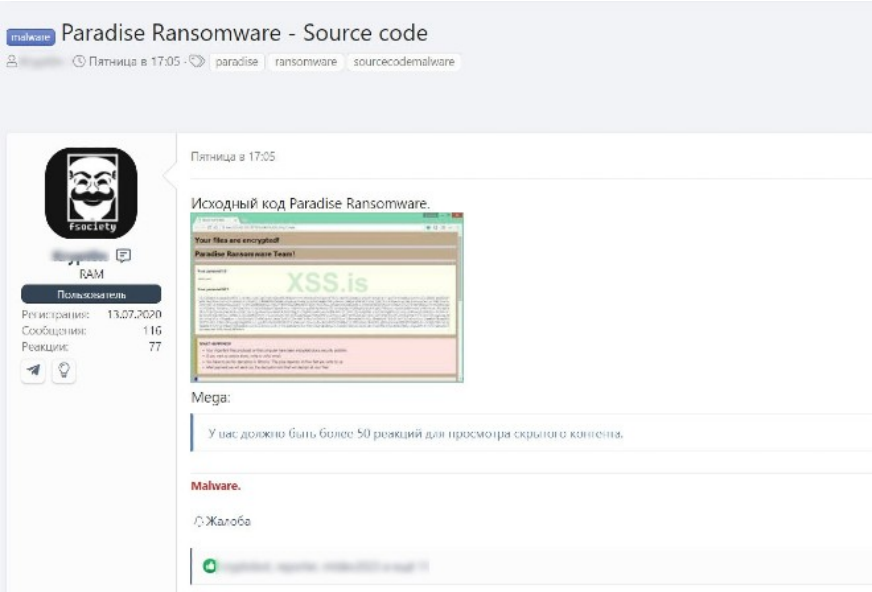
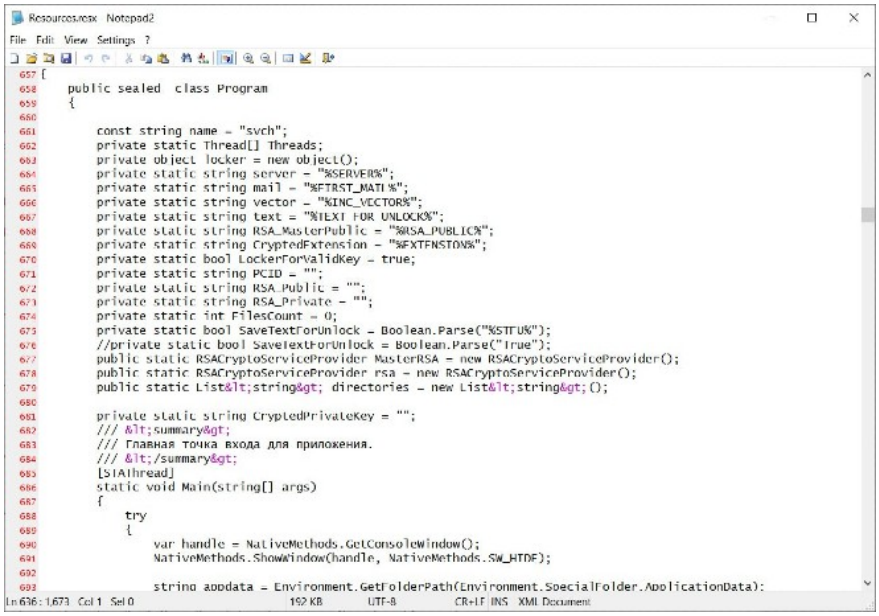
Paradise ransomware source code shared on hacker forum

The entire source code of the Paradise ransomware has been shared on a hacker forum called XSS.is. Based on this source code, even novice cybercriminals can create their own custom ransomware.

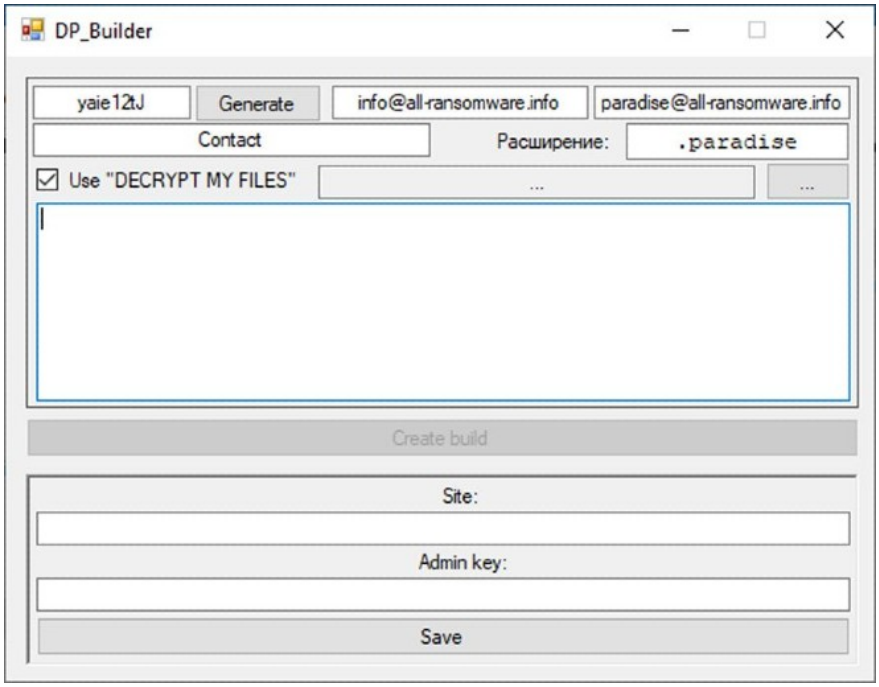
The Paradise source code is publicly shared, available for download by all active members of the XSS.is forum. XSS.is is a forum for hackers, mostly Russian hackers.



Security researcher Tom Malka downloaded the source code then compiled it and confirmed that it produces three executables. The first file is the ransomware configurator, the second is the encryptor, and the third is the decrypter.



Scattered inside the source code are lines of comments in Russian. This shows that the author of this ransomware uses Russian.



Once they have the source code, hackers can create their own custom ransomware. Customizable sections include control server, encrypted extension file statement, and contact email address.

After the customization is complete, the hacker can deploy and distribute to the victim.

Welcome to Paradise

Ransomware Paradise first appeared in September 2017 through phishing emails containing malicious IQY attachments. Clicking on this file, the ransomware will be downloaded and installed on the victim's machine.

Over time, many versions of Paradise have been released because the first versions contained vulnerabilities that security experts could easily decipher. On the new versions, Paradise has used RSA encryption method, so it is much more difficult to decrypt.

According to Michael Gillespie, the creator of the decryptor for the first version of Paradise, the Paradise ransomware has the following versions:

1. Paradise - Original version with holes
2. Paradise .NET - .NET secure version switches to RSA encryption algorithm
3. Paradise B29 - A variant that only encrypts the end of the file

Ransomware Paradise, which was heavily distributed in the period from September 2017 to January 2020, suddenly reduced the frequency of terrorizing victims. Until now, it is very rare to see computers infected with this ransomware.

Maybe Paradise will return once the source code is shared publicly.