

Learn about Repl virus

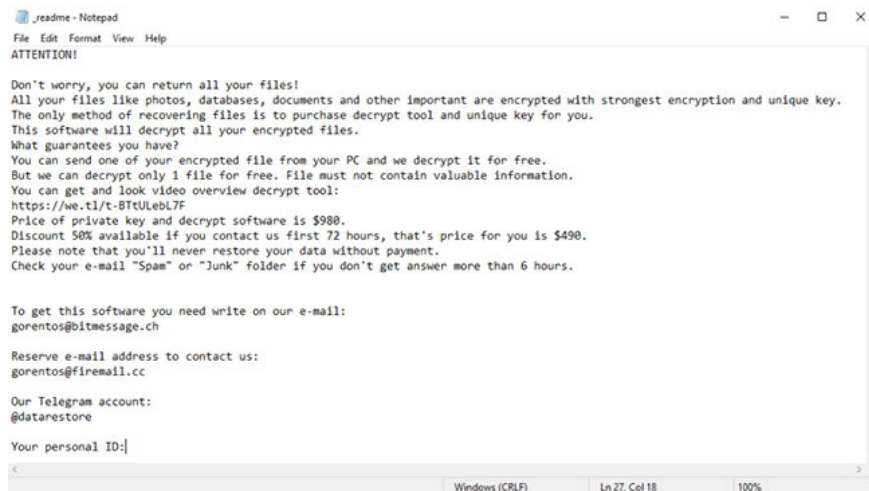
Repl belongs to ransomware DJVU family. This virus infects and encrypts important personal files (videos, photos, documents). The encrypted file has the extension '.repl'. So you absolutely cannot open them.

What is repl?

Repl is identified as ransomware. Ransomware is a specific virus that encrypts your documents and then forces you to pay to restore them. Note that the DJVU ransomware family (also known as STOP) was first revealed and analyzed by virus analyst Michael Gillespie.

Repl is similar to the other ransomware in them: Maas, Zida, Pykw. Repl encodes all common file types. Therefore, users cannot open their documents. Repl adds its own **.repl extension** to all files. For example, the video file '**video.avi**' will be changed to '**video.avi.repl**'. As soon as the encoding is done successfully, Repl will issue a special file '**_readme.txt**' and add it to all directories containing the modified files.

This text requires payment to recover files via decryption key:



The encryption algorithm used by Repl is AES-256. Therefore, the files are encrypted with a specific decryption key, unique and no other copy. The sad fact is that it is not possible to recover information without this unique key.

In case if Repl works in online mode, you cannot have access to AES-256 key. It is hosted on a remote server owned by scammers who have distributed Repl virus.

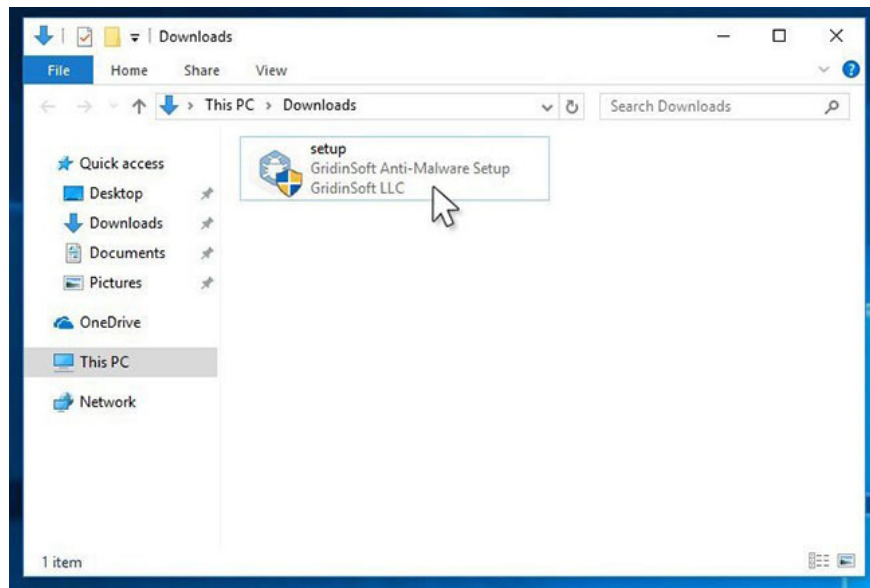
To receive the decryption key, you need to pay the payment of \$ 980 (over 22 million). In order to obtain payment details, victims are encouraged to text the contact via email (helpmanager@mail.ch) or via Telegram.

How to remove Repl virus

In addition to encrypting the victim's files, Repl also started to install Azorult Spyware on the computer to steal account login information, e-wallets, files on the desktop, etc.

There is no better way to identify, remove, and prevent ransomware than to use anti-malware program from GridinSoft.

