MiTek

GN GUIDELINES NO.228

ANOTHER MITEK ADVANTAGE – JULY 2016

By Daniel Heathershaw, IT Manager

Ransomware Part 1: What is it?

You may have heard stories about Ransomware, or even seen it on the news – stories of small businesses, hospitals and even government agencies that have had their files encrypted and a ransom demanded to decrypt them. But what is it, what are the consequences of becoming infected and how do you prevent it? In the first of this two-part series I'll explain the basics of Ransomware, and in Part 2 I'll delve into the consequences and some of the strategies you can use to protect your company.

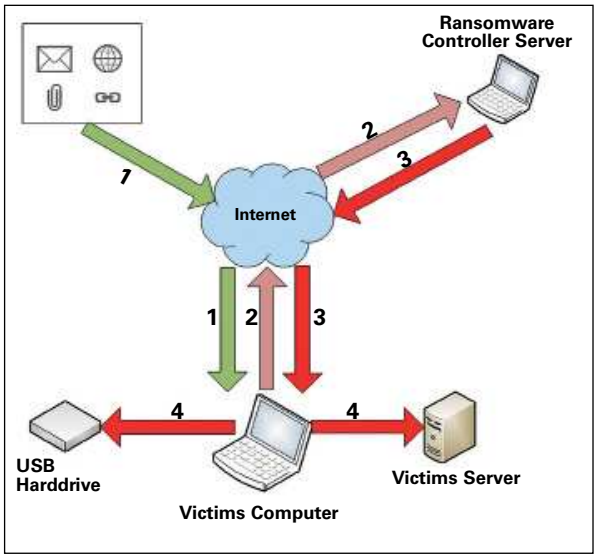
WHAT IS IT?

Ransomware is a type of malicious software (Malware) that is designed to prevent you from using your computer and accessing your files. There are a number of different variants of Ransomware. Some will encrypt the files on your computer and any computers you're connected to, and some will prevent you from using your computer by displaying a full screen message that leaves you only one option – to pay up! The end goal for the criminals is to make you pay to have your files decrypted or your computer unlocked. A fairly simple business plan, but business is booming!

HOW DO YOU GET INFECTED?

Ransomware is spread in a similar fashion to most other types of Malware.

- Email is one of the most common methods, and infection usually occurs by opening an email or an attachment from someone you don't know. You've probably all received an "invoice" or "AusPost" email that you've been tempted to open. Clicking on a malicious link in an email can also lead you to an infected website or install Ransomware directly.
- Browsing the internet and visiting an infected website can result in a Ransomware infection. Even websites that you use every day can be hijacked and become a source of Ransomware infections.
- Social media sites such as Facebook, Twitter and Instagram can contain links that will result in an infection.
- Skype and other instant messaging programs can also contain bad links.



HOW DOES RANSOMWARE WORK?

Explained below is a basic description of how some common variants of Ransomware work:

1. A person receives an email containing a malicious attachment, or visits a hijacked website.
2. The malicious software is installed and executed on the person's computer. The Ransomware then attempts to connect with its controller server on the internet.
3. Once connected, the Ransomware is assigned a unique encryption key which is sent to the victim's computer and used to encrypt files.
4. The Ransomware will now seek out and encrypts files on any connected USB drives or mapped drives.

WHAT'S NEXT?

As always, education is the key. Don't open any emails that you're not expecting or look suspicious, and don't browse to any websites that you're unsure of. In Part 2 I will discuss the consequences of an infection and some of the easy steps you can take to prevent an infection or mitigate the risk. T

> "The end goal for the criminals is to make you pay."

Visit mitek.com.au for all guidelines

MiTek®

GN GUIDELINES NO.229

ANOTHER MITEK ADVANTAGE – AUGUST 2016

By Daniel Heathershaw, IT Manager

Ransomware Part 2: Consequences

The consequences of a Ransomware infection can be mild or they can be extremely severe – severe enough that it could potentially put you out of business. If one unimportant computer becomes infected and has its files encrypted, you could probably continue working, but if that computer is connected to a system critical to your business, you could be in a lot of trouble. How long could you work without access to your financial systems or the machinery used to cut and press trusses? Even with today's powerful computers, the time to fully recover from a Ransomware infection can range from days to weeks.

Aside from the monetary implications, consider the damage to your reputation as well. How would your customers react if you can't provide your normal service to them, or if your systems – which may contain their personal and financial information – have been compromised?

HOW CAN YOU PREVENT RANSOMWARE INFECTION?

Malware, and Ransomware in particular, is constantly evolving and becoming increasingly sophisticated, which makes prevention very difficult, but there are some simple strategies you can put in place to reduce the risk.

• Make sure your all of your software is up-to-date. Ransomware infects computers by using security holes in software such as Java, Adobe products and even the Windows Operating System. Software companies put out alerts and patch their software on a regular basis, but end users seldom apply the patches.

• Install some good Antivirus and Antimalware software on all PCs, laptops and servers. There are software packages that can make the management of Antivirus and Antimalware easy.

• Remove Administrator rights for end users if possible. This can prevent some Ransomware from being installed. It won't stop everything, but it is best practice to use a limited account whenever possible.

• Don't enable Microsoft Office Macros. With Macros disabled, certain Ransomware cannot take hold.

• Back-up all of your important data! Restoring data is a quick way to recover from a Ransomware infection. A good strategy to deploy is called the 3-2-1 Rule:

1. Make sure you have three copies of all your data.
2. Store the copies on two different types of media (USB and DVD, for example).
3. Store one of the copies offsite, for example at home in a safe, or in a secure offsite facility.

• Educate your staff regularly on email and internet safety. Create logical IT policies and enforce them. If you can prevent the Ransomware from ever getting installed you have already won the battle.

A more sophisticated strategy can be used by implementing a third party Domain Name System (DNS) such as OpenDNS. DNS is sometimes described as the phonebook of the internet and is used to convert human readable addresses such as www.google.com into numerical internet addresses that computers understand, such as 216.58.199.78.

Without getting too technical, companies such as OpenDNS maintain massive address databases. OpenDNS handles something like 50 billion DNS requests every day and they use sophisticated techniques to determine which addresses are used by the Ransomware Controller servers. They then block these addresses, so if your computer gets infected it's unable to connect back to its Controller Server to retrieve an encryption key. (See GN Guidelines in the July issue of *TimberTrader News* for a description of how Ransomware works).

CONCLUSION

Computer security needs to be taken seriously by all staff, from the top down, especially in this day and age. Becoming infected can have devastating consequences for a small business, however if you have the right security systems and policies in place and educate your staff, you can prevent infections or – at the very least – reduce an infection's effect. T

Visit mitek.com.au for all guidelines