December 2012

blackfoot Newsflash

ADVISE >

ASSESS >

ASSURE >

DEXTER MALWARE

DEXTER MALWARE

Blackfoot has been advised that a new piece of malware named Dexter has been discovered targeting Point of Sale systems, and is being reported in many IT news websites and blogs.

According to the reports the malware will sit on your till Operating System and send memory dumps of the card data from your POS solution. It is unlikely to be a coincidence it has been installed in the run up to what is the peak trading time for many of you, with the hackers wanting to gain the maximum amount of data in the shortest possible time. There has been no release of which POS solutions are vulnerable; only that the major systems in use across hotel, restaurant, retail and parking sectors have been affected.

At the time of writing this alert investigations have not found how the systems are compromised, but early research has shown that in over 50% of infected systems Windows XP was running, and over 30% of cases were running some variation of Windows Server (which include Windows Home Server, Server 2003, Server R2 or Server 2008). To a lesser extent (approx 10% total) Windows 2000, Vista and 7 have also been noted as in use. No information on whether any Internet Explorer versions are weaker than others is currently available.

Due to the severity of this piece of malware, Blackfoot strongly recommends that if you run a POS system on a Windows platform you check your tills for this vulnerability (19% of cases have been in the UK as of Tuesday 13th December). How you approach checking your stores should be determined by both your network configuration and security practices. The more controls you have in place then the less checking you will need to carry out. An example might be that those with flat retail networks will likely need to check around 1% of your stores, where as those that run segmented store networks may choose to investigate fewer than this.

We have come up with what we think is the simplest way for you to check if your system may have been infected, which is detailed below.

On a sample of machines, use the registry editor to examine the values of:

HKEY_LOCAL_MACHINE\Software\Microsoft\Window s\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\Run

If iexplore.exe (or dexter.exe) is listed, the machine may be infected and further investigation such as anti-virus scanning, checking whether iexplore.exe is running, examining outbound HTTP connections and event log analysis should be performed.

We can offer some support to our VCO clients and should you have any questions please either call us or email qsa@blackfootuk.com.

Should any Blackfoot client suspect that systems are infected after following the above process, please do not alter anything. Contact us for help in what action to take next.