What Is Ransomware?

Introduction

In today's world, Cyber-attacks are getting much more covert and sophisticated in nature. Gone are the days when an attacker would be merely content by simply deploying a Trojan Horse virus to see secretly what is going on in your computer. They are now bent on a total destruction of the end user's machine, and from there even launching Botnet style attacks in order to infect and destroy thousands of other computers in the process.

What It Really Is

But, there is now a new trend occurring these days: Cyber attackers want to hold your computer hostage until you literally pay a ransom payment. This kind of attack is known as "Ransomware", and it can further elaborated on as follows:

"It is a type of malware that prevents or limits a user's access to their computer system, either by locking the system's screen or by locking the user's files unless a ransom is paid."

(SOURCE: https://www.trendmicro.com/vinfo/us/security/definition/ransomware)

So, as you can see from the definition Ransomware is literally virtual kidnapping. You cannot access anything on your computer unless you pay that ransom which is demanded by the Cyber attacker. But the caveat here is that the Cyber attacker does not want to be paid in the normal currency; rather he or she wants to be paid in terms of a virtual currency, known as the "Bitcoin".

How Ransomware is Deployed

There are two primary ways in which your computer can get infected with Ransomware:

1) Via MalSpam:

   This is essentially a spam e-mail that comes into your inbox, but it contains a Malware based .EXE code that will launch itself once the attachment is downloaded and opened up. These types of attachments are typically .DOC, .PPT and .XLS files. You can also get Ransomware by clicking on a phony link in the content of the e-mail message. The techniques of Social Engineering are very often used in this regard in order to make the e-mail look like it is authentic and coming from either a trusted, legitimate organization or personal contact.

2) Via Malvertising:

   This is when a Cyber attacker uses online advertising in order to capture the unwitting attention of the end user and ensnare them into clicking on a genuine looking hyperlink. If this does happen, then the servers that are used by the Cyber attacker will collect details about the soon to be victim's computer, and even where it is geographically located at. Once this has been accomplished, then the Ransomware attack is subsequently launched. Malvertising very often makes use of what is known as an infected "iframe". This is actually an invisible webpage element, and will redirect the end user to an authentic looking landing page. From there, the malicious code is then deployed onto the end user's computer.

The Types of Ransomware Attacks

There are three types of Ransomware attacks:

1) Scareware:

   As the name implies, this kind of attack is just merely designed to scare or frighten you. These kinds of attacks primarily make use of annoying pop messages. One of the most "famous" of these is the pop up which claims that some sort of malware has been detected on your computer, and in order to get rid of it, you have to pay a small ransom. You will know if you if you have been hit by this kind of Ransomware attack if these pop ups keep constantly appearing. The only way to get rid of it is to install antimalware software, such as the ones available from Norton and Kaspersky.

2) Screen Lockers:

   This is the next step up in terms of the severity level of Ransomware attacks. With this, your computer screen locks up, and as a result, you are completely frozen from accessing your files and folders. To make matters even worse, the message that appears will typically have an FBI, Secret Service, or a Department of Justice official seal, in order to make it look like that you have been caught doing some sort of illicit activity online. In order to unfreeze your screen, there will also be a message that you have pay a rather hefty fine. But keep in mind that these government agencies would never ask you to pay up. Probably the best way to get your screen unlocked is to take it to a local Geek Squad to clean your computer of the Ransomware. If this doesn't work, you may then have to get a new computer all together.

3) Encrypting Ransomware:

   These are deemed to be the worst kind of attack. In these particular instances, the Cyber attacker will steal your files, and encrypt them with a very complex mathematical algorithm, which will be very difficult to crack. In order to get your files back, the Cyber attacker will demand a large amount of money, to be paid by Bitcoin. Once they get this money, they claim that they will send to you the decryption key in order to not only retrieve your files, but to unscramble them as well into a decipherable state (in other words, making them like they were before they were hijacked). But most often this never happens, because once you pay up, the Cyber attacker often disappears. Since you have paid with a virtual currency, there is no way of tracking them down either (unlike paper currency, where you can use marked bills for these purposes).

It is important to keep in mind that these are just some of the very basic concepts of what Ransomware is all about. A future blog will go into more detail about it, as well as the steps in which you can take to protect yourself.

In the meantime, if you have any questions, please contact us!