Application Note

Using Tofino™ to control the spread of Stuxnet Malware

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

Background

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 only attempts to make modifications to controllers that are model S7-300 or S7-400 PLCs. However, it is aggressive on all networks and can negatively affect any control system. Infected computers may also be used as a launch point for future attacks.

How Stuxnet Spreads

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

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

- via infected removable USB drives;
- via Local Area Network communications
- via infected Siemens project files

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.

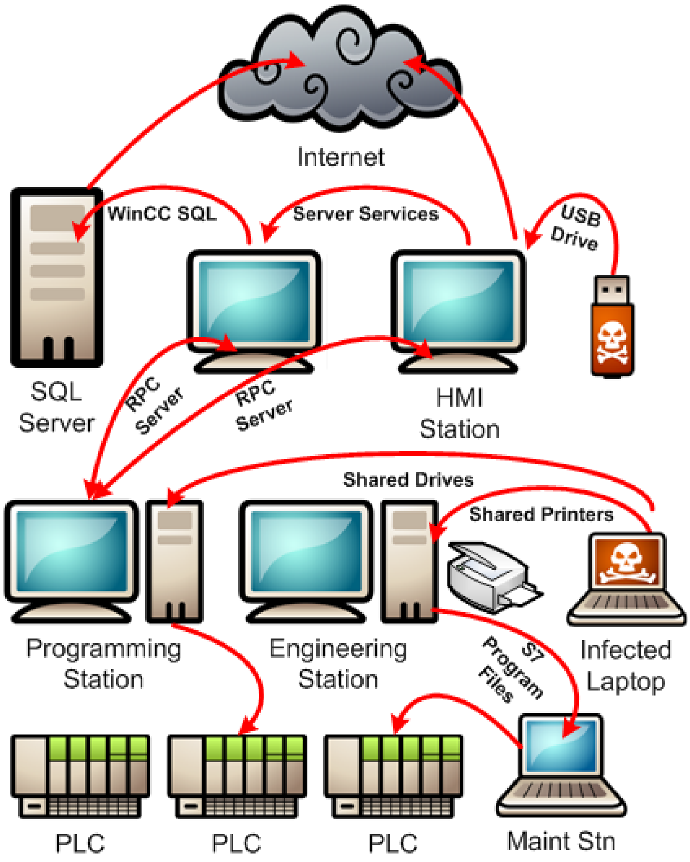


Figure 1: Multiple Pathways for Stuxnet Infection

Finally, it has an Internet-based command and control mechanism that is currently disabled, but could be reactivated in the future.

Many people mistakenly believe that by preventing USB drive infections, the risk from Stuxnet is zero. Unfortunately this is not true. The diversity of attack methods complicates any attempt to control the spread of Stuxnet and requires a “Defense-in-Depth” 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 guidance and suggested reading for dealing with the other pathways.

Preventing USB-Driven Infections

Stuxnet infects computers via USB drives (even when AutoRun is disabled) via 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 Byres Application Note AN-118 "*Stuxnet Mitigation Matrix*".

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 defenses as described in the ANSI/ISA-99.02.01 and IEC-62443 standards. The concept is to break up the network into security zones. Between the zones, industrial firewalls are installed with rules that block the protocols that 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:

- Safety Integrated System (SIS) zone,
- Basic Control/PLC zone,
- Supervisory/HMI zone,
- Process Information/Data Historian zone,
- IT Network zone.

Security breaches in each of these systems would result in different consequences, so it makes sense to handle each individually. For additional security and reliability, each of these primary zones can be further divided 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 clean-up costs if an infection were to occur.

Installing Tofino Security Appliances

Once zones are defined, the Tofino Industrial Security Solution is used to limit network traffic between zones to only what is needed for the system to operate (for an overview of Tofino, see the box on the last page of this application note). Figure 2 shows a typical example of Tofino Security Appliances (Tofino SAs) being deployed in a petroleum refinery.

