



Monitoring emerging threats: SCADA Security

Next step in cyberterrorism

Manuel Santander, GCFA, GCIH
Manuel.santander@epm.com.co
msantand@isc.sans.org



Agenda

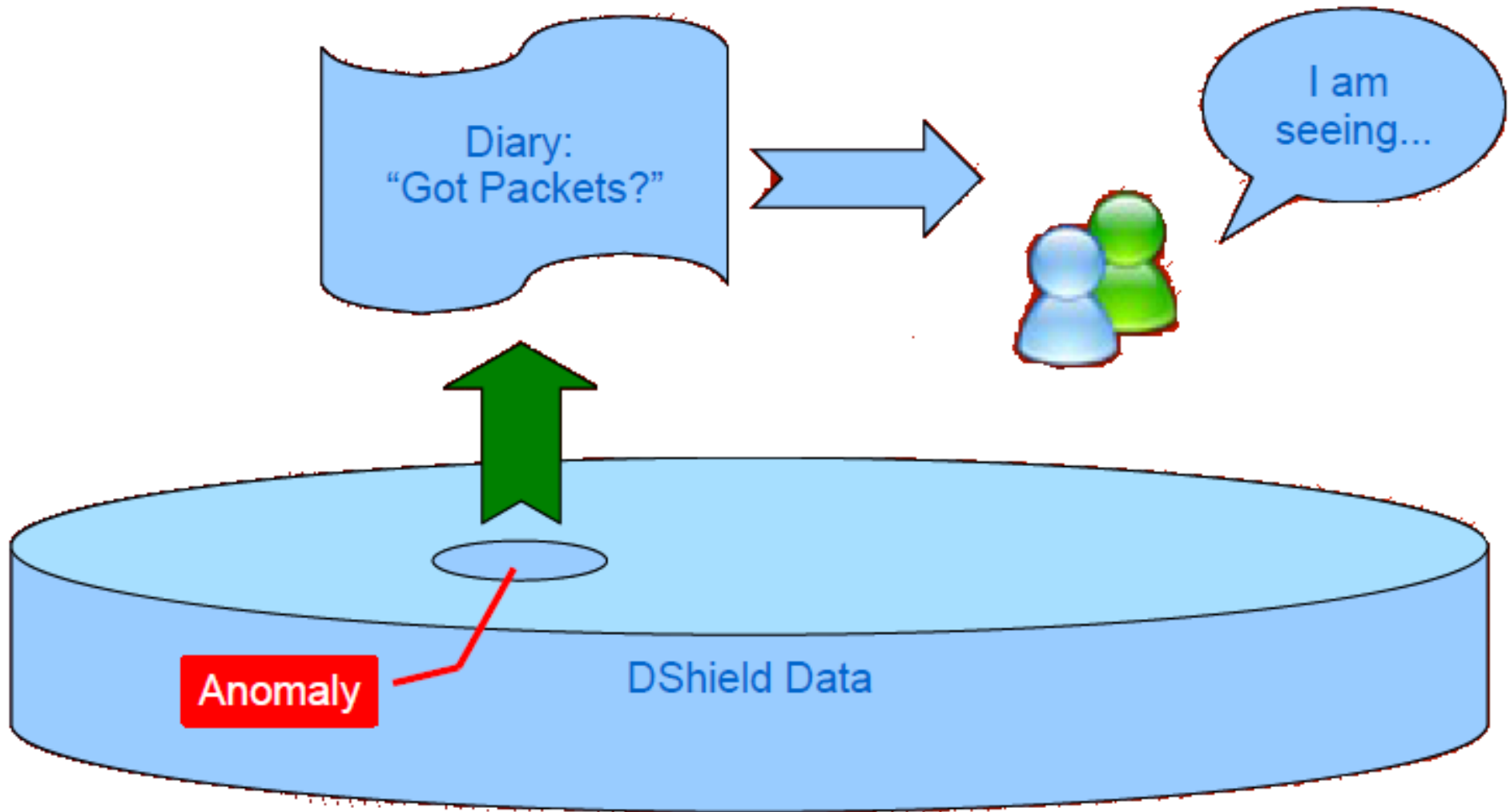
- Introducción
- Riesgos sistemas SCADA
- Stuxnet: Amenaza para el ciberterrorismo
- Medidas de seguridad para sistemas SCADA
- Conclusión

