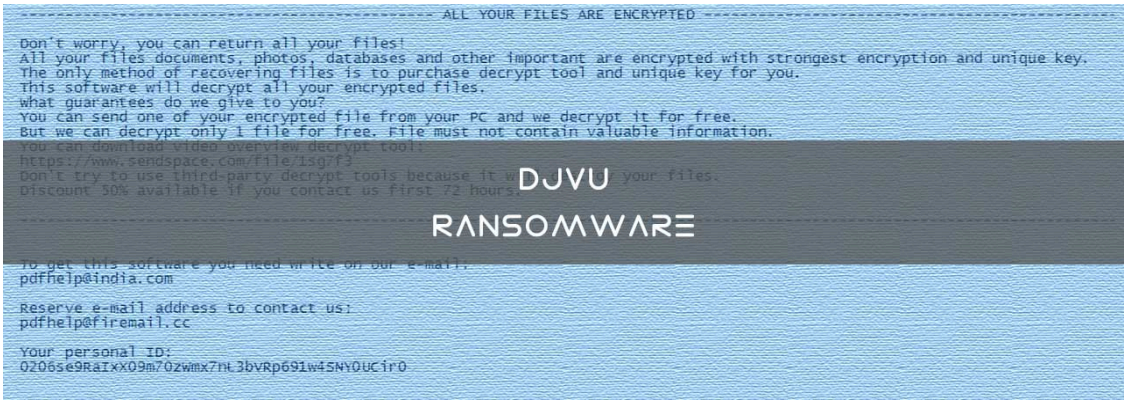
# Djvu Ransomware Spreading New .TRO Variant Through Cracks & Adware Bundles

By Lawrence Abrams

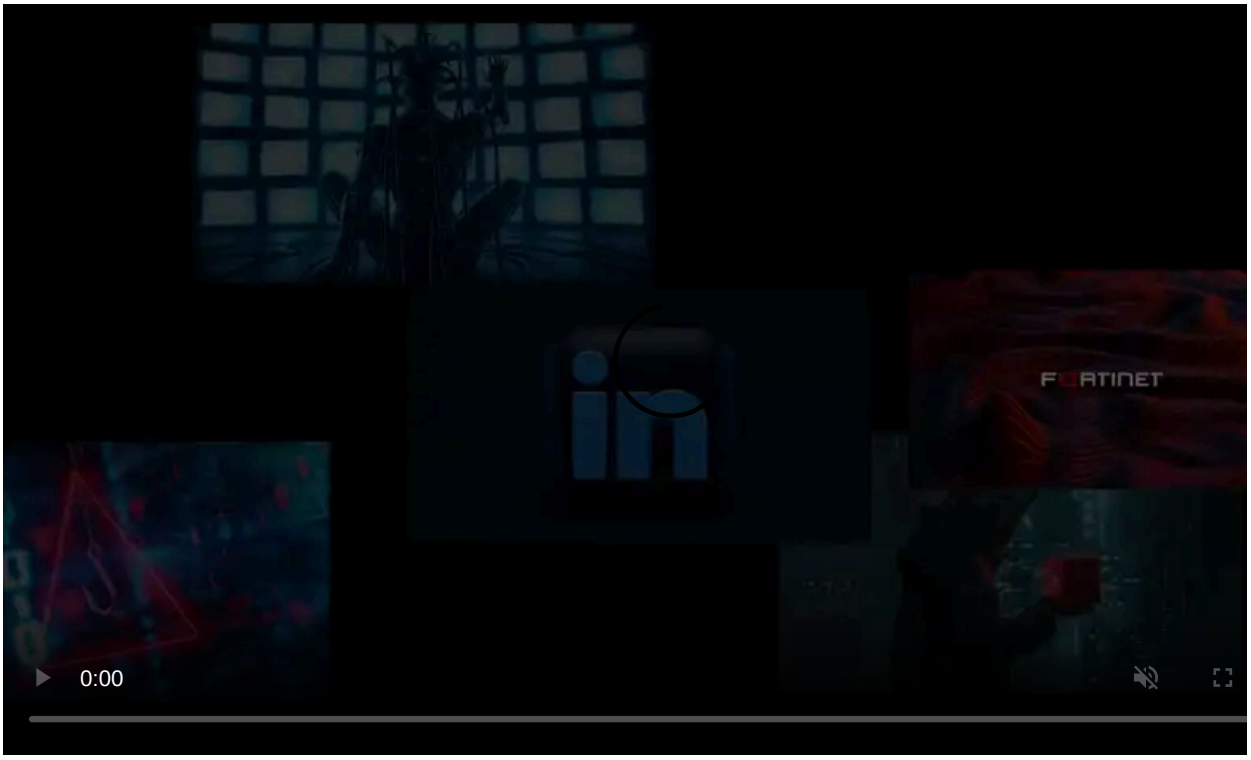
Published: 2019-01-16 · Archived: 2026-04-05 19:11:18 UTC

