Can we stay safe against the threat of ransomware?

August 10 2015, by David Glance

Ransomware demands increase.

The possibility of losing all of your files and photos on your computer is

a frightening prospect for most people. So much so, that large numbers of users are choosing to pay the criminals holding them to ransom rather than lose their data. In Australia alone, ransoms totalling AUD $1 million were reported to have been paid in 2014. A willingness to pay may be the reason behind Australia's rise to being the second most targetted country in the world for these types of attacks in the 1st quarter of 2015.

The ransomware attacks begin with trojan malware being downloaded inadvertently and run on their computer. The malware is delivered either as an attachment on a spam email or through an infected website that the user has browsed. Once on the computer, the malware encrypts all of the user's files, typically documents, photos, movies and music and then pops up a notice asking for a ransom to be paid in order to get a key to decrypt the files and get them back. The encryption of files followed by a ransom demand are why this type of software is called "crypto ransomware".

Ransom victims are asked to pay on average US $300 using the relatively untraceable cryptocurrency, Bitcoin. About 2% of victims of crypto ransomware agree to pay the ransom despite security experts recommending that this is not the best option. They point out that even after paying, there is no guarantee that all of the files will be recovered.

Although it has been found that a great number of ransomware is not particularly sophisticated, and could, in theory, be dealt with without paying a ransom, the average user is unlikely to be able to deal with the subtlety and is faced with one of two choices, pay the criminals or wipe their computers and start again.

Options for recovery after choosing not to pay

For those users who have backed up their computer, re-installing their

system may not be too much of a problem. However, if the backups were on a computer drive attached to the computer when it was infected, it is possible that those files could be encrypted also, rendering them useless. Ransomware called TeslaCrypt 2.0 will do this and so the only way to avoid this happening, is to backup the computer and disconnect the drive immediately it has finished.

A better approach is to backup to the cloud using a service like CrashPlan which is unlikely to be affected by ransomware because the backups are not directly attached to the computer.

For users who store their documents in cloud storage like Dropbox, their files may also end up being encrypted because of the fact that it synchronises a copy of those files stored on the local computer. The good news is that Dropbox does allow previous versions of files to be recovered, although unless a request is made to Dropbox to do this for all of the affected files, a user will have to go through each of the files individually to recover them.

In terms of other protective measures that users can take to protect themselves against ransomware, these include keeping up-to-date with the latest software releases, not using software like Flash and other plugins on browsers and never clicking links on emails without knowing where it is going.

Ransomware, a problem for all devices

Ransomware is not just confined to computers and certainly not just a problem with Windows. There are versions that will infect Macs and more worryingly, target mobile devices. The types of ransomware that attacks phones is called "locker ransomware". This software simply blocks the user from accessing the normal functionality of the device until a ransom is paid.

Even worse however, is the threat to other devices such as smartwatches and even smart devices in the home.Although criminals have not turned their attention to the smartwatch, the threat has been shown to be very real. Speakers at a recent security conference, BlackHat 2015 painted scenarios where criminals could potentially took control of a car and refused to let someone regain control until a ransom was paid.

The personal threat of being exposed to cybercrime is greater now than it has ever been and simply being connected to the Internet exposes everyone to that risk. Given that society has moved to a permanently connected and Internet-dependent world, that threat is now an ever present, persistent danger.

Source: The Conversation