INTRODUCCIÓN

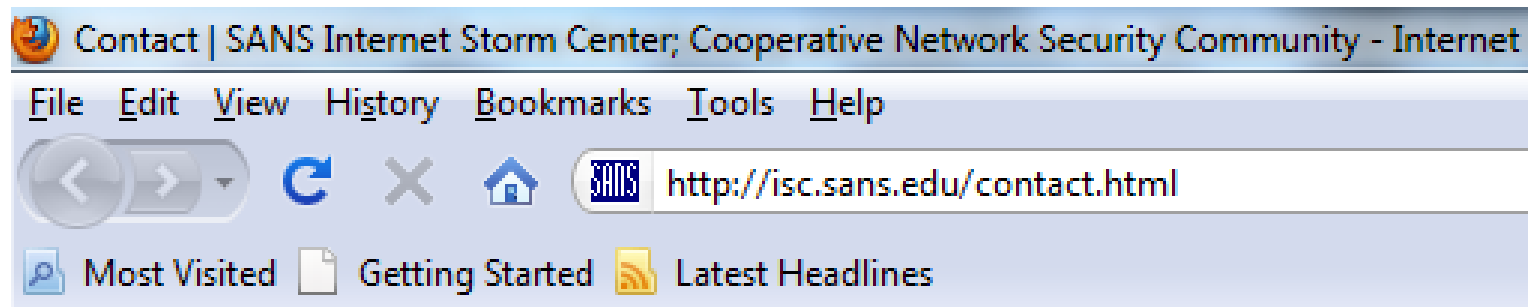
SANS INTERNET STORM CENTER

- Nuestro objetivo: alertar a las personas sobre los eventos de seguridad más relevantes ocurridos en internet
- Somos un grupo de 39 personas alrededor del mundo de varias industrias: bancos, servicios públicos, gobierno, universidades
- Cada día, uno de nosotros toma el cargo de *Handler on Duty*, haciendo turnos de 24 horas iniciando a las 00:00 GMT
- Nuestra labor es monitorear anomalías en Internet y alertar a nuestros lectores (<http://isc.sans.edu>)

DSHIELD: Distributed log correlation



Recibimos otros reportes ...



SANS Contact | SANS

Contact Form

Please use

You may w

- Sh
- SU
- No

from dzus@fas.harvard.edu ☆
subject **ISC# [2727860] malware found on web server MYDYN**
to handlers-2727860@sans.org ☆

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Name: Paul Dzus
E-Mail: dzus@fas.harvard.edu

/* handlers@sans.org is an alias for all ISC handlers.
Please include the list in all replies to keep everyone informed.
You may receive more than one response */

Múltiples formas de fraude

- Virus configurado específicamente para la compañía que usted guste = \$50,000 USD
- Virus reciclado modificado para que no sea detectado por virus = \$200 USD
- 10 millones de direcciones de correo electrónico = \$160 USD
- Número de tarjeta de crédito = \$2~6 USD
- Número de tarjeta de crédito con código de seguridad = \$20~60 USD
- Alquiler de equipo que controla una botnet de 5,000 a 10,000 equipos = \$100/day

Fuente: G-Data

Recibimos este reporte

from watcher60@gmail.com ☆
subject **ISC# [8792102] lnk vuln starting to be used MNDYNY**
to handlers-8792102@sans.org ☆

 reply  reply all  forw

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Name: Matt Whitehead
E-Mail: watcher60@gmail.com

