Mole ransomware: analysis and decryptor

cert.pl/en/news/single/mole-ransomware-analysis-and-decryptor/

Mole ransomware is almost month old ransomware (so it’s quite old from our point of view), that was distributed mainly through fake online Word docs. It’s a member of growing CryptoMix family, but encryption algorithm was completely changed (…again).

We became interested in this variant after victims contacted us asking for a decryptor. Remembering that all members of this family so far were plagued with serious crypto flaws, we decided to give it a try and reverse-engineered it thoroughly. It turned out to be a good idea – we were successful and managed to create working decryptor that you can download from: https://nomoreransom.cert.pl/static/mole_decryptor.exe.

In the rest of this article we will share detailed results of our research.

Campaign and Behaviour

Mole ransomware was distributed through malspam linking to fake Microsoft Word documents. Said documents prompted users to download and install a malicious plugin.

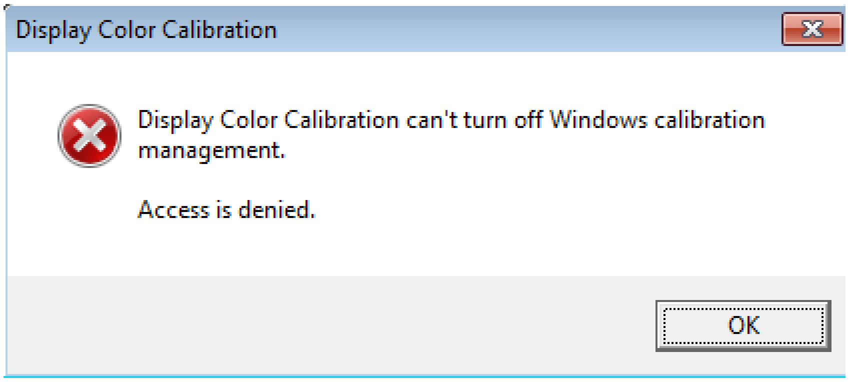
Because this variant is not new, it was analyzed by quite a lot of researchers before us. We don't intend to copy their good work, so for anyone interested in the dynamic analysis we recommend looking at following links:

Instead, we'll focus on a static analysis of the code and the encryption method.

Static analysis

As in many malware families, Mole won't run in most Russian-speaking countries. Literally the first thing the binary does after being run is checking keyboard layout and charset – detecting Russian ones leads to immediate process termination. Otherwise, malware achieves persistence (by adding itself to the Autorun in the system's registry), removes shadow copies (after Windows' version check), and proceeds to the actual encryption:

After being started ransomware tries to bypass the UAC and displays fake dialog message:



Display Color Calibration

Display Color Calibration can't turn off Windows calibration management.

Access is denied.

After that, UAC prompt is shown and the user probably clicks "Yes" believing that he/she agrees to "Display Color Calibration". Instead, as usual, malware relaunches itself with admin privileges, and Shadow Volumes are deleted.

Of course ransomware doesn't encrypt every file type. Interestingly, encrypted extensions are obfuscated – they were not hardcoded directly, but compared inside giant function, after transformation with following algorithm:

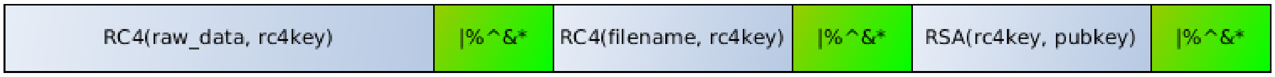
List of encrypted extensions:

And as usual, the most interesting thing in any ransomware is actual file encryption algorithm. In this case it can be summarized as follows (half-decompiled, half-handwritten pseudo-c++ code with non essential parts omitted):

Or in terse pseudocode:

This method is not perfect for a lot of reasons, but we'll skip detailed cryptanalysis here.

General structure of encrypted file looks like this:



RC4(raw_data, rc4key)	|%^&*	RC4(filename, rc4key)	|%^&*	RSA(rc4key, pubkey)	|%^&*

It’s very similar to Revenge ransomware, that is why we believe that Mole is next version of Revenge. On the other hand, RC4 is used here instead of more sophisticated (and stronger) AES. It doesn’t change much, as RC4 is still strong enough for most ransomware purposes, but we’re not sure why ransomware creators decided to take this step back.

Hashes/patterns

Sha256 hashes of binaries:

Network communication:

Ransom note: