G DATA
Whitepaper 2018/02

Analysis of

Win32.Filecoder.Crypt888.B

Analysis by: https://twitter.com/RansomBleed

G DATA Software AG | Malware analysis | February 2018

Contents

1. Introduction

With the increasing adoption of cryptocurrencies and the therefore rising price of those, more and more malware authors are grabbing their piece of the cake.

The simplicity and the scope of functions is making AutoIt a popular choice of criminals. In addition to that, there are lots of already written source codes for almost any use-case online. Those two prerequisites combined give criminals an easy game to play. Unfortunately, this doesn't benefit the average person. In fact, the opposite is the case. It's making the life of ordinary people a lot harder and disturbing their private life. Many security companies in the world – just like G DATA – are doing their absolute best trying to protect the people. The reports about the different kinds of malware on this blog are for educational purposes. We all should know about the dangers of diseases and their future impacts. People prevent to be infected by diseases with vaccination. Similarly, we should at least be informed about the general dangers of malware to then further decide if we want to protect us or not. Because once a disease has started in our body or on our computer, it can't be stopped that easily anymore. Prevention helps.

2. Ransomware functions

Crypt888.B[1] is using several cryptographic functions of a publicly hosted source code on github[2]. The most important functions are listed below.

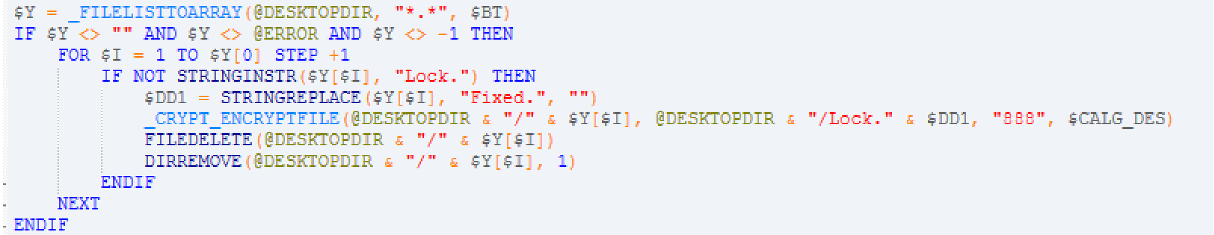
Function	Functionality
_Crypt_Startup	Initialize the Crypt library
_Crypt_Shutdown	Uninitialize the Crypt library
_Crypt_DeriveKey	Creates a key from algorithm and password
_Crypt_DestroyKey	Frees the resources used by a key
_Crypt_EncryptData	Encrypts data using the supplied key
_Crypt_EncryptFile	Encrypts a file with specified key and algorithm

As you might already see, there are encryption but no decryption functions inside the list. This tells us that this ransomware can't decrypt the files by itself. It's likely that the author is sending a decryption tool for the files once the victim has followed the instructions.

3. Heart piece

The main functionality can be seen in figure 1. The ransomware is creating a list of all the files listed at the desktop. Further, it checks if the file has already been decrypted. Now we are getting to the actual file encryption method. Here it encrypts all files with the hardcoded key “888” and adds a “Lock.” In front of the original filename.

This encryption routine is executed for the desktop, “AppData/Roaming”, “AppData/Local”, music, pictures, videos and the documents directory.



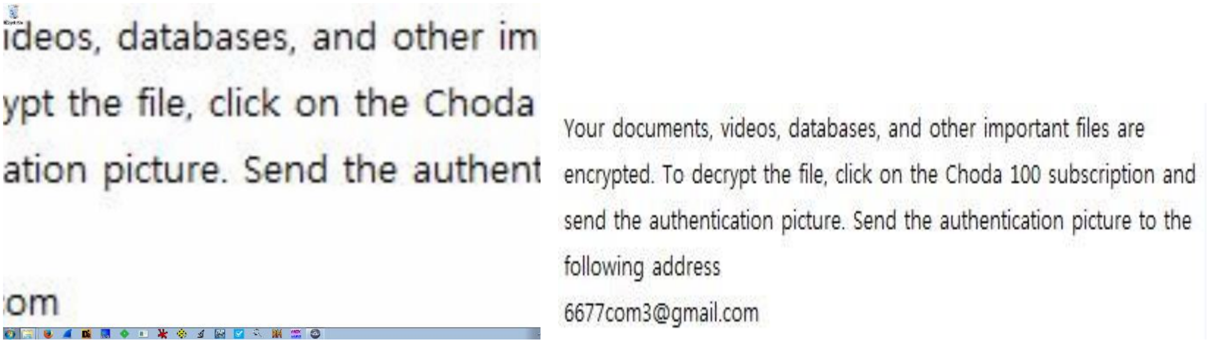
```
$Y = _FILELISTTOARRAY(@DESKTOPDIR, "*.*", $BT)
IF $Y <> "" AND $Y <> @ERROR AND $Y <> -1 THEN
    FOR $I = 1 TO $Y[0] STEP +1
        IF NOT STRINGINSTR($Y[$I], "Lock.") THEN
            $DD1 = STRINGREPLACE($Y[$I], "Fixed.", "")
            _CRYPT_ENCRYPTFILE(@DESKTOPDIR & "/" & $Y[$I], @DESKTOPDIR & "/Lock." & $DD1, "888", $CALG_DES)
            FILEDELETE(@DESKTOPDIR & "/" & $Y[$I])
            DIRREMOVE(@DESKTOPDIR & "/" & $Y[$I], 1)
        ENDIF
    NEXT
ENDIF
```

