Introduction

With the development of computer systems, the development of computer malware also begins to develop. The first viruses were of an entertaining nature and did not cause harm. But after a while, malicious programs began to harm users and a huge family of malicious programs appeared:

1. Viruses
2. Trojan programs
3. Spyware programs
4. Rootkits
5. Ransomware
6. Worms
7. Botnets

The most dangerous viruses, in our opinion, are Stuxnet, Duqu, Flame, Gauss, which had a very complex structure and unique methods of both infecting and hiding traces. In this article, we want to consider malware like ransomware and understand how they infect a computer, what encryption methods they use, and how they can not only be detected but also "hacked".

Ransomware evolution

The first documented ransomware attack was carried out in December 1989 by evolutionary biologist Joseph L. Popp. He sent out about 20,000 letters to the participants in the international AIDS conference. He demanded that the ransom be transferred to his bank account in Panama. Soon he was calculated and caught, but not tried. After that, the era of computer ransomware begins. With the development of encryption, the emergence of new methods of encrypting data, viruses began to use them. Since about 2006, viruses have started using RSA to encrypt files. In recent years, ransomware programs have begun to actively exploit 0day vulnerabilities to infiltrate corporate networks and infect servers, demanding multi-million dollar ransoms.

As it is already clear, the main goal of ransomware is to encrypt your files and demand a ransom for decrypting your files. Decryption is the provision of the victim with a key to the encryption algorithm. Let's see what types of encryption are used by ransomware.

1. Symmetric encryption method

   In this case, the encryption and decryption keys are the same. After files encryption the key sending to the server and when a payment is made, the ransomware virus receives from the server the key that encrypted the files.

2. Asymmetric client-side encryption.

   In this case, are generated a pair key is public and private. The private key is sent to the server, and the files are encrypted with the public key. When the victim pays the ransom, the ransomware requests a private decryption key from the server.

3. Asymmetric server-side encryption.

   Public and private key is generated on the server-side. The virus receives a public key from the server and starts the encryption.

4. Hybrid model.

Two key pairs are generated on the server and the client (server_pub & server_priv | client_pub & client_priv). The ransomware looking for files on the computer that need to be encrypted. Then it encrypts the files using client_pub. And client_priv (which is the key for decrypting files) encrypts using server_pub. Ultimately, to decrypt the files, you need to get server_priv, which ideally can be achieved by paying the ransom.

TOP Ransomware

For example, here are the 5 most dangerous and most common ransomware (taken from the Caspian block).

1. Maze
2. Conti
3. Revil
4. Netwalker
5. DopplerPaymer

Maze

This is one of the first ransomware viruses that, in addition to encryption, too used data theft. In cases where the victim did not pay for decryption, the ransomware threatened to publish private data. Also, the difference between this group and the other is that they reported attacks through the media.

Conti

Conti appeared at the end of 2019 and has been active throughout 2020. During its existence, it accounted for about 13% of all ransomware attacks. As in the case of Maze, Conti also copied files to a remote server, and also offered instructions for fixing the vulnerability through which they entered the network.

REvil

This ransomware virus was detected at the beginning of 2019. This virus attracted attention because it was very professionally written and bypassed defense mechanisms. This virus was also used to spread according to the RSAAS (ransom-as-a-service) scheme. Approximately 11% of all infections occur in Revil.

NetWalker

During the activity, netwalker accounted for Approximately 10% of all infections. They included corporate networks as targets. In 2021, one of the main people of the creator of the virus was caught, which led to the destruction of NetWalker.

DopplerPaymer

This ransomware distribution company also targets corporate networks, 9% of all infections were caused by this ransomware.

The problem

The problem with ransomware is not how to detect and remove them, but how you can bypass encryption and decrypt files without paying the ransom.

Let's imagine a situation when a ransomware virus got on the victim's computer.

1. When there is an anti-virus program on the computer

   Ideally, if the antivirus can understand that this file is malicious before it is launched, then the user's files will not be encrypted. But there may be cases when the antivirus program failed to catch the virus during startup and was able to catch it only after a while, when many files are already encrypted or, in the worst case, all are encrypted. And what does the antivirus do when it finds a malicious process? That's right, just kills the process and then removes the executable.