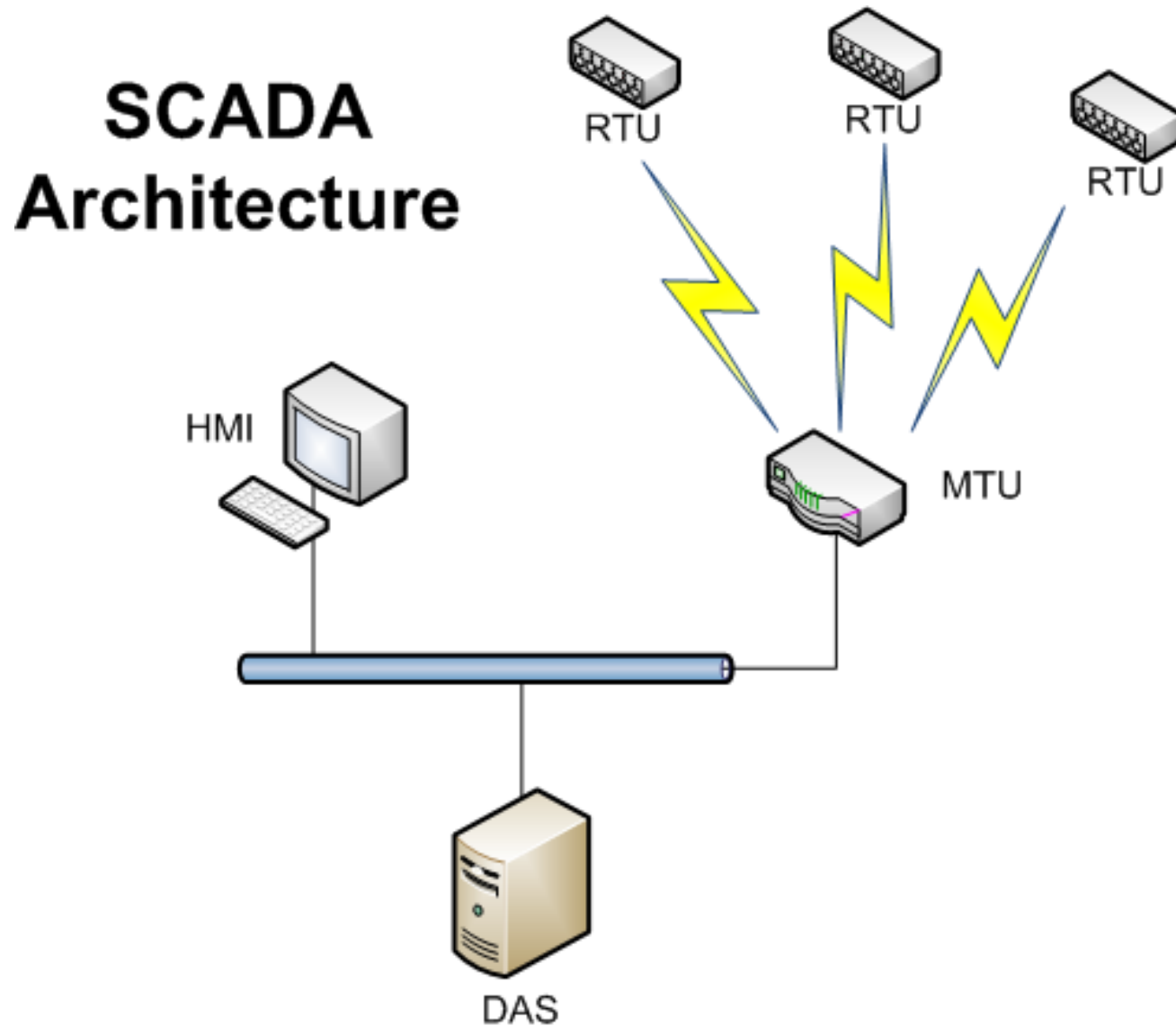
/* handlers@sans.org is an alias for all ISC handlers.
Please include the list in all replies to keep everyone informed.
You may receive more than one response */

Thought I'd just bring it to your attention incase not seen but the lnk/pif vuln' is starting to be used:

<http://blog.eset.com/2010/07/22/new-malicious-lnks-here-we-go>

RIESGOS SISTEMAS SCADA

Componentes del Sistema SCADA



Componentes del Sistema SCADA (2)

- Unidad Terminal Remota (RTU): Recopila datos de los dispositivos de campo en la memoria hasta que la MTU solicite esa información y procesa los pedidos del HMI.
- Master Terminal Unit (MTU): Inicia la comunicación con las unidades remotas y las interfaces con el DAS y el HMI.
- Adquisición de Datos (DAS): la información del DAS se reúne a partir de la MTU, y genera alertas que necesita la atención del operador.
- Interfaz Hombre-Máquina (HMI): El panel de operador se define como la interfaz donde el operador se conecta a monitorear las variables del sistema. Reúne información del DAS.

