CryptoMix: Avast adds a new free decryption tool to its collection

By Jakub Křoustek 21 Feb 2017

Avast now provides a decryption tool for ransomware CryptoMix (offline only)

In cooperation with researchers from CERT.PL, we are happy to announce the release of another decryptor tool, for the ransomware,CryptoMix. CryptoMix has multiple aliases, including CryptFile2, Zeta, or the most recent alias CryptoShield.

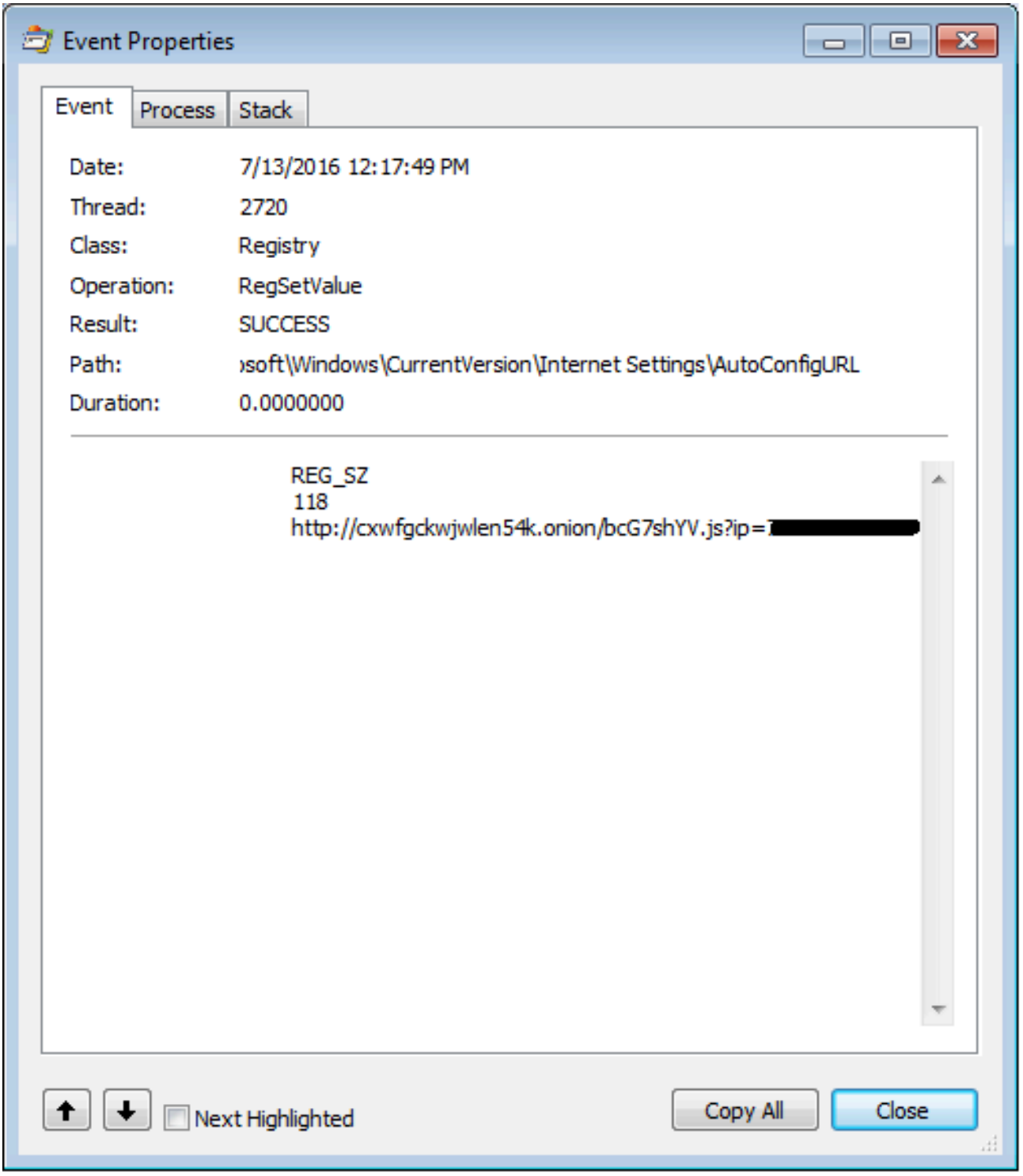
Please note: a successful decryption is not always possible. See a description of the limitations below.

