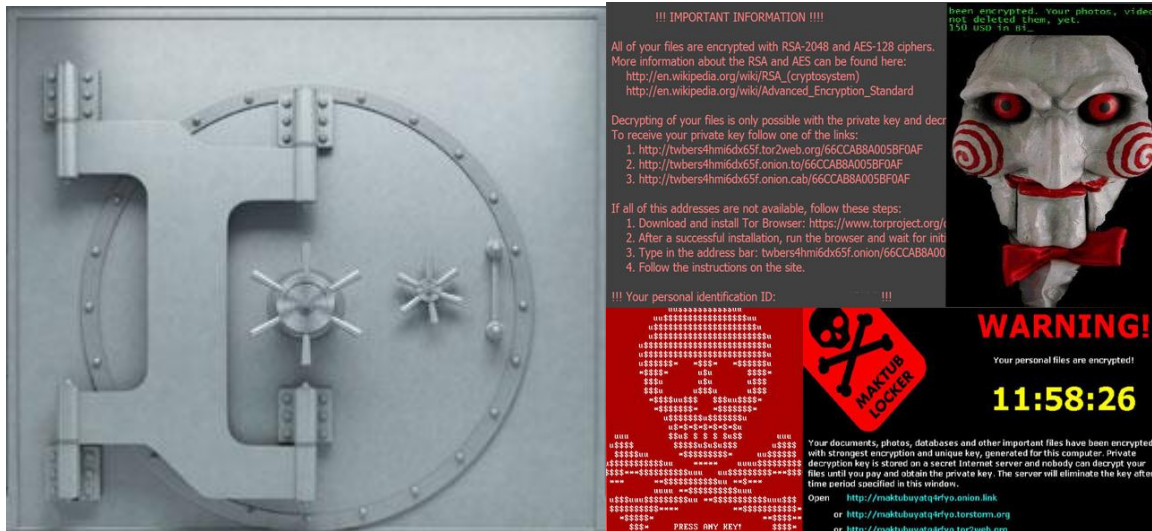




The safe backup solution

PRESS RELEASE For immediate release

2 May 2016



The

choice is simple.

Low Cost Safe Certain Vaulted Backup or risk Ransomware Infected Backups.

We are under attack from thieves who want to use digital information to steal, from enemies who want to destroy information, from competitors who want use information to cheat, and now from criminals who to withhold information for ransom.

Currently ransomware attacks are not preventable by virus scanners which may not detect new or zero-day malware.

The solution to the plague of ransomware attacks is simple.

Good safe certain backup, which means backup that is vaulted from ransomware attack that is certain, easy cheap and is fast to recover.

With good safe backup there is no need to pay ransom demands.

Henry Ford disrupted transport, not by inventing the car, but by reducing cost and complexity. 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.

Ransomware restricts access to a computer system that it infects, demanding that the user pay a ransom to the operators of the ransomware to remove the restriction.

Ransomware targets locally attached drives and network shares that most backup solutions typically use.

Backups are open to attack by ransomware, unless they are vaulted.

The BaQapp endpoint app backs up files and disk images, over the LAN to a 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 a joint Australian and German backup solution offering novel low cost technologies to ensure that valuable data is as safe as it can be.

BaQapp will be giving live demonstrations of a ransomware attack, and then show how easily and quickly BaQapp can make a complete recovery on Stand 30 at CeBIT on 2 -4 May 2016.

See the BaQapp information page at <https://www.baqapp.com.au/features.php> with links to multiple expert articles on detecting and preventing Ransomware.

Too many users and organisations do not backup safely.

Their backups are not vaulted, making them open to malware infection.

They forget to backup, may set their backup to automatic, but there is no 3rd party monitoring to ensure backups are occurring.

Their backups are not encrypted, increasing the risk of data theft.

They do not have image backups to make quick and complete, even bare metal recovery of endpoints when ransomware attacks, a drive fails, or a computer is lost or damaged.

They have no near offsite backup, which is available quickly and easily for disaster recovery.

They pay high fees and depend on the cloud with limited transfer speeds, which itself has risk, although small.

They pay extra per endpoint, making the cost prohibitive for multiple endpoints.

Their backups do not take advantage of deduplication and compression, limiting backup space and adding extra storage costs.

