Infraestructuras Críticas

Lic. Cristian Borghello, CISSP – CCSK – MVP

www.segu-info.com.ar
info@segu-info.com.ar
@seguinfo
@CursosSeguInfo

SEGU·INFO
SEGURIDAD DE LA INFORMACION

AGASSI

Sobre Cristian Borghello

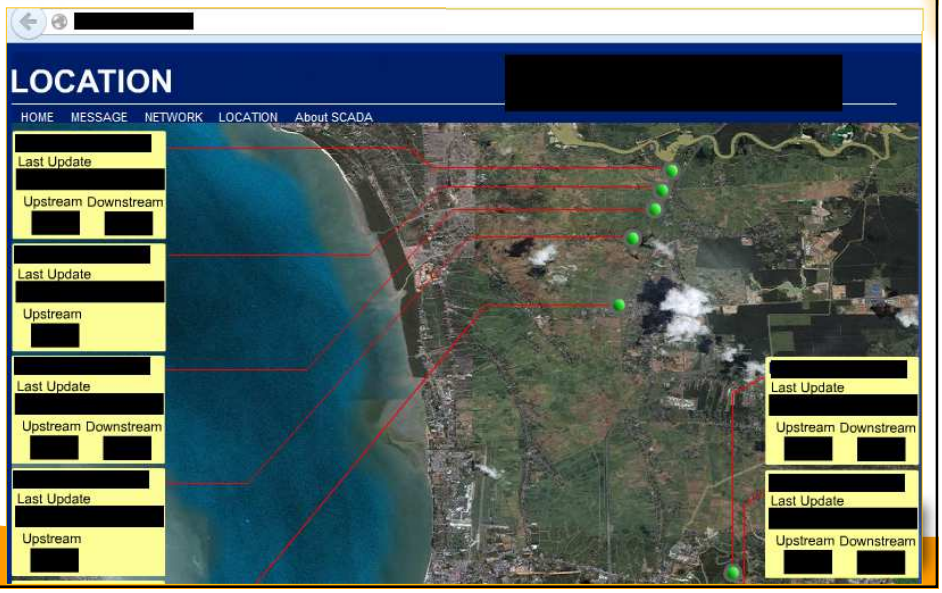
- Licenciado en Sistemas UTN desde 2000
- Desarrollador desde los 8 años
- CISSP (Certified Information Systems Security Professional) desde 2008
- Microsoft MVP Security (Most Valuable Professional) desde 2010
- CCSK (Certificate of Cloud Security Knowledge) desde 2014
- Creador y Director de Segu-Info
- Consultor independiente en Seguridad de la Información

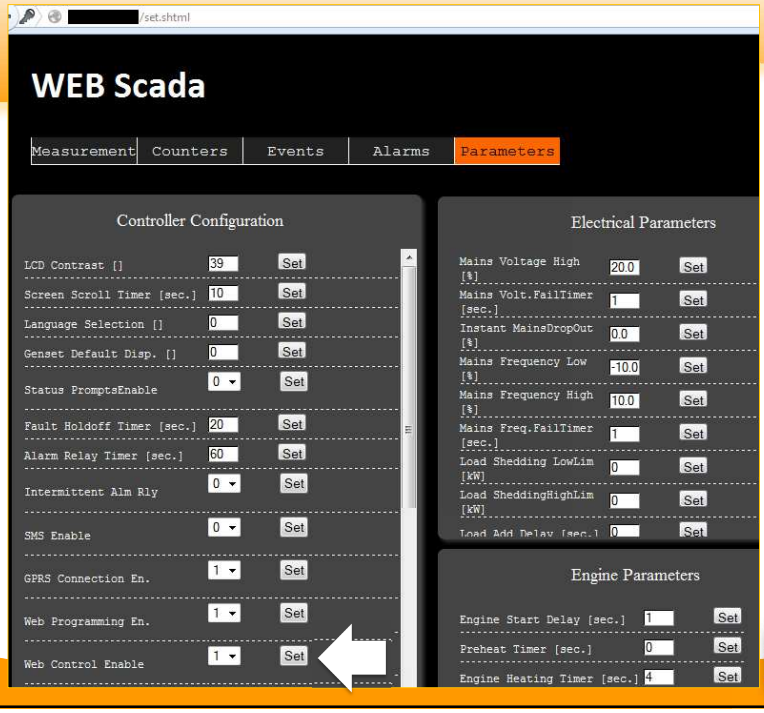
Infraestructuras Críticas

Son aquellas infraestructuras que proporcionan servicios esenciales cuyo funcionamiento es indispensable para el país, no permiten soluciones alternativas y, por lo tanto, su perturbación o destrucción tendría un grave impacto sobre la vida de las personas

Infraestructuras Críticas

Se desea actualizar e integrar sistemas antiguos con instalaciones modernas y… ¡se los conecta a Internet!





