Ransomware 2017

By Chuck Warren

There is a type of virus called “ransomware” that is becoming more and more common every day. It is extremely lucrative for the virus’s creators, and it is also extremely damaging, and costly, to any home or business computer environment unlucky enough to be infected by it.

The name describes the virus perfectly - ransomware locks up all of your files with unbreakable cryptography and demands that you pay an average of $500 to get your data back. Just to add insult to injury, the ransom will double every few days that it is left unpaid, and in the end if you still have not paid the demanded fee your data will be permanently deleted from the computer.

The rate of infection rose from 1.5 million cases in 2014 to more than 5 million by the end of 2015. More than 50 new variants of ransomware were created in the first 5 months of 2016, making the estimated total close to 100 new strains by year end. A recent report from Symantec shows more than 35,000 new ransomware cases were reported in March of 2016 alone and worldwide an estimated 40% of all businesses have experienced an attack.

The FBI has stated that, in most cases, it is easier to pay the price and recover the data than to try to restore files from backup. Several police stations have had to pay up to recover their evidence and case files, and one hospital in Los Angeles paid approximately $17,000 to recover their data. During the 6 hours they battled with the infection the hospital’s staff were forced to move patients to other facilities because necessary lifesaving equipment had been shut down.

The threat is so dire that a recent study in England showed that approximately 30% of British businesses are storing up Bitcoins to use as payment in case of infection. Because of the untraceable nature of the digital currency almost every case of ransomware infection in the last several years has demanded the ransom payment be made in Bitcoins. Since the account necessary to acquire and transfer Bitcoins is challenging to set up and takes time to fund, setting up an account ahead of time only makes sense.

Many of the big, industry standard antivirus companies have released statements telling the public that they cannot protect them from ransomware infection. Since new strains of the virus pop up faster than the security companies can find and target there is no way to prevent a ransomware virus from being launched by the click of a user’s mouse. The virus creators appear to be commonly located in Eastern Europe, Russia, and similar countries where US laws cannot touch them so there is little our criminal justice system can do.

If you are not nervous, you’re not paying attention.

Many IT professionals have not seen or fought with ransomware yet. It’s easy to write it off as just another virus infection, but ransomware is different. Once it has locked up the data on the

host computer the clock starts ticking, and at that point the decision must be made - how much is that data worth?

If that data includes all of the files and folders your business needs to open it's doors, then the decision comes down to - how long will it take to restore from backup, and can we be offline for that long? Even if you are able to restore from backup there will be data loss due to the viruses long reach. In far too many cases it is easier to pay then to try to recover, which is why the virus continues to spread.

This following information about ransomware that is critical to the safety and security of all of the data on any computer or network, whether it's in a business or home environment. This information is the only **real** defense there is against this devastating form of virus infection.

Your only defense against Ransomware is education.

There is a lot of information below and it is all important. However, if you don't wish to read the whole message, here is the most critical paragraph on the entire page -

If you are working on ANY computer and you think you have clicked on something destructive, or if you click on something and there is suddenly a flurry of unusual pop-ups and activity on your screen, IMMEDIATELY UNPLUG YOUR COMPUTER. DO NOT STOP TO THINK - YANK THE POWER PLUG OUT OF THE COMPUTER OR THE WALL. IF YOU HAVE A LAPTOP- HOLD DOWN THE POWER BUTTON UNTIL IT DIES.

Do not turn the computer back on for any reason. If you do turn the computer back on you risk destroying data that could have been saved by leaving it powered off. Or, you risk having your backup program overwrite your good data with the files that have become encrypted.

Leave the computer turned off until you can have a professional technician take a look at it, but be sure to ask if the tech has direct experience with a ransomware infection. Tell him exactly what happened so he does not plug it into his own network and risk infection, or turn the computer back on and do further damage. If the technician is not up to speed on dealing with ransomware, find another technician.

If you are unsure of what you saw or feel you absolutely must turn the computer back on, unplug the network cable before you push the power button so you protect the other computers around you from being infected. DO NOT plug in the network cable unless you are absolutely certain there is no chance of data loss.

The number one virus, and especially ransomware, delivery method is through email.

This is the reason education becomes so important. If you are an IT Professional you must educate yourself on ransomware and it's current patterns, and then educate your users on how to avoid it. If you are a home user, educate yourself on email best practices and how to avoid infection.

Email delivery is the easiest and most effective method of infection. It's easy, cheap, and has a very far reach. Every single email should be treated with suspicion, especially when there is an attachment. However, a link can also do the trick. Trust nothing. If you received a message from someone you know but the subject seems out of character, or if anything about the email seems odd, delete it and then send them a note asking if they did truly send you something. If they did they can always send it again. If they didn't send it, you dodged a bullet.

The only way to survive the Internet these days is to trust absolutely nothing and no one. You cannot trust any update messages that pop up on your screen, or any warnings that claim you've been infected with 8,567 viruses in the last 2 minutes. And you especially cannot trust anything that arrives in your inbox. Nothing. Not even if it's from someone you know.

There have been instances where ransomware and other viruses were installed by clicking a link in an email, and instances that were installed when something popped up on the screen. The most common delivery method is through email attachments. So, how do you know what's safe to click and what isn't?

You don't.

Ransomware (and other viruses) can also launch when you click on the X to close a pop-up window. Or, if you click the link in that weird message that came from your brother in law. In most cases clicking on a virus or spyware is an uneventful experience. Your computer might do something odd like send you to the wrong page when you search for something, or change your homepage, or pop ads up that try to get you to buy stuff.