Riesgos del Sistema SCADA

- Aumento de la rotación de las turbinas de generación , aumentando el flujo de energía superior a la capacidad de una línea de transmisión o simplemente apagar las turbinas de una central eléctrica.
- Desbordamiento de los tanques de agua y ruptura de tuberías en las calles
- ¿Causas?
 - Robo de identidad
 - Malware
 - Acceso no autorizado
 - Aprovechamiento de vulnerabilidades

Riesgos del Sistema SCADA (2)

- Los sistemas SCADA se hicieron orientados a tiempo-real
 - Las alertas de datos y órdenes a los sistemas deben llegar en el menor tiempo posible, pues un retardo adicional de 10 ms puede incluso ocasionar un apagón
- Los sistemas SCADA funcionan bajo configuraciones muy específicas
 - Orientadas al funcionamiento y no a seguridad
 - Los vendedores casi nunca soportan parches
 - Medidas externas para aseguramiento

STUXNET: AMENAZA PARA CIBERTERRORISMO

STUXNET se volvió popular ...

MD5: f3a781bafa67ba01c02c90a52de93481	SHA1: 2d333662bc68e23887c443e08ae5ad2812eb95a9
SHA256: 08c7d22134b1831ed897af7e032a90dcac72e014c7655cb21338545aa5b2645f	
Original Submitted Filename: sioup.scr.stuxnet	Date Added: 2010-07-21 07:54:12.43804
Magic File Type: PE32 executable for MS Windows (GUI) Intel 80386 32-bit	Packer Signature: Microsoft Visual Basic v5.0/v6.0 [171,685] Microsoft Visual Basic v5.0 [170,681]
Anti-Virus Results: ClamAV Trojan.VB.Chinky-2	

MD5: 74ddc49a7c121a61b8d06c03f92d0c13	SHA1: 0ccbc128dd8bf73dc7b3922fb67d26bbcdbcaa89
SHA256: 743e16b3ef4d39fc11c5e8ec890dcd29f034a6eca51be4f7fca6e23e60dbd7a1	
Original Submitted Filename: ~wtr4132.tmp	Date Added: 2010-07-19 15:40:10.086223
Magic File Type: PE32 executable for MS Windows (GUI) Intel 80386 32-bit	Packer Signature:
Anti-Virus Results: ClamAV Trojan.Stuxnet	
Tags:	

STUXNET se volvió popular ... (2)

- Software hecho para atacar sistemas SCADA
- Modifica funcionamiento de componentes
- Aprovecha cuatro vulnerabilidades de Windows
- Permite interacción remota
- Ciberterrorismo

Infección de STUXNET a PLC

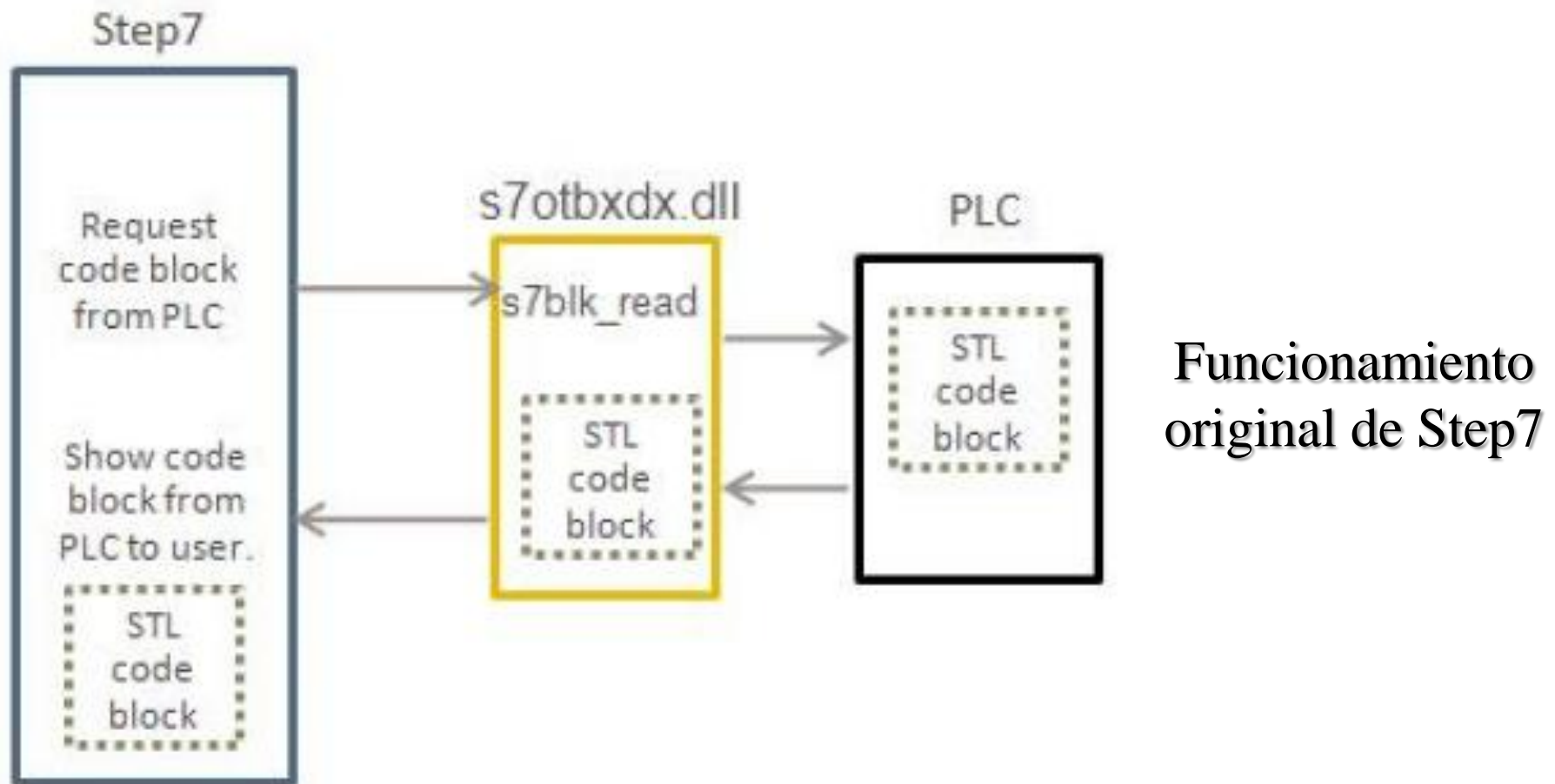
- Afecta al software WinCC/Step7
- El programador puede conectar el PLC y acceder a la memoria , reconfigurarlo y bajar un nuevo programa



