Dipen Delvadiya

Research Paper

ITMS-478

Ray Trygstad

09/29/2016

Understanding Ransomware and why is it so successful?

Computers and mobile devices have become extremely important part of our daily lives. People have started depending on them for communication, online shopping, payments, and entertainment. Almost all the industries have started using the Internet technologies as a basic and common part of their business operations, which got an attention of hackers to make an easy money by hacking their websites or computers. How do they hack? Obvious answer would be by using virus and malware. Many people think that malware and virus are same term. First let me explain the difference between virus and malware: a virus is just a type of a malware, and malware is any malicious software including virus, adware, spyware, worms, Trojan, ransomware, and many more. Basically malwares are software written in different computer languages to harm and infect any computer or wireless system. There are many ways to infect anyone's PC with malware, and it can be from any executable code, scripts, websites, or installed apps. To some experts, malware is a big threat to world as terrorism.

Malware has been in world since a while, and it has done big damage to many big industries. For an example, currently 500 million Yahoo accounts were hacked, and that was considered to be one of the biggest attacks on Yahoo (Seth Fiegerman, 2016). Malware has become biggest threat in cyber security especially in baking and business world. Ransomware is an advanced type of malware which are surging since attackers have found new developed and advanced ways to break through any system with different techniques. According to Raimund Genes, CTO at trend micro, "ransomware attacks are happening because hackers have perfected their techniques while security professionals have failed stopping them" (Varun Haran, 2016). As security professionals have been trying to make secure system on daily basis, attackers have been looking for more intelligent and intensive ways of developing something more powerful software. The result of this effort, they came up with new viruses like Cryptolocker, Cryptowall, and TeslaCrypt, which all are part of powerful hacking tool "ransomware" (Chris Stobing, 2015). In this paper, I am going to explain how Ransomware work and why it continues to be successful.

2. Ransomware Attacks

2.1 Why it has succeed

These attacks are so strong that it can prevent users from using their computers. Ransomware holds all the victim's data and files from ransom. These attacks are little different than malware. Malware usually runs in the background without user's knowledge. Malware hides its presence to steal passwords, credit card, or any sensitive information. However, ransomware works with the user's knowledge. Once it succeeds to infect computer files, it locks down user's computer or files, and it will show its presence to user (Shafqat Mehmood, 2016). After infection, it pops up a message that user's files are locked, and it usually asks for payment to unlock their computers. Also sometimes they add timers to stress the victims. Typically, countdown timer starts with 72-hour limit in which they have to make a payment (Shafqat Mehmood, 2016). Any failed attempt to stop cryptolocker or payment, it might result in diving time by some factor. And failing to make a payment before due time, it can lead to lose all the data or payment to be doubled before next due time (Shafqat Mehmood, 2016). Some new versions of ransomware pop up the list of encrypted files, so victims can make sure that their file are safe. In windows, all the files are encrypted using RSA encryption (Posted & Rouse, 2014). This algorithm uses two keys: one to encrypt the data and second to decrypt data. This algorithm uses different keys for each one, so it makes almost impossible to recover once the data is encrypted. Hence, hackers ask for money to decrypt their files, and many people pay them since they have really sensitive data that they cannot give up.

During 2013-2014, cyber security has reported less cases than past few years, because security community came across to work with each other and law enforcement to identify any ransomware they could (Robert Leong). In late 2014, ransomware toolkit authors came up with a new idea of automated business model, in which anybody could sign up easily and financial rewards were significant as well. According to FBI's internet, "victims reported more than $18 million loss between April 2014-June 2015" (Robert Leong). Also some worse users started telling other victims that the attacker were good at their word, and would release the data as soon as they get the payment. That movement motivated other victims to do same instead of fining some alternate solutions (Chris Stobing, 2015). One of the main reasons for encouraging hackers to ask for money is bitcoin. This invention really sparked hackers' imagination of demanding money, because this service is pseudonymous, meaning that the people using bitcoin get a significant amount of privacy.

Hence, new invention of bitcoin and continuous efforts to make system security more secure, hackers found new ways to hack the system and encouraged to use ransomware as their hacking tool.