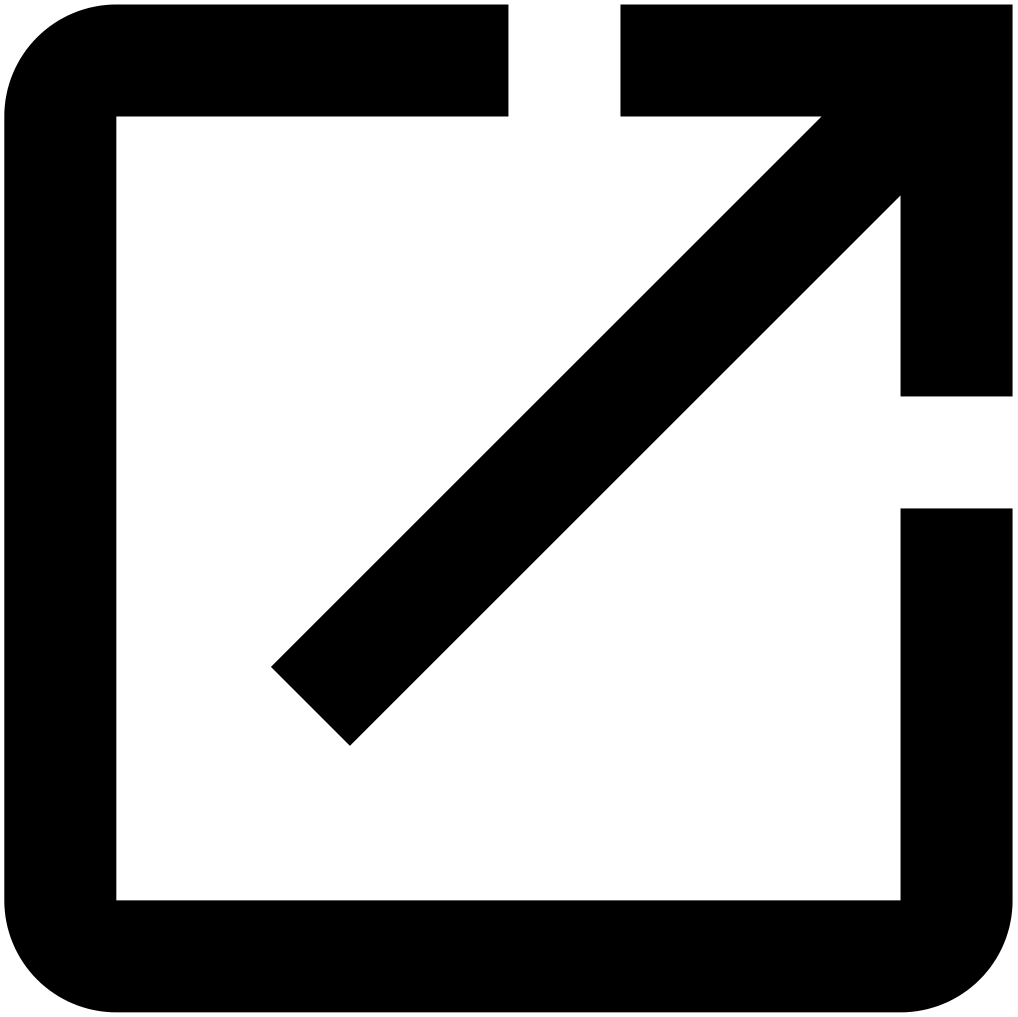


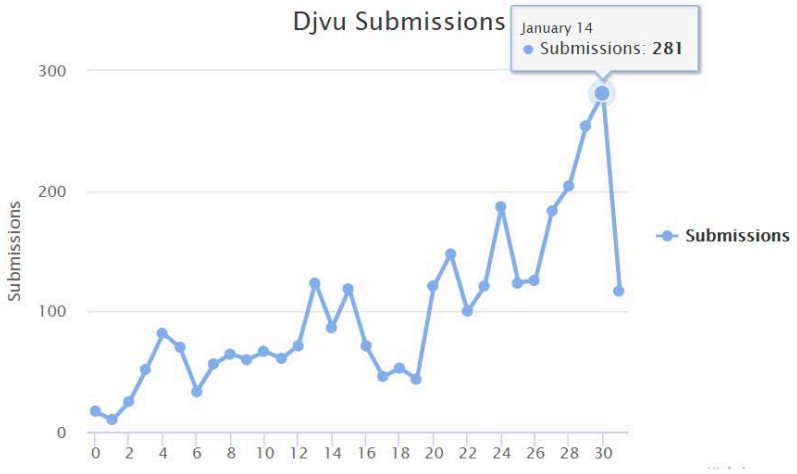

In December 2018, a new ransomware called Djvu, which could be a variant of STOP, was released that has been heavily promoted through crack downloads and adware bundles. Originally, this ransomware would append a variation of the .djvu string as an extension to encrypted files, but a recent variant has switched to the .tro extension.

When first released, it was not known how the ransomware was being distributed and a sample of the main installer could not be found. When discussing the infection with the numerous victims who reported it in our forums and elsewhere, a common theme was noted; most of the victims stated that they became infected after downloading a software crack.

This campaign has been very successful, with ID-Ransomware reporting numerous victims submitting files to their system on a daily basis.


0:00






**ID-Ransomware Submissions**

The good news is that it may be possible to receive help in recovering your files for free. If you are infected with STOP Ransomware (.djvu, .tro, or .rumba), please see this post about using Michael Gillespie's decryptor.

If that fails to help, then please register an account and post the following information in a new reply to our dedicated STOP Ransomware Support & Help topic:

- Network card's MAC address. This can be gotten from using the command **getmac /v**. If you are not sure which MAC address to use, feel free to copy the entire output.
