# How to delete ransomware creates a .boot file

If the image, document, or file is encrypted using the Boot extension, it means your computer has been infected with ransomware STOP (DJVU).

If the image, document, or file is encrypted using the Boot extension, it means your computer has been infected with ransomware STOP (DJVU).

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

**Warning:** This guide will help you to remove ransomware from creating a .boot file, but it will not help recover the file. You can try ShadowExplorer or free file recovery software to recover data.

## Instructions to remove ransomware create .boot file extension



## 1. How does Ransomware create a .boot file? How do I get to your computer?

Ransomware creates bootable files distributed via email that contain ransomware-infected attachments or enters by exploiting holes in the operating system and installed software.

Cybercriminals spam email with fake information to trick you into sending messages from shipping companies like DHL or FedEx. The email notifies you that you have an order, but for some reason it cannot be sent to you. Or sometimes, an email notifying you of the order you have made. Either way, it makes people curious and open the attachment (or click on the link embedded in the email). As a result, your computer is infected with ransomware creating a .boot file.

Ransomware creates a .boot file that can also be hacked by hacking Remote Desktop Services (RDP) ports. Attackers scan systems running RDP (TCP port 3389) and then perform brute force attacks on system passwords.

# 2. What is Ransomware creating a .boot file?

**Ransomware Series** : STOP (DJVU) ransomware

**Extensions** : Boot

**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 .boot file that restricts access to data by encrypting files. It then tried to blackmail the victim by requesting a ransom in Bitcoin cryptocurrency 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 .boot file that looks for files with specific file extensions for encryption. 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 Boot 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

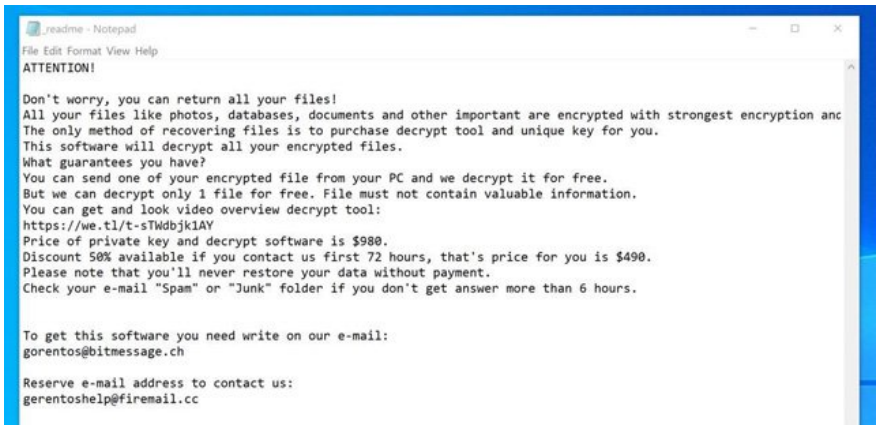
When the file is encrypted with the Boot extension, this ransomware will create the file _readme.txt, explaining how to retrieve the file and ask for a ransom in each folder where the file is encrypted and on the Windows desktop. These files are placed in every encrypted file folder and contain information 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 so that it cannot be used to recover encrypted files.

# 3. Is your computer infected with ransomware creating a .boot file?

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 Boot 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).

Here is the ransom notification in the _readme.txt file:




# 4. Is it possible to decrypt files encrypted with ransomware to create .boot files?

Unfortunately, the answer is no. You cannot recover files that are encrypted with ransomware, create a .boot file, because you need a private key to unlock encrypted files, which only cyber criminals have.

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

# 5. How to remove ransomware to create .boot file extension

**Warning:** It is important to note that with this approach you will lose your files. Malwarebytes and HitmanPro can detect and remove this ransomware but these programs cannot recover documents, photos or files. Therefore consideration should be given to this process.

### Use Malwarebytes to remove ransomware and create a .boot file

Malwarebytes is one of the most popular and most used anti-malware software for Windows. It can kill many types of malware that other software may miss.

Refer to Effective virus removal with Malwarebytes Premium software to know how to use this malware.

### Use HitmanPro to scan for unwanted malware and programs

HitmanPro is a scanner that implements a unique cloud-based method to scan for malware. HitmanPro scans the behavior of active files and files in locations where malware normally resides to perform suspicious activities. If a suspicious file is found to be unknown, HitmanPro will send it to the cloud for two of the best antivirus tools Bitdefender and Kaspersky to scan.

