cyber SNAPSHOT

Exploring and Assessing Current Topics

MICHIGAN CYBER COMMAND CENTER (MC3)

Unclassified//For Official Use Only TLP: GREEN

Free Ransomware Decryption Tools

May 31, 2017
CS-02-2017

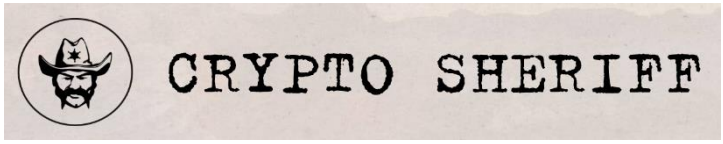
The Michigan Cyber Command Center (MC3) *Cyber Snapshot* is provided for situational awareness of current events in the cyber realm. Critical incidents and better security practice "options for consideration" are also included for review. **Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.**

Summary

Ransomware is a type of malicious software which has infected millions of systems in the United States and abroad. Once infected, ransomware will encrypt user files, making them inaccessible, and demand payment in order to access them. There are multiple free services available whose goal is to help victims of ransomware. They provide information and tools to help decrypt files which have been encrypted by ransomware.

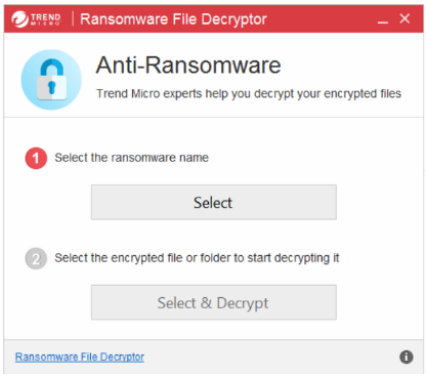
NoMoreRansom.org

Nomoreransom.org is a free service with the goal to help victims of ransomware. This project provides information and tools to help decrypt files that have been encrypted by ransomware. Initially introduced by the Dutch National Police, Europol, Intel Security and Kaspersky Lab in July of 2016, the "No More Ransom!" project is now supported by dozens of Law Enforcement and private sector partners. To date, there are approximately 40 tools that have been made available by project partners. These tools can be accessed through the **nomoreransom.org** web site. In addition to the tools, the project also provides information designed to educate users about how ransomware works and what can be done to help prevent infection.



If you have become infected and you do not know what variant you have been infected with you can upload encrypted files utilizing the "Crypto Sheriff" service. If available, you will be provided a link to the tool that can decrypt your files. Although many of the ransomware variants that are supported by **nomoreransom.org** target victims outside of the United States, it is possible United States citizens have been victimized by the variants they do support.

Trend Micro Ransomware File Detector

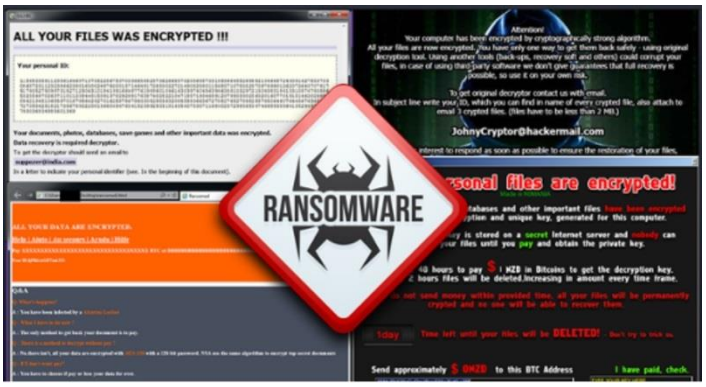


Trend Micro has a free ransomware file detector. It currently has the ability to decrypt files encrypted by 26 different ransomware types and families. Support for the original version of WannaCry (WNCRY, and WCRY) is one ransomware available for decryption through this site as well. If the user does not know the exact name of the ransomware they were infected with, this tool can analyze a locked file and attempt to detect which version it is. Trend Micro requires users to accept their End User License Agreement (EULA) prior to use. Additional information can be found at https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor

This document is the property of the Michigan Cyber Command Center (MC3) and is prepared for the limited purpose of information sharing. This information is designated **UNCLASSIFIED//FOR OFFICIAL USE ONLY** ***and is shared in confidence****. This document must not be reclassified in any way, in whole or in part. Further distribution is restricted without the consent and prior approval of the MC3. Release to the media of any information in this document is prohibited. Violation of these restrictions will be cause for removal from MC3 distribution lists.*