SHOWTIME

Hacking a Firmware de aviones

8/05/2014 08:35:00 a. m. Comenta primero!

eventos, hacking, infraestructuras críticas, vulnerabilidades

Twittear 50

Ruben Santamarta, consultor español de la empresa IOActive, expondrá los detalles de su investigación en el congreso Black Hat, esta semana.

Ruben dijo que descubrió como hackear el equipo de comunicación satelital de los aviones de pasajeros a través de su conexión inalámbrica a Internet y los sistemas de entretenimiento a bordo, en una afirmación, que de confirmarse, podría detonar la revisión de la seguridad aérea.

- Los Boing 747 tienen Solaris, con TELNET habilitado por defecto
- Y... SÍ, los ingenieros pueden conectarse a él en el aire para “recalibrar el motor”

Problemas industriales

- Ciclo de vida del equipamiento: la evolución de las TIC se miden en meses y el de los equipamientos industriales en décadas, por lo que su seguridad es obsoleta y dependen de sistemas heredados diseñados y construidos hace tiempo y que no cumple con los estándares actuales
- Heterogeneidad de sistemas: la gran diversidad de fabricantes y configuraciones brinda una baja percepción del riesgo a ataques

Problemas industriales

- La robustez y fiabilidad son prioridad: los entornos industriales son “duros” y todo se diseña con estándares de seguridad pero es impensable una “parche” porque podría volver inestable el sistema
- Tiempo real: todo se controla de manera continua y se elimina todo aquello que no sea imprescindible. Por ej., el cifrado requiere tiempo adicional y no es implementable directamente
- Inexistencia de entornos de prueba: hay baja evolución del entorno y el costo es alto

RuggedCom hardware, sistema operativo y aplicaciones que gestionan infraestructuras críticas (ferrocarril, control de tráfico, centrales eléctricas, instalaciones militares, etc)


```
[redacted]x$ telnet [redacted]62
Trying [redacted].62...
Connected to [redacted]-62-m[redacted]comcastbusiness.net.
Escape character is '^]'.


            Rugged Operating System v3.8.0 (Mar 05 2010 08:45)

    Copyright (c) RuggedCom, 2008 - All rights reserved

    System Name:     US23MM0600SW
    Location:        US23 at [redacted] Yard
    Contact:         [redacted]
    Product:         RS900-HI-D-TX-TX-00
    Classification:  Controlled
    MAC Address:     00-0A-DC-40-CC-80
    Serial Number:   900-0410-27787

    Enter User Name:
```

Puerta trasera

User: factory
Pass: MAC Address

Dispositivos vulnerables

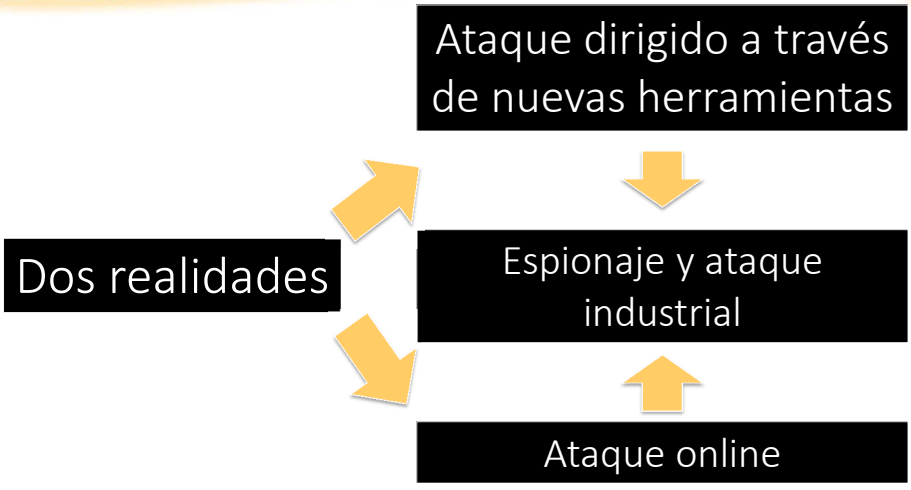
digital bond

	A-B	Schneider Electric	GE	SEL	Koyo
Firmware	!	✗	!	!	!
Ladder Logic	!	!	✗	!	✗
Backdoors	!	✗	✗	✓	✓
Fuzzing	✗	✗	✗	!	!
Web	!	✗	N/A	N/A	✗
Basic Config	!	!	✗	!	!
Exhaustion	✓	✓	✗	✓	✓
Undoc Features	!	✗	✗	!	!