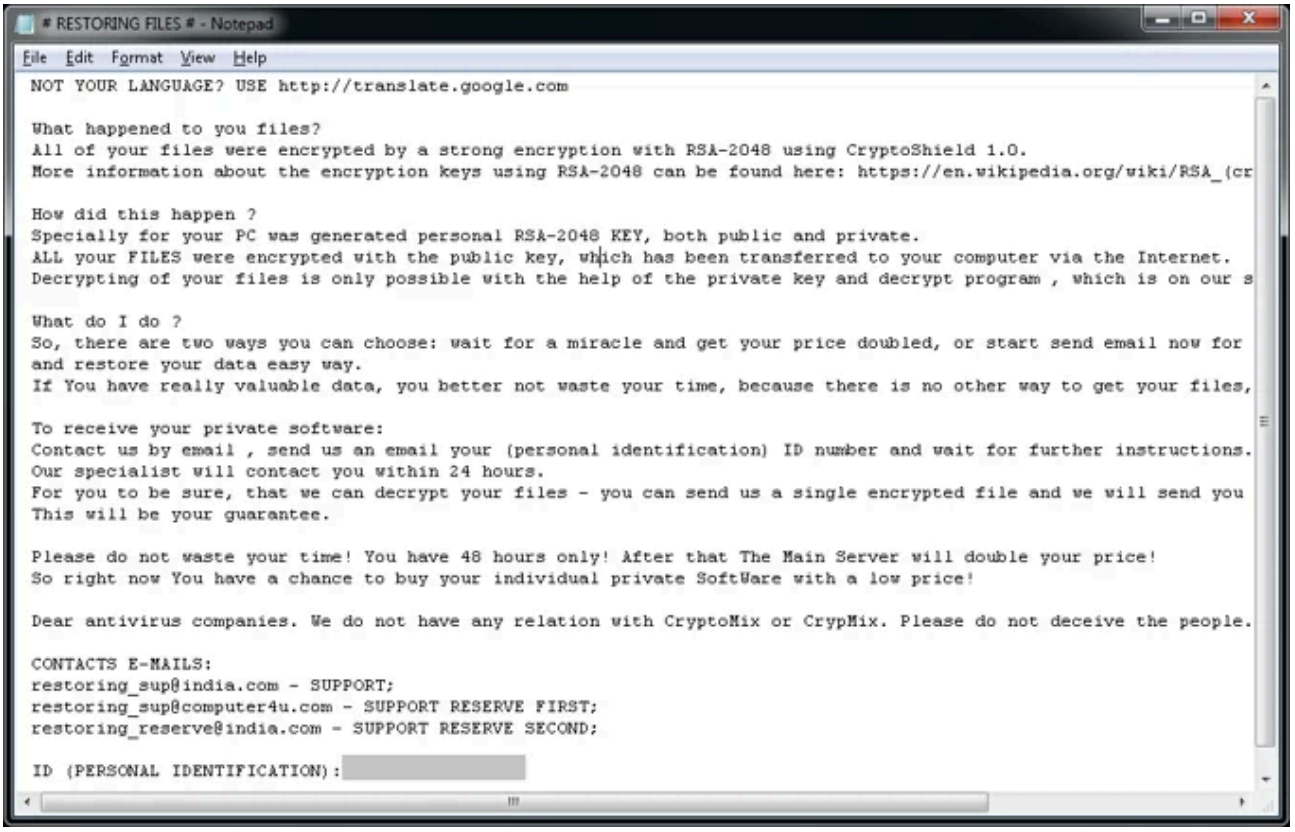
CryptoMix is a ransomware strain that was first spotted in March 2016. In early 2017, its author(s) renamed CryptoMix to CryptoShield. The spread of this ransomware could be described as a medium level of prevalence and has been steady since its discovery. It uses exploit kits (RIG at the moment) as its main delivery method.

Once CryptoMix infects a machine, it tries to communicate with its Command and Control (C&C) server to establish a key to encrypt files (the AES-256 algorithm is used). However, if the server is not available or if there is a connection issue (e.g. blocked communication by a firewall), the ransomware will encrypt files with one of its fixed keys, or “offline key”.

Our decryption tool for CryptoMix can decrypt files that were encrypted using the “offline key”. In cases where the offline key was not used to encrypt files, our tool will be unable to restore the files and will not modify any files.