BaQapp solves it all, efficiently, reliably and very cost effectively.

- BaQapp offers vaulted backup defence against ransomware, so that backups are protected, unlike connected mapped drives, and most low cost or free backup systems.
- BaQapp runs effectively on low cost hardware, with NO additional endpoint charge, no renewal fees, and offers low cost monitoring.
- BaQapp is a network application that not only runs on x64 processors, but also on the low cost ARM processors used in mobile phones and other devices, familiarising stand alone ARM devices to the office network.
- The ease with which BaQapp runs on Virtual Machines introduces new users to the free Microsoft Hyper-V and Oracle VM VirtualBox or other commercial hypervisors.
- BaQapp offers optional independent low cost global reports of multiple endpoints for \$90.00 a year, generated independent of the BaQapp software, ensuring that backups are not forgotten.
- BaQapp offers as standard, deduplication, encryption, error correction redundancy, global monitoring, cloning for offsite storage, RAID, incremental and image backups with bare metal restores.

The **BaQappBoxx** for unlimited endpoints is a plug and play credit card sized network device with 8 core 64 bit with USB3 for fast storage and Gigabit Ethernet for quick network transfers. The unit is supplied boxed with power supply, Cat 5e cable, manual and recovery CD and USB, all for just \$299.00 including Australian GST.

The full working **BaQappVM** for unlimited endpoints for Hyper-V, VMware and VirtualBox, can be downloaded for a free 30 day trial, and then requires once only activation by online payment of \$299.00.

More detail

BaQappBoxx device technical details

The BaQappBoxx comes pre-configured in a supercharged Raspberry Pi type credit card sized device called the ODROID-XU4 a new generation of computing device with more powerful, more energy-efficient hardware and a smaller form factor, that offers amazing data transfer speeds.

The ODROID-XU4 has dual 4 core A15 2Ghz and Cortex™-A7 Octa core CPUs, 2 GB RAM, Gigabit Ethernet, 2 USB3 connector, HDMI 1.4a for display. Also supplied with the BaQappBoxx is 240V power supply, Cat 5e cable, manual and recovery CD and USB. The size is 82 x 58 x 22 mm approximately.

Backup recovery

To recovery files, just select the files or folders, even choosing which version by date, drag and drop.

To recover to bare metal, or a replacement drive, download and create a BaQapp boot CD or USB, (also supplied with the BaQappBoxx), and watch BaQapp recreate your drive as fast as your network can transfer.

Installation

To install the BaQappBoxx all that is required is to plug in power, connect Ethernet, open your browser, type baqapp/ at any endpoint and a registration interface appears asking for an email address for reports, an optional SMS number for urgent reminders, a name for the device, and a password. These details are then automatically printed for future reference. BaQapp then asks you to attach USB storage, usually a HDD or SSD, then confirm formatting.

Install the client application in each endpoint that you want to back from a download or from the supplied USB or CD.

BaQapp is accessed through the password using any browser, except Internet Explorer.

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.

Vaulted storage

Many users are not aware that an infected computer can spread the infection to other connected computers, mapped drives, network file shares or even cloud drives that appear as network drives, encrypting them too. Ransomware can even spread to an attached thumb drive or externally attached hard drives.

Ransomware can disable Windows volume shadow copies (VSS) or System Restore functions you might otherwise deploy.

BaQapp protects ransomware by vaulting the backup data from attack, and if a recent backup has been infected, it will not spread to the older incremental backups.

BaQapp has the ability to go back in time to totally recover multiple endpoints prior to the infection, a feature not previously available in multiple endpoint backup software at this price.

History

BaQapp Pty Ltd is a combination of talents.

Martin Raiber, security programmer in Germany who developed the software on which BaQapp is based, UrBackup. UrBackup has been translated into 13 languages and used in 1,000s of networks worldwide, including the US Government National Institute of Standards and Technology.

James Brough, Australian IT technician who has adapted and working with Martin made BaQapp easy to install and use.

Bernhard Kirschner, Australian innovator, who pioneered instant printing services, personal computer stores, on-site data archiving, CD duplication and other applications of disruptive technologies.

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

Request email on info@bagapp.com.au or available as soft copy with images on USB at CeBIT stand S30.