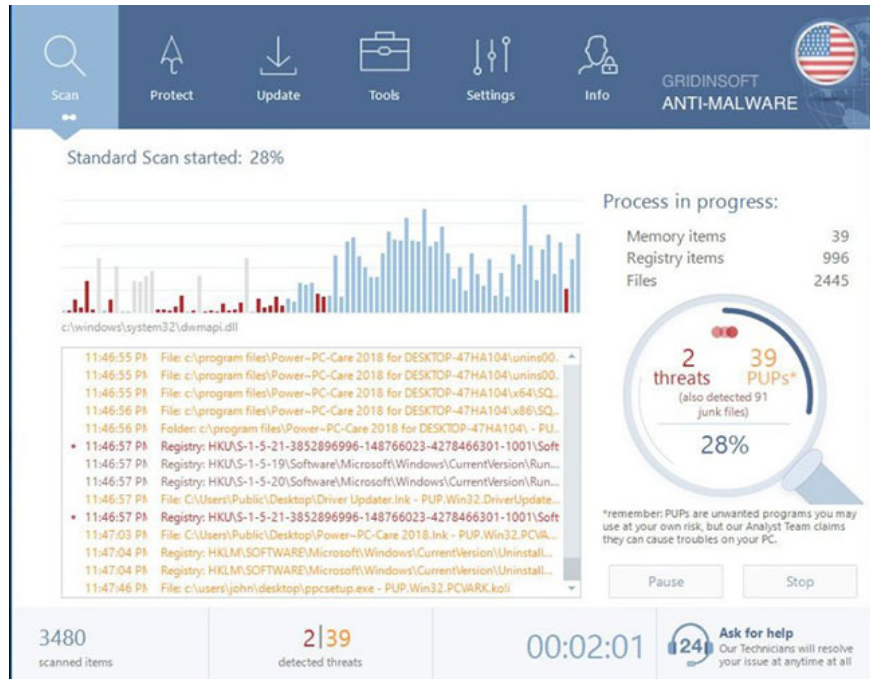
1. Download removal tool: You can download GridinSoft Anti-Malware here.
2. Run the setup file.
 1. Once the setup file has finished downloading, double-click the **setup-antimalware-fix.exe** file to install GridinSoft Anti-Malware on the system.



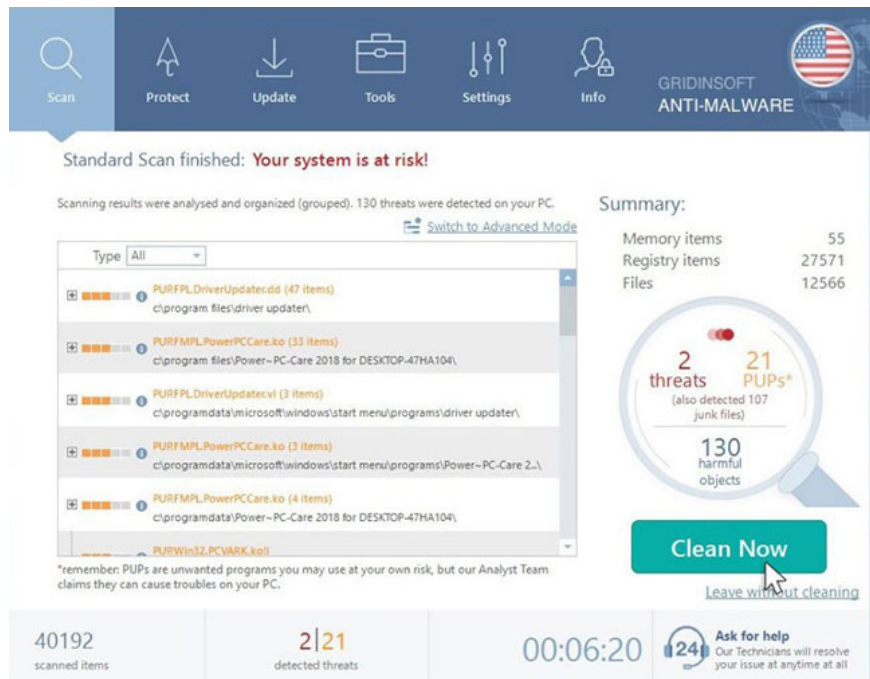
1. **User Account Control** will ask you whether or not you allow GridinSoft Anti-Malware to make changes to the device. So you should click **Yes** to continue the installation.
2. Click the **Install** button .



1. Once installed, Anti-Malware will automatically run.
2. Wait for the Anti-Malware scan to complete. GridinSoft Anti-Malware will automatically start scanning your PC to detect Repl infections and other malicious programs. This process can take 20-30 minutes, so you can take advantage of other work and periodically check the status of the scan.



1. Click the **Clean Now** button : When the scan is complete, you will see a list of infection viruses that GridinSoft Anti-Malware has detected. To remove them, click the **Clean Now** button in the right corner.



Recovery solution for .repl files

Try removing the .repl extension on some large files and opening them. It is possible that Repl has read and unencrypted the file, or it is corrupted and does not add a filemarker. If your files are very large (over 2GB), then the latter is most likely. Please let everyone know in the comments, if this helps you.

You can also download and try the following decryption tool: Decryptor for STOP Djvu.

You finished reading the article "**Learn about Repl virus**" 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.