S4

http://www.digitalbond.com/blog/2012/01/19/project-basecamp-at-s4/

Ataques dirigidos



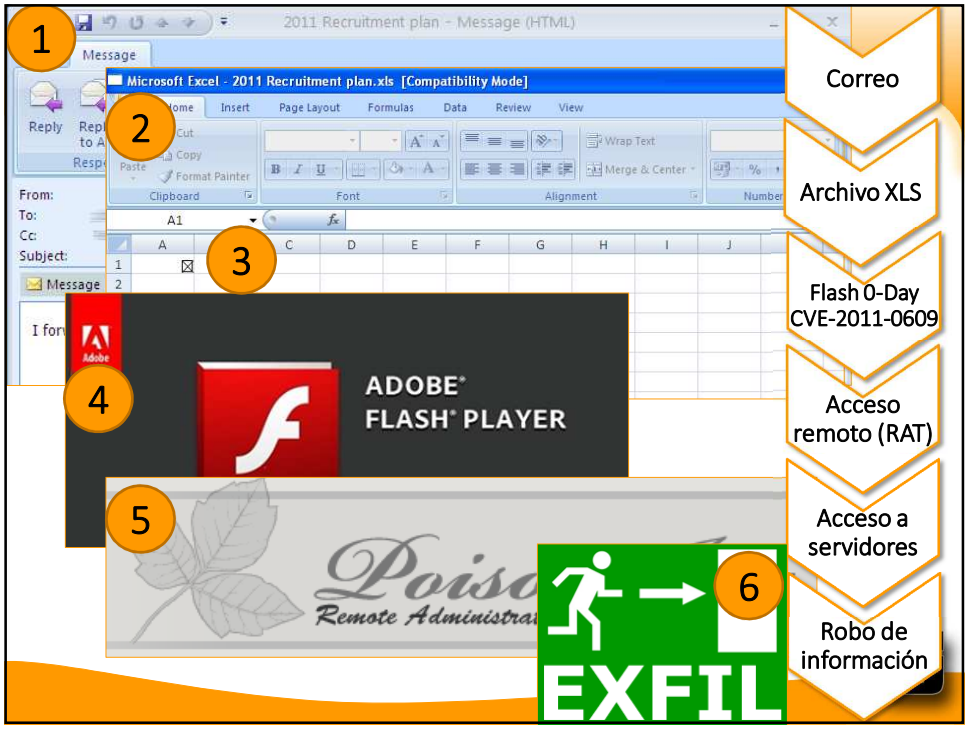
Amenazas Persistentes (APT)

- Amenaza: malware con objetivos específicos, desarrollados por delincuentes calificados, motivados, organizados y bien financiados
- Persistentes: se da prioridad al objetivo, sin beneficios inmediatos, un enfoque de bajo perfil, sigiloso y lento en el tiempo
- Avanzada: se utiliza un amplio espectro de técnicas y tecnologías. Los componentes individuales no suelen ser “avanzados” pero su combinación es la clave del éxito

Amenazas Persistentes (APT)

Our investigation has led us to believe that the attack is in the category of an Advanced Persistent Threat (APT). Our investigation also revealed that the attack resulted in certain information being extracted from RSA's systems. Some of that information is specifically related to RSA's SecurID two-factor authentication products.

SHA256:	454f624958298bf76c5b7ffa1509159b827856095d41672707fcf6416a818ddb
Nombre:	survey-questions_2011.xls
Detecciones:	40 / 53
Fecha de análisis:	2014-08-09 21:01:06 UTC (hace 2 minutos)



