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.

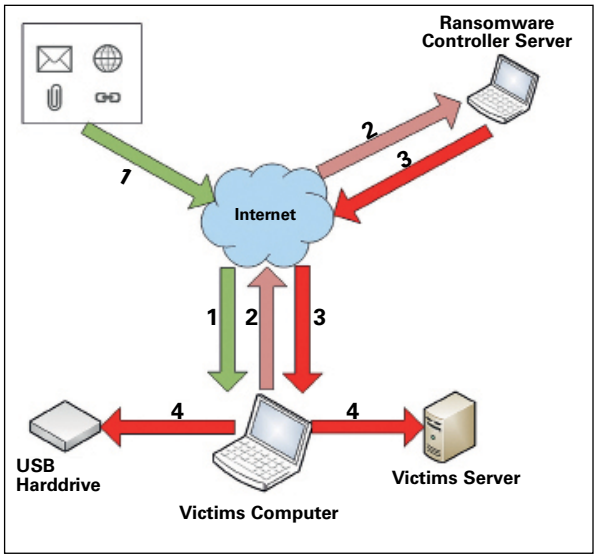
WHAT IS IT?

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