- A link to two encrypted files. You can use the Wetransfer service for this.
- Your personal ID from the ransom note.

After you submit this information, we will try and help you, but please be patient..

If you have any questions or need help, feel free to ask here or in our dedicated STOP Ransomware Support and Help topic.

## How the Djvu Ransomware encrypts a computer

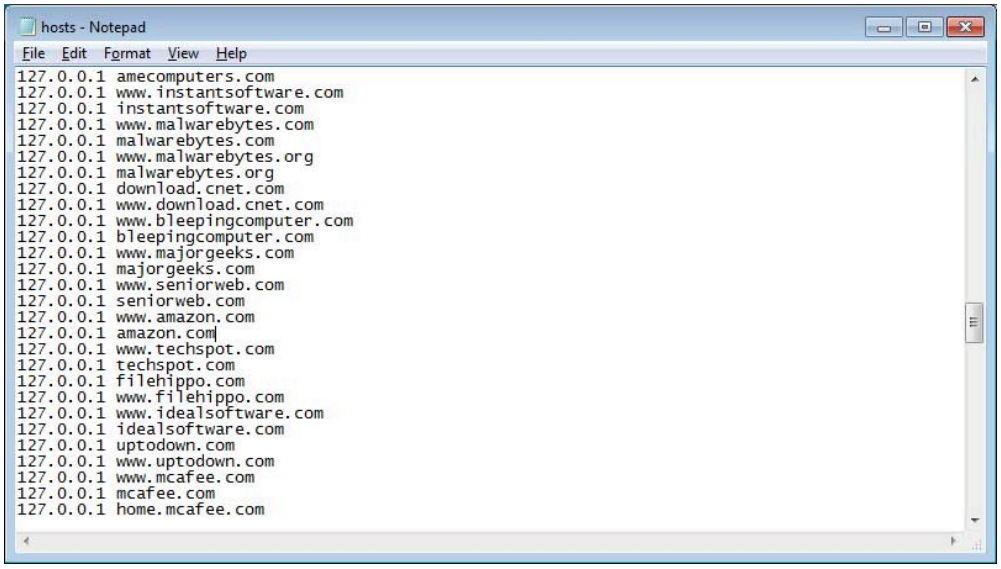
Certain cracks and adware bundles are installing this ransomware onto victim's computers. When these cracks are installed, the main installer will be installed as %LocalAppData%\[guid]\[random].exe and executed. This program is the main ransomware component and will first download the following files to the same folder:

```
 %LocalAppData%\[guid]\1.exe
%LocalAppData%\[guid]\2.exe
%LocalAppData%\[guid]\3.exe
%LocalAppData%\[guid]\updatewin.exe
```

When executed, 1.exe will execute various commands that remove the definitions for Windows Defender and disable various functionality. This executable will also execute a PowerShell script called Script.ps1, which disabled Windows Defender's real-time monitoring using this command:

```
Set-MpPreference -DisableRealtimeMonitoring $true
```

The ransomware will then execute 2.exe, which adds numerous security sites and download sites to the Windows HOSTS file so that victims are unable to connect to them for help. BleepingComputer is one of the sites added to the HOSTS file as shown below.




