Ransomware

The Essentials Things to Know

Over the past few years, organisations around the world have seen an increased number of attacks of the new cybercrime known as Ransomware. Whilst many of us have heard the term Malware and understand that it's a problem for many consumers and business alike, we don't necessary understand the impact it could have on our business and lives, nor do we understand the true differences between malware and ransomware.

Outlined below are the essential things you need to know, how this threat operates and how to best protect yourself and your organisation, protection through technology, people, procedures and policies.

1. What is Ransomware: Ransomware is a type of malware, except instead of tracking your computer usage, it blocks or limits access to your computer or files. In line with the name a ransom is demanded by the scammer to unlock your computer or files. In order to block or limit access to files, users are generally required to download a file. This could be a to watch a video – also known as a codec, or it could take the form of music, movies, a game or an application fix a computer problem. Files are then locked using an encryption key known only to the scammers. Once your files are locked, scammers demand a fee to unlock your files. In recent times scammers have jumped onto the Software as a Service (SaaS) model. Instead of a onetime payment, regular payments must be paid to ensure the continued access to files. Even then there is no guarantee you will get access to your computers or files again. Scammers have been known to go back on their 'word'.

2. Anti-Ransomware: Also known as Malware Checkers or Malware Scanners are similar to Virus Checkers, except they have been specifically developed to check for known malicious files and prevent attacks by blocking files from downloading. If computers do become infected these applications can generally remove malware, but there are very few cases where they have successfully unencrypted files affected by ransomware.

3. Why you should Patch and Update Applications: Patching or updating your applications is one of many preventative measures you can take to protect your files. Applications providers like Microsoft, Adobe or Java, to name just a few, are continually looking at ways to protect your data files from attacks. The updates you receive from the providers are often patching identified security gaps in the products.

4. Windows Policies can help: In recent times, ransomware applications have been known to delete your files locally stored backups. One course of action is to block access to Volume Shadow Copy Services (VSS) to stop deletions of backups. By blocking the ability for the computer to delete your backups, you may be left with a useable restore file.

5. Disable Script Hosting: Depending on the complexity of the ransomware program, these applications have been known to download additional files in the background. By disabling windows script hosting, blocks the ransomwares ability to download additional files to execute its tirade on your system.

6. Don't Phish: Phishing is a term used when users are taken to a fake website that looks like the real thing. In order to maintain this type of appearance, website often have the same logo and branding of legitimate sites. In fact, many phishing sites are hard to tell apart from the real site. Often the only giveaway is the URL (or Domain name) in the address bar. But normally at this point, it's too late. By then tracking cookies may have been downloaded. Never visit a website unless you have first checked the legitimacy of the address on other documentation provided by the organisation.

7. Filter '.exe' Files: Also known as an executable file, by blocking these files in your modem/router can prevent the installation of these malicious programs. By denying the download of these files, also means emails are less likely to receive an executable file from downloading, and stops the temptation staff feel to open the files.

8. Backup: Backing up your computers and data files, especially retaining multiple copies over time is one of the most important things you can do. In the event such an attack is successful, you will have the ability to 'roll-back' to a time prior to the installation of the ransomware. It only takes one momentary lapse of judgement opening an email, or downloading a file and your entire computer network could be infected.

9. Educate Users: Are your staff and family aware of these risks? One of the best preventions to ransomware attacks is to ensure other users are briefed on the same information. It is recommended that you educate other computer users to never open files attached to suspicious emails, especially ones from unknown senders. It is also important that all emails and recommended file downloads be treated as suspect until verified. Victims that have fallen to pray to these attacks may have had a program installed on their system that sends the same ransomware on to email address saved in their address book. Additionally staying current of ransomware developments, the most different and most dangerous strains and who's most at risk, will help defend against attacks.

10. Don't Panic: In the event of an attack, remain vigilant and isolate the infected computer to stop the spread of attack through the rest of the network. Contact your anti-ransomware provider and advise the situation. These organisations will have the most amount of knowledge to assist. They may have a solution or be working on one already. If attempts to remove the ransomware are unsuccessful, and providing regular backups have been maintained, a full clean of your computer, and reinstallation of your application, and data from your backups is the only way to know conclusively that your computer has been returned to its original state. .

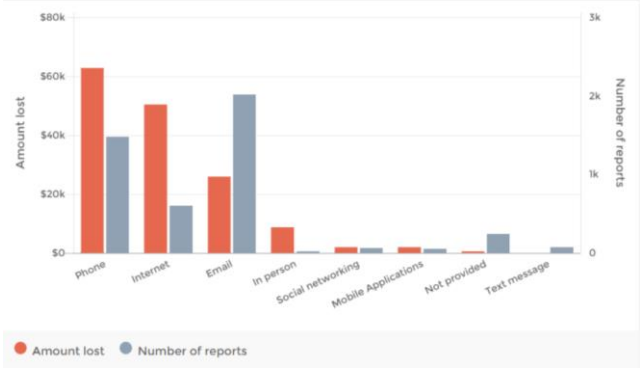
*Statistical information regarding the number of attacks and those targeted at the time of writing have been included on the second page.

As of September 2016

Amount lost	Number of reports	Reports with financial losses
$152,806	4,573	2.6%

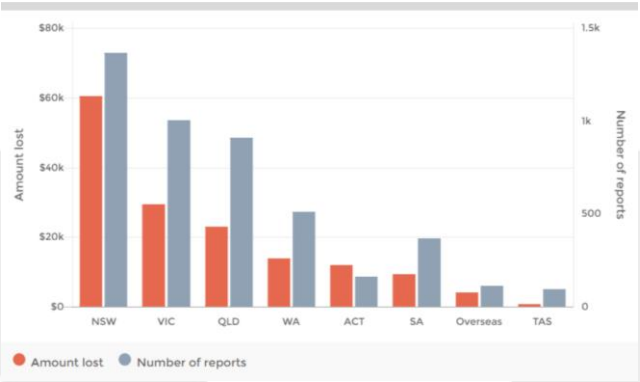
Amount Lost and Number of Reports

Delivery Method

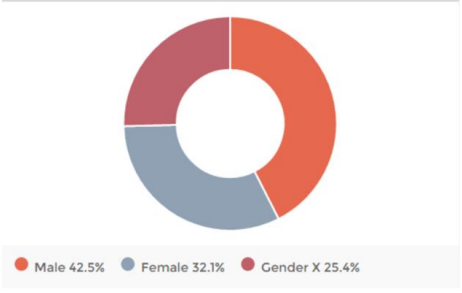


Age Group

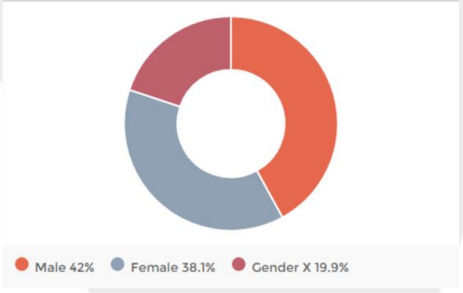
Location



Gender – Amount Lost



Gender – Number of Reports



This data is based on reports provided to the ACCC by web form and over the phone.
The data is published on a monthly basis. Our quality assurance processes may mean the data changes from time to time.
Some upper level categories include scam reports classified under 'Other' or reports without a lower level classification due to insufficient detail provided. Consequently, upper level data is not an aggregation of lower level scam categories.
Note: Due to a technical error, some scam reports from previous months are included in July 2016 causing an increase in reports for some categories. This error has been fixed for future months.