Today we're going to talk about...

- a certain kind of software.
-
-

Today we're going to talk about...

- a certain kind of software.
- This kind of software has just made a breaking news.
-

Today we're going to talk about...

- a certain kind of software.
- This kind of software has just made a breaking news.
- We are not going to talk about AlphaGo.

Ransomware

Chris Xiong

Created with LaTeX

2016-04-15

Ransomware?

- Ransom + ware

Ransomware?

- In conventional ransom cases, the criminal often kidnaps someone, who is often called the "hostage", to ask for money.
-

Ransomware

- In conventional ransom cases, the criminal often kidnaps someone, who is often called the "hostage", to ask for money.
- However, for criminals behind these ransomwares, their hostage would be your precious data.

Ransomware

How does it work?

When your computer is infected by a ransomware, such as Cryptowall...

- You will find that most of your files have turned into unreadable scrap.
- Several new files will appear in your folders, which read "Your personal files are encrypted, if you don't pay us in x days, your files will be permanently encrypted. Nobody will ever be able to decrypt them after that".
- The new files mentioned above also tells you how to pay the money.

Ransomware

How does it work?

- They use an encryption algorithm, called "RSA", to encrypt your files.
- RSA algorithm is based on the fact that factorizing a huge number is very difficult.
- When you are using the RSA algorithm, it generates two keys: the public key and the private key.
- The public key can be used to encrypt files, but the encrypted files have to be decrypt with the private key.
- You can give your public key out so that other people can send encrypted data to you.

Ransomware

How does it work?

- Ransomwares take the advantages of the RSA algorithm.
- When your computer is infected, the server of the malware generates a pair of keys, sends the public key to your computer, and the client will start to encrypt all your files with it.
- However, you cannot decrypt them because the private key can only be found on the server.
- After you have paid the ransom, the private key will be sent to your computer, so you can decrypt your files.

Ransomware

Really permanently?

Short answer: yes.
Contemporary computers cannot factorize large integers efficiently.
The time it takes grows in an exponential manner.
Factorizing integers on a laptop with an Intel Core i7 processor

Length in bit	Time took to factorize
256	35 minutes
260	an hour

Integers used by the RSA algorithm is at least 2048 bits long.

Ransomware

Really permanently?

According to Shor's algorithm, quantum computers can factorize integers efficiently!
However...
There's no quantum computer with enough 'quantum bits' to factorize an integer that is 2048 bits in length.
The largest number successfully factorized by a quantum computer is 56153, which has... 16 bits.

Ransomware

So how many computers have been infected?

There are many...
According to the FBI, Cryptowall have grabbed over $18 million by June 2015.
However to implement a ransomware is not very hard – in fact, you can write a simple one yourself...

Ransomware

What should I do to prevent a ransomware infection?

Some ransomwares variants are very hard to be detected by anti-virus softwares.
However, most ransomwares spread via spam mails and "drive-by attacks".
So to prevent an infection you can...

- Do not even open spam mails.
- Do not visit untrusted sites.
- Make frequent backups of your data!

Ransomware

My computer is infected! What could I do?

In my opinion, you have three choices...

- Pay the ransom.
- Forget about your data.
- ~~Wait for the invention of quantum computers with sufficient quantum bits...~~

If fortunately, the ransomware that infected your computer is written by a careless programmer, you may be able to get your files back without paying anything...

Ransomware

Is there anything we can do to fight against ransomware?

Those ransomwares are usually hosted on a anonymous server, so finding the criminals is extremely difficult.
However it's possible to bring their server down without finding them...
As far as I am concerned, you can...

- Find an old computer.
- Run the ransomware deliberately.
- Revert the computer to its state before running the ransomware.
- Repeat the process zillion of times.

Ransomware

Is there anything we can do to fight against ransomware?

After that, the free space on their server will be filled with all those generated keys.
Thanks to the virtualization technology, the steps above can be done very fast on a single modern supercomputer.
~~Mission accomplished!~~

Ransomware

References

- https://en.wikipedia.org/wiki/Ransomware
- https://en.wikipedia.org/wiki/Shor%27s_algorithm
- http://arstechnica.com/security/2015/06/fbi-says-crypto-ransomware-has-raked-in-18-million-for-cybercriminals/
- http://www.reuters.com/article/us-apple-ransomware-idUSKCN0W80VX
- https://labs.bitdefender.com/2015/11/linux-ransomware-debut-fails-on-predictable-encryption-key/

Alternatively, you can scan the QR Code below.

Ransomware

Thank you for listening.