2. When there is no antivirus program on the computer

   With this part, everything is quite simple - the virus encrypts files and demands a ransom.

The possible solution

The weakness of ransomware viruses is contained in their memory. If encryption is performed with a symmetric algorithm, viruses after encryption try to delete the encryption key from memory so that during memory analysis, special programs would not be able to obtain the decryption key. Before approaching the solution of the problem, let's see which TOP viruses use similar functions.

Malware	Win API function
Maze	CryptGenRandom
Lockbit	CryptGenRandom
REvil(2019)	CryptGenRandom
Ryuk	CryptGenRandom
Conti	CryptGenRandom

As you can see from the table above, viruses mainly use the CryptGenRandom function to generate random data (keys). Using simple API monitors, you can understand what data was generated when this function was called.

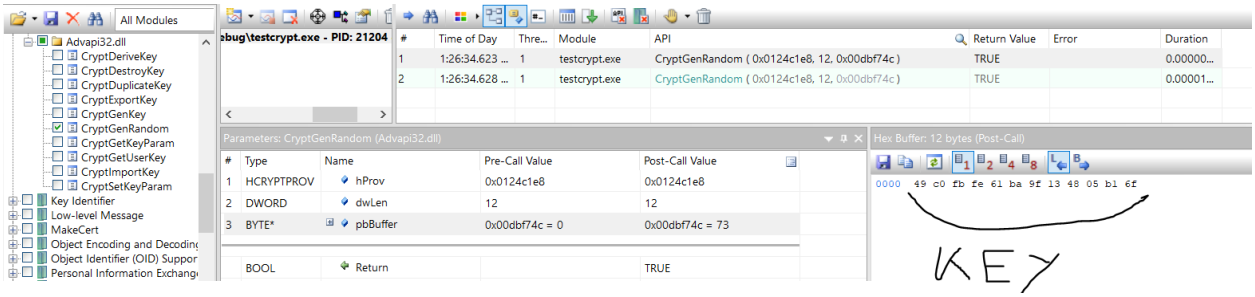
Let's take a look at some sample code where CryptGenRandom is used.

```
int main()
{
   srand(time(NULL) - 3);

   HCRYPTPROV hCryptoProvider = NULL;
   BYTE pbData[16];

   LPCSTR providerName = "supersecretstorage";
   CryptAcquireContext(&hCryptoProvider,
      (LPCWSTR)providerName,
      NULL,
      PROV_RSA_FULL,
      0);
  CryptGenRandom(hCryptoProvider, 12, pbData);
}
```

Here 2 WinApi functions are used, the first CryptAcquireContext -> declare the crypto provider, the second CryptGenRandom -> generate random bytes, in this example the length of random data is 12. How can we understand what data is generated in the program if we do not have access to debug the program? ApiMonitor can be used. ApiMonitor intercepts WinApi requests and shows which functions were called and which parameter values were passed to these functions.



well, using the WinAPI hook it is easy to understand which keys were generated in ransomware.

Actually, what decision can be made to not only detect but also decrypt files.

1. Allocate some area on the disk (possible_keys_storage) which will be accessible only in the “secure boot” mode.
2. Before stopping the already working process of the virus, it is necessary to dump the memory of the process, since it can store the key for encrypting and decrypting files, write the dump to possible_keys_storage, and not destroy the process.
3. Intercept calls to CryptGenRandom, CryptEncrypt ... and other functions that are often used in ransomware viruses, and writes the generated data to possible_keys_storage.
4. When the user realizes that his files have been encrypted, he will be able to boot in safe mode and receive the possible encryption keys that were generated.

Conclusion

Using API hook antiviruses, or the Windows operating system can intercept which random keys/certificates were generated. When someone from the researchers or antivirus companies can figure out what algorithm was used for encryption and release the decryptor, the user will be able to boot in safe mode, take possible keys that can be decryption keys, and, with the help of the decryption program, decrypt the files.

Credits

Aram_Simonyan https://twitter.com/Aram_Simonyan_

Hayk Sargsyan

Alik Mazmanyan https://twitter.com/mazmanyan_alik

Tigran Avanesyan

Artyom Badalyan