



## Post-Stuxnet Industrial Security: Zero-Day Discovery and Risk Containment of Industrial Malware

**A White Paper presented by:**

Torsten Rössel  
Director of Business Development  
Innominate Security Technologies AG  
Berlin, Germany

**U.S. Contact:**

Phoenix Contact USA  
P.O. Box 4100  
Harrisburg, PA 17111-0100  
Phone: 717-944-1300  
Fax: 717-944-1625  
Website: [www.phoenixcontact.com](http://www.phoenixcontact.com)



## Post-Stuxnet Industrial Security: Zero-Day Discovery and Risk Containment of Industrial Malware

### Key concepts:

- Although the Stuxnet worm has received a great deal of media attention, the greater threat to most control systems is that copycats could use Stuxnet as a blueprint for future attacks.
- An ideal network security appliance with both preventive and diagnostic functions can boost security against Stuxnet-like attacks and reduce their associated risks.
- While such a device will not completely prevent malware infections, fast and reliable discovery of such infections is a key aspect of protection.

### Introduction

Following its discovery in June 2010, the Stuxnet worm caused a worldwide sensation. It is the first publicly known rootkit attack targeted at industrial plants. It has infected tens of thousands of PCs, and abused and manipulated automation software running on Windows® operating systems. Its ultimate purpose: to infiltrate malicious code into the controllers of specific real-world industrial installations.

Experts have long warned that malware and insufficient IT security pose a threat to automation networks, but Stuxnet offers concrete proof that these threats can no longer be ignored. The actual hazard, however, no longer originates from Stuxnet itself, but rather comes from mutations that copycats can now create with the same basic techniques. And while Stuxnet focused on products from the Siemens SIMATIC family and on STEP 7 PLC projects with very specific properties, such mutations could affect components from other vendors as well, ultimately turning out malware a lot less selective in its damaging impact.

Apart from the fact that industrial PCs are often not (and cannot be) equipped with antivirus software, Stuxnet has also made clear that conventional virus scanners do not provide protection against this caliber of attacks. The analysis of Stuxnet has shown that the worm had been around in the wild unnoticed for at least 12 months before its discovery. Because Stuxnet did not use any of the known malware signatures, existing antivirus programs did not detect it during that time.

### Damaging Impact in Four Steps

To plan protective measures against future Stuxnet-like attacks, a basic understanding of the worm's activities is essential. It unfolds its damaging impact in four steps on different layers.

**1. Infection of Windows PCs:** The worm uses an aggressive mix of mechanisms to spread onto and contaminate both networked and non-networked Windows PCs via USB flash drives. To do this, it utilizes four previously unknown vulnerabilities (by so-called zero-day exploits). These weaknesses have existed in several generations of Windows operating systems. To date, security patches have only partially fixed them. Besides a number of encrypted files which the worm stores in the %SystemRoot%\inf\ directory, Stuxnet installs two device drivers: %SystemRoot%\system32\drivers\MrxNet.sys and %SystemRoot%\system32\drivers\MrxCLS.sys.

These drivers have been signed with private digital keys stolen from Realtek and JMicron. Therefore, they contain certificates rated as trustworthy by Windows operating systems.

**2. Abuse and Manipulation of Automation Software:** If Stuxnet comes across installations of WinCC visualization and/or STEP 7 engineering components on an infected PC, it abuses and manipulates any found

WinCC databases and STEP 7 projects. This will further proliferation and persistency on the PC and help it to locate the controllers referenced in those projects as potential targets for step 3.

Furthermore, Stuxnet renames the dynamic link library `s7otbxdx.dll` in `%SystemRoot%\system32\`, the directory responsible for the communication between the SIMATIC Manager and the S7 controllers, to `s7otbxdsx.dll`, and replaces it with a wrapper DLL of its own under the name of `s7otbxdx.dll` in the same directory.

**3. Injection of Malicious Code into Controllers:** This manipulated wrapper DLL enables Stuxnet to infiltrate arbitrary malicious code into the compromised PLCs, hide those malicious code changes from the programming engineer, and safeguard them from later overwriting. Stuxnet injects this precise malicious code selectively, only into controllers and projects with very specific properties, which is a remarkably sophisticated capability. According to the latest expert findings, the worm is supposed to permanently manipulate frequency converters and turbine controls as inconspicuously as possible. The goal is to disrupt the controlled processes and ultimately destroy the affected equipment.

The malicious code, targeted at the S7-417 series of controllers, combines denial-of-control and denial-of-view techniques into a so-called man-in-the-middle attack in ways hardly considered feasible up to now. Under the attack, the legitimate PLC program completely loses control of the process without the PLC or the operating staff in front of their HMIs in the control room even noticing. The attack vector as such is generic. It could be packaged into and provided by exploit tools such as Metasploit, and then—contrary to common belief—even persons without comprehensive insider knowledge could use the information for attacks.

**4. Communication with Control & Command Servers on the Internet:** From infected PCs, the worm attempts to contact several command and control servers on the Internet. Once it establishes a connection, information collected from the target and its environment can be uploaded to those servers. In addition, the worm can receive updates and execute its malicious payload. This adds an extra portion of dynamics to the worm's potential for espionage and sabotage. Combined with the worm's capabilities to spread and update itself via peer-to-peer connections and USB flash disks, all of this can have collateral effects even on systems without a network connection, let alone Internet access.

