DeBug Tech Tips

Ransomware

Maybe you have heard of it, maybe you haven't, either way there is a new generation of malware evolving posing an ever increasing threat to your data. This new class of threats is most commonly referred to as ransomware, and although the medium through which they come may differ, and the success of the removal methods may not always be consistent, the goal of the infection is the same, encrypt your data and make it unusable.

If you are one of the unlucky few you may have already been affected by it, or know of someone who has. Targets of this malware spread across all demographics, from the home user all the way up to the medical offices such as, Hollywood Presbyterian Medical Center which had their data encrypted recently. If you are not familiar with this threat the general way it works is by encrypting your data with a key and demanding a ransom in exchange for said key to restore the data. If the ransom is not met within the given time period they key is destroyed and in most cases the data is lost. Typically the ransoms are about $300 but in the case of the Hollywood Presbyterian Medical Center, they ended up paying the attackers $17,000.

So what can be done to prevent this? As with any threat that is out there today there are preventative measures you can take but none are 100% effective. Even secure websites can become compromised, emails from friends and relatives can be infected and there are "backdoors" into your computer. That being said, you should still take as many steps as possible to keep yourself secure. One of the most important things one can do is keep their PC and all software up to date. This includes things like Windows updates, Flash and Java, your antivirus software, and any other software you may have installed. Often when updates are released they are for security flaws, closing those backdoors to make it harder for attackers to get in.

If taking preventive measures won't guarantee your security what can be done to protect your data? One of the simplest methods to safeguard yourself is to purchase an external hard drive and keep a current back up on it, and keep it disconnected from your PC when not in use. If your backup drive is connected to your computer and you are infected with ransomware there is a really good chance the backup will be encrypted as well. Other options include offsite cloud based backups which will keep your data out of harm's way as well.

Here at DeBug Computer, we have seen our fair share of clients that have either lost their data or have had to go to extreme measures to recover it. Some versions of the malware are "crack-able" in which case the data encryption key has been made public and data can be restored. In other more serious cases, where there is no viable backup, the ransom must be paid to recover data. We have seen the headaches and even heartaches this has caused to our clients, losing priceless photos and documents, and hope we can prevent further frustrations! **KnowBe4** has released a great **pdf** that they recommend printing and keeping on your desk and handing out to your employees to help guide, and keep you protected from threats.

If you need any advice on backups, antivirus software, or would like more information on the topic please feel free to contact us!

Call: 775.883.3630 Email: Info@DeBugComputer.Net Web: DeBugComputer.Net