

6 August 2010

Reference: Customer Advisory - 08

Re: First Known Malware Targets Industrial Control Systems

To Our Customers:

While many vulnerabilities have previously been disclosed for ICS, this month the first known case of a vulnerability being adapted into malware (hostile code, such as a computer virus) has been revealed. The current malware is targeted at Siemens PCS7 and WinCC environment. The primary propagation happens through USB keys or Windows file sharing by taking advantage of a previously known LNK exploit. The international response is significant including Siemens, antivirus vendors, and multinational Cyber Emergency and Response Team (CERT) organizations. More information is available at the [ICS-CERT](#) home page. This is an excellent reminder to any asset owners to review their cyber security architecture and design, policies and procedures for USB devices, and to implement recommended antivirus and software patch updates. Guidance on implementing such practices can be found in standards such as ISA-99 and other industry recommended practices.

Keep Safe,

Bryan L Singer, CISM, CISSP, CAP
Principal Investigator

Disclaimer:

This customer advisory provides information of a general nature concerning some industry practices involving engineered safeguards. These should not be taken as typical, suggested, or recommended levels of protection. The application of engineered safeguards is highly dependent on process-specific and site-specific factors that have a great deal of influence on the actual degree of hazard control strategy. Neither Kenexis nor its corporate officers make any representations, warranties, or guarantees concerning the content of this document.