### Early Discovery Mitigates Risks

An ideal network security appliance should comprise a set of preventive and diagnostic functions which can boost security against Stuxnet-like attacks and reduce their associated risks. While such a device may not actively prevent 100 percent of infections with malware due to the diversity of proliferation paths, fast and reliable discovery of such infections is a particularly important aspect of protection. Quick detection will keep the worm from slipping through unnoticed and affecting plants for a long period, as Stuxnet did.

### Discover Malware on Day Zero: Integrity Monitoring

Due to the general problems with the deployment of antivirus software on industrial PCs and the timely provision of malware signatures, alternative techniques of integrity assurance are gaining relevance for the protection of industrial systems.

One solution is the CIFS Integrity Monitoring feature offered on Phoenix Contact's FL mGuard security devices. CIFS, or Common Internet File System, is a file-sharing protocol used by Windows and other operating systems. Viewing files on network file servers and using shared network drives are common activities that utilize CIFS. With Integrity Monitoring, the user can monitor configurable sets of files for unexpected modifications of executable code. When initialized, Integrity Monitoring computes a baseline of signatures for all monitored objects and then periodically checks them for any deviations. This process works without any external supply of virus signatures, without the risk of disrupting operations through "false positives," without installation of software, and with only a

moderate load on the monitored PCs, while primarily utilizing the resources of an mGuard security appliance. The mGuard thus discovers suspect file modifications promptly, and reports them via SNMP and e-mail to network management systems or responsible administrators.

In a test study performed at the University of Ostwestfalen-Lippe in Lemgo, Germany, researchers from the independent inIT institute for industrial IT ([www.hs-owl.de/init/en/](http://www.hs-owl.de/init/en/)) have been able to verify that **mGuard CIFS Integrity Monitoring** would have **recognized infections with Stuxnet on day zero as unexpected manipulations** and warned asset operators against it long before any antivirus product. The device drivers installed by Stuxnet, as well as the modifications performed by the worm on the pivotal SIMATIC Manager DLL, would have been discovered in the process.

### **Contain Proliferation, Prevent C&C Contacts: Firewall**

When spreading across networks and respective vulnerabilities in operating systems, malware often takes advantage of network connections that are not necessary for the productive operation of a plant. By installing a firewall on industrial PCs and controllers, or groups of such devices (“security segments”), the plant can reliably block these unnecessary and unsolicited connections and contain the proliferation of malware to a large extent.

Many plant managers however, install firewall protection only on incoming connections and neglect outgoing connections. Stuxnet demonstrates that both incoming and outgoing connections can potentially spread infection among healthy systems. Therefore, firewalls not only must protect incoming connections, but should also filter the often-neglected outgoing connections as much as possible. This will prevent contacts via outgoing connections to command and control servers on the Internet, reducing the associated potential for espionage and dynamic or evolving threats.

### **Authenticated and Authorized PLC Programming: User Firewall**

Most PLCs on the market today barely offer authentication and authorization functions to protect the process of their own programming. Contrary to popular beliefs, programming and other manipulations of such controllers do not require a specific or officially vendor-authorized engineering software package. Whoever has network access to the programming port and adheres to the correct protocol will be in the driver’s seat and rule the PLC. Protective measures are typically limited to an access control list (ACL), which restricts programming access to a number of IP addresses. So long as users and programs access the PLC from one of the assigned IP addresses, there is often no further checking or authorization.

Insidiously, Stuxnet uses those exact programming and visualization PCs for its attack on the PLCs. The malware’s access to the controllers originates from allegedly authorized nodes. This makes both the ACLs and any static firewall rules useless here.

A user firewall can prevent manipulation of controllers by unauthorized programming access. When in place, the user firewall requires an authorized user to unlock the programming port through an authentication process. The malware cannot provide this authentication on its own. After a specified time, reauthentication can be required, preventing an “always open” door to the PLC.

### **Conclusion**

Bearing in mind the manipulations performed by Stuxnet on the engineering software, it becomes apparent just how important it is to combine the techniques described above. Authorized users should, of course, unlock access through the user firewall only after having assured themselves of the programming environment’s integrity. In turn,

the mGuard Integrity Monitoring supports this action because it can detect whether or not the programming PC has been compromised.

More advanced security technologies, such as application whitelisting or intrusion prevention, will be restricted to future generations of automation equipment. But all of the methods presented in this paper lend themselves perfectly for retrofitting into existing installations and providing protection now rather than later.

Author: Torsten Roessel  
Director, Business Development  
Innominate Security Technologies AG  
Berlin, Germany ([www.innominate.com](http://www.innominate.com))  
December 2010

### **About Phoenix Contact**

Phoenix Contact develops and manufactures industrial electrical and electronic technology products that power, protect, connect and automate systems and equipment for a wide range of industries. Phoenix Contact GmbH & Co. KG, Blomberg, Germany, operates 47 international subsidiaries, including Phoenix Contact USA in Middletown, Pa. Phoenix Contact's formal Integrated Management System is registered to ISO quality, environmental and safety standards (ISO 9001:2008, 14001:2004 and OHSAS 18001:2007).

### **References**

Symantec W32.Stuxnet Dossier, Version 1.3 (November 2010), available for download at <http://www.symantec.com/business/theme.jsp?themeid=stuxnet>

Langner Communications GmbH, Hamburg, Blog on Stuxnet available at [http://www.langner.com/english/?page\\_id=45](http://www.langner.com/english/?page_id=45)