# ISSUE: User Files are Encrypted and Held for Ransom

355 Faye Buckley June 16, 2016 Security

**Problem:**

User entered a ticket stating that all of their files had been encrypted and now would have to pay a "ransom" to have their files decrypted. Sure enough, every .doc, .docx, .xlsx, .pdf, music file and picture were appended with the .crypt ending and would not open. Each encrypted folder contained **de_crypt_readme.bmp**, **de_crypt_readme.html** and **de_crypt_readme.txt**. Strangely none of the .pub files were encrypted.

**Solution:**

**Note:** The steps below will have to be done under the user's profile. Also the steps are just a general overview. If more specific information is needed please let me know.

First you have to find the source of the virus and kill it and the process. Each one may be different, keeping that in mind, I only have a solution for the one that I encountered. Avast, and SuperAntispyware would not detect the infection. Did not test Malwarebytes. Below is how I solved the problem:

1. Downloaded Spyhunter from Enigma Software http://www.enigmasoftware.com/products/spyhunter/. This program will not remove the infection unless you purchase the full version, but that is not the purpose of using this software. The purpose is using it just to find the infected files. Once found you can go back and removed them manually.
2. The main virus load is found usually in C:ProgramData. You will have to show hidden files and then remove the file with a filename in braces {…} filled with a string of numbers. If the file cannot be deleted through Windows, because the file is in use, then you will have to reboot the machine in Safe Mode with Command Prompt and remove it that way. To do this:

1. Boot into Safe Mode with Command Prompt and navigate to the root of C:.
2. To show the hidden files use attrib –s –h –r /s /d.
3. Change directory to ProgramData and then list the directory (dir). Locate the file name in braces.
4. Type del and the folder name and that will delete the contents of the folder.
5. Reboot the machine and log into the users account.
6. Navigate to C:ProgramData and delete the folder with the name in braces if it remains. The contents will be already deleted.

3. Once logged back into the users machine open the Task manager and be sure that Notepad.exe and msiexec.exe are not running. This ensures that the virus has not fired again. To be sure that it does not rebuild itself, go to root of C: and locate any file with a .dat ending that was created on the day that user stated that the encryption occurred and delete it. Also delete any files that were found during the scan with Spyhunter.
4. There may be some registry keys that will need to be deleted also. **Note: Only delete files that you do not recognize.**They are located at,

HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun

HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun

HKEY_LOCAL_MACHINESOFTWAREWow6432NodeMicrosoftWindowsCurrentVersionRun

5. Reboot the machine, log into the user's profile and open Task Manager. Once again ensure that Notepad.exe and Msiexec.exe are not running. **Note: The reason why you have to keep checking to make sure that these files are not running is because you will be connecting an external drive or usb drive to the machine. If these files are running, that means the virus is still active. Once you connect your external drive all files on it will be encrypted.**
6. Since the virus will delete previous versions of the documents, you will need a third party software to recover them. Go to http://www.shadowexplorer.com/downloads.htmland download and install the latest version of Shadow Explorer. Once installed, go to the upper left corner and open the dropdown menu and select a date close to the data of infection, but not the date of the infection. You will then be able to navigate to the user's profile and open his/her files and export them to an external drive. You can export individual files or entire folders.

**References:**


http://deletemalware.blogspot.com/2015/08/files-encrypted-crypt-extension.html

http://www.enigmasoftware.com/products/spyhunter/

http://www.shadowexplorer.com/downloads.html

http://visihow.com/Show_Hidden_Files_Using_Command_Prompt

Online URL: https://hdkb.clemson.edu/phpkb/article.php?id=355