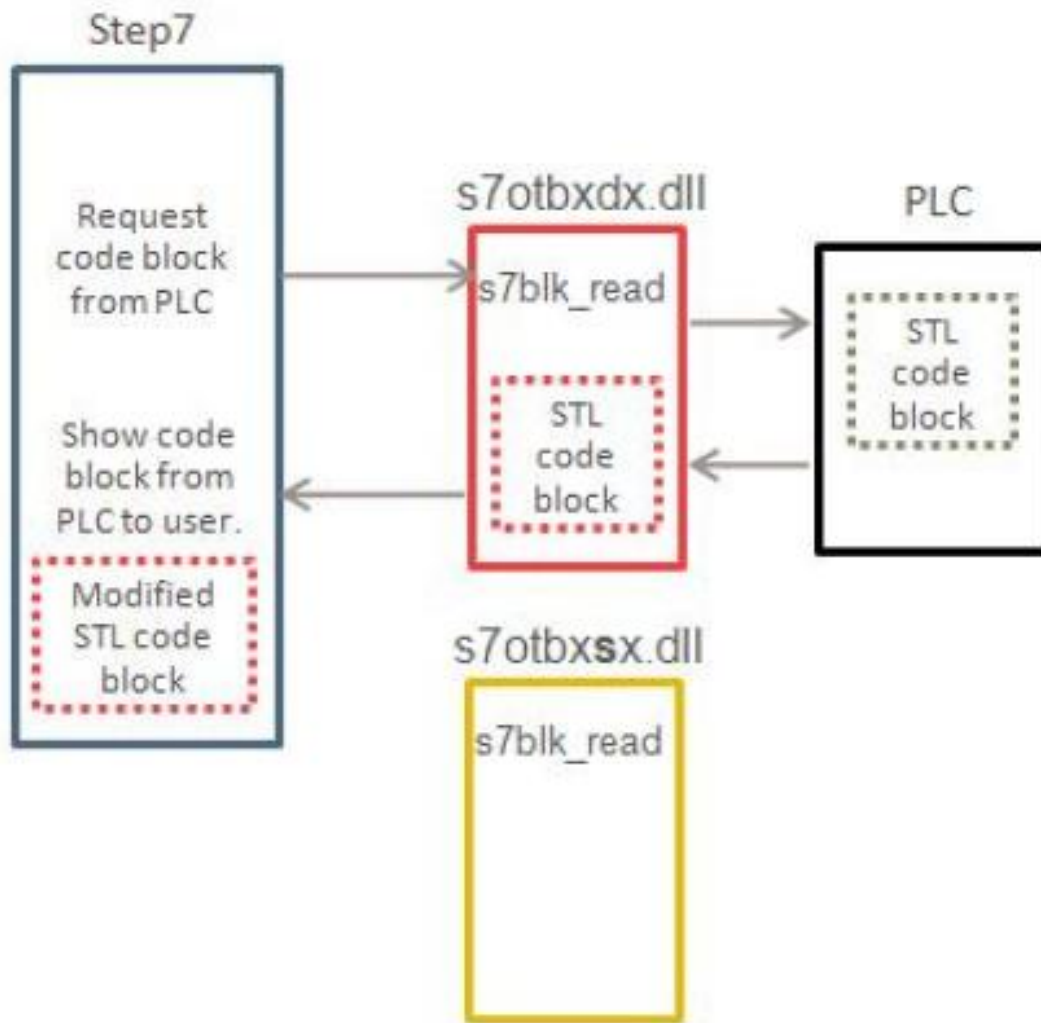
Infección de STUXNET a PLC (2)

