White Paper: Malware

Sick just got sicker

Introduction

There have been several high profile ransomware cases recently, including the NHS outbreak which almost cost lives, but certainly cost a lot of wasted time and money. Computer viruses are nothing new, but a new type known as ransomware is a little different, and it's worth taking the time to understand this risk and what steps you can take to reduce your exposure to it - plus what recovery paths you should consider. This white paper will explain what it is, how it can hit, and how you can ensure you are protected in the event of an infection.

What is it?

Ransomware is a type of computer virus that can infect via a link you click on or attachment you open in a spam email, or via a "poisoned" (hacked) advert on legitimate websites. It will lock you out of your files by encrypting them and displaying a message like the below, informing you that you need to pay the attacker money (usually via BitCoins) to decrypt your files and get them back.

Surely it's just a scam?

Sadly, no. The encryption techniques they use mean that even the best IT person in the world couldn't get your files back; the "key" to unlock the encryption is totally unique and is held by the attacker only. Lots of criminals have made a lot of money from ransomware because people have had no choice but to pay the money (typically a few hundred pounds) to get their vital files back. The only other way you can get your files back is to restore them from a backup – assuming you have one. Always check with us first though, NEVER give your payment details to anyone.

What about my anti-virus program; that will protect me won't it?

Probably not, because it would not see encrypting your files as a bad thing. Normal anti-virus programs monitor your computer for the tell-tale signs of unusual traffic coming to or from your PC and can then isolate the program doing it, and remove it. Ransomware is different because it does not behave in this way, it simply installs itself on your computer and then encrypts your files. The US company Malwarebytes has released an trial of an anti-ransomware program that is one of the first of its type in the world, which you could try for free yourself here, but it can't guarantee protection.

So what can I do?

First and foremost, don't open attachments in emails from people you don't know! This is the most common vehicle for ransomware – an attachment that is a virus disguised as a PDF. We have a separate White Paper all about spam email protection tip on our knowledgebase, by the way.

Second, and equally as vital: **make sure you have a backup of your files**! In almost all cases, this is the *only* way to recover your files without having to pay hundreds of pounds to the attacker.

If you are reading this at work, ask the question of your IT department or vendor. It may be your only line of defense. Backups should exist on a totally separate medium and system than the day to day files, and ideally should run every night. Ask your IT what the recovery process would entail and how long it might take, so you know how long your files will be out of action for should you get hit. Also ask them to check who can access your shared drive, and consider updating those permissions so that people only see the folders they need to. If staff can access all your shared files, then a ransomware infection on anyone's PC **could infect the entire shared drive, for everyone – this is very important to understand and discuss with your IT team**.

If you are thinking about your home PC, then buy yourself a basic external hard drive like this. Windows includes built-in features to easily set up a simple backup of all your files and photos onto an external drive; here is a guide you can follow. Remember to unplug the backup drive from your PC once the backup finishes, else that could get infected too!

Our Conclusions

Ransomware is nasty stuff. The only true guaranteed protection is to make sure you have robust backups in place – at home and at work. This goes without saying anyway, but when was the last time you actually tested your backups work? What if someone in your company got an infection simply by opening a spam email and it infected your whole shared drive – could you recover? Being able to answer these questions shows you take data security seriously, and will be a godsend if you are unlucky enough to experience ransomware first hand.

Please do get in touch with us should you wish to discuss this or any other White Paper further.

Further Reading

Good BBC article on Ransomware: http://www.bbc.co.uk/news/technology-35091536

A full walk through of what a typical Ransomware infection looks like: http://www.bleepingcomputer.com/virus-removal/cryptowall-ransomware-information

Tips for backing up your data: http://www.pcadvisor.co.uk/how-to/software/how-back-up-your-pc-laptop-3356160/