2.2 How it works

The idea of using public-key cryptography was first introduced by Adam L. Young and Moti Yung in 1996 (Robert Leong). In this concept, they introduced the use of encryption key by one party to perform encryption or decryption and the use of different key for reverse operation (Robert Leong). They used same key for both of the operations, but in asymmetric public key cryptography, it allows to use a public key to encrypt items on a system while never leaking the private key

(Robert Leong). Same concept was used in ransomware, so anyone cannot find the key to undo the operation.

One of the recent ransomware attacks was cryptolocker, which has done high amount of harm in 2013. This malware was injected by Russian hacker, Evgeniy Bogache (Saurav Modak, 2016). When the malware is injected to the system, it scans the hard drive and target some specific extension files like docs. This program uses 2048-bit RSA key pair, and private key uploaded to the server (Saurav Modak, 2016). After they get in to the system, they are supposed to contact the command-and-control for further instructions (Shafqat Mehmood, 2016). Most of the antivirus can block that from happening. So attackers started using Dynamic Domain Generation Algorithm Technique, which generates 1200 domains and try to make successful connection with them (Shafqat Mehmood, 2016). This ransomware produced almost $3 million before it was shut down (Robert Leong).

After cryptolocker was shut down, new ransomware named as cryptowall 2.0 was appeared in early 2014. According to New York Times Report, "this ransomware attacked computers in a similar way as cryptowall" (Saurav Modak, 2016). It attacked really important documents like tax receipts, bills, and any other sensitive information (Saurav Modak, 2016). The payments were getting doubled if someone fails to pay before given time. Also some report says that it has been updated to version 3.0, which makes it even danger than before.

Now the question is how do they enter the system? There are many ways ransomware can enter the system. Most common ways are spam emails, and installation of any malware injected applications. For an example, they might send email saying that victim has violated traffic rules and ask to open the link for more details. That is the easiest way to inject malware in personal PCs.

2.3 Alternative solutions

"Prevention is better than cure (Saurav Modak, 2016)". Unfortunately, there are no solid solutions for powerful ransomware, because they say attackers have been developing new ransomwares every day, yes there are some alternative solutions:

- To be on safe side, always back up your data
- Install antivirus so it can clean any small viruses it can
- Never install any apps from unknown sources
- Always be aware with your emails
- Update your software regularly

Conclusion:

This advancement in ransomware has been growing really rapidly, there is no doubt that it is going to be biggest threat for people to keep their private and sensitive information private. We are getting used to high technology, but most of the people do not know that we are also developing huge threat for the future generations. Hackers are keep getting smarter every day by looking for intensive ways to get through intelligent security systems. Hence, there is no permanent solution of ransomware, but we should understand how important our personal information is! People need to little aware and always be prepared to be one step ahead of ransomware.

Bibliography

1) Haran, V.(n.d.). Why Is Ransomeware So Successful? Retrieved September 29, 2016, from http://www.databreachtoday.com/interviews/is-ransomware-so-successful-i-3328

2) Stobing, C. (2015, June 06). Ransomware is the new hot threat everyone is talking about; what do you need to know? Retrieved September 29, 2016, from http://www.digitaltrends.com/computing/what-is-ransomware-and-should-you-be-worried-about-it/

3) Mehmood, S. (2016, April 30). SANS Institute InfoSec Reading Room. Retrieved September 29, 2016, from https://www.sans.org/reading-room/whitepapers/incident/enterprise-survival-guide-ransomware-attacks-36962

4) Posted, & Rouse, M. (2014, November). What is RSA algorithm (Rivest-Shamir-Adleman)? - definition from WhatIs.Com. Retrieved September 29, 2016, from RSA algorithm (Rivest-Shamir-Adleman), http://searchsecurity.techtarget.com/definition/RSA

5) Leong, R. Retrieved September 29, 2016, from Understanding Ransomware and Strategies to Defeat it, http://www.mcafee.com/us/resources/white-papers/wp-understanding-ransomware-strategies-defeat.pdf

6) Modak, S. (2016, January 12). Ransomware Malware: Everything you need to know about it Retrieved from http://beebom.com/ransomware/

7) Fiegerman, S. (2016, September 22). Yahoo says 500 million accounts stolen. *CNN*. Retrieved from http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/