Technical analysis

cert.pl/en/news/single/technical-analysis-of-cryptomixcryptfile2-ransomware/

Campaign

CryptoMix is another ransomware family that is trying to earn money by encrypting victims files and coercing them into paying the ransom.
Until recently it was more known as CryptFile2, but for reasons unknown to us it was rebranded and now it's called CryptoMix.
It was observed in the wild being served by the Rig-V exploit kit.

This malware stands out from among others, but not necessarily in a good way.

Price

First unusual thing about this family is very large amount of money requested – 5 bitcoins is an insane amount of money (especially considering that CryptoMix is really primitive under the hood, but we'll get to it). We don't know how many victims have paid, but probably few were desperate enough.

Additionally we have stumbled upon following comment discouraging anyone from paying the ransom:

> DO NOT PAY FOR THIS!!!
> we were infected and they asked for 10 bitcoins, after some negotiations the price was lowered to 6 bitcoins. they provided 1 decrypted file to prove concept. we paid 6 bitcoins and they asked for another .6 as the c&c server will not provide the key due to late payment. after promptly paying another .6 bitcoins (about $4800 in total) there has been no communication from them! its been 2 weeks and nothing.
> WHATEVER YOU DO, DO NOT TRUST THEM, THEY WILL NOT DECRYPT YOUR FILES!!!!

We can't verify if this is true, but it sounds plausible – if someone is desperate enough to pay 6 bitcoins for his files, he probably can be coerced into paying even more. As usual, we discourage anyone from supporting the criminals by paying the ransom.

Payment portal

Additionally CryptoMix doesn't have any payment portal in the Tor network. Or any payment portal, for that matter – victim have to write an email and literally wait some time before malware operators kindly send the decryption keys
(assuming that they will do it, instead of bargaining for even more money).

For example, ransom message can look like this (most recent variant):

Or like this (older variant):

We don't think that this strategy was well thought out. First of all, using emails for communication with victims is bothersome and need constant attention.
Automated portal would be much more reliable and secure for both sides. Additionally, emails are prone to being deleted/locked, effectively cutting malware authors from their "clients".

Charity

Content of exchanged emails is very unusual too. Actors claim to be a charity organization (!) that is going to sponsor presents and medical help for children. For example:

That's really original, but unfortunately also obviously false.

Leaving aside strange quirks of ransomware "interface", let's get more technical. In its heart, CryptoMix is just a bare bones encryptor – it doesn't have any fancy features, it doesn't have a web portal, it doesn't change user wallpaper, the only thing it does is encrypting every file on the victim's disk and on the mounted network drives.

CryptoMix is protected by a very primitive packer – the real binary is stored in resources, and xored with a hardcoded key. For some reason, Cuckoo has problems with automatic unpacking of cryptomixer, so we had to write our own unpacker. Using pefile and Yara is very

easy:

After decryption ransomware checks whether it's being debugged – but no antiVM techniques are employed, so everything works as it should under VirtualBox.

Before file encryption starts, the ransomware checks internet connectivity (using InternetOpenUrl function). If everything is ok, an encryption key is generated on victim's PC and sent to the C&C server.
Otherwise, depending on malware version, either a hardcoded encryption key is used or malware is spinning in an infinite loop until the internet connection is restored.

The main function can be expressed as follows:

After encryption key is generated/selected, it is stored in windows registry. Registry key used for malware specific data varies depending on version, but for example SoftWare\Microsoft\Windows\Shell\Nodes Slots, SoftWare\Microsoft\Windows\Shell\FlashPlayerPluginK or Software\Adobe Reader LicensionSoftWare\AdobeLicensionSoftWare can be used (malware probably tries to hide its presence by impersonating another software).

The list of supported extensions constains more than 1250 entries:

That's quite a lot of extensions, but nothing special (for comparsion: CryptXXX supports 933 extensions, CrypMIC 901). Most unusual thing here is inclusion of another ransomware extensions (for example .zepto, .locky, .crypt, .locked, .cryptolocker, .cryptowall, etc).

Encryption

Let's get back to ransom message for a while:

Malware claims that our files are "encrypted with 2048bit RSA KEY". Well, it's not entirely true. Yes, 2048bit RSA key is generated with windows Crypto API – but after RSA key is selected, it is hashed with SHA256 to create a real encryption key and every file on disk is encrypted with that key. Encryption algorithm used is AES 256 in CBC mode without initialization vector.

Encryption routine can be summarized with this (simplified) code:

This function is called for every file, so hashing rsaKey and deriving AES key every time doesn't make much sense. But there is bigger problem with it – there is no need for such things as "public" and "private" keys, because this encryption routine is entirely symmetric – RSA serves here just as (unnecesarily slow) random number generator.

So yes, in a way RSA is "used for encryption", but files are not encrypted with RSA and encryption is entirely symmetric.

UserID given by CryptoMix is not random – it is generated from username and serial number for first disk.

This doesn't seem like a good idea, because UserIDs absolutely have to be unique, and neither username nor volume serial number is designed to be unique – so userID collisions are possible and very plausible (after taking low entropy of userID and birthday paradox into account).
Why is this a problem? Because when UserID collision happens, malware creators have no way of distinguishing two users apart – so they don't know which encryption key belongs to which user, and can't send the right one. It's also possible that in case of collision old key will be overwritten in database and lost.

Finally, CryptoMix achieves persistence by copying itself to user documents and writing to HKEY_CURRENT_USER\SoftWare\Microsoft\Windows\CurrentVersion\Run registry key.

As a final measure, all shadow copies are removed (if user doesn't have admin account, UAC window is shown before):

Cryptomix Decryptor

Due to a cryptographic flaw in encryption, we are able to decrypt CryptoMix (and CryptFile2), **but** only sometimes and only if files were encrypted with a vulnerable version.
If your files were encrypted by CryptoMix and you don't want to pay a ransom, you can contact us at and we'll see what we can do.
Please attach a single encrypted file without changing it's filename after encryption (for example warnings.h.email[]id[7e5973f5e0ce337d].lesli).

Hashes/patterns

Cryptomix packer (old and new):

Cryptomix payload (after unpacking):

hashes:

c2f30cd537c79b6bcd292e6824ea874e sample0

befc0e43b38fe467ddc3ddd73150a9fc sample0 decrypted

8c413e31f39a54abf78c3585444051f7 sample1

0d1206246bf15c521474cee42f13fc09 sample1 decrypted

b778bda5b97228c6e362c9c4ae004a19 sample2

042a38a32cd20e3e190bb15b085b430a sample2 decrypted