Ransomware: two pieces of good news

By AMR

Published: 2019-09-25 · Archived: 2026-04-05 14:35:17 UTC

“All your files have been encrypted.” How many times has this suddenly popped up on your screen? We hope never, because it’s one of the most common indicators that you’ve lost access to your files. And if there are no publicly available decryptors or you don’t have any backup copies, you’re in trouble.

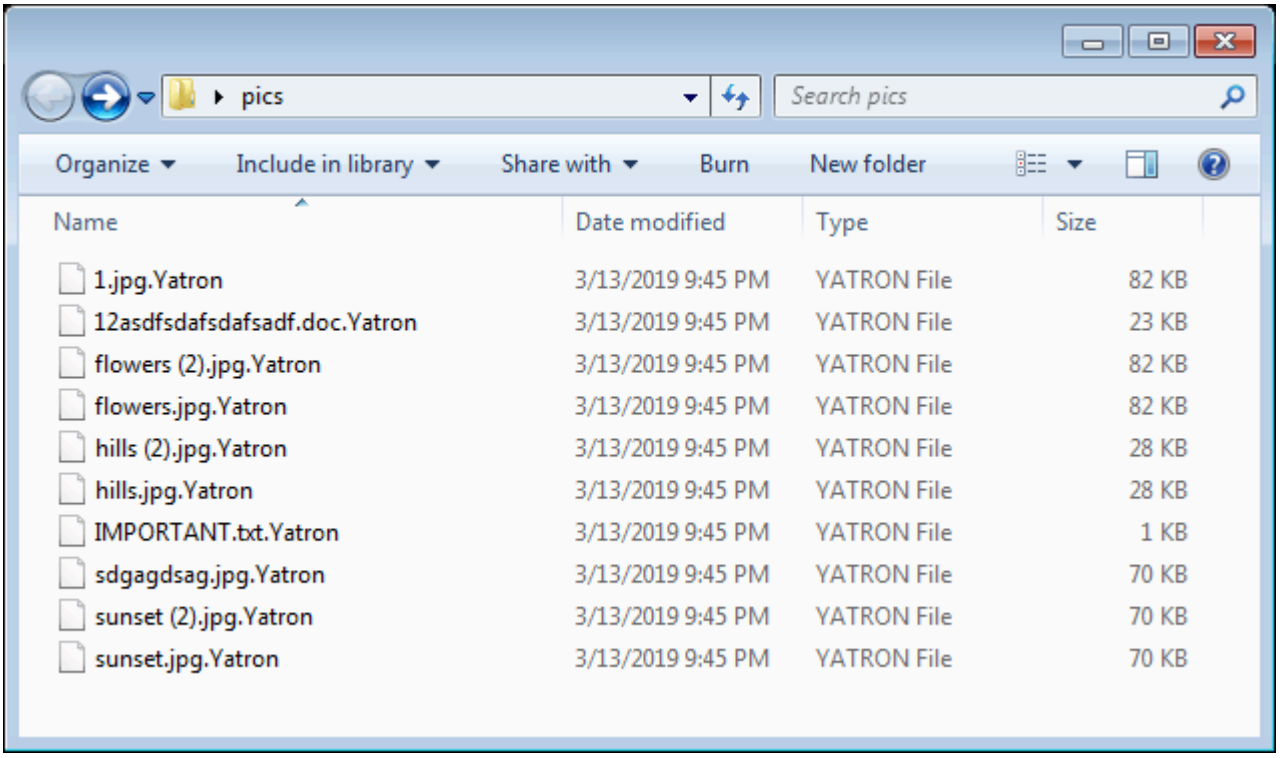
Nowadays, cybercriminals have a thousand and one ways of creating and spreading ransomware. There are two common scenarios behind the creation of this kind of malware: in one, the criminals prefer to just reconfigure existing malicious source code; in the other, they choose to write their own ransomware, sometimes even using very specific languages.

However, don’t despair, because those fighting ransomware are not standing still either. In fact, we have two pieces of good news to share with you.

Good news #1

We’ve released a decryptor for the Yatron ransomware. The authors of the ransomware chose the first scenario mentioned above and based their ‘creation’ on the code used in Hidden Tear, a well-known sample of open-source ransomware. According to our statistics, during the last year alone our products have prevented more than 600 infections by various modifications of Trojan-Ransom.MSIL.Tear, with most attacks recorded in Germany, China, the Russian Federation, India and Myanmar.

Among the numerous modifications of Trojan-Ransom.MSIL.Tear, this one can be distinguished by the extension .Yatron that’s appended to encrypted files.



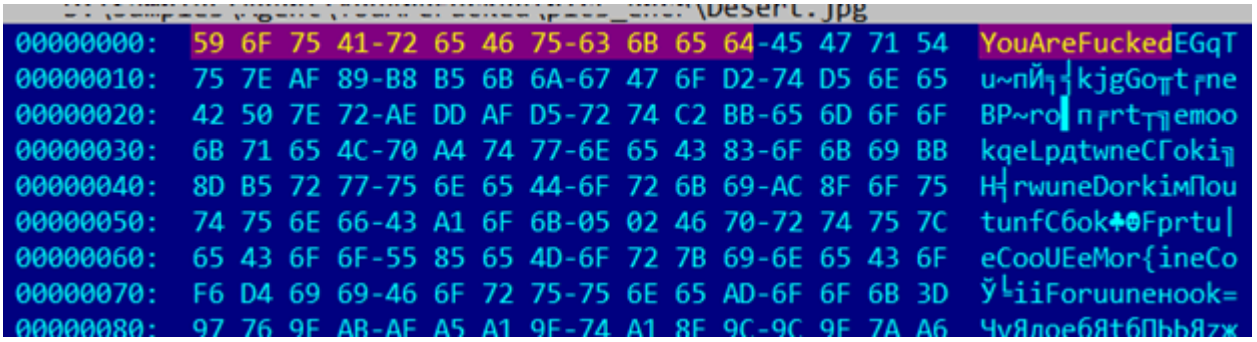
However, using third-party code without checking it raises the risk of critical vulnerabilities affecting the overall effectiveness of the program. That's what happened here. Due to mistakes in the cryptographic scheme we were able to create a decryptor.

