RDP) port. Attackers scan systems running RDP (TCP port 3389), then perform brute force attacks on system passwords.

2. What is Ransomware that creates a .bora file?

Ransomware Series : STOP (DJVU) ransomware

Extensions : Bora

Ransom file : _readme.txt

Ransom : From 490 USD to 980 USD (in Bitcoin)

Contact : gorentos@bitmessage.ch, gerentoshelp@firemail.cc or @datarestore on Telegram

Ransomware creates a .bora file that restricts data access by encrypting the file. Then blackmail the victim by requesting a ransom in electric money from Bitcoin to regain access to the data. This ransomware targets all versions of Windows including Windows 7, Windows 8 and Windows 10. When first installed on the computer, this ransomware will create an executable file named randomly in the% AppData% folder. or% LocalAppData%. This executable will launch and start scanning all drive letters on your computer for encrypted data files.

Ransomware creates a .bora file extension looking for specific file extensions to encrypt. The files it encrypts are usually important documents and files such as .doc, .docx, .xls, .pdf, etc. When it is found, it will change the file extension to bora so that it cannot be opened anymore. .

Below is a list of file extensions that this ransomware targets:

.sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .zip, .sie, .sum, .ibank, .t13, .t12, .qdf , .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .hplg,. hkdb, .mdbackup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mov, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .vcf, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x , .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0, .mpqge, .kdb, .db0, .dba,. rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, wallet, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c, .p7b, .p12, .pfx, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raw, .raf , .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe,. jpg, .cdr, .indd, .ai, .eps, .pdf,. pdd, .psd, .dbf, .mdf, .wb2, .rtf, .wpd, .dxg, .xf, .dwg, .pst, .accdb, .mdb, .pptm, .pptx, .ppt, .xlk, .xlsb, .xlsm, .xlsx, .xls, .wps, .docm, .docx, .doc, .odb, .odc, .odm, .odp, .ods, .odt

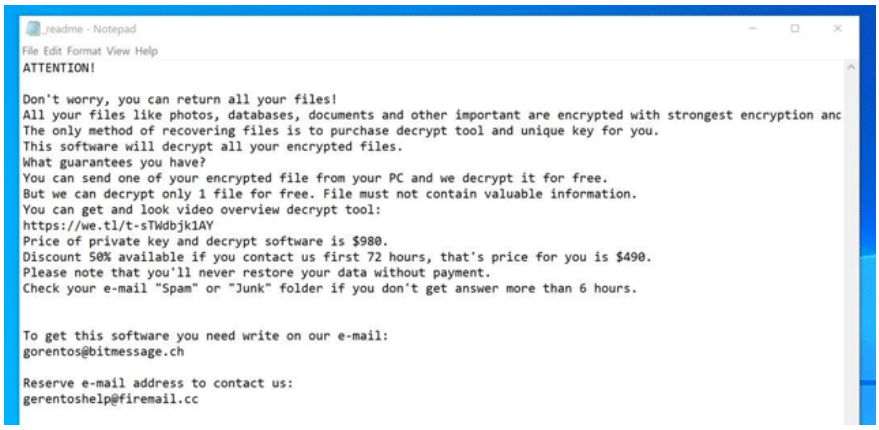
When the file is encrypted with the bora extension, this ransomware creates _readme.txt, explaining how to get back the file and asking for a ransom in each folder that the file has been encrypted and on the Windows desktop. These files are placed in every encrypted file folder and contain information on how to contact cyber criminals to retrieve the files.

When the scan is completed, it will also delete all Shadow Volume Copy on the infected computer that cannot be used to recover encrypted files.

3. Is your computer infected with ransomware creating a .bora file extension?

When the computer is infected with this ransomware, it scans all drive letters to find the target file type, encrypts them and then adds the bora extension. When these files are encrypted, you will not be able to open them with normal programs. When this ransomware completes encrypting the victim's file, it also displays a file containing instructions on how to contact a cyber criminal (gorentos@bitmessage.ch or gerentoshelp@firemail.cc).

This is a ransom notification in the _readme.txt file.



4. Is it possible to decrypt files encrypted with ransomware to create .bora extensions?

Unfortunately, you cannot restore files encrypted with ransomware to create .bora extensions because a private key is required to unlock, which only criminals can have.

However, you also do not have to pay to recover files. Even if you pay for them, there's no guarantee you'll get your file access back.

5. How to delete ransomware to create .bora file extension

Refer to the section on how to delete ransomware in the article How to delete ransomware to create .boot file to know how to delete ransomware to create .bora file.

To prevent your computer from ransomware creating a .bora file, you need to install an antivirus program on your computer and always back up personal documents. You can also use a program called HitmanPro.Alert to prevent file encryption malware from running on the system.

I wish you successful implementation!

You finished reading the article "**How to delete ransomware creates .bora file extension**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.