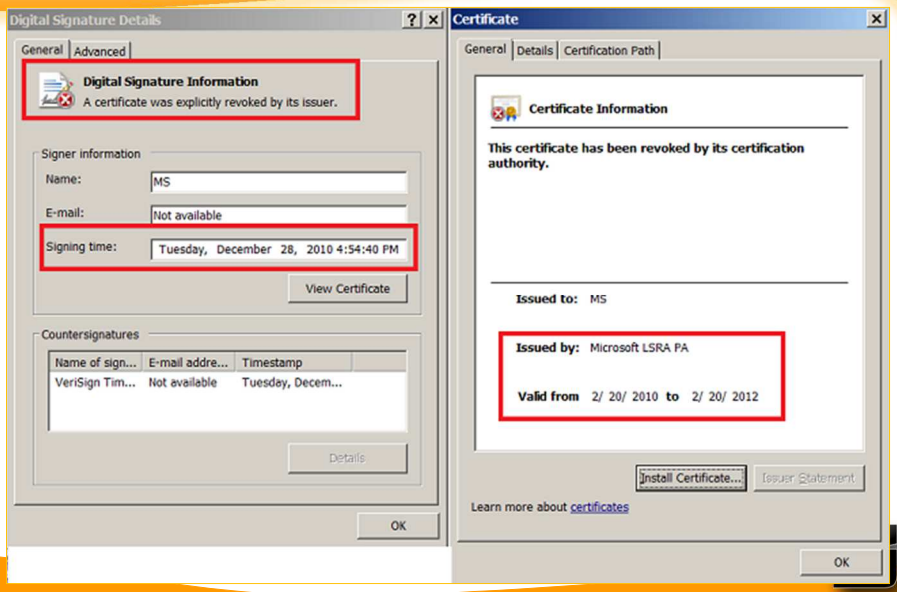
Amenazas Persistentes (APT)

- Si un atacante es capaz de infiltrarse en la red, tendrá "la suerte" de visualizar y controlar otras industrias, y tener una fuente ideal de información para la infiltración de las empresas asociadas
- Los ataques no se limitan a robar información financiera
- Las relaciones que tiene con sus socios y su cadena de suministro es más valiosa para un atacante

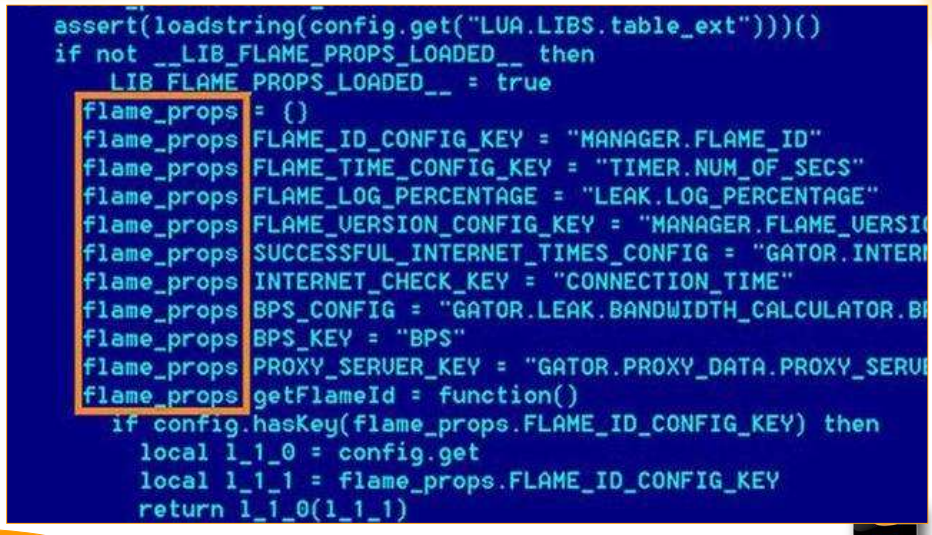
Los ataques dirigidos siguen siendo relativamente raros, pero pensar “a mí no me va a pasar” es el principio del fracaso