Good news #2

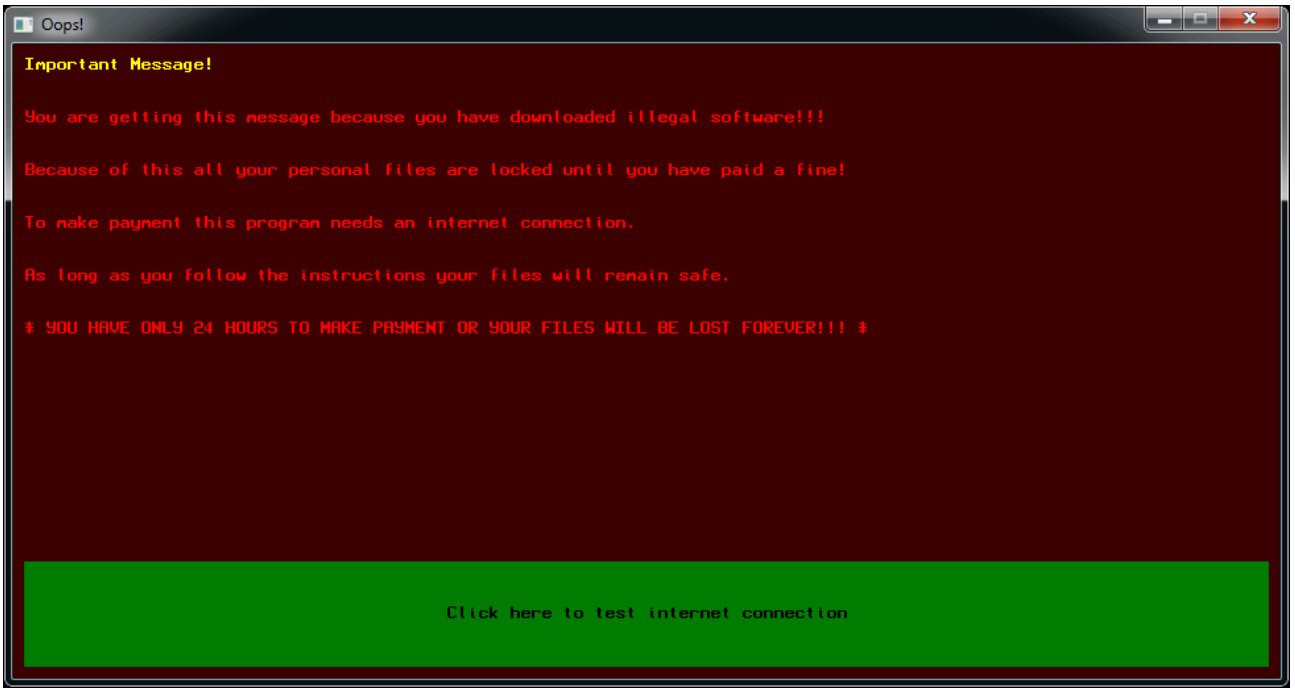
We've released a decryptor for the unique FortuneCrypt ransomware. To describe this malware, we could paraphrase Archimedes: give me a programming language, and I will write a ransomware program. The main feature of this ransomware is that it was compiled using a BlitzMax compiler. As Wikipedia states: "Being derived from BASIC, Blitz syntax was designed to be easy to pick up for beginners first learning to program. The languages are game-programming oriented but are often found general-purpose enough to be used for most types of application". We've seen lots of ransomware written in C/C++, C#, Delphi, JS, Python, etc., but FortuneCrypt is the first ransomware we've seen that's written in Blitz BASIC.

During the last year, our products registered more than 6,000 attacks carried out by the numerous variations of the malicious Trojan-Ransom.Win32.Crypren family (FortuneCrypt is part of this family). The top five countries attacked by the malware are: the Russian Federation, Brazil, Germany, South Korea and Iran.

The cryptor changes neither the file extension nor the file name; instead, it marks encrypted files by adding a text string to the beginning of an encrypted file.



The only indicator of infection visible to the victim is a ransom text that appears on the screen.



After some analysis, we found that the cryptographic scheme used by the malware is weak and the encrypted files can be easily recovered.

Decryptors

Both the decryptors mentioned here have been added to our RakhniDecryptor tool, which can be downloaded from the following sources:

https://support.kaspersky.com/viruses/disinfection/10556

https://www.nomoreransom.org/en/decryption-tools.html

IOCs

Yatron ransomware

- 7910B3F3A04644D12B8E656AA4934C59A4E3083A2A9C476BF752DC54192C255B

FortuneCrypt

- E2B9B48755BCA1EDFBA5140753E3AF83FB0AE724E36D8C83AB23E262196D1080
- C26192E7B14991ED39D6586F8C88A86AF4467D5E296F75487BB62B920DEA533F
- F2DCD2308C18FDB56A22B7DB44E60CDB9118043830E03DF02DAC34E4C4752587
