



**HIRSCHMANN**

A **BELDEN** BRAND

# Technical Bulletin

**TB 1002HE**

## Hirschmann™ EAGLE Tofino™

Using EAGLE Tofino™ to Control the Spread of Stuxnet Malware



**This Technical Bulletin describes how to use the EAGLE Tofino Industrial Security Solution to prevent the spread of the Stuxnet worm in both Siemens and non-Siemens network environments.**

### What is Stuxnet?

Stuxnet is a computer worm designed to target one or more industrial systems that use Siemens PLCs. The objective of this malware appears to be to destroy specific industrial processes.

Stuxnet will infect Windows-based computers on any control or SCADA system, regardless of whether or not it is a Siemens system. The worm will not attempt to make modifications to controllers that are not S7-300 or S7-400 PLCs. However, it is highly aggressive on all networks and can negatively affect any control system. Infected computers may also be used as a launch point for future attacks.

Within these pathways, it takes advantage of seven independent mechanisms to spread to other computers. Stuxnet also has a P2P (peer-to-peer) networking system that automatically updates all installations of the Stuxnet worm in the wild, even if they cannot connect back to the Internet. Finally, it has an Internet-based command and control mechanism that is currently disabled, but could be reactivated in the future.

### How Stuxnet Spreads

Stuxnet is one of the most complex and carefully engineered worms ever seen. It takes advantage of at least four zero-day vulnerabilities, has multiple propagation processes and shows considerable sophistication in its exploitation of Siemens control systems.

A key challenge in preventing Stuxnet infections is due to the large variety of techniques it uses for infecting other computers. It has three primary pathways for spreading to new victims:

1. via infected removable USB drives;
2. via Local Area Network communications
3. via infected Siemens project files

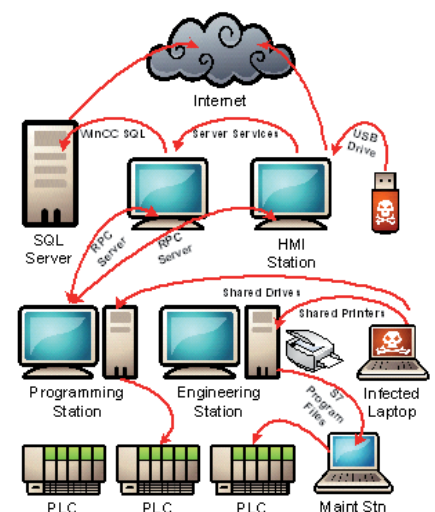


Figure 1: Multiple Pathways for Stuxnet Infection



Many people mistakenly believe that by preventing USB drive infections, the risk from Stuxnet is zero. Unfortunately this is not true. The diversity of attacks complicates any attempt to control the spread of Stuxnet and requires a multi-tiered approach if security is to be effective.

Any security design must include mitigations for all Stuxnet pathways, including USB, network and project file driven infections. This application note focuses on preventing network-driven infections, but also provides brief guidance and suggested reading for the other pathways.

### Preventing USB-Driven Infections

Stuxnet infects computers via USB drives (even when AutoRun is disabled) using a previously unknown Windows shortcut (i.e. \*.lnk file) vulnerability. Most analysts assume this is the starting point for new infections, although other mechanisms such as infected laptops, are a strong possibility. For information on mitigating the USB infection pathway, see the White Paper "Analysis of the Siemens WinCC / PCS7 "Stuxnet" Malware for Industrial Control System Professionals" at <http://www.tofinosecurity.com>.

### Preventing Network-Driven Infections

Numerous Stuxnet analysts have commented on how difficult it is to remove the worm from an infected control system. Once it has a foothold, Stuxnet aggressively spreads over local area networks to other computers. Security experts generally agree that the most effective way to prevent the rapid spreading is to make use of zone-based defences as described in the ANSI/ISA99.02.01 and IEC63443 standards. The idea is to break up the network into security zones. Between the zones, industrial firewalls are installed with rules that block the protocols Stuxnet uses for infection and communications. This way, if a Stuxnet infection does accidentally occur, it is limited to a small number of machines in a single zone.

### Dividing the Control Network into Security Zones

The first step in Stuxnet prevention is to divide the control system into zones. A zone is simply a grouping of assets that share common security requirements based on factors such as control function, operational requirements and criticality.

The simplest solution is to create the following zones based on the ISA-95/Purdue model:

1. Safety Integrated System (SIS) zone,
2. Basic Control/PLC zone,
3. Supervisory/HMI zone,
4. Process Information/Data Historian zone;
5. IT Network zone.

Security breaches in each of these systems would have different consequences, so it makes sense to handle each individually. For additional security and reliability, each of these primary zones can be divided further into sub-zones, based on operational function. Increasing the number of zones progressively restricts the spread of Stuxnet to fewer computers, reducing both risk and cleanup costs if an infection were to occur.

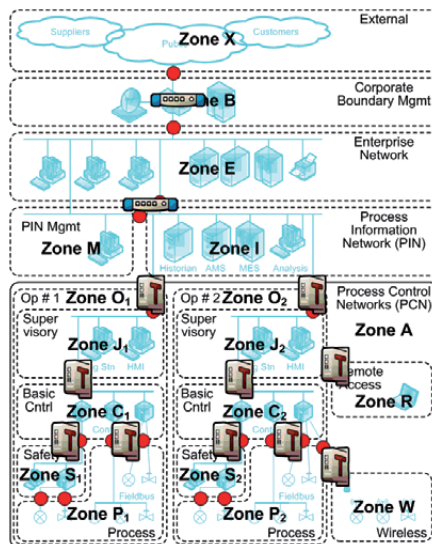


Figure 2: Installing EAGLE 20 Tofino Appliances between Operational Zones

### Installing EAGLE20 Tofino Security Appliances

Once the zones are defined, EAGLE20 Tofino Security Appliances are installed between zones to limit network traffic to only what is needed for the system to operate. Figure 2 shows a typical deployment in a petroleum refinery.

### Blocking Protocols Used by Stuxnet

With the EAGLE20 Tofino Appliances in place between zones, they need to be loaded with the appropriate Loadable Security Modules (LSMs). For Stuxnet control, the following are recommended:

1. EAGLE Tofino Firewall LSM
2. EAGLE Tofino Secure Asset Management LSM
3. EAGLE Tofino OPC Enforcer LSM
4. EAGLE Tofino Event Logger LSM

With the LSMs loaded, each appliance is configured to prevent the protocols that Stuxnet uses from passing between zones. In particular three protocols need to be managed – Web (HTTP) traffic, Remote Procedure Call (RPC) traffic and, in Siemens systems, MSSQL traffic.

### Blocking Outbound HTTP Traffic

The simplest traffic flows to deal with are the HTTP messages that Stuxnet uses to connect back to its command center on the Internet. The EAGLE20 Tofino Firewall is designed to block all protocols by default, so unless HTTP is specifically needed in the control system, it should be blocked between zones. If it is required (for example to allow IT access to a data historian) it should be restricted to only the web server in question and only for inbound access. Figure 3 shows the typical rules to allow a range of IT clients access to the Data Historian using Web traffic. Note the Direction is set to "Incoming".

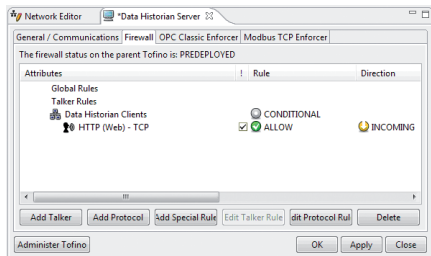


Figure 3: Restricting HTTP Web Client Messages to the Data Historian Server

### Blocking RPC Traffic

Stuxnet makes extensive use of RPC, so controlling this protocol is essential. As noted earlier, the EAGLE20 Tofino Firewall blocks protocols by default, so if RPC is not required, the EAGLE20 Tofino can be used with its default settings to prevent Stuxnet RPC traffic between zones.

Unfortunately, it is rarely this simple. RPC is the same protocol that is used for Windows file and printer sharing, Microsoft Event Log, OPC Classic and a number of other critical services. Thus blocking all RPC traffic may have negative consequences for the industrial process.

To have the least impact on the control system, a mixture of allowed and blocked RPC ports is recommended. All the standard RPC protocol variations are included in the EAGLE20 Tofino protocol set and can simply be dragged and dropped as needed. First, to prevent Stuxnet from using the network to spread, the NetBIOS Session Service and Server Message Block protocols (TCP ports 139 and 445) should be either completely blocked or only allowed for very specific servers. This will also prevent file and print sharing between zones, so these rules should be added with care.

Where NetBIOS Session Service and Server Message Block protocols must be allowed, specific rules can be set up to restrict the traffic to the appropriate servers. For example, the Event Log service manages messages that are generated by both programs and the Windows operating system. This service uses the same protocols as Stuxnet, so blocking it completely may not be acceptable. The

solution is to restrict these protocols to a designated Event Log Server, using rules similar to those shown in Figure 4. In this case, a Global Rule allows RPC to the Event Log Server. All other RPC messages are blocked by default.

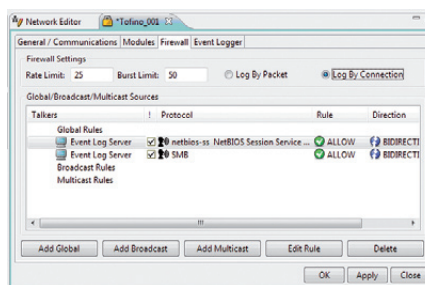


Figure 4: Restricting SMB and NetBIOS Session Service Messages to Event Logging Server

Similar rules may also be needed for Print Servers and File Servers. The goal is not to allow uncontrolled RPC traffic to all computers, but rather restrict it to specific servers that are carefully patched and monitored for infection.