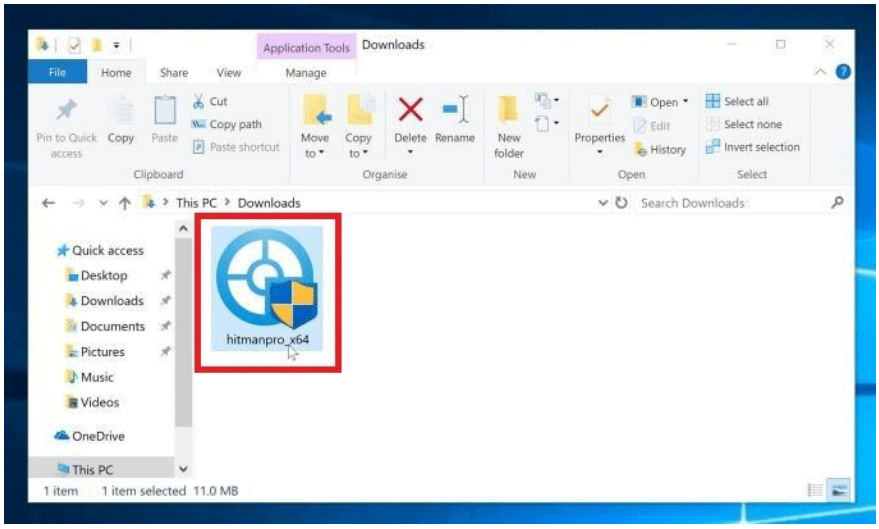
Although HitmanPro is shareware, it costs $ 24.95 for a year with a computer, but practically unlimited scanning. Limited only if you need to remove or quarantine the malware detected by HitmanPro on the system and then you can activate the 30-day trial to clean.

**Step 1.** Download HitmanPro

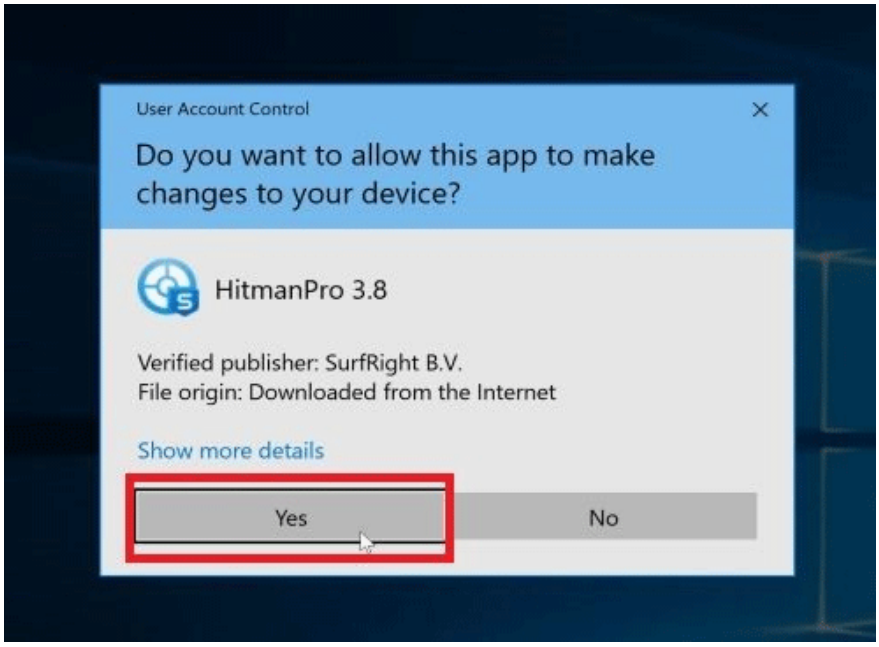
1. Download HitmanPro for 32-bit Windows
2. Download HitmanPro for 64-bit Windows

**Step 2.** Install HitmanPro

After the download is completed, double click 'hitmanpro.exe' (for 32-bit Windows) or 'hitmanpro_x64.exe' (for 64-bit Windows) to install the program on your computer. Usually, the downloaded file will be saved to the Downloads folder.

