Computer-Ease
Complete Computer Solutions
www.CVWare.com

Custom Programming IT Services Network Management Websites Computers

Good afternoon all. This afternoon we are going to be continuing on the topic of security, with a little info on ransomware and then start on the long topic of email security!

We keep hearing and reading about ransomware, and how a business can be crippled by it, but what exactly does that mean to us, and to you the home user. Well, first lets start of by understanding the motivation of all this ‘nonsense’, and of course that is money – and LOTS of it!

Ransomware attacks and some of the costs and issues associated with them are pretty devastating. With the average cost of a malware attack being $2.6 million its pretty obvious that there is a pay off here for the bad guys. The average total cost of a data breach is currently $3.86 million… and with more and more of these attacks taking place, we need to do better in protecting ourselves, companies and customers. And now, with many people working from home, those HOME computers need to be considered and protected as well as office computers.

SO.. how does this all work and apply to you? Well, the method of ransomware is typically a ‘broadcast method’, seeing who of interest can be caught and then it begins. (Think of that initial broadcast like a commercial fisherman – casting a net and when that net is pulled in **then** he see’s who he has caught.)

If it stopped there for home users, that would be awesome, but unfortunately it has grown far past that. Today’s bad guy utilizes tool kits that invade and infect your computer, send your data back to the bad guys, and after some research on who you are and what your data is, they decide a price and if it is worth moving forward with it – regardless if that computer is a home computer or in a business!

If they believe they can get some dollars from you, then the data on your machine, (usually all documents, pictures, spreadsheets, backups, text, database and even backups,) is encrypted with a password they know, and then you are notified that you have to pay dollars (usually bitcoin) to them to unlock your machine. And you are left with messages saying your under a ransomware attack when you attempt to open most anything or log into your computer.

Lets let that sink in a moment and understand that concept…

If you are being attacked with ransomware, your computer is compromised, all access to almost everything on your computer is denied and you are essentially locked out of your computer.

Almost always notification of this attack happens ON your machine when you go to open something up or even log in. The notification message of being compromised is almost NEVER in email!

While you MAY receive email’s SAYING your machine has been compromised, almost 95% of the time this is a scam that has NOTHING to do with a real ransomware attack, and some bad guy is just trying to see what they can con you out of!

And you know REALLY QUICKLY that your hacked when you log in or turn your computer on!!

The bottom line is if you are hit with ransomware you really have three possible choices to recovery:

1. Pay it – bad idea, and while it MAY work, there are many cases were the bad guys are long gone and you cannot recover data, even after paying the ransom.

2. There are some tools available to decrypt some encryption schemes and there is a small chance that you may be able to have your data recovered. The chance is small, and the costs are usually fairly high.

3. An off-site backup. This … is your best recovery from ransomware. While keeping a “swap and backup” strategy may also save you, there is a high probability that your onsite back up has been compromised as well.

OK, so … now we know the “How its done”, and some recovery methods, so how do we protect ourselves against it?

An off-site backup is really the only protection method to save yourself. A service such as Spider-Oak, Backblaze, Acronis, carbonite, etc can provide you with a highly secure, off-site safe backup. I prefer SpiderOak because of its encryption system, speed and ease of use. AND, not only is the cost very inexpensive ($8 to 12 a month avg), but it provides revisions of your data as well! (I will go into revisions and cover additional useful SpiderOak features in another topic.)

In all reality, you should have an off-site backup to protect yourself against a catastrophic event anyway. (Fire, theft, crash, etc). If the pictures, documents, data on your computer matters to you, then you should have a backup that will save your data in the event bad happens!

The other methods of protection are really only meant to try to <u>prevent</u> ransomware and nothing is 100% guaranteed against it. Those methods are a GOOD antivirus, and understanding what NOT to do with your email. (I will cover these both of these things in more depth later!)

Understanding the most-common attack vectors used in ransomware attacks, (email, bad websites, remote access, and supply chains) help us go a long way to realize how these attacks can come at us and how to avoid them, but 90% of the attacks come in through email and this is where YOU need to focus your attention.

Since this email is getting long already :-) … I am only going to touch on two EXTREMELY important email points that cover not only ransomware, but should be applied for email security in general.

While many of us receive lots of email every day, and most are benign, emails are the most common attack vector for a lot of bad things. The bad guys get your email from either website breaches, paid lists of compromised email addresses, paid lists of valid emails for marketing purposes, or from hacking an email account or computer. (ie your friend, family, acquaintance or a business / website you are signed up on!)

The latter, a hacked email account or computer, is preferred since it is a known, valid entity and usually they have some time before they are discovered. Bad guys compromise or get an email list and then use it to exploit that person’s contact list and you end up with an email that can mean serious trouble.

SO.. the two EXTREMELY important email points ….

1. You should never… and I will repeat that **NEVER** click on links that come in your email!!

   Unless you are a) expecting an email from that person or business, and b) 100% positive that the link is going where you think it should, don’t click it!

   Bad guys can make a link **APPEAR** to be going to one place, yet will deliver you to some other place. (And honestly... it is pretty darn easy to fool most people!)

2. It is critical to treat **ALL** email as suspicious!!

   Even when an email is from someone we know very well and trust. Friends, family, and yes even businesses and clients can be a threat if their system is compromised. Usually, a compromised email has an unusually short sentence, (more like a few words really), and then almost always will contain a link to something “they want you to look at”.

   Typically the email will say something like “thought you might like this” or “what we discussed” or “check this out” and then the link. Typically, the email is very short, trying to NOT give away that the email was not sent by the person you know.

I can fill many paragraphs on unsolicited links in email, and what a valid link is about, etc… And even unsubscribe links can be extremely dangerous. (Another known good method to trap you!!)

The next email we shall deep dive far further into email security, what to look for and how to navigate through the mess. I have written five pages so far on how to “survive email”, and I will attempt to edit that to essentials and not subject you to it all :-)

But, understanding that you should **NEVER click on links that are sent to you** … is the single most important thing you can take away from this email.

And you can read about these issues and more at: www.cvware.com/articles.html

This article in PDF is at: www.cvware.com/articles/Ransomware-and-Starting-Email-Security.pdf