The NetBIOS Name Service (UDP port 137) and the NetBIOS Datagram Service (UDP port 138) can be permitted if required, since Stuxnet does not appear to use these services. This will allow browsing of computers by name, but will not allow file sharing.

If OPC Classic traffic is present, then the EAGLE Tofino OPC Enforcer™ module must be used to manage the traffic. OPC Classic's core technologies, namely RPC and DCOM, were designed before security was widely understood. As a result, OPC Classic uses a technology called dynamic port allocation impossible to secure using conventional IT-style firewalls.

The reason is that unlike most other network applications (such as a web server or Modbus TCP slave), OPC servers dynamically assign TCP port numbers to each executable process serving objects to clients. The OPC clients then discover the port numbers associated with a particular object by connecting to the server and asking what TCP port they should use. Because OPC servers are free to use any number between 1024 and 65535, OPC

becomes very „firewall unfriendly“ - configuring the firewall to leave such a wide range of ports open presents a serious security hole and is generally considered unacceptable practice.

The EAGLE Tofino OPC Enforcer module solves this issue by automatically tracking and managing OPC Classic's dynamic port problem using a technique called Deep Packet Inspection. The firewall can be installed into any network carrying OPC DA, HDA or A&E traffic, and requires no changes to the existing OPC clients and servers.

To configure the EAGLE Tofino OPC Enforcer to allow traffic between an OPC Server and Client, open the Firewall tab for the appropriate OPC server. Then drag and drop the OPC client's icon onto the Server Talkers list, select the protocol "OPC Classic" and change the Rule from "Allow" to "Enforcer". Figure 5 shows these settings. Additional details can be found in Application Note AN-105 "Protecting OPC Systems Using the Tofino OPC Enforcer".

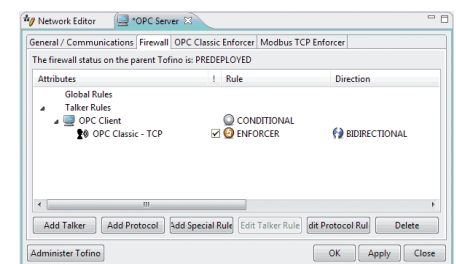


Figure 5: Using the OPC Enforcer to Manage OPC Traffic between a Client and Server

### Blocking MSSQL Traffic

For users of Siemens WinCC products, Stuxnet can infect computers by using Siemens "internal" system passwords to log into the WinCC SQL server. It then transfers a copy of itself to the server and executes it locally. The ideal solution would be to block all MSSQL traffic on the network. However, this is not recommended, as it will also prevent WinCC clients from receiving process information. Instead, users of WinCC are directed to install the latest SIMATIC Security Update from the Siemens website.



**WARNING:** Before deploying any mitigation to a live control system, confirm the mitigation with the system vendor and test on a non-critical system.

### Detecting Stuxnet Infections

Once the EAGLE 20 Tofino Appliances are in place, configured and tested, they provide excellent "watchdogs" to warn if an infection is occurring. Specifically, Stuxnet generates a significant amount of event traffic that can be captured using either the EAGLE Tofino CMP or EAGLE Tofino Event Logger LSM. The attempts of Stuxnet to contact external web servers are particularly good markers.

### Additional Guidance for Siemens WinCC and PCS7 Users

Siemens WinCC and PCS7 products make heavy use of RPC for communications between various WinCC servers and clients. Thus blocking all RPC communications between zones may cause loss of view or control. The EAGLE Tofino Test mode can be used to determine the rules needed to allow Siemens RPC traffic.

Users of Siemens products should contact their Siemens representative or review the Siemens document "Security concept PCS 7 and WinCC" before deploying firewall rules.

### Additional Information

The following provide information on other mitigation methods effective in controlling Stuxnet:

Stuxnet Mitigation Matrix:

<http://www.tofinosecurity.com/professional/stuxnet-mitigation-matrix>

Analysis of the Siemens WinCC / PCS7 "Stuxnet" Malware for Control System

Professionals: <http://www.tofinosecurity.com/professional/siemens-pcs7-wincc-malware>

Siemens Malware Information:

<http://support.automation.siemens.com/WW/view/en/43876783>

### Summary

Stuxnet is a complex and aggressive computer worm that can infect computers in any control system. While it is critical for Siemens product users to avoid infection, it can negatively impact other products and systems as well. Preventing the spread of Stuxnet over control networks is key to maintaining safe, reliable and secure industrial systems. The EAGLE Tofino Security Solution can mitigate the effects of the Stuxnet virus, while protecting your industrial network against numerous other methods of accidental or malicious attack.