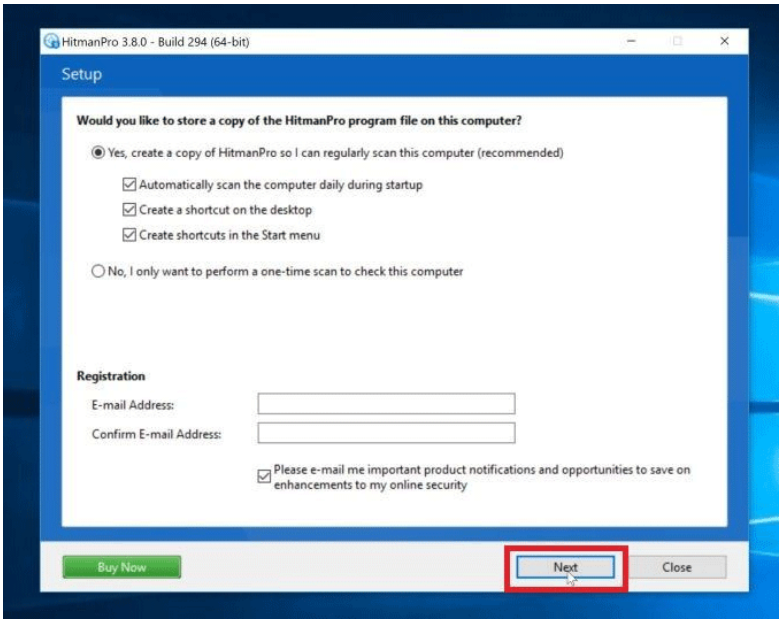



If the UAC message appears, click **Yes** .



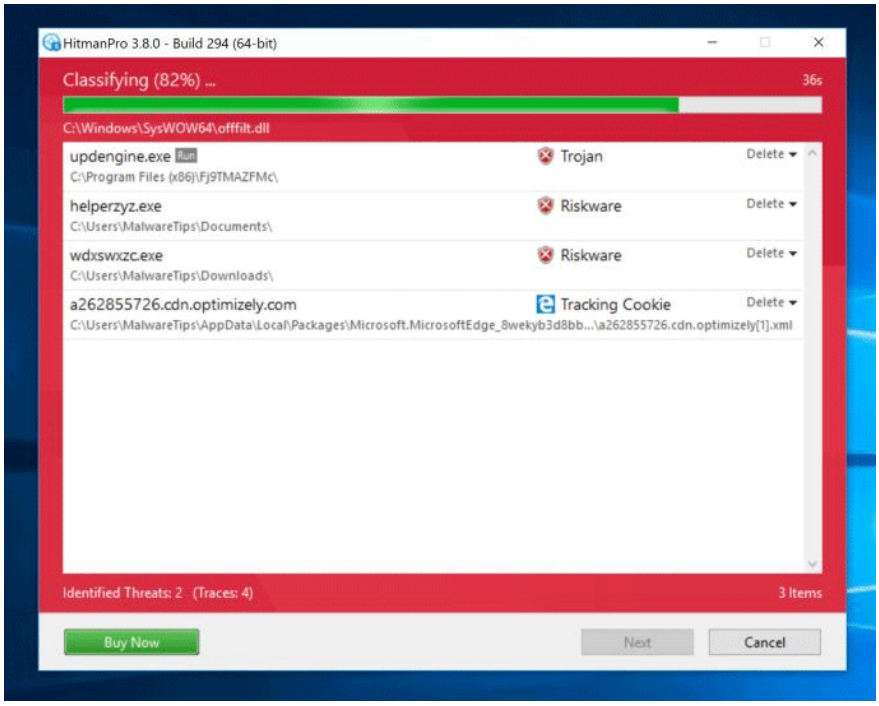

**Step 3.** Follow the instructions on the screen

When starting HitmanPro, you will see the boot screen as shown below. Click the **Next** button to perform a system scan.