**HOSTS File**

A file called 3.exe will then be executed, which we have not been able to find a sample of, so are unsure as to what it does.

During this process, the ransomware will generate a unique ID for the machine, which according to Michael Gillespie is a MD5 of the system's MAC address, and connect to it's Command & Control server at the url http://morgem[.]ru/test/get.php?pid=[machine_id]. The server would then reply back with the encryption key that should be used to encrypt a victim's files.

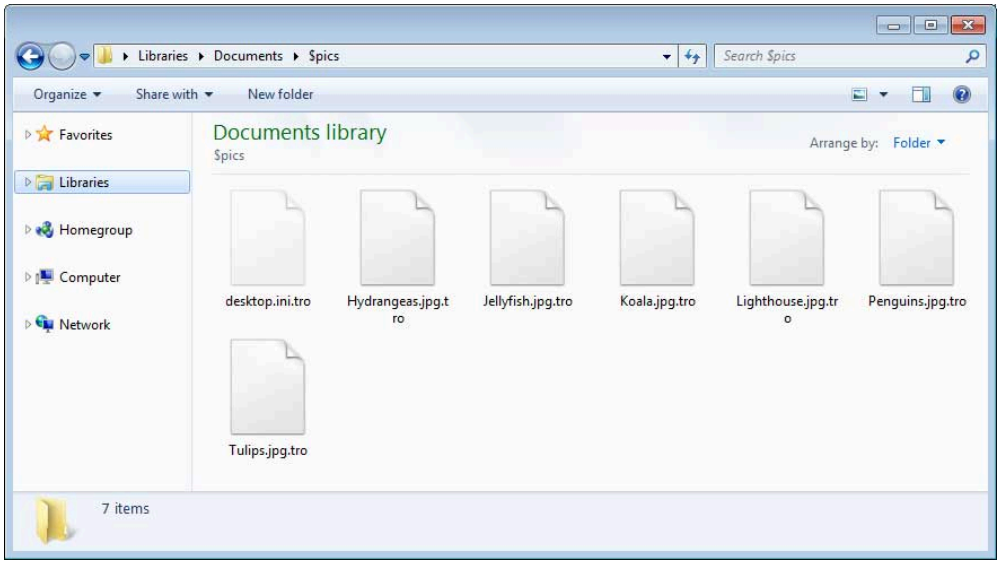
If you are using sflow, netflow, or sniffing traffic on your network then it may be possible to recover your encryption key when the C2 server sends it to the victim's computer.

The ransomware will now begin to encrypt the files on the computer and at the same time execute the updatewin.exe. Updatewin.exe will display a fake Windows Update screen in order distract the user while their files are being encrypted and to make it seem normal that disk activity has increased.


**Fake Windows Update**

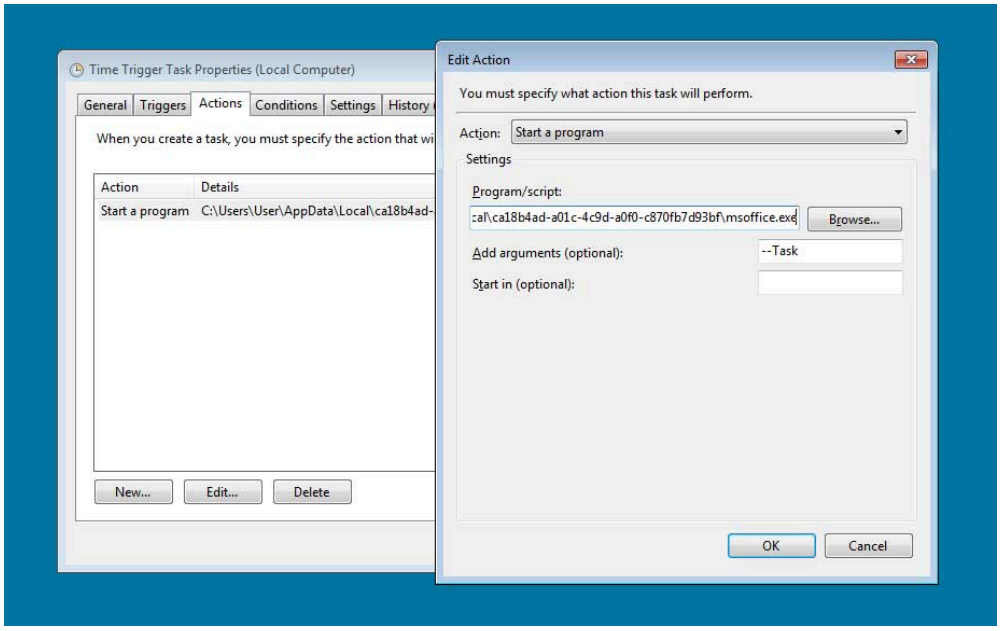
During encryption, the ransomware will encrypt almost all files on the computer, including executables. When encrypting files, the older variant would append a variant of the string **.djvu** to the encrypted file's name. For example, test.jpg would be encrypted and then renamed to test.djvu, test.djvus, or test.djvut.