- Stuxnet necesita acceder al PLC
- Necesita intervenir la comunicación entre el programador y el PLC
- Modifica el dll de comunicaciones s7otbxdx.dll utilizado para la comunicación. El original se renombra a s7otbxsx.dll
- El nuevo queda con el nombre que el ejecutable invoca
- 93 exports del dll se reenvían al original de fábrica
- 16 exports se modifican para que stuxnet infecte el PLC

Infección de STUXNET a PLC (3)



Infección de STUXNET a PLC (3)



Funcionamiento
modificado de Step7

¿Cómo son los programas de PLC?

- Bloques de código y datos que el operador carga
- Tipos de Bloques
 - Bloques de datos: Argumentos para los bloques de organización
 - Bloques de Datos de Sistema: Contiene información específica sobre cómo está configurado el PLC
 - Bloques de organización: Corresponden los entry points de los programas. Stuxnet usa los siguientes:
 - OB1: Entry point del programa del PLC. Se ejecuta cíclicamente
 - OB35: Watchdog ejecutado cada 100 ms para propósitos de monitoreo

Secuencia de infección del PLC

- Stuxnet inicia la secuencia de infección si:
 - La CPU del PLC es referencia 6ES7-417 y 6ES7315-2
 - El System Data Block contiene los valores 7050h y 9500h
- Modifica el código del coprocesador DP_RECV, teniendo con esto comunicación al bus industrial Profibus (comunicación con los dispositivos de la red industrial)
- Modifica el bloque OB1 instalando código troyano al inicio del bloque, para que el virus se ejecute al inicio de cada ciclo

¿Cómo se camufla stuxnet?

- No puede permitir que sobrescriban el código del virus que ya existe en los bloques infectados
- No puede mostrar al operador/programador que existen bloques infectados
- Los siguientes exports son vitales:
 - s7blk_read: No se muestran los bloques infectados
 - s7blk_write: Se asegura que los bloques OB1 y OB25 continúen infectados si son modificados
 - s7blk_findfirst/s7blk_findnext: Se usan para enumerar los bloques en el PLC. No se muestran los infectados

