Report Update

Team member: Jingchi Zhang; Shanshan Yang; Qiqing Huang

By look through the resources from the internet and papers, we have a basic learn of the mechanism of bitcoin and blockchain. We also noticed that there are ransomware invented by attackers that are used to extort money from victims. The ransomware there can be virus, they are downloaded by victims and take control of their computers and encrypt their important files using a key. And if the victims want to recover their files, they need to transfer bitcoin to attacker. The reason that attacker choose bitcoin as payment method is that bitcoin has the characters of anonymity and hard to find sources. But the transaction process cannot be guaranteed, because there are three conditions: 1 the attacker give out the key but not receive bitcoins 2 the attacker receive bitcoins but not give out the key 3 the attacker give out the key and receive bitcoins.

We are going to design software to avoid the condition 1 and 2 and make sure the success of the transaction. Through the process of literate review, we find it is possible to design a mechanism to guarantee the transaction process, in other words, we can let ransomware work better.

Initially, we have come up with the specific implementation process:

Part 1-Ransomware:

1. Attacker generates RSA key pair {P_k, S_k} and hardcode P_k into Ransomware.

2. Victim loads ransomware and ransomware take control of the computer.

   It generates a random RSA key pair {P'_k, S'_k} and AES-512-CBC symmetric key K_{enc} (block size 512 bit) on victim's computer.

3. Encrypt

   Then it encrypts all the files F using K_{enc} and save Enc{K_{enc}, F} as the Content And then encrypt K_{enc} using P'_k and get Enc{P'_k, K_{enc}} as the Header and put it ahead of the Content and get F'. Finally, zero out the original files F.

   The structure of F' looks like:

   Header Content

   | Enc{P'_k, K_{enc}} | Enc{K_{enc}, F} |
   ----

4. Encrypt S'_k using P_k and get Enc{P_k, S'_k} and upload it to attacker's server and then clear the generated keys {P'_k, S'_k, K_{enc}} in memory.

Part-2 Transaction

R: Ransomware Info
B: Bitcoin Environment
V: Victim
A: Attacker
BC: the number of Bitcoin as needed

The transaction process should be:

R, BC R

V-------------------->B--->A

F' Dec{Sk, Enc{P_k, S'_k}}, Encryption Info

V-------------------->B<--A

S'_k BC

a) if S'_k valid V-------------------->B--->A

BC error

b) if S'_k invalid V<--------------------B--->A

1. When the victim notices that his files are encrypted and have prepared for the Bitcoin, he broadcast the Ransomware and Bitcoin balance information to other Bitcoin nodes and waits for this information been validated. If the Bitcoin provides the victim is enough to unlock his files, it will temporally hold in the middle.

2. Attacker receives the Ransomware information and use its own private key S_k to decrypt the encrypted ransomware's RSA private key, S'_k. And broadcast the S'_k to other Bitcoin nodes. At the same time, bitcoin network demands the encrypted file F' from the victim.

3. Based on the Encryption information, like how the files are encrypted and the encryption mode used, the bitcoin network dispatches the verifying work to other bitcoin nodes.

4. If S'k is valid, the held BC will finally transfer to A, and the valid S'_k will send to V

5. If not, the held BC will be released and return to V