The safe backup solution

PRESS RELEASE **For immediate release**

2 May 2016

The oldest guy in the room offered the solution to the latest IT problem – ransomware

BaQapp, the low cost backup enterprise grade backup solution for the rest of us launched successfully at CeBIT in Sydney today.

Bernhard Kirschner, aged 75 and James Brough showed in minutes how BaQapp simply recovered a hard drive that had been infected by ransomware, and dealers and users were buying BaQapp there and then.

Good safe certain backup is the best solution to the plague of ransomware attacks, which means backup that is protected or vaulted from ransomware attack and is fast to recover.

Most popular backup software does not offer automatic ransomware protected backups, and external connected USBs storage is particularly vulnerable to ransomware.

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

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

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 cyber security field is not entirely prepared for its resurgence. Attacks are more successful when effective countermeasures are not in place.

The best 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).

Says Kirschner; "*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*."

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 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.

BaQapp have not invented safe vaulted network backup software, but made it more available to the rest of us, but by reducing cost and complexity.

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

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.