Ransomware Targeting Computers Running Windows Remote Desktop

October 22, 2015 â€“ There is a new type of ransomware being used to target computers running the Windows operating system. It specifically targets computers running Windows Remote Desktop or Terminal Services; encrypting key files on the computer and then charging the owner of those files around $1,000 to unlock them again. You could be vulnerable and not even know it but there are some things you can do to protect yourself. First, a little background.

For those who have never heard the term Ransomware, it is pretty much what it sounds like. If your computer gets infected with it, you can expect to have to pay some criminal on the other side of the globe if you ever want access to your files again. If you donâ€™t pay, you arenâ€™t likely to ever gain access to them.

Ransomeware has become an especially bad problem for small to mid-sized businesses. Thatâ€™s because the hackers making this software have learned that businesses are much more likely to pay than individuals. Therefore, businesses have become a primary target.

Until now, most computers became infected with ransomware when the computer user opened an infected email attachment or by clicking on a bad hyperlink. This latest version doesnâ€™t require that however. All it requires is a computer running Windows Remote Desktop, or its predecessor, Terminal Services. You could be using either one of these programs and not even know it.

Remote Desktop is used for a number of things. Letâ€™s say want to access your office computer while working at home. Or perhaps you call a technical support hotline for some software you own and the tech you are talking to walks you through

a process that allows him to take control of your computer. In both instances, you are probably using Remote Desktop.

You may not have a need to be using these programs every day. Still, they could be actively running in background on your computer. And that is where you can run into trouble.

The latest ransomware searches for computers running Remote Desktop. Once it finds one, it uses something called â€œbrute forceâ€• to steal your computer password. It then infects your computer which maps all of your hard drives (including any network drives you may be connected to) and it searches for files with specific extensions; encrypting them as it goes. When finished, it cleans up after itself by deleting its own key files â€“ making it nearly impossible for anyone to reverse engineer the program â€“ and placing a text file in each directory that it encrypted. That text file will direct you to pay the ransom or forever give up the use of your files.

The easiest way to protect yourself from this is to change some of your computerâ€™s settings. If you never use programs like those described above, you can disable remote desktop entirely. If you do use them periodically, then you can set them to open only when needed.

To do this, go to Windows Services. In Windows 10, simply click the Search icon on your taskbar and type in the word â€œservicesâ€• without the quotes. At the top of the list that appears, you should see an icon of some gears. Click on it and then look for all of the remote desktop services available. Double click each of them and a properties box will appear. If you have no need for remote desktop, then disable each of the services. If you have a periodic need, set each of the services to â€œmanualâ€•. Once you are finished, reboot your computer.

If you are running an older Windows operating system like XP, then instead of Remote Desktop you will be looking for Terminal Services. The same procedures above can be used to modify your settings for that program.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS