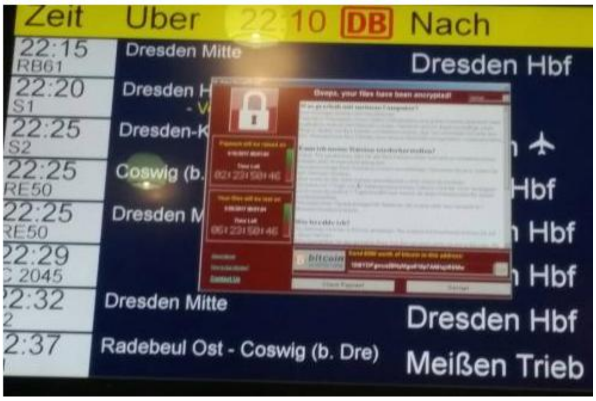
BaQapp

The safe backup solution

PRESS RELEASE **For immediate release**

15 May 2017



Why does Toyota recall 10 year old cars with faulty Takata airbags while Microsoft refused to fix a dangerous known file sharing vulnerability flaw in popular Windows XP Operating Systems and other unsupported versions of Windows?

Ransomware such as *WannaCry* only succeeds where there is ignorance, lethargy, incompetence and arrogance!

WannaCry is the ransomware that has used NSA 0-Day exploits to go on a rampage affecting organisations worldwide including about 40 NHS organizations across the UK. Non-emergency operations had to be suspended and ambulances diverted as a result of the attack.

You could blame:

(i) The NSAs having and then losing hacking software like ETERNALBLUE and DOUBLEPULSAR

(ii) Organisations like the Shadow Brokers which made this software public earlier this year

(iii) That so many computer systems were not updated when Microsoft issued the “MS17-010" security update on 14 March that closed this vulnerability for later operating systems. This is understandable when it comes to individual users, but there is no excuse for IT professionals.

(iv) Are Microsoft responsible through their arrogance in not normally fixing flaws in older versions of their Windows Operating System such as XP, where until yesterday there was no fix for this vulnerability. It is estimated that about 90 percent of care facilities in the U.K.’s **National Health Service** are still using Windows XP – an operating system that was still being sold by Microsoft in 2010 that functions perfectly well in many situations, but has had this defect from day one.
Imagine the outcry if Toyota refused to supply parts or accept responsibility for defects in older usable cars so that you are forced to scrap your car!

(v) Too many organisations staff are not educated to ‘Think Before They Click’ when they receive any out of the ordinary emails. The initial spread of WannaCry is coming through spam, with which fake invoices, job offers and other lures are being sent out to random email addresses. Within the emails is a .zip file, and once clicked that initiates the WannaCry infection. Although many of these dangerous emails look so convincing the even experts can be fooled.

(vi) Too many organisations there is limited virus protection software, and even when some of the best is used, even they claim only 99% protection, and with 100s of thousands variants that leaves a lot of openings.

(vii) Ignorance of users and unwillingness to learn about the computers that they depend on. Few users would even know how to switch on automatic updates, or how to update Windows. Many systems can be simply updated by pressing your start button, usually in the bottom left corner, typing in "Windows Update" and then following the instructions, or looking for help in your search engine

Just as there is no such thing as a thief proof safe and an unsinkable ship, there is no such thing as 100% malware protection.

That's why we have insurance. The insurance against ransomware is backup. However the backup must be vaulted, versioned and verified with fast and full recovery.

- **Vaulted** means your backups cannot be corrupted by ransomware because they are 'hardened' and stored safely.
- **Versioned** means that many periodic backups are stored, so it will be possible to find an older clean backup that can be used for recovery.
- **Verified** means that there is independent notification if backups have been missed, and reminds you to check restoration regularly.
- **Fast and full recovery** means that there should be a local backup of all systems, software and data that can be used to recreate damaged computer systems.

Additionally a backup system must be affordable, and that is why we have BaQapp.

For more information on ransomware and backup options see www.baqapp.com.au and contact Bernhard Kirschner on 0416 237667 or James Brough on 0438 237667.