

*newsletter*

# Stuxnet & Co

## IT-specific risks to industrial process control systems

**Malware used to surface mainly in personal computers, office applications and on the internet, to steal access data (such as user names and passwords), for example. 2010 ushered in a new generation of malware in the guise of Stuxnet, a trojan specifically designed to attack industrial process control systems. Information technology (IT) experts recently discovered yet another malware, Duqu, whose intended purpose was to spy on companies involved in designing industrial installations. These examples illustrate how malware-based attacks on process control systems are fast emerging as a potential hazard that will need to be taken into account in managing and assessing IT risks going forward.**

### **Automation and process control systems**

IT systems used in controlling, monitoring and testing industrial installations are referred to collectively as distributed control systems (DCS) or supervisory control and data acquisition (SCADA) systems. A defining feature of such systems is their modular design consisting of separate components. Examples include programmable logic controllers (PLC) as used in electronically controlling machinery or defined process elements. SCADA systems are used in virtually every type of process infrastructure that controls physical processes – from systems control in refineries to power generation and distribution to traffic control systems and industrial-style goods manufacturing.

### **Increasingly standardised and networked**

In recent years, state-of-the-art IT has been making deeper and deeper inroads into the realm of conventional process control and automation technology. Industrial control systems used to run on IT systems that communicated with each other using separate, mutually incompatible protocols and technology and were based on proprietary software solutions. In the past, this meant keeping these systems autonomous and separate from conventional data-processing and office-communication IT.

Ethernet and TCP/IP networking technology along with standard software applications, having been ubiquitous elsewhere, are gradually pervading these environments as well. The spectrum here ranges from the use of standard software, such as databases, to standard hardware equipped with Windows or Unix-based operating systems. This convergence is delivering more and more synergistic potential and opportunities for standardisation, along with greater flexibility and improved data exchange. In this context it is the ability to analyse and visualise process data for centralised management, and the cost efficiencies to be achieved in developing and procuring the systems, that are seen to be the key benefits.

Generally, safety and security are far advanced in many areas of the industrial process environment but tend to focus on issues such as reliability, explosion prevention, workplace safety or electrical safety.

Until recently, far less concern was paid in the same environment to data security risks, such as computer viruses, denial of service (DOS) or hacker attacks, which have long been a routine part of life with the conventional IT used in conventional data processing and office communication.

## **Stuxnet**

Stuxnet is the name of a malware discovered in the summer of 2010. It made waves among the general public as well as professionals because its complexity and its target signalled a paradigm shift in malware. Stuxnet was specifically programmed to sabotage industrial installations. Its code was designed to reprogram a certain system made by Siemens and used for controlling and monitoring industrial processes. Stuxnet mainly targeted the control software Windows Control Centre (WinCC) and the process control system SIMATIC PCS 7. Stuxnet's infection process exploits multiple Windows flaws simultaneously that are unknown to the developer at the time of the attack (zero-day exploits) and uses stolen certificates of reputable hardware manufacturers.

In a first step, the malware is spread via removable drives such as USB flash drives. Once inside the target system, Stuxnet attempts to mask itself in the system and may then spread in various ways via networks. Stuxnet is able to reprogram code in the control systems infected, to enable third parties to gain control of systems unnoticed by the operators.

The software infected industrial installations all over the world, although most cases were reported from India, Indonesia and Iran. Iran's nuclear facilities were perceived to be the primary target of the Stuxnet attacks. Stuxnet was speculated to have infected specific computers in Iran's nuclear reprocessing facilities and, via control systems, to have sabotaged the centrifuges used in enriching uranium, ultimately subverting the enrichment process altogether. Security experts acknowledge Stuxnet's unprecedented technological sophistication and high degree of complexity. Developing the software will have required vast amounts of specific expertise and human and financial resources on a matching scale.

## Duqu

In October 2011 a type of malware was detected which specifically targets firms involved in designing industrial installations. This new breed of malicious code is known as Duqu, a trojan that seeks to capture data specifically from makers of industrial control systems and to relay those data to Duqu's authors.

Because Duqu is thought to be at least partly derived from Stuxnet's software code, experts dubbed it Stuxnet's "little brother". It is suspected that the information captured by Duqu can be used to stage future attacks on industrial installations.

## Information for Underwriting

The Stuxnet attack highlighted the very real possibility today, and increasing likelihood going forward, of attempts to attack critical infrastructure and associated industrial process control systems. Duqu shows, among other things, that Stuxnet-specific know-how such as its source code has already spread further among the hacker community. At their current protection levels, industrial installations are more likely to experience a successful attack in the future.

The Duqu attack drew a global spotlight on a little-noticed weak spot – IT security in industrial process control systems and in IT systems connected to them. The existing security concepts underpinning industrial process control systems should be scrutinised, adapted and updated where necessary to effectively address these new threats. Industrial process control systems will continue to grow ever more dependent on standardised and networked IT.

By tampering with processes and equipment, cyber attacks on industrial process control systems may cause fires and explosions, among other events, and business interruption as a consequence thereof. From an insurance perspective, most attacks of this kind tend to fall under property, machinery breakdown and business interruption (BI/CBI) cover, and from a casualty point of view, under commercial and environmental liability cover, and may trigger loss events insured under the relevant terms.

Given the pervasive and networked use of industrial process control systems, there is also significant potential for accumulated losses.

## Contact

AssTech GmbH  
P.O. Box 1211  
85766 Unterföhring bei München  
Tel. + 49 89 3844 1585  
Fax + 49 89 3844 1586  
info@asstech.com  
[www.asstech.com](http://www.asstech.com)