GarrettCom®

January 25, 2010

Dear GarrettCom Customers,

This letter is in response to frequent requests to clarify GarrettCom product compliance with CIP 007 R4 - Malicious Software Prevention requirement. The following statements apply to GarrettCom's Magnum 6K, DX, and DynaStar product families.

Because these GarrettCom switching, routing, and security products use specialized embedded operating systems, the implementation or integration of any third party anti-virus or anti-malware software is not feasible. However, due to the unique nature of these operating systems, and the absence of outward facing software application interfaces, there are no known hooks for viruses to use to invade the system. Further adding to the security of the system, the software for this system consists of a single executable file, compiled from proprietary source code.

As such, there is no known way to introduce a virus or other malware because this software does not call any routines outside of its pre-compiled software image. Therefore, any un-intended software that was somehow introduced into the memory or storage of this system would not run, as there is no means in the software to call external files. Further, introduction of a virus or malware into the single executable software image would require a complete re-compilation of the software, which requires access to the Magnum MNS6K, DX, or DynaStar source files which are proprietary to GarrettCom and otherwise unavailable.

I believe that this should address concerns regarding compliance to CIP 007 R4 – the Malicious Software Prevention requirement, as we are confident that the these products provide very safe and reliable solutions for NERC / CIP implementations.

Best Regards,

Lee House
CTO and VP Engineering
GarrettCom, Inc.
510-580-2953

GarrettCom,Inc.
47823 Westinghouse Drive
Fremont, CA 94539-7437
Tel 510.438.9071
Fax 510.438.9072
Email: mktg@garrettcom.com
www.GarrettCom.com