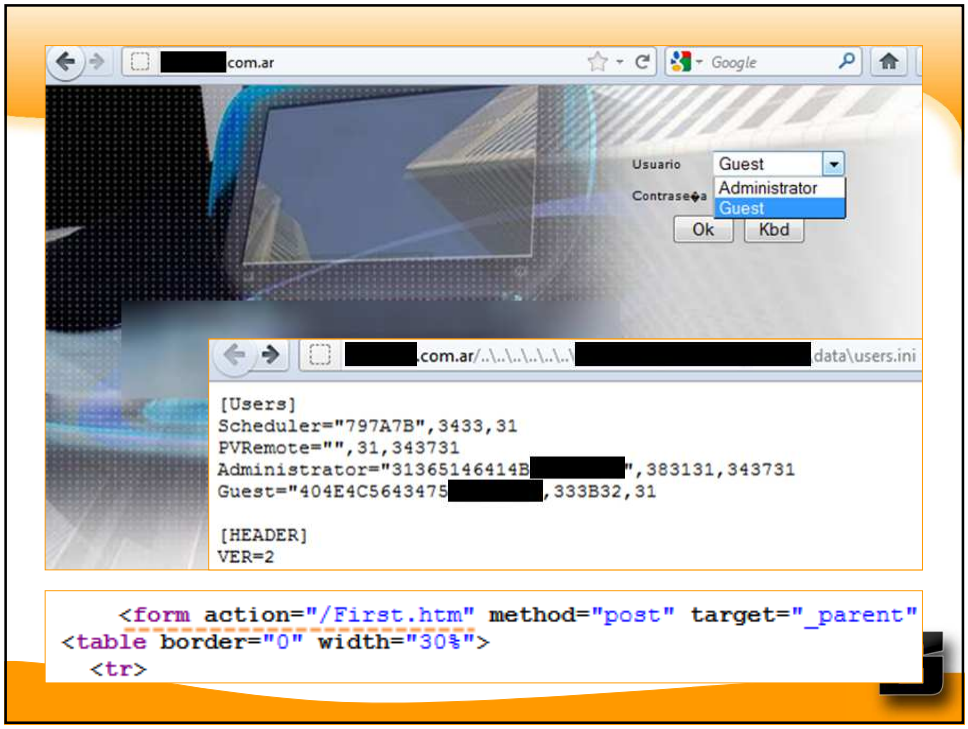
SDFG

Stuxnet



SDFG





ICIC GICI | Grupo de Infraestructuras Críticas de Información

Encargado del relevamiento, identificación y clasificación de las infraestructuras estratégicas y criticas de la información, así como el monitoreo de los servicios que el Sector Público Nacional brinda a través de Internet y aquellos que se identifiquen como infraestructura crítica, para la prevención de posibles fallas de seguridad

Resolución JGM 580/2011 (JEFATURA DE GABINETE DE MINISTROS)
http://www.infoleg.gov.ar/infolegInternet/anexos/185000-189999/185055/norma.htm
http://www.icic.gob.ar/paginas.dhtml?pagina=98

ICIC GICI | Grupo de Infraestructuras Críticas de Información

Identificación y análisis de las infraestructuras críticas de información

Coordinación de planes de acción, prevención y monitoreo con organismos públicos y privados.

Generación de un marco metodológico para el control de la correcta administración de la información de las Infraestructuras Críticas.

Sólo un ejemplo…

En otros lugares…

- (España) La Comisión Nacional para la Protección de las Infraestructuras Críticas (CNPIC), designó 37 operadores críticos que gestionan más de 150 infraestructuras críticas. La electricidad, el gas, el petróleo, el sector nuclear y el sector financiero se consideran infraestructuras críticas
- (EE.UU.) Según la estrategia de seguridad nacional, el DoE establece que la energía es una infraestructura crítica. Se realizaron una serie de evaluaciones sobre dispositivos SCADA para garantizar su funcionamiento

http://www.infodefensa.com/es/2014/07/21/noticia-interior-constituye-comision-nacional-proteccion-infraestructuras-criticas.html

Cuestiones candentes (I)

1. Adopción de una postura ofensiva
2. Evaluación de la capacidad ofensiva de los países
3. Protección de un sistema global gradualmente más integrado
4. Determinación de la seguridad de los sistemas SCADA
5. Seguridad frente a privacidad
6. Neutralidad de la red
7. Transición hacia reglamentos internacionales
8. Construcción de una ciberarquitectura más sólida
9. Búsqueda de soluciones a los problemas que plantean los países más débiles
10. Protección de la cadena logística de Internet

Cuestiones candentes (II)

11. Aumento de la concienciación sobre el nivel del problema
12. Adopción de un enfoque global
13. Fomento del diálogo entre técnicos y dirigentes
14. Definición del papel de los gobiernos
15. Intercambio de información a nivel internacional
16. Nuevos punto de vista sobre la ciberseguridad
17. Concienciación ciudadana
18. Disminución del secreto
19. Armonización de códigos y legislaciones
20. Definición de los ciberataques preventivos

Ciberdefensa: Las reglas del juego a nivel Mundial
http://www.fba.unlp.edu.ar/tic/archivos/R04.pdf

Agradecimientos

A la Comunidad de Segu-Info que todos los días [nos] aporta conocimiento a través de los distintos grupos de discusión

¡GRACIAS!

Lic. Cristian Borghello, CISSP – CCSK – MVP

www.segu-info.com.ar
info@segu-info.com.ar
@seguinfo
@CursosSeguInfo

SEGU·INFO
SEGURIDAD DE LA INFORMACION

AGASSI