# Report Update

By look through the resources from the internet and papers, we have a basic learn of the mechanism of bitcoin and block chain. We also noticed that there are ransomwares invented by attackers that are used to extort money from victims. The ransomwares 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 a software to avoid the condition 1 and 2 and make sure the success of 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 generate RSA key pair {Pk, Sk} and hardcode Pk 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 Kenc (block size 512 bit) on victim’s computer.

1. Encrypt

Then it encrypts all the files F using Kenc and save Enc{Kenc, F}as the Content

And then encrypt Kenc using P’k and get Enc{P’k, Kenc}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, Kenc}| Enc{Kenc, F}|

---------------------------------------

1. Encrypt S’k using Pk and get Enc{Pk, S’k}and upload it to attacker’s server and then clear the generated keys {P’k, S’k, Kenc} 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{Pk, S’k}}, Encryption Info

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

S’k BC

1. if S’k valid V-------------------->B--------------------------------------------------->A

BC error

1. if S’k unvalid V<--------------------B--------------------------------------------------->A
2. When victim noticed that his files are encrypted and prepare the Bitcoin needed, he broadcast the Ransomware and Bitcoin balance information to other Bitcoin nodes and waited these information been validated. If the Bitcoin provided from the victim is enough for this ransomware payment, it will temporily hold on the
3. Attacker receive the Ransomware information, and use its own private key Sk to decrypt the encrypted ransomware’s RSA private key, S’k. And broadcast the S’k to other Bitcoin nodes. At same time, bitcoin network demands the encrypted file F’ from vicitim.
4. Based on the Encryption information, like how the files encrypted and the encryption mode used, the bitcoin netword dispatch the verifying work to other bitcoin nodes.
5. If S’k is valid, the holded BC will finally transfer to A, and the valid S’k will send to V
6. If not, the holded BC will be released and return to V