Newer variants are instead appending the **.tro** extension to encrypted file's names as shown by the image below.



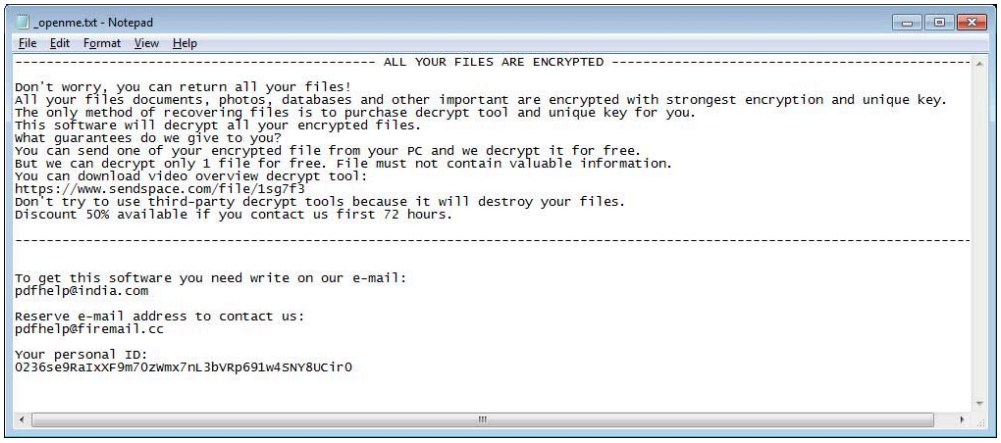

**Encrypted TRO Files**

Finally, the ransomware will create a scheduled task named "**Time Trigger Task**". This task will launch the ransom at various intervals in order to encrypt any new files that are created.




**Scheduled Task**

While encrypting files, it will drop ransom notes named **_openme.txt** in each folder that files are encrypted. This ransom note will contain information regarding what happened to the victim's files and two email addresses that they should contact in order to receive payment instructions.




**Djvu Ransom Note**

As previously stated, if you are infected with this ransomware, then it may be possible to recover your files for free. To request help, please see the instructions at the beginning of this article.

## IOCs

### Hashes:

```
Main installer: 5d294a14a491dc4e08593b2f6cdcaace1e894c449b05b4132b9ba5c005848c58
1.exe: 6966599b3a7786f81a960f012d540866ada63a1fef5be6d775946a47f6983cb7
2.exe: 91a1122ed7497815e96fdbb70ea31b381b5243e2b7d81750bf6f6c5ca12d3cee
updatewin.exe: 74949570d849338b3476ab699af78d89a5afa94c4529596cc0f68e4675a53c37
```

### Associated Files:

```
%LocalAppData%\[guid]\[random_numbers]tmp.exe
%LocalAppData%\[guid]\1.exe
%LocalAppData%\[guid]\2.exe
%LocalAppData%\[guid]\3.exe
%LocalAppData%\[guid]\updatewin.exe
C:\Windows\System32\Tasks\Time Trigger Task
```

### Associated Registry Entries:

```
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SysHelper
```

### Associated Email Addresses:

```
restoredjvu@india.com
restoredjvu@firemail.cc
helpshadow@india.com
helpshadow@firemail.cc
pdfhelp@india.com
pdfhelp@firemail.cc
```

### Network Traffic:

```
api.2ip.ua
morgem.ru
```

**Ransom Note Text:**

```
---------------------------------------------- ALL YOUR FILES ARE ENCRYPTED ----------------------------------------------

Don't worry, you can return all your files!
All your files documents, photos, databases and other important are encrypted with strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees do we give to you?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can download video overview decrypt tool:
https://www.sendspace.com/file/1sg7f3
Don't try to use third-party decrypt tools because it will destroy your files.
Discount 50% available if you contact us first 72 hours.

------------------------------------------------------------------------------------------------------------------------



To get this software you need write on our e-mail:
pdfhelp@india.com

Reserve e-mail address to contact us:
pdfhelp@firemail.cc

Your personal ID:
[id]
```

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---