Figure 1. Encryption routine

Because there is a hardcoded key, the decryption of the original files is a piece of cake. To build such a decryption tool, it would be necessary to create a reversed routine as seen in figure 1. For example the “_CRYPT_ENCRYPTFILE” should be replaced with “_CRYPT_DECRYPTFILE” from the Github source[2]. Also other useless functions for the decryption process like setting the background image should be removed. Luckily such a tool has already been created and can be downloaded at Bleepingcomputer[3].

4. Second part

Within the second part of the ransomware, a background image with the ransomware note is set. As you can see at the left side of figure2, the text shown on the image isn’t readable at all. Only when viewing the file located at “C:\Users\User\AppData\Local\Temp\wl.jpg” directly, the text becomes readable. Even now as the text is readable, it’s not absolute certain what the author really wants. When searching for “Choda100”, a YouTube channel is shown. Most likely the ransomware author wants to get subscriptions by blackmailing his victims.



ideos, databases, and other im
ypt the file, click on the Choda
ation picture. Send the authent
om

Your documents, videos, databases, and other important files are encrypted. To decrypt the file, click on the Choda 100 subscription and send the authentication picture. Send the authentication picture to the following address
6677com3@gmail.com

Figure 2. Background image on the left, .jpg file on the right

Furthermore, the ransomware checks whether chrome.exe, firefox.exe, iexplore.exe, opera.exe, tor.exe or skype.exe is running. If a running process is found, it gets terminated. This functionality is possibly used to stop the victim from finding help online by quitting popular communication processes.

5. Final words

This ransomware is by far the laziest written one I have ever seen. It can be assumed that the ransomware author didn’t spend more than a few hours on this ransomware, since no proper instructions are provided and not displayed correctly either. The whole ransomware code seems to be shared somewhere on the internet, because variants like this[4] are out there. In future, there will possibly be more variants of Crypt888. If those variants will be using hardcoded encryption keys just like in Crypt888, they won’t be that effective since a decryption tool for the encrypted files can be easily written. Another popular ransomware, which also shows how easy it is to create ransomware is CryptoWire[5]. This ransomware is also using a hardcoded encryption key, just like Crypt888. It has the option to generate the encryption key at runtime though. The whole source code is well-commented, which makes it more easy to use the ransomware for other people.

In conclusion, it’s clearly visible that ransomware authors are currently having a very simple process of creating new ransomware. In some cases - just like with CryptoWire - no coding skills at all are required. A simple download and a further configuration of the ransomware is enough to get ransomware authors started.

6. File hashes and resources

[1] 354ea103d9ec5e7a83b19dca776678561a3ed0d30a4fd665880bb29e3c733765

[2] https://github.com/dbkaynor/AutoIt3/blob/master/Include/Crypt.au3

[3] https://download.bleepingcomputer.com/demonslay335/MirCopDecrypter.zip

[4] 86b28b6039367eb8692c40f2dcfdd0c5c29008865610b87a2b9cc36983a4b1b7

[5] https://github.com/brucecio9999/CryptoWire-Advanced-AutoIt-ransomware-Project

If you want to stay updated about malware, be sure to follow these accounts:

RansomBleed - My personal twitter account about the latest malware reports.

GDataSoftwareAG – G DATAs twitter company account.

Blog – The G DATA blog about all kinds of security-related news.