However, clicking on a ransomware virus will cause lots of stuff to pop up on the screen immediately and quickly make it's presence known. If you suspect for one second that you have launched something really bad, or if you click on something and there is a sudden flurry of activity on your screen, or if you have even a flicker of concern that what you see happening in front of you might be destructive -

IMMEDIATELY UNPLUG YOUR COMPUTER. DON'T STOP TO THINK, YANK THE POWER PLUG OUT OF THE COMPUTER OR THE WALL. IF YOU HAVE A LAPTOP HOLD DOWN THE POWER BUTTON UNTIL IT DIES.

Or, this is what will happen next.

First - The virus will probably have set off about 15 black Command windows which will flash on your screen until they have all carried out their master's mission of doom.

Second - The virus will pop up several windows with text on them which will all say the same thing. They will say something like "What happened to your files?" and then give a description of the damage inflicted upon your computer. This is the ransom note, which will also have a price and a countdown timer. The description usually gives you 5 days or so to pay the price, which averages about $500. If you don't pay by the time the clock ticks down the price doubles and the clock resets. This cycle may continue indefinitely, or it may stop after three cycles and permanently delete all of your data. Yes, you read that right.

Third - By the time you finish reading the information that pops up the virus will have infected everything it can touch and will have encrypted all of that data, which means it will still be there but will be unreadable and unusable. It will have encrypted the following -

1. Everything on the computer itself including your My Documents, Pictures, Videos, and other common files.

2. Everything in any kind of USB device attached to the computer, including thumb or flash drives, or external USB hard drives. Where do most people backup their data? To external USB hard drives. So, what happens if that backup drive is attached and the ransomware virus is launched? Yep, you got it. Gone. No more backup.

3. The newer variations of the virus will also reach across any mapped drive used to connect to shared data. In other words, if you connect to a shared departmental drive in a business by clicking on My Computer and then opening the "S" or "T" drive for example. those drives are fair game and will also be encrypted. That data will also be unreadable.

4. The virus will also reach across any drive that is mapped so that a program can run, and will generally make the program cease to function. If this happens to be a program that is critical to your businesses workday, productivity will be crippled or stopped altogether.

5. Almost forgot! You can also kiss anything in Google Drive, Dropbox or OneDrive goodbye if you have their sync tool installed. And, if you are using Carbonite and leave the computer on once it has become infected you will also lose that backup data.

So what do you do if you think you have clicked on something destructive, or if there is a lot of unusual activity on the screen?

IMMEDIATELY UNPLUG YOUR COMPUTER. DON'T STOP TO THINK, YANK THE POWER PLUG OUT OF THE COMPUTER OR THE WALL. IF YOU HAVE A LAPTOP HOLD DOWN THE POWER BUTTON UNTIL IT DIES.

Even more fun - once you are infected the virus is often easy to remove. However, if you do remove it you disable the ability to pay the ransom and receive a decryption key. That means fixing the virus destroys your data.

Here's the best part. As previously stated, at this time there is no antivirus or firewall that will prevent a ransomware infection. Nothing will detect it or stop it from carrying out its mission of death and destruction. If you click on a carrier link, email attachment, or pop-up - it's game over.

Should you pay the ransom? Yes. Or no. There are many cases where people received a decryption key after paying the ransom. There are also many cases of the opposite, and people paid the price but never received a key. So what is the right answer? That depends on how much you have to lose and how good your backup is.

In an extreme case risking $500 seems like it would be a chance worth taking. In a case where there is a good backup available and little to lose, ignoring the ransom is probably best bet. Only you can make that call, but understand that there are no guarantees that paying the ransom will get you the key.

If you pay the ransom, and are lucky enough to receive a restore key that works, you will also receive instructions on how to use the key and a little utility that restores your data - kind of like a reverse virus.

How do you clean up after an infection? If you ignore the ransom and decide to restore your lost data from backup your best approach is to completely wipe the hard drive clean, reinstall Windows and all of your programs, and then restore your data. Attempting to clean out the virus is risky but can work. However, if it doesn't work you will need to wipe and restore anyway.

How do you protect yourself from data loss? Off-site backup. If the data is critical or valuable, or the loss of that data would cripple or destroy your business, you must at the very least backup to an external drive that is then unplugged and stored away. Backup your data regularly to ensure you will not lose something that you can't live without.

However, even a disconnected hard drive can be destroyed in a fire, or flood, or even by a strong electromagnetic field from something like a large speaker. It can also be mistakenly

put into use. Locking it in a safe deposit box is a good idea but a challenging way to maintain a current backup.

Your best option is to use a cloud-based backup product like JungleDisk, Mozy, CrashPlan, or any of the other products available today. Regularly copying data to a drive is fine, but can often be put off or forgotten. A hands-off approach is the is best way to ensure your data stays safe and secure.

The Internet is a rich and powerful resource which makes valuable information available to anyone who wants or needs it. It connects the world together, making friends of people who may never stand in the same room together. However, it is also a jungle full of tigers and snakes who make their living by robbing people through one means or another. For too many people a false step has led to disaster and the loss of irreplaceable memories in the form of pictures, communications, or important business information.

Take the steps necessary to protect yourself. But, whether you have or have not yet done so, please remember this -

If you think you have clicked on something destructive, or if you click on something and there is suddenly a flurry of unusual pop-ups and activity on your screen, IMMEDIATELY UNPLUG YOUR COMPUTER. DO NOT STOP TO THINK - YANK THE POWER PLUG OUT OF THE COMPUTER OR THE WALL. IF YOU HAVE A LAPTOP HOLD DOWN THE POWER BUTTON UNTIL IT DIES.

Enjoy the Internet!

Chuck Warren
1/9/17