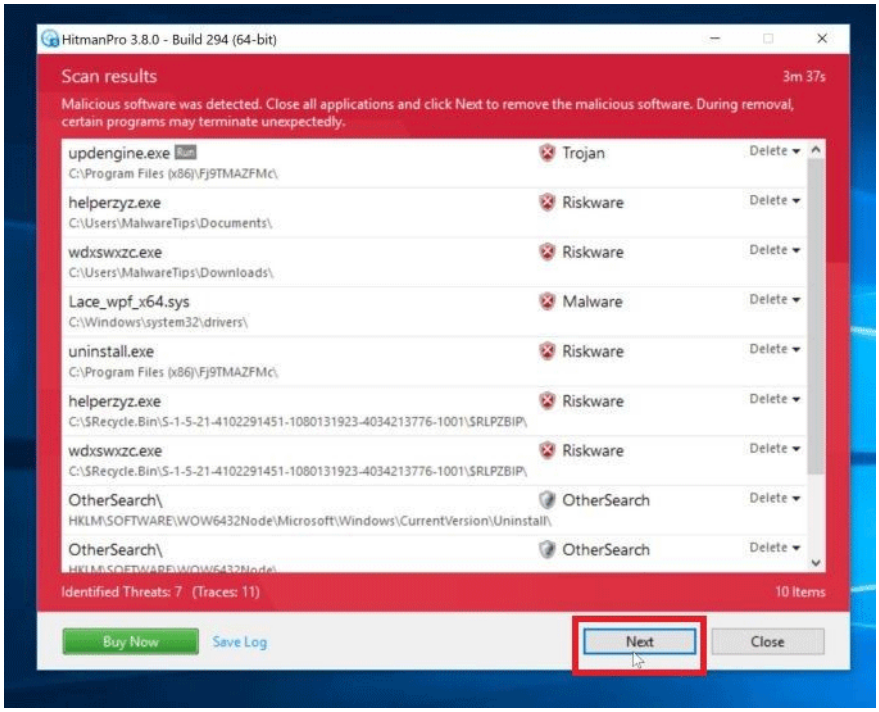

**Step 4.** Wait for the scan to complete

HitmanPro will start scanning your computer for malicious programs. This process may take several minutes.



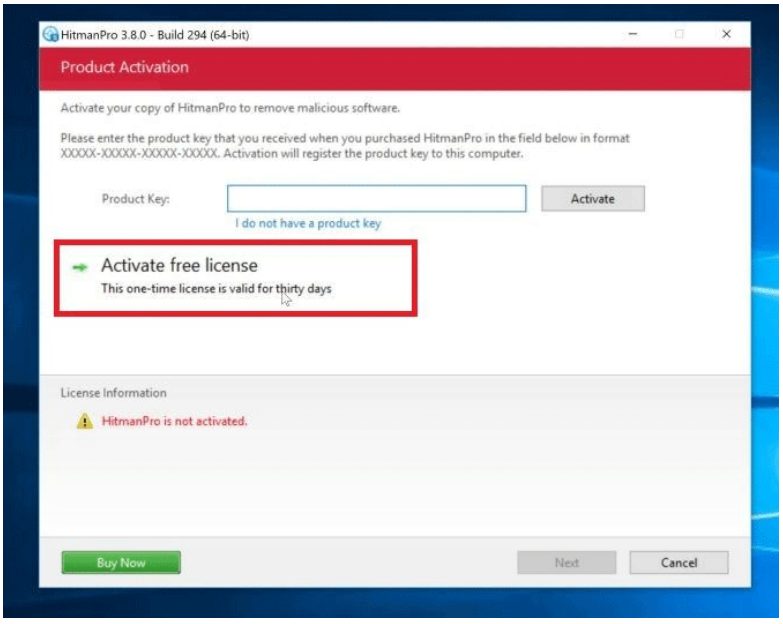

**Step 5** . Click on **Next**

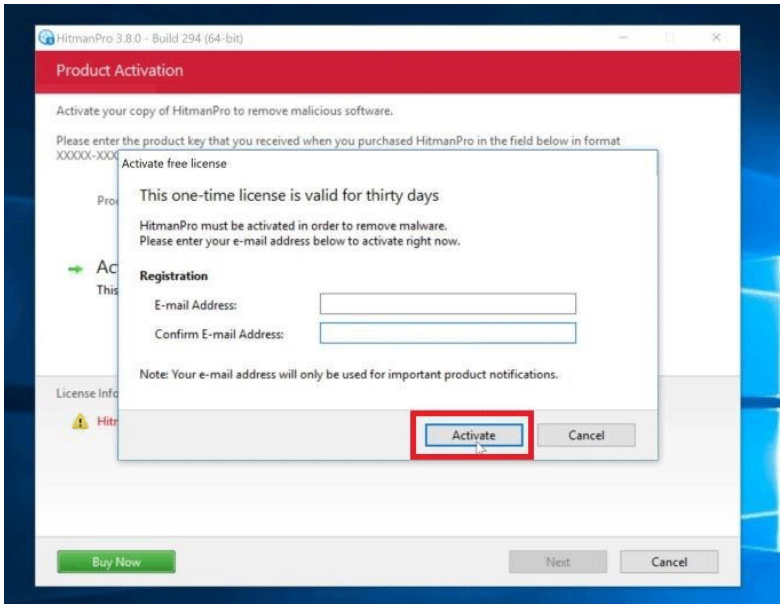
When HitmanPro finishes scanning, it will display a list of all malware found. Click **Next** to remove the malicious program.




**Step 6** . Click on **Activate free license**

Click the **Activate free license** button to start your free 30-day trial and remove the malicious file from your computer.






When the process is complete, you can close HitmanPro and continue the rest of the tutorial.

## Recover files encrypted with ransomware to create .boot file with recovery software

In some cases, it is possible to restore an earlier version of an encrypted file using Boot Restore or other unusual recovery software that contains a shadow copy of the file.

Below is a tool to decode encrypted STOP ransomware files, created by experts on the Bleeping Computer security forum, you can try to see if you can retrieve your data. If this doesn't work, try other solutions below.

```
https://download.bleepingcomputer.com/demonslay335/STOPDecrypter.zip
```

### Option 1: Recover encrypted files with ransomware and create .boot file extensions with ShadowExplorer

Ransomware creates a .boot file extension that will attempt to delete all shadow copies when it first launches any executable file on the computer after being infected with ransomware. Fortunately, ransomware cannot eliminate shadow copies, so you should try to recover your files using this method.

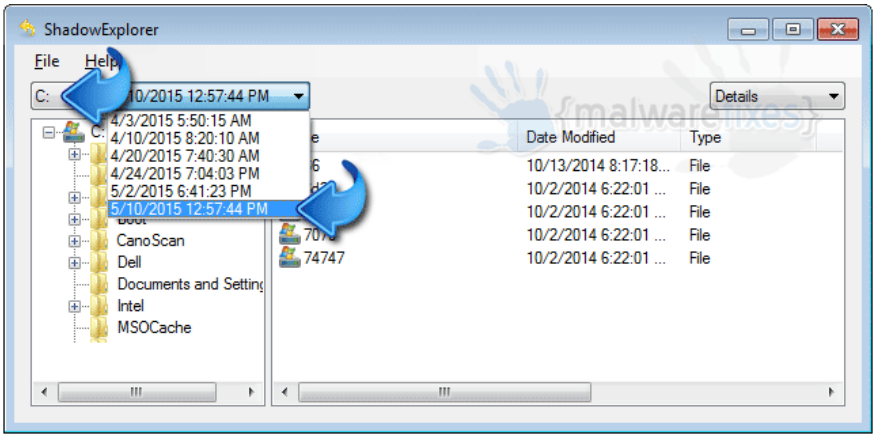
**Step 1** . Download ShadowExplorer by following the download link below.

1. Download ShadowExplorer for Windows

**Step 2.** Install the program with default settings.

**Step 3.** The program will run automatically after installation. If not, double click on the ShadowExplorer icon.

**Step 4** . You can see the drop down list at the top of the dashboard. Select the drive and the most recent shadow copy you want to recover before ransomware gets infected with a .boot file extension.




**Step 5** . Right-click on the **Drive** , **Folder** or **File** you want to recover and click on **Export .**

**Step 6** . Finally, ShadowExplorer will notify you where you want to save the restored file copy.

**Option 2: Recover encrypted files with Boot extension with file recovery software**

When the file is encrypted, this ransomware first creates a copy of them, encrypts the copy and then deletes the original. Therefore, there is a small chance you can use file recovery software to recover deleted files such as Recuva, EaseUS Data Recovery Wizard Free, R-Studio.

**Option 3: Use the Previous Versions tool of Windows**

Windows Vista and Windows 7 have a feature called Previous Versions. However, this tool can only be used if the restore point was made before ransomware infection created the .boot file extension. To use this tool and restore ransomware-infected files, follow these steps:

**Step 1** . Open **My Computer** or **Windows Explorer** .

**Step 2.** Right-click the infected file or folder ransomware. From the drop-down list, click **Restore previous versions** .

**Step 3** . A new window will open showing all backups of the files and folders you want to restore. Select the appropriate file and click **Open** , **Copy** or **Restore** . Restore selected files to overwrite existing encrypted files on the computer.

# 6. How to prevent a computer from being infected with ransomware to create a .boot file extension

To prevent your computer from ransomware creating a .boot file extension, 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!