November 2013

blackfoot Newsflash

ADVISE >
ASSESS >
ASSURE >

Cryptolocker Malware

The National Crime Agency has recently issued a warning about an outbreak of the Cryptolocker ransomware.

Spam emails mainly purporting to be from financial institutions, Companies House or the Government Gateway (gateway.gov.uk) are in circulation. The emails have a file attached that when opened downloads the Cryptolocker ransomware. The malware will encrypt files on the infected machine along with any network shares visible to the user. A ransom demand is then shown which offers a decryption key in return for 2 bitcoins (an amount recently reported as being approx. £536) or 300 Euros.

Currently those susceptible to this malware are running Microsoft Windows OS versions 8, 7, Vista and XP.

Our advice is:

- Ensure email gateway filtering, anti-virus, IDS and IPS signatures are up to date
- Instruct employees not to open emails from unexpected sources (particularly financial services) and report suspicious emails to the helpdesk
- Ensure user created files are backed up routinely and preserved off the network
- Create a software restriction policy that prevents executables running from file paths that have been used by this malware
- Secure open-share drives by limiting write access to groups and users based on need
- Do not operate PCs with full admin rights on the default user account, instead enable UAC (User Access Control) so that actions requiring a higher privilege level (e.g. installation of software) automatically request a secondary user ID and password. For Windows XP where UAC is not supported, use the "runas" feature. (This advice applies to Administrative users as well as Business users)
- If you think you have been infected you should disconnect infected computers from the wired and wireless network to prevent further infection, and contact us.

More information is available on the **NCA website** but as always, if you are concerned you may have been infected please contact us by telephone on **0845 805 2409** or through Basecamp messaging if you are an existing supported customer.