BaQapp

The safe backup solution

PRESS RELEASE **For immediate release**

2 May 2016

What is Safe, vaulted backup?

25 years ago the internet was new, and virus was something that made you sick.

Today not having antivirus in your computers is considered negligent.

Backup is the simple solution to ransomware, but it is useless unless "vaulted".

Not having backup that is vaulted will soon be considered negligent.

Most popular backup software does not offer automatic ransomware protected backups, and external connected drives are particularly vulnerable to ransomware.

Ransomware will infect network connected computers, mapped drives, file shares or even cloud drives that appear as network drives.

Ransomware can spread to an attached thumb drive or externally attached hard drive.

Ransomware will infect system files, Windows volume shadow copies (VSS) or System Restore functions you might otherwise deploy.

The main reason that ransomware is so effective is that the cybersecurity field is not entirely prepared for its resurgence. Attacks are more successful when effective countermeasures are not in place.

The real solution is to use intelligent/network backup systems (NAS backup Appliances) that have "Read" permission of your data, but your PC doesn't have "Write" permission on their storage device... In other words, don't trust USB backup systems - use only IP based solutions (including network shares/NAS).

We have yet to develop any universally accepted description for **vaulted, hardened, sealed, protected, fortified, resilient, re-enforced, or another term that means another layer of (data) protection.** We like vaulted, because it is an easy concept to convey.

That Ransomware is a major problem cannot be disputed.

The problem is compounded by the wrong advice given by many 'experts'.

They advise backup, but fail to explain that backups that are not 'vaulted', or protected from infection are vulnerable to ransomware infection, as in the following extract.

"*Ransomware is not going anywhere. It's a perfect crime tool, with black market logic -- easy to implement, high ROI. We're going to have to learn how to live with it, so backing up data to external drives on a regular basis must become everybody's habit*." respected network security expert - Sue Marquette Poremba, but there is no mention that backups must be vaulted

A backup that is not safely vaulted, is likely to be just as encrypted by ransomware as the files in your PCs.

So what can you do to protect yourself?

Cloud backup is usually safe, and should always be used for critical files, but the time to originally backup and then recover a complete drive or image, especially in Australia can be too slow.

Large and medium enterprises use powerful high speed backup appliances which can be costly and difficult to set-up.

Low end appliances are usually designed as servers, with unsophisticated USB backup solutions which are useless to prevent ransomware infection unless someone configures/secures it properly which does take some technical know-how.

However there is a new solution for safe backup, provided by **BaQapp**.

BaQapp have not invented safe vaulted network backup, but made it more available to the rest of us, but by reducing cost and pre-configuring to make installation easier.

BaQapp offers, deduplication and compression that reduces storage size, error correction to prevent data loss over time, simple cloning for offsite storage with encryption should a drive be lost, plus optional independent monitoring to ensure backups remain current.

BaQapp is low cost, $299.00 irrespective of the number of PCs or servers, and it's a once only cost.

BaQapp offers versioning of both full images and files with the ability to go back in time to recover prior to the infection If a recent backup has been infected, it will not spread to the older incremental and full backups.

The **BaQapp** endpoint app backs up files and disk images, over the LAN to a local Debian Linux, **BaQapp** server. This provides a "hardened" OS environment which makes it extremely unlikely that ransomware will be able to deliver their "payload" or attack.

BaQapp is accessed through the password through your browser. The administrator with the password has the ability to change settings such as backup frequency and see the status both file and image backups of all endpoints.

With good safe backup there is no need to pay ransom criminal demands, buy bitcoin and hopefully wait for a decryption key.

For more information contact Bernhard Kirschner on 02 9955 7373 or 0416 237667
or James Brough on 02 9955 7373 or 0438 237667.

This and other press releases are available as soft copy with images at https://www.baqapp.com.au/press.php or by request on USB and CD.