Avast

Avast has a free ransomware decryption tool. This tool can decrypt 18 different types of ransomware as of the writing of this document. Decryption tools available on this site address ransomware impacting Mac and Windows Operating Systems. FindZip, for example, is a ransomware type impacting Mac Operating Systems which is able to be decrypted by this tool. Avast has partnered with other organizations on the release of some of its decrypt tools, such as for the CryptoMix ransomware. Additional information can be found at https://www.avast.com/ransomware-decryption-tools



Emsisoft Decryptor

EMSISOFT Decrypter

Emsisoft is another security company offering free ransomware decryption tools. They currently offer decryption capabilities for 38 ransomware forms. Some decryption tools available through this organization require multiple files. For example, the decryptor for CryptON Ransomware requires the owner to provide two versions of the same file. Specifically, it uses an encrypted and unencrypted version of the same file to brute force the decryption key. Once it has guessed the correct key and decrypted the file, it provides the key to the user and uses it to decrypt all of the other files on the computer. Additional information can be found at https://decrypter.emsisoft.com/

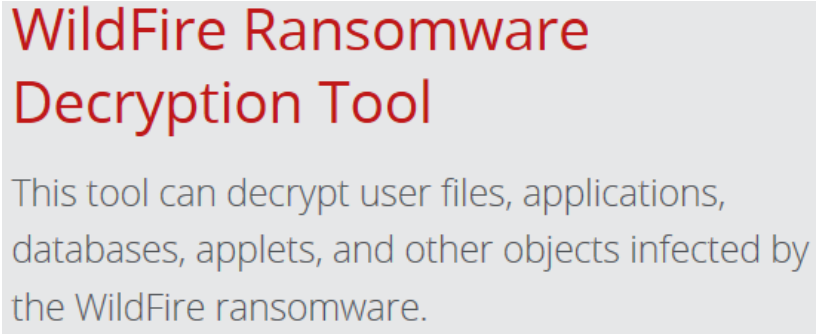
AVG Ransomware Decryption Tools

AVG also offers a free ransomware decryption tool. At this time, they have the ability to decrypt 7 different forms of ransomware. Like with Emsisoft tools, some decryption tools available through AVG utilize brute force techniques and require owners to have an encrypted and unencrypted version of the same file. The Bart ransomware decryption tool is an example of this. Additional information can be found at http://www.avg.com/us-en/ransomware-decryption-tools

This document is the property of the Michigan Cyber Command Center (MC3) and is prepared for the limited purpose of information sharing. This information is designated **UNCLASSIFIED//FOR OFFICIAL USE ONLY** ***and is shared in confidence****. This document must not be reclassified in any way, in whole or in part. Further distribution is restricted without the consent and prior approval of the MC3. Release to the media of any information in this document is prohibited. Violation of these restrictions will be cause for removal from MC3 distribution lists.*

McAfee Anti-Malware Tools

McAfee offers free ransomware decryption tools available for Shade, TeslaCrypt, and WildFire. While working collectively with global law enforcement and another security vendor, McAfee was able to develop a tool capable of unlocking user files, databases, applets, applications, and other objects infected by the Shade and WildFire ransomware. Decryption tools for WildFire and Shade are also available as part of the "No More Ransom" project. Tesladecrypt, a tool available to decrypt TeslaCrypt, has the ability to decrypt .mp3, .micro, .xxx, and .ttt file types. Additional information can be found at https://www.mcafee.com/us/downloads/free-tools/index.aspx



Analysis

If you have been infected and there is not currently a tool available to decrypt your files it is recommended you store your files as there may be a tool available in the future. While MC3 does not endorse any of the tools listed above, they may be able to provide assistance when dealing with a ransomware incident.

To help protect against ransomware attacks, the following should be considered:

- Keep your system up to date – Most versions of ransomware exploit neglected and unpatched systems. Keeping your Operating System and applications patched and updated may prevent ransomware from infecting your system.
- Back up your files to an external device or the cloud – This is good practice as you never know when your hard drive might fail. Keep a copy of the files that are important to you on a hard drive and in the cloud. Be sure to disconnect your external device from your system because ransomware will detect connected devices.
- Use antivirus software – Antivirus software may also help prevent ransomware infections. If you already have antivirus software be sure it is enabled and up-to-date.
- Be vigilant – Be wary of links on web pages and in email. Scan all email attachments with your antivirus software. Malicious links and email attachments are the most common causes of ransomware infection.

This document is the property of the Michigan Cyber Command Center (MC3) and is prepared for the limited purpose of information sharing. This information is designated **UNCLASSIFIED//FOR OFFICIAL USE ONLY** ***and is shared in confidence****. This document must not be reclassified in any way, in whole or in part. Further distribution is restricted without the consent and prior approval of the MC3. Release to the media of any information in this document is prohibited. Violation of these restrictions will be cause for removal from MC3 distribution lists.*