DRAFT: June 3, 2010

A SIMPLE SOLUTION TO THE WEAKEST LINK IN THE DATA SECURITY CHAIN

by: Paul Comessotti

It's the nightmare of every executive...

An employee of fictional International Conglomerate Ltd – let's call her Ms Demeanor -- has taken work home.

She plugs her USB flash drive into her children's computer. Then she opens her work documents, using the pirated software the local computer store loaded onto her hard drive years ago. Those applications remain un-patched. Consequently her PC is a veritable Typhoid Mary of malicious software. Now her infected system is connected to the Internet, with her employer's documents open.

Up late, Ms Demeanor forgets to close her applications and log off before heading to bed. All night her PC is probed by individuals with nefarious purposes, attempting to remotely install malware.

After dropping her children off at daycare, Ms Demeanor stops at the Interweb Cafe. While standing in line she receives a sudden flash of inspiration regarding the project due that Friday.

She inserts her USB flash drive... opens documents... and logs onto her employer's VPN. The Cafe PC she selects has updated AV and AS software, and is fully patched. It also has hidden malware, for a purpose only the developer knows.

The PCs she uses have been compromised, yet the data belonging to International Conglomeration Ltd remains safely untouched. How?

Ms Demeanor's flash drive is an Abra -- a hardware-encrypted flash drive with its own operating system and security software.

Abra writes and instantly encrypts files and data using its own virtual file system and registry. It launches a secure conduit to applications installed on the host PC, allowing use of those applications without transferring data to or from the host.

Ms Demeanor's – or more accurately International Conglomerate Ltd's -- data remains safe in the separate, secure, Abra virtual PC running parallel to the host PC.

…/more

That's because prior to issuing her Abra, IT administrators at International Conglomerate Ltd configured permitted applications and actions and VPN connectivity that prevent Ms Demeanor from copying and printing files between Abra and any host PC.

Inserting Abra into the USB port of a PC opens a new Windows desktop with the user's shortcuts, bookmarks, and documents. No driver is required.

In any North American airport, Ms Demeanor is traveling without lugging or worrying about a company laptop. She smiles while walking past other road warriors unpacking and repacking their laptop cases. When arriving at her destination, she'll have everything she requires for her meetings on her Abra.

The surly inspectors are too busy peering into other travelers' laptop cases and directory files to notice the Abra discreetly attached to her keychain.

And if for some reason an airport inspector demands Ms Demeanor surrender her keychain for further investigation, the data is encrypted.

Her employer-issued Abra protects data via secure virtualization, secure connectivity, and is portable as well as plug-n-play.

Allowing users to forget how well you've secured your corporate data is easy when you've provided a secure, virtual, portable workplace.

-30-

(Paul Comessotti is Canadian Country Manager, Check Point Software Technologies, Inc.)