You can distinguish CryptoMix by its new file extensions added to the original file names: .CRYPTOSHIELD, .scl, .rscl, .lesli, .rdmk, .code, or .rmd. Furthermore, the ransom notes are located in files with the names HELP_DECRYPT_YOUR_FILES.HTML, # RESTORING FILES #.TXT, etc.


Event Properties
Event
Process
Stack
Date: 7/13/2016 12:17:49 PM
Thread: 2720
Class: Registry
Operation: RegSetValue
Result: SUCCESS
Path: ›soft\Windows\CurrentVersion\Internet Settings\AutoConfigURL
Duration: 0.0000000
REG_SZ
118
http://cxwfgckwjwlen54k.onion/bcG7shYV.js?ip=[redacted]
Next Highlighted
Copy All
Close



CryptoMix is a nasty ransomware strain that has been spreading for a while. Its code quality is pretty low compared to its competitors and it even contains flaws that may cause your files to become undecryptable. You can easily find online complaints left by victims that paid the ridiculous amounts of extortion (5-10 bitcoins ~ $5,000-$10,000) and that were left without decrypted files. This might be the reason why its authors are changing the name so often - would you even consider paying someone with such a negative reputation?

As always we advise you to not pay the ransom! There's always a chance that your files can be decrypted, for free, in future. The decryption tool released by us today, might be hope for at least some affected by CryptoMix.

How to protect yourself from ransomware

- Make sure you have antivirus, like Avast, installed on all of your devices. Antivirus will act like a safety net and block ransomware before it can cause any damage, in case you accidentally try to download it.
- Be smart and alert. Ransomware distributors often use social engineering tactics to trick people into downloading the ransomware. Be careful which links and attachments you open and what you download on the web. Make sure you verify the source of emails including links and attachments and only download software and visit trusted sites.
- Backup your data properly on a regular basis. Be sure to not keep your backups connected to your devices all the time, otherwise, your backups could be held ransom as well.

If you do become infected with ransomware, make sure to check out our free ransomware decryptor tools to see if we can help you get your files back!

Acknowledgment

We would like to thank the researchers from CERT.PL for their detailed analysis of CryptoMix and for the set of offline keys they provided us, to supplement our list. Furthermore, a special thanks also goes to my colleague Ladislav Zezula for preparing this decryptor.

IOCs

00b3ff8a88232c22e87555c511156c1d317b2aa23026fcfb11e201cc360ad05b

05fe9891388d3e59d91b20f2ee22844533dc00ee409628a4f3c605035d24bad3

085024acc25a30a32f948cffd72f3bbdb68858a41b2292125b438787306a7bc1

0c31c8f8bc57d9f77a5c872c4afabba53596e61a5a738fb7c3f9b3248cdfee65

10e37d164ece6d4cea25093a4f86b3254f4abd9bf19a93a277b21e6d6ebbc630

1b04669a8d13ab06d0f23c8609260e7c8b50debac743c343f1c534683aa4ae77

1e8ae4562cdc4d3fc9f2fe9d849b2c6c11e8d6f408d303c46785c668537749cc

27cb3b60f4d55757918460afaeef33fbfc04f7426546252a11be8bcb55823de2

2a6451715b2ada3535712450eb738d160807ea3e61d833092599e68532200e62

2f62cc79686524ac992ffa99871a4d6e60f488cccd86df90e9a8cbb23b33a790

30092f8f01c8d275c5f4a7cfa81b5e47e0d482dd3f4cfc107091e606fa48b43f

60345157df00b5b36b8bad5ff0e5ffee0a73c6c4d639670052c566f0d7d7b4c5

6751c308f39cc4e1a918136179c307c48b9066d343a2f1155e937f5bb2b70e25

72eca63c67d055b17901517794f0a538a916ec5d75f4113edf5d238d805a7f81

9198f1b53136a8229c18e4e5bc023b693a0276aed91b6e18dfe0ec8395ef8141

d56fb2bdad7a50ab1f6ef76c67669452ed4da2bf865beafcf4956ab30bfa20fc

da98d21ebd555c4b0e7c627dfce85bb62611779e0ef2eee42bd2f98c454f9e71

fcf050b91c98c55dc3b2680b9d14699b53e78ff7d9a1dd9a9afc6bfb45376687
