Industrial Control System Security Best Practices Inadequate in Blocking Advanced Malware Threats

New White Paper by three leading industrial security experts describes Stuxnet infection pathways and discusses how to protect SCADA systems

February 22, 2011 - British Columbia, Canada

Eric Byres, CTO of Byres Security Inc., Andrew Gintner, CTO of Abterra Technologies and Joel Langill, CSO of SCADAhacker.com announce today the release of their joint White Paper "How Stuxnet Spreads – A Study of Infection Paths in Best Practice Systems." It is the first paper to detail how Stuxnet could infect a control system site protected by a high security architecture using modern, vendor-recommended best practices. The paper shows that current best practices are insufficient to block advanced threats. It then discusses what operators of control and SCADA systems need to do to protect their critical systems from future threats of this type.

Stuxnet is the first known malware to have been designed specifically to compromise a control system and sabotage an industrial process. It has been described by Symantec's forensic experts as the "most sophisticated" piece of malware they have ever seen.

The paper follows the progress of the worm as it moves through a hypothetical control system, configured according to vendor-recommended security best practices. In spite of strong security measures, the worm is able to compromise a sequence of machines, culminating in the compromise of the PLC devices which directly control the physical process.

While Stuxnet is presumed to have targeted the Siemens WinCC and PCS7 systems used at Iran's uranium enrichment plants, its existence creates a new cyber security standard for all

byres security inc. intrinsically secure

ABTERRA TECHNOLOGIES

SCADAhacker.com

automation and critical infrastructure sites around the world.

Andrew Ginter remarked “The Stuxnet worm is the best-documented example of an advanced threat designed to sabotage an industrial control system. Other recent attacks have targeted control systems for industrial espionage. Control systems are now targets of advanced threats and today's best-practice defenses must be improved before they can stand against these kinds of adversaries.”

“By explaining how Stuxnet works, our paper helps security professionals understand what it takes to properly secure a state-of-the art industrial control system,” said Joel Langill. “The reality is that the majority of critical facilities are protected much less thoroughly than the hypothetical site described in our paper, and now they need to step up and protect against Stuxnet-like malware.”

“Our paper goes into great detail on Stuxnet infection pathways and highlights the difficulty of preventing infection from an advanced threat. While best practices for prevention should be implemented, control system operators should also put into practice early detection, mitigation, and containment strategies,” remarked Eric Byres. “Such strategies include putting into practice zone-based security as described in ANSI/ISA-99 Standards, paying particular attention on securing last line of defense critical systems, and understanding the unique security challenges of control systems versus IT systems.”

The paper concludes that changes to improve the cyber security of industrial control systems are urgently needed.

To download the White Paper, go to:

www.tofinosecurity.com/how-stuxnet-spreads

About Eric Byres and Byres Security Inc. (www.tofinosecurity.com)

Eric Byres (P. Eng., ISA Fellow) is recognized as one of the world's leading experts in the field of critical infrastructure security. He has been responsible for numerous standards and best practices for controls systems security and has received the rare honor of ISA Fellow by the International Society of Automation (ISA) for his outstanding achievements in science and engineering.

Byres Security Inc. provides practical and effective industrial network security and SCADA security products that are simple to implement and that do not require plant shutdowns. Its flagship product, the Tofino Industrial Security Solution, is a unique hardware and software security system that facilitates the implementation of Plug-n-Protect™ zones of security for equipment with common safety requirements. *Tofino* is used by the process control, SCADA, manufacturing and automation industries.

About Andrew Ginter and Abterra Technologies (www.abterra.ca)

Andrew Ginter (ISP, CISSP) draws on extensive experience developing industrial control system products at both Hewlett-Packard and Agilent Technologies. He was the architect of the security product line at Industrial Defender, and is a regular author on industrial cyber security.

Abterra Technologies is focused on securing industrial control systems. It provides research, consulting, and services for control system vendors, security technology vendors, and operators of industrial control systems.

About Joel Langill and SCADAhacker.com (www.scadahacker.com)

Joel Langill (SCADAhacker) developed his expertise through more than 25 years of in-depth involvement with industrial control systems in the areas of architecture design, implementation, and upgrades. His unique approach emphasizes that the best strategy for comprehensive security balances People, Processes and Products (technology). His work has been recognized in industrial automation and industrial security publications, he serves as an officer for Cyber Security Forum Initiative (CSFI.us) Department of Critical Infrastructure and he is a SCADA security instructor with InfoSec Institute.

For further information please contact:

Eric Byres	Andrew Ginter	Joel Langill
CTO	CTO	CSO
Byres Security Inc.	**Abterra Technologies**	**SCADAhacker.com**
eric@byressecurity.com	aginter@abterra.ca	joel@scadahacker.com
+1 250 390 1333	+1 403 875 2416	+1 623 476 9667
www.tofinosecurity.com	www.abterra.ca	www.scadahacker.com

~ ENDS ~