THE RANSOMWARE SCOURGE

The ransomware virus is a particularly malicious virus, that once enabled, will encrypt the data on all your computer and the computer systems that your computer is attached to, rendering it unusable. The end user will receive a message demanding a ransom paid to some unknown entity in order to get "the key" to un-encrypt your data and possibly make it usable once more.

This ransomware virus is mostly delivered through phishing emails to end users. In its early days, ransomware emails were often generic in nature, making it easier for end users to realise it was not a legitimate email, and delete it immediately. In more recent times however, these emails have evolved and now are more geared in their approach to target both the organization and the individual, making it easier for the end user to fall into its trap.

The Allure of Law Firms

Quite simply, ransomware is a malware which restricts access to information stored on a computer and demands the user of that computer to pay money in order to remove the restriction. Failure to pay the ransom money demanded will result in a permanent deletion of all encrypted files by the hackers.

Firms providing legal services are particularly attractive targets for ransomware attacks for the sole reason of storing confidential information of reputable clients they have in their computer systems. Law Firms are then forced into paying these cyber criminals merely to avoid the negative reputational consequences which arise from the failure to protect their clients' sensitive information.

How It Works?

Step 1

End user receives an innocuous looking email. These emails are generally made up of two kinds:

1. The offending email contains malicious attachments, including .pdf, .doc, .xls, and .exe file extensions. These attachments are described as something that appears legitimate, such as an invoice or electronic fax, but contain malicious code and will be triggered once it is downloaded by the user.
2. Receipt of an email that appears legitimate but contains a link to a website hosting the malware. When the user opens the malicious file or link in the phishing email, the most frequent end result is the encryption of files and folders containing business-critical information and data.

Steps 2 & 3

The malware is downloaded onto the host's computer and proceeds to encrypt all the files on its computer. Most malware also extends to encrypt files stored in the Firm's entire systems if the host computer is attached to it. Encryption of these files mean that is becomes "locked" and unusable to the Firm. The Firm will not be able to work on these files, make copies, or save backups. It is lost forever.

Step 4

The end user receives a ransom notice from the hacker providing details such as ransom amount, payment method, and deadline for payment.

Step 5

Once payment (Note: it is advised to never pay, see below) is made, the Firm will be issued a "key" code to unlock their encrypted files. These files will hopefully once again become useable to the Firm.

Never Pay The Ransom

Although it is tempting to just pay up the ransom and retrieve your information, many cyber security specialist advice not to, as more often than not, the chances of retrieving the encrypted data are almost non-existent even if you pay.

Also, when a ransom is paid just the one time, you will be attacked over and over again because you've proven once that you will pay to have your information back. The best way to protect against this type of ransomware is prevention.

Users can prevent being hit by ransomware by doing the following:

1. **Avoid clicking suspicious links**. Firms should concentrate on creating awareness and provide information to their staff to be more vigilant against these sorts of attacks. These include being able to spot the threat of ransomware via email and phishing websites.

2. **Backup important data**. If a device or system is infected, backups may be the best way to recover your critical data. At best, you will only lose a few days' worth of data. Your Firm's data must be backed up on a regular basis by a competent staff. Simply backing-up data is not enough, **as** all backed-up data must also be verified for its integrity and done so securely. Back-up data must not be connected to the same computer or network that is secured – back-up should be done into an external drive, cloud storage or a physical storage offline. Some ransomware can even go as far as locking (encrypting) cloud-based backups when systems continuously back up in real time.

3. **Double check everything.** Verify the email sender and double check the message content. See page 6 for tips on email security.

4. **Ensure your software is updated.** Make sure your that Firm's anti-virus and anti-malware solutions are set to automatically update and that regular scans are conducted.

5. For more tips on guarding yourself against possible cyber threats, read the tips provided on page 6.