Dealing with Ransomware

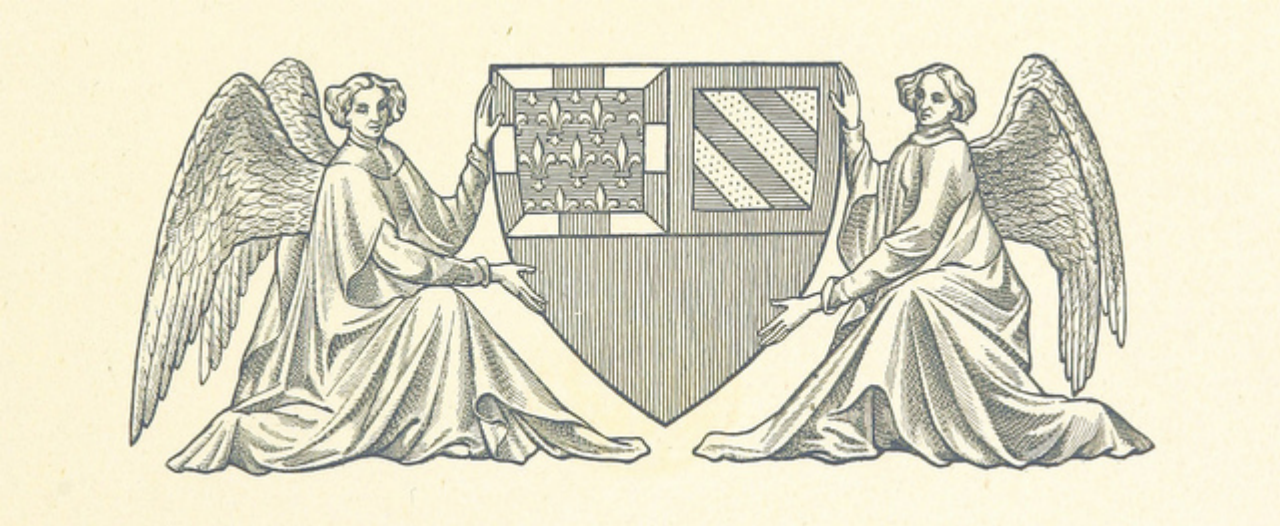
Recently a friend got hit with some ransomware. He is tech savvy and still fell victim to it, after helping him deal with it I thought I'd share some some of the things I learn with you.

To start off let's look at what ransomware is. Ransomware is a very simple attack, once the attacker gets access to your computer they encrypt all of your files. Once that is done they offer to give you the key to all your files in exchange for a payment within a certain amount of time. If you choose not to pay within the time then generally the price goes up, and if you never pay you never get the key from them. Ransomware is a threat to you both on a personal and organizational level, on the personal level they typically demand 300-600 dollars while at the

organizational level it can be tens or hundreds of thousands of dollars, they

There are fortunately many ways to reduce your chances of falling victim and to mitigate the damage should the worst happen. There are two broad stratagies to dealing with ransomware, damage prevention to prevent it from ever taking hold and damage control to mitigate damage once you have been attacked. Ideally you would never need the latter but mistakes will happen eventually and it's important to know what steps to take.

Damage Prevention



Keep Up to Date

Keep all of your software up to date. One of the common ways they get into your computer is through an out of date plugin. It doesn't matter that the exploit has been found and fixed if you haven't downloaded the patch.

Lock Things Down

Limit permissions on your computer. There are lots of little things that you can close down that will limit their ability to get at your computer. If you aren't using things like Remote Desktop Protocol disable that, and if you can operate without it disable files from running from the AppData and LocalAppData folders.

Show Extensions

Show hidden extensions. Sometimes malicious files arrive with the extension ".pdf.exe". Since windows hides extensions by default that file will show as file.pdf which looks innocuous if you aren't paying close attention. Setting windows to show extensions will make this sort of scheme

much easier to spot.

Educate your Staff

Ultimately the main cause for failure is user making a mistake, anything from opening the wrong

and then bringing it to work. Strong

ong way to keeping things secure.

Backups

First of all you should be creating and maintaining backups anyways as part of your routine. Even without malicious intent hard drives fail and accidents happen. Being

able to simply restore from from a backup turns an attack from a huge problem to an

inconvenience that takes a little time. Remember when making backups you need to make at least to backups in addition to the original and keep one of those off site. Having a portable hard drive with your backups next to your computer do little good if you lose your office in a fire or a thief steals both. It is important is to store the backup disconnected from your computer, if you leave it plugged in then ransomware will simply encrypt it too.

Also important is to test your backups regularly. Like any other physical medium they degrade over time, if you don't verify them you could be in rude shock when you least expect it.

Immediate Damage Control

If you realize you just opened a suspect email attachment or ran a file you think contains ransomware you can limit damage if you act quickly. First of all disconnect from the internet and any networks you are on and remove and external devices like phones or external hard drives, also turn off Wi-Fi and Bluetooth. The ransomware will encrypt pretty much everything it can see so it's important to limit its spread.

More Backups

After getting everything encrypted make a backup of all the encrypted files somewhere. If all else fails a way to decrypt the files may discovered at some point in the future, and in one case one of the attackers had a pang of conscience and put out a code so everyone they hit could decrypt their files.

Check for Solutions

A few versions ransomware have had some weaknesses in their encryption that have allowed third parties to crack them, check out these resources to see if is an option for you.

https://noransom.kaspersky.com/

Wrapping Up

In the end while getting hit with ransomware can be devastating there are a few easy steps that can drastically reduce the risk of getting hit and the severity of the damage if that slim chance happens. If you want to learn more check out this guide created by KnowBe4. It is well written and covers the topic in more depth.

As it happens my friend was was lucky, he had been hit with Coinvault and the decrypter linked to above managed to fully decrypt all of is files. You can bet that he has taken some of these steps I listed above and should it happen again he will be prepared.