MEDIDAS DE SEGURIDAD PARA EL SISTEMA SCADA

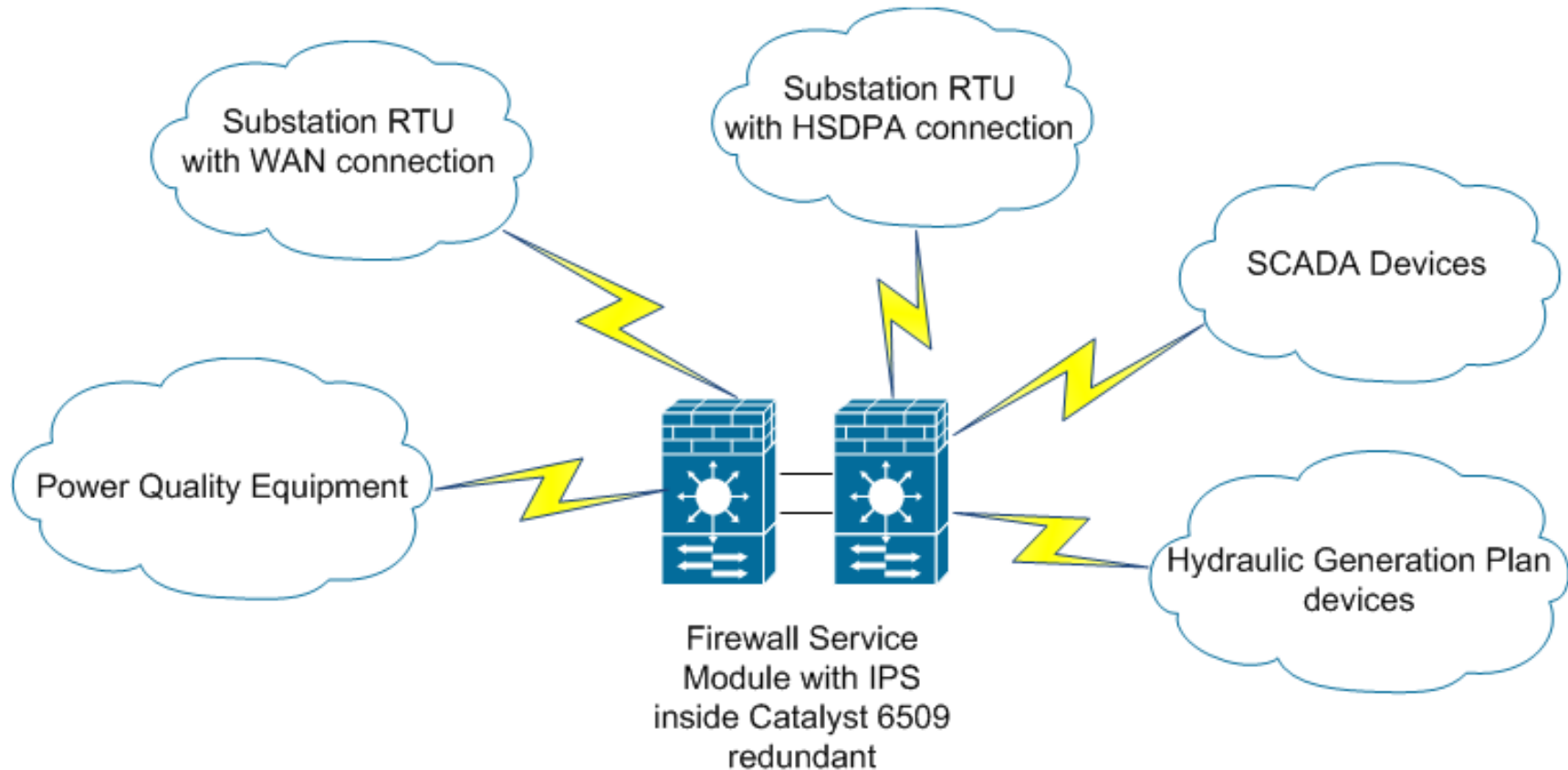
Controles para sistemas SCADA

- Premisas
 - No pueden modificar el desempeño del sistema
 - Deben preservar las funcionalidades originales de los protocolos
 - El más mínimo retardo puede ocasionar una catástrofe
- Puntos de control
 - Sistema de seguridad perimetral: Intercambio de información
 - Control de modificación de configuraciones en las máquinas

Controles para sistemas SCADA (2)

- Puntos de control
 - Uso de nuevos protocolos que incorporan sistemas de seguridad
- Controles tecnológicos
 - Firewalls, IDS e IPS: Vitales para establecer un monitoreo de lo que ocurre en la red, ya que el SCADA es un sistema distribuido que funciona a través del intercambio de mensajes
 - Monitoreo de integridad de archivos: Con esto se verifica que no se modifiquen los parámetros de configuración de los elementos SCADA (<http://www.solidcore.com>)

Diagrama ejemplo



SCADA NETWORK PERIMETER DESIGN

CONCLUSIÓN

Ciberterrorismo es una posibilidad real

- Sistemas SCADA con poca seguridad
 - Los proveedores no incorporan medidas de seguridad fiables en sus sistemas
 - Los ponen accesibles a los usuarios a precios astronómicos
- La seguridad es un costo para la organización
 - ¿Cuál es la postura de riesgo de la compañía?
 - ¿Debemos esperar a que ocurra un desastre para invertir?
 - El esquema de monitoreo es vital para determinar que ocurre

¿Preguntas? ¿Inquietudes?

Manuel Humberto Santander Peláez

<http://manuel.santander.name>

<http://twitter.com/manuelsantander>

**msantand@isc.sans.org /
manuel.santander@epm.com.co**