BaQapp

The safe backup solution

PRESS RELEASE **For immediate release**

9 May 2016

```
!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
   http://en.wikipedia.org/wiki/RSA_(cryptosystem)
   http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decr
To receive your private key follow one of the links:
   1. http://twbers4hmi6dx65f.tor2web.org/66CCAB8A005BF0AF
   2. http://twbers4hmi6dx65f.onion.to/66CCAB8A005BF0AF
   3. http://twbers4hmi6dx65f.onion.cab/66CCAB8A005BF0AF

If all of this addresses are not available, follow these steps:
   1. Download and install Tor Browser: https://www.torproject.org/c
   2. After a successful installation, run the browser and wait for initi
   3. Type in the address bar: twbers4hmi6dx65f.onion/66CCAB8A00
   4. Follow the instructions on the site.

!!! Your personal identification ID:                 !!!
```

```
been encrypted. Your photos, videos,
not deleted them, yet.
150 USD in Bi_
```

```
PRESS ANY KEY!
```

```
WARNING!
Your personal files are encrypted!
11:58:26
Your documents, photos, databases and other important files have been encrypted
with strongest encryption and unique key, generated for this computer. Private
decryption key is stored on a secret Internet server and nobody can decrypt your
files until you pay and obtain the private key. The server will eliminate the key after a
time period specified in this window.
Open     http://maktubuyatq4rfyo.onion.link
      or http://maktubuyatq4rfyo.torstorm.org
      or http://maktubuyatq4rfyo.tor2web.org
```

Can ransomware kill?

1. **If ransomware infect were to medical equipment like a pacemaker that would be a killer app.**
2. **When terrorist form the "United Cyber Caliphate" we can expect them to use Ransomware to not only damage computer systems, but the funds used to finance the terror attack that kills you!**

   Five different pro-Daesh (a.k.a. ISIS/ISIL) groups get the most attention when the topic of ISIS and hacking enters the conversation. In the past, they've coordinated on a few campaigns, pooling talent and resources, but remained largely individual when it came to action. Earlier this month, that all changed, when they announced the formation of a "United Cyber Caliphate."

   See http://www.csoonline.com/article/3062706/techology-business/pro-daesh-hackers-more-bark-than-bite-lacking-in-skills-and-resources.html
3. **When ransomware attacks hospitals, as has happened in Melbourne and in the USA, it places patients in danger, threatening life and health. There are many other critical systems that can kill, such as an attack on our transport systems.**
4. **A ransomware attack without safe backup is going to cause a lot of stress, but in most cases will not kill.**

   David Lewis, neuropsychologist and director of Mind Labs International, said there was evidence people attempting to get meeting room technology to work experienced stress.

   That is why 90% actually prepared for technology failures by using print outs as alternatives to collaboration technology.

   Ever thought what stress would be caused by finding all your files encrypted, and imagine the stress if it was just before an important meeting?

Have you prepared for data loss with a safe backup?

A safe backup is one that is "hardened" against infection from malware by being isolated, insulated, and restricted, from your data and operating system.

That is a lot of damn good reasons to have safe backups and not be tempted to pay the ransom.

The California Senate Committee recently passed ransomware legislation, outlawing the act and making it the criminal equivalent of extortion. http://healthitsecurity.com/news/calif.-senate-committee-passess-ransomware-legislation.

Comments Bernhard Kirschner, director of BaQapp Pty Ltd, whose backup system creates vaulted backups that are protected from ransomware attack.

"Like outlawing drugs and terrorism made a difference. Reminds me of King Canute.
Perhaps they would have more success if they made safe backup compulsory so that there would be no need to pay any ransom. I wonder how long it will take before paying the ransom will be illegal so you have a choice to pay the ransom or commit a crime, making life even more difficult for us"

That Ransomware is a major problem cannot be disputed.

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

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 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).

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 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, reward criminals and possibly support terrorists, and then 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.