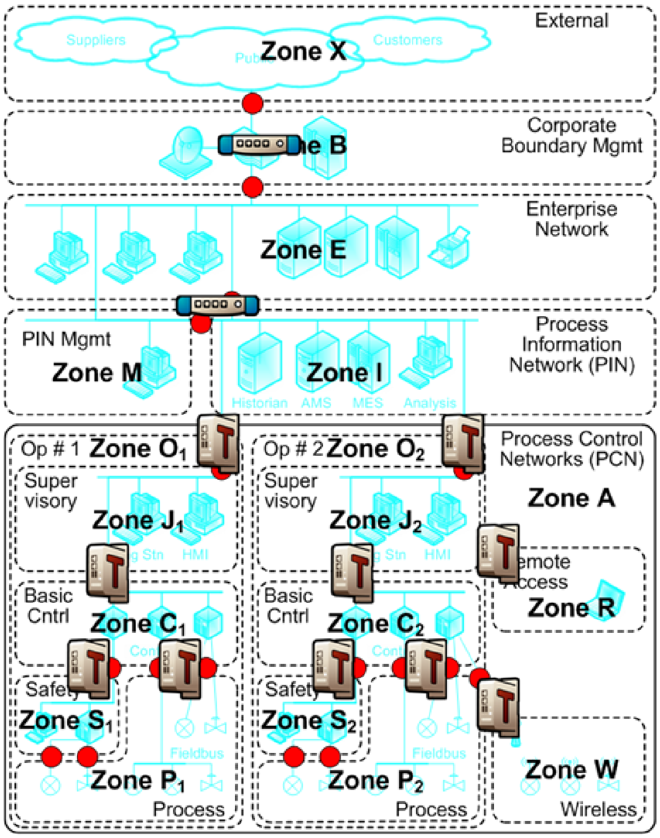


Figure 2: Installing Tofino Security Appliances between Operational Zones

Each of the Tofino SAs are customized as needed with software modules, known as Loadable Security Modules (LSMs), and configured by a central server, known as the Central Management Platform (CMP). For Stuxnet control, the following LSMs are recommended:

- Tofino Firewall LSM
- Tofino Secure Asset Management LSM
- Tofino OPC Enforcer LSM
- Tofino Event Logger LSM

Blocking Protocols Used by Stuxnet

Once the LSMs are 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. These are summarized in the table below and discussed in detail in the sections that follow.

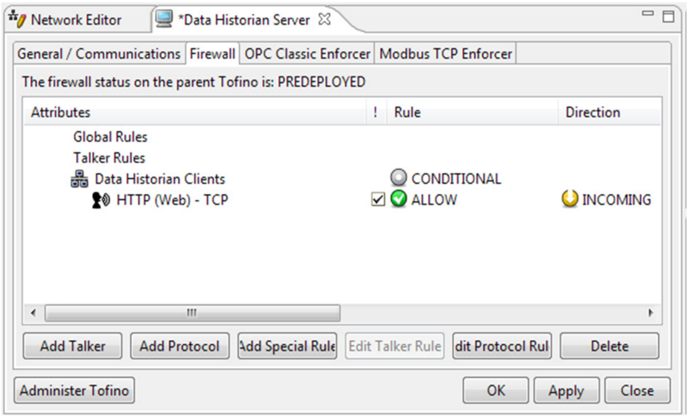
Protocol	Port No.	Common Application in SCADA/ICS	Used by Stuxnet for
HTTP (Web)	TCP 80	HMI web clients Historian web clients	Connection to Internet Control
RPC - DCOM	TCP 135 Random TCP ports *between 1024 - 65535*	OPC Classic, Certificate Services, Group Policy	Worm P2P Upgrade System
RPC - SMB	TCP 139 TCP 445 UDP 139 UDP 445	File and Print Sharing, Event Log, Netlogon, WinCC Web Nav	Open Shares File Share Exploit Print Spooler Exploit
MSSQL	TCP 1443	WinCC Client-Server Interaction	WinCC SQL Server Infections

Table 1: A Partial List of Protocols used by Stuxnet and the SCADA Services Affected

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 Tofino Firewall LSM 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 HTTP traffic is required (for example to allow IT clients to access a data historian) it should be restricted to only the zone and web server in question and only for inbound access. Figure 3 shows the typical rules to allow a range of IT clients to access the Data Historian using HTTP. Note the Direction is set to "*Incoming*", since each web client would initiate the session to the server and the server would have little reason to initiate a session out of its zone.



The firewall status on the parent Tofino is: PREDEPLOYED

Attributes	!	Rule	Direction
Global Rules			
Talker Rules			
Data Historian Clients		CONDITIONAL	
HTTP (Web) - TCP	☑	ALLOW	INCOMING

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

Blocking RPC Traffic

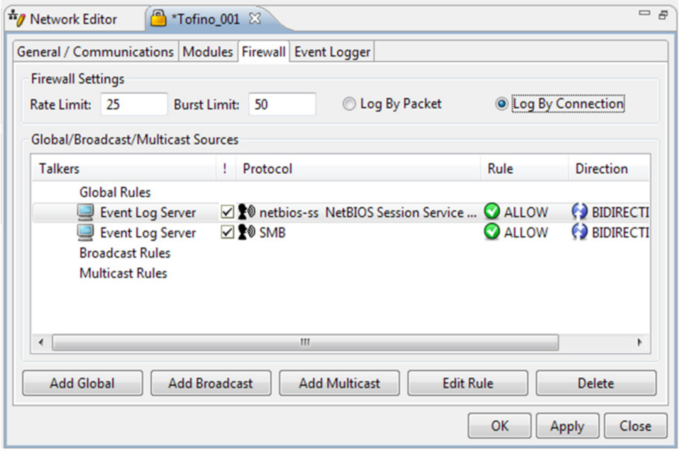
Stuxnet makes extensive use of RPC, so controlling this protocol is essential. As noted earlier the Tofino Firewall LSM blocks protocols by default, so if RPC is not required, the Tofino SA can be used with its default settings to prevent Stuxnet RPC traffic between zones.

