Seguridad en infraestructuras criticas

Prueba de evaluación continua 1 - Sergio Roselló

Stuxnet

Como se ha encontrado la referencia a la Vulnerabilidad? Que referencias se han utilizado?

Ya había oído hablar de Stuxnet al leer el libro 'Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon'.

Durante la lectura del libro recomendado para la asignatura, también se hace referencia a Stuxnet, sus implicaciones y la importancia del suceso.

Para realizar este trabajo, me he centrado en ambas fuentes descritas anteriormente, ademas, de algunos artículos, citados en la parte inferior de este documento.

Su naturaleza, los recursos a los que afecta, su nivel de peligrosidad, como fue detectada?

Stuxnet es un programa informático, descrito como worm, o gusano, diseñado por los Estados Unidos, en conjunto con Israel para retrasar la producción uranio enriquecido de la central nuclear de Matan, en Israel. Su medio de transmisión se origina desde un USB, el cual, seguramente se dejo en una zona transitada por oficiales de la central nuclear de Irán. Al conectar el USB a un ordenador, este usaba un 0-day de Windows, que permite a usuarios locales o atacantes remotos ejecutar código a su elección a través de un fichero de acceso directo (1) .LNK o (2) .PIF manipulado, el cual no es manejado adecuadamente mientras se muestra el icono en el Explorador de Windows. [INCIBE-CERT]

Este ataque, cuando salio a la luz, forzó un antes y un después en la industria de la ciberseguridad en infraestructuras criticas.

Dada la complejidad y especificidad de los componentes que forman una infraestructura critica, se pensaba que la mejor baza de seguridad para protegerse ante hackers era esta misma complejidad y diversidad de componentes.

Para que un hacker se infiltrase lo suficientemente adentro en una infraestructura critica para producir alguna consecuencia desastrosa, tendría que saber exactamente como funciona la red industrial interna, ademas, de todos los componentes y protocolos de comunicación que se usan en esta.

De esta forma, podría ir escalando privilegios (En el caso de stuxnet, utilizando varios 0-days encontrados en el sistema operativo Microsoft Windows) e infiltrarse en la capa critica, como, en el caso de Stuxnet, buscando controladores con el programa Siemens Step7.[STEP_7]

Este programa esta diseñado para controlar controladores lógicos programables. (PLC's) A su vez, estos PLC's controlaban las centrifugadoras de la central nuclear, y en manos del los hackers, que podían acceder a los datos que estos controladores leían de las centrifugadoras e incluso podían hacer que las centrifugadoras se rompieran, cambiando una serie de parámetros desde el PLC.

A nivel de usuario normal, este gusano no es peligroso, porque esta altamente dirigido. Si detectaba que el sistema operativo no tenia el programa Step7 instalado, infectaba a un numero N de nuevos ordenadores y posteriormente, se desinstalaba automáticamente. Se entiende que esto se hizo de esta manera, para mantener un gran numero de posibilidades de llegar a un ordenador con el software de Siemens, pero evitar ser detectado, por posibles efectos secundarios en otros usuarios.

A nivel de usuario afectado, (Se entiende que por usuario afectado, se refiera al usuario para el que va dirigido este ataque) las consecuencias, podrían haber sido devastadores, porque la operación entera de la central nuclear podía ser controlada por un agente externo.

Tiene (O podría tener) algún tipo de relación con las inseguridades relacionadas con el mal uso, administración, etc... De las políticas del personal?

En este caso, como ha sido mencionado brevemente en la sección anterior, el ataque entero se basa en que un oficial de alto mando, o un empleado que trabajen en la planta de producción de uranio enriquecido de Matan recoja el USB y lo conecte a un ordenador Windows dentro de la red (Infraestructura critica) de la central.

Cuando se esta al mando de una central nuclear, se tienen que tener una serie de consideraciones de seguridad tremendas. Ya que las consecuencias de que un virus, tanto de forma coordinada o por coincidencia, pueden ser demasiado graves como para poder correr el riesgo.

Si tiene una solución aceptada

En el momento en el que se descubrió Stuxnet, se habían hecho previamente una serie de estudios, Pruebas de concepto o simulacros controlados en laboratorios, que advertían de la posibilidad de una intrusión en infraestructuras criticas, pero nunca se había demostrado en "la vida real" que era posible.

Desde la "demostración" de Stuxnet, se ha empezado a tener mas en cuenta la seguridad en las infraestructuras criticas y hoy en día, estas están mas protegidas, con sistemas de control, como IDS, IPS, Firewalls o técnicas de seguridad pasiva, como una defensa en profundidad, en la que los equipos mas críticos, deben estar protegidos en redes internas.

Aun así, dados los requisitos de negocio de empresas con infraestructuras criticas,

se complica la seguridad porque estos demandan que, de alguna forma, estén conectados a Internet, ya sea de forma directa o indirecta.

Si ha sido objeto de seguimiento

El gusano en si, fue descubierto tras su propósito, pero si que existen muchos ordenadores hoy en día que siguen teniendo ese agujero de seguridad, mayoritariamente, en países no tan desarrollados.

El gusano, hoy en día sigue siendo motivo de estudio, ya que desde entonces, no se ha descubierto otro gusano que consiga la misma complejidad. Ademas, siguen habiendo partes del código que no quedan claras del todo, aunque el propósito general, si que se haya descubierto.

Ha conocido directamente alguna situación parecida en su entorno laboral?

En mi entorno laboral, no he conocido ninguna situación parecida.

Tipo de vulnerabilidades a la luz de lo estudiado en el curso

Como se ha dicho brevemente anteriormente, Stuxnet se aprovecha de tres vulnerabilidades 0-day, estas son, vulnerabilidades que no son conocidas por la comunidad de seguridad, de forma abierta, y que no hay un patch para ellas.

Ademas de estas tres vulnerabilidades, el error mas grande que se cometió por los empleados de la central, fue conectar el USB a un ordenador dentro, o con acceso de la infraestructura critica. A partir de ese momento, la seguridad de esta infraestructura, ya no estaba en sus manos.

Bibliografía

- STEP_7
- INCIBE-CERT_