

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE ISSUED: April 29, 2015

DATE UPDATED: May 1, 2015

SUBJECT: Talos/Cisco Release of Decryption Tool For TeslaCrypt

A tool was released recently, developed by Talos, which claims to decrypt files on machines that have been infected by TeslaCrypt/TesCrypt. Talos released a Python script, a Microsoft Windows executable, and the source code for the executable. The tool relies on the presence of the "key.dat" file, which is usually located in the user's Application Data directory in order to recover the master encryption key. While the ransom documents claim that the files are encrypted with RSA-2048, Talos discovered the files were actually encrypted using AES.

CIS tested the recovery tool against an image affected by TeslaCrypt with varying degrees of success. The Python script did not correctly decrypt the files in the test case, however the Windows executable did, as long as the master key was recoverable from the "key.dat" file, and the tool was used from the command line. CIS was able to fully recover the files from the affected machine using the tool. The tool also has a command line option that allows for the removal of the TeslaCrypt dropper if it's found active on the system.

MAY 1 UPDATE: A variant of TeslaCrypt, called Alpha Crypt, has been observed in the wild. This variant appends the file extension name ".ezz" to encrypted files, whereas the original TeslaCrypt would be named ".ecc." During testing, CIS was able to successfully decrypt these files by simply renaming them from the ".ezz" to ".ecc" file extension and running the previous steps. This is due to the decryption tool looking specifically for the ".ecc" file extension to find encrypted files. As the source code for the decryption tool is freely available, it can be altered to look for the new file extension.

RECOMMENDATIONS:

It is possible that this tool could successfully recover the files from a system infected with TeslaCrypt. The affected entity can download the tool from the Cisco blog (referenced below) and take the following steps:

1. Extract the TeslaDecrypter.exe from the TeslaDecrypt_exe.zip file.
2. Open a command prompt and change directory to the location of the TeslaDecrypter.exe
3. Run TeslaDecrypter.exe using the following parameters:
TeslaDecrypter.exe /keyfile:<location of the key file> /dir:<directory of encrypted files>. This will recurse into the directory. If the TeslaCrypt malware is still present on the system, also use the /deleteTeslaCrypt option on the command line in order to remove it.
4. Verify that the files were successfully recovered.

REFERENCES:

<http://blogs.cisco.com/security/talos/teslacrypt>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>