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 number of other common services. Thus blocking all RPC traffic may have negative consequences on the industrial process.

To have the least impact on the control system, a mixture of allowed and blocked RPC ports are recommended. All the standard RPC protocol variations are included in the Tofino SA 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 (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.



Firewall Settings

Rate Limit: 25 Burst Limit: 50 ○ Log By Packet ● Log By Connection

Global/Broadcast/Multicast Sources

Talkers	!	Protocol	Rule	Direction
Global Rules				
Event Log Server	☑	netbios-ss NetBIOS Session Service ...	ALLOW	BIDIRECTI
Event Log Server	☑	SMB	ALLOW	BIDIRECTI
Broadcast Rules				
Multicast Rules				

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

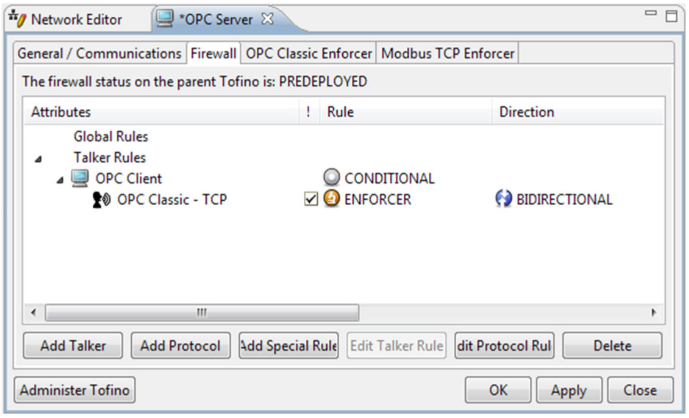
Similar rules may also be needed for Print and File Servers, although it is generally better to not allow sharing between zones. The minimum goal is to prevent uncontrolled RPC traffic to computers, so restricting it to specific servers that are carefully patched and monitored for infection can be acceptable in some situations

The related protocols, NetBIOS Name Service (UDP port 137) and 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 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 that has made it impossible to secure using conventional IT-style firewalls.

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 Tofino OPC Enforcer module solves this issue by automatically tracking and managing OPC Classic's use of dynamic ports 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.



The firewall status on the parent Tofino is: PREDEPLOYED

Attributes	!	Rule	Direction
Global Rules			
Talker Rules			
OPC Client		CONDITIONAL	
OPC Classic - TCP	☑	ENFORCER	BIDIRECTIONAL

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

To configure the 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 Byres AN-105 "*Protecting OPC Systems Using the Tofino OPC Enforcer*".

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 form the Siemens website.

Testing the Firewall Configurations

Because Stuxnet uses many of the same protocols as valid control system applications, special care must be taken to ensure that the firewall rules do not disrupt the industrial process.

Fortunately, Tofino offers a mode of operation called Test mode, which allows all network traffic to pass, but reports any traffic that would have been blocked by the firewall had it been in Operational mode. These reports are shown as a firewall exception alarm in the Event View of the Tofino CMP and separately recorded by the Event Logger LSM (if installed).

Test mode is ideal for confirming firewall rules without accidentally blocking traffic that should be allowed, and thus impacting plant operations. We recommend that all Tofino Industrial Security Solution installations be run in Test mode for at least 24 hours before switching to full Operational mode.

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 Tofino SAs are in place, configured and tested, they provide excellent "watch-dogs" to warn if an infection is occurring. Specifically, Stuxnet generates a significant amount of event traffic that can be captured using either the Tofino CMP or the 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 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.

Users of Siemens products face a propagation path not faced by users of other systems, namely infected STEP 7 Program files. Unfortunately there is no confirmed mitigation for this exploit.

For Further Information

Additional references regarding Windows system patching, USB drive management and other Stuxnet prevention topics can be found at:

www. tofinosecurity.com/stuxnet-central

This includes:

- Byres AN-118: *Stuxnet Mitigation Matrix*
- White Paper: *Analysis of the Siemens WinCC / PCS7 "Stuxnet" Malware for Control System Professionals*
- Links to Siemens Malware Information and Software Updates
- Links to other key industry materials

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 Tofino Industrial Security Solution can mitigate many of the effects of the Stuxnet virus, while protecting your industrial network against numerous other methods of accidental or malicious attack.

The Tofino™ VPN Server and Client LSMs are components of the Tofino™ Industrial Security Solution

Tofino Security Appliance

Hardware platform that creates Plug-n-Protect™ zones of security on control and SCADA networks

Loadable Security Modules

Firmware modules that customize the security features of each Tofino SA:

- **Firewall**: Directs and controls industrial network traffic
- **Modbus TCP Enforcer**: Content Inspection and connection managament for Modbus and OPC
- **Secure Asset Management**: Tracks and identifies network devices
- **VPN**: Secures remote communication
- **Event Logger**: Reliably logs security events and alarms

Tofino CMP

Software that provides coordinated security management of all Tofino Security Appliances from one workstation or server