Try2Cry

Threat: **Ransomware**

Author: **Jeffrey Farnan**

Date Originally Published: **November 26th, 2020**

1. SUMMARY

Try2Cry is a .NET ransomware variant which searches for removable drives connected to the computer, it assigns a copy of itself named *Update.exe* to the root folder of every USB flash drive connected. It hides all files on the removable drives while replacing them with Windows shortcuts (LNK files) using the same icon. Once the user has clicked the LNK file, the original file is opened while also activating Update.exe and executing the Try2Cry ransomware payload in the background.

2. MALWARE FAMILY

- **Type** = Ransomware.
- **Sub-type** = USB Worm.

- Try2Cry comes from the "Stupid" ransomware family which can be found on GitHub and has numerous variants. This name was given by the malware authors themselves, they are not very advanced programmers, who use open-source code, making modifications and creating their own samples. GitHub is a place where people can share ideas, projects and source code and is mostly used for educational purposes. Ransomware code was originally posted on GitHub, as education proofs-of-concepts but since than variations of the code have been used in a variety of ransomware attacks.

3. MALWARE CHARATERISTICS

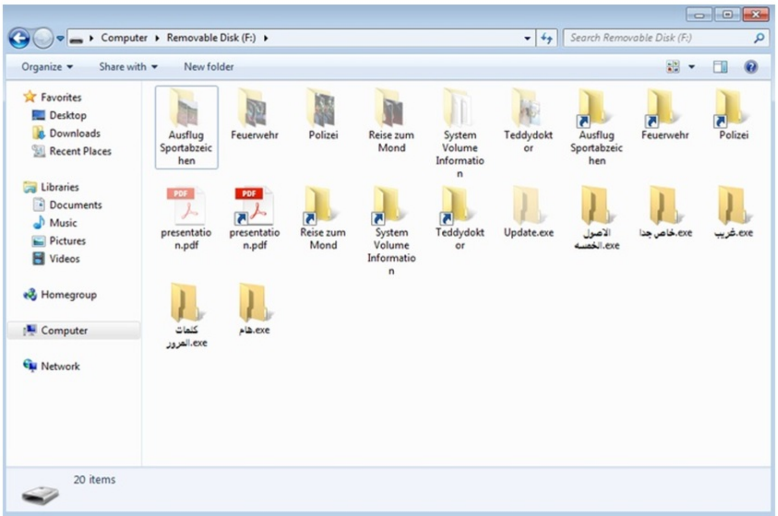
- **Suspected country of origin** = United States.
- **First seen date/period** = July 2020.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = November 12th, 2020.

4. MALWARE HISTORY

- Try2Cry was first discovered by a malware researcher called Karsten Hahn while analyzing an unidentified malware sample. Karsten was checking Yara detection signatures used to check USB worm components implemented in some variants of .NET based RATs which triggered an alert. The main feature of Try2Cry is its wormlike spreading capability, back in the old days, this sort of worm would simply use the autorun feature of Windows to automatically infect a machine when plugged in. On modern machines, with autorun disabled, malware authors have to be more creative in order to spread.

5. MALWARE DESCRIPTION

- The goal of Try2Cry is to spread to Ransomware to other windows operating systems by spreading via USB flash drives.
- The worm component looks for connected USB devices, when found, it sends a copy of itself called "update.exe“, to the USB's root folder. The next step is to hide all the files, folders and apps on the removable device and replace them with Windows (LNK files) with the same icon. When these shortcut links are clicked they open the original file plus launch the Update.exe Try2Cry ransomware payload in the background.



- The malware also creates visible copies of itself on the USB drives, using Arabic names on folders, in the hope curious victims will click on them and infect themselves. This is a dead giveaway and easily spotted, allowing users to see something is not right with their USB drive. When the Arabic names are translated to English we get: “Very special, Important, Passwords, A stranger, The Five Origins”.
- The ransomware encryption method uses Rijndael, which is a predecessor of AES. The encryption key is hard coded and is created by calculating a SHA512 hash of the password and using the first 32 bits of this hash. The ransomware targets multiple file types, including .doc, .ppt, .jpg, .xls, .pdf, .docx, .pptx, .xls, and .xlsx files, and appends a .Try2Cry extension to all encrypted files. The developer created two encryption exceptions for machines named DESKTOP-PQ6NSM4 and IK-PC2, any machine with these names would not be encrypted. This is probably the developers own machines used while testing.

6. POTENTIAL CUSTOMER DEFENSE

- Like other variants of the “Stupid” ransomware family, this ransomware is decryptable. It seems that this is just one of many variants of copy & paste ransomware created by criminals who can barely program.
- There are ways and methods a system can be decrypted or restored after the infection has been removed, System Restore, Shadow Explorer or a Data Recovery Tool can be a big help.
- The best method is to constantly back up your files.

Research Sources:

- https://securityaffairs.co/wordpress/105528/malware/try2cry-ransomware.html
- https://cybersecuritynews.com/try2cry-ransomware
- https://hackaday.com/2020/07/10/this-week-in-security-f5-novel-ransomware-freta-and-database-woes

Disclaimer: All opinions expressed in this article are the opinions solely of the author.