Tecnicatura Universitaria en Ciberseguridad

Introduccion a la Seguridad de la Información

Actividad 01 - Casos Reales

"Stuxnet La Primer Ciberarma"

Agustin E. Guida

Rosario, Santa Fe, Argentina – Febrero 2024

Contenido

Consignas

Seleccionar un caso real de un **Ciberincidente** aparecido en una nota de prensa, ya sea global, regional, local, etc. y responder las consignas:

1. ¿Por qué es importante?
2. ¿Qué pilar y componente fue afectado?
3. ¿Estuvo involucrado alguno de los elementos que vimos en el encuentro? (ransomware, organización delictiva, etc.)
4. Es posible estimar el monto asociado al evento?

Introducción

Stuxnet es un poderoso gusano informático diseñado por la inteligencia estadounidense e israelí para desactivar una parte clave del programa nuclear iraní. Dirigido a una instalación aislada y concreta, se extendió inesperadamente a sistemas informáticos externos, lo que planteó una serie de preguntas sobre su diseño y propósito.

Stuxnet aprovechó varios *zero days* de Windows previamente desconocidos. Eso dejó claro que el malware era parte de una operación de sabotaje de alto nivel llevada a cabo por los estados-nación contra sus adversarios.

Desarrollo

En la primera década del siglo XXI, el panorama geopolítico estaba marcado por una creciente preocupación sobre la proliferación nuclear, con el programa nuclear iraní en el centro de la atención internacional. Esta preocupación se fundamentaba en la sospecha de que Irán estaba persiguiendo capacidades nucleares con objetivos militares, a pesar de las afirmaciones del gobierno iraní de que su programa era exclusivamente para fines pacíficos. Esta situación exacerbó las tensiones regionales e internacionales, generando un escenario propicio para la emergencia de conflictos y estrategias de disuasión por parte de otros actores estatales interesados en la estabilidad de la región.

En este contexto tenso, la seguridad cibernética se convirtió en un tema cada vez más relevante, ya que las infraestructuras críticas, como las plantas de energía nuclear, eran vulnerables a los ataques informáticos.

En marzo de 2010, los operadores de la planta de enriquecimiento de uranio en Natanz, Irán, notaron un comportamiento inusual en las centrifugadoras utilizadas para el enriquecimiento de uranio. Las centrifugadoras experimentaron aceleraciones y desaceleraciones inexplicables, lo que provocó daños significativos en las instalaciones y una disminución en la producción de uranio.
Cuando Stuxnet infecta un ordenador, comprobaba si ese ordenador estaba conectado a modelos específicos de controladores lógicos programables (PLC) fabricados por Siemens. Los PLC son la forma en que las computadoras interactúan y controlan la maquinaria industrial, como las centrifugadoras de uranio en este caso. Si no se detectan PLC de los modelos S7-315 o el

S7-417, el gusano no hace nada; si los detecta, Stuxnet altera la programación de los PLC, para que las centrifugadoras giren de forma irregular, dañándose o destruyéndose en el proceso. Mientras esto sucede, los PLC le dicen a la computadora controladora (incorrectamente) que todo está funcionando bien, lo que dificulta detectar o diagnosticar lo que está fallando hasta que es demasiado tarde.

Los ingenieros y operadores de la planta estaban desconcertados por estos problemas recurrentes, que parecían indicar un sabotaje o fallas técnicas graves. Sin embargo, desconocían que estaban siendo atacados por un malware sofisticado que más tarde se conocería como Stuxnet.

¿Cómo ataca Stuxnet?

Stuxnet ataca todas las capas de su infraestructura objetivo: Windows, el software de Siemens que se ejecuta en Windows y que controla los PLC y el software integrado en los propios PLC. Está diseñado para ser entregado a través de una unidad extraíble como una memoria USB (se sabía que la instalación de Natanz donde se estaba llevando a cabo el enriquecimiento de uranio estaba aislada, con sus sistemas no conectados a Internet), pero también para propagarse rápida e indiscriminadamente de una máquina a otra en una red interna.

Stuxnet incluye capacidades de rootkit tanto en modo de usuario como en modo kernel. Para instalar el rootkit en modo kernel, utiliza controladores de dispositivo firmados digitalmente que utilizan certificados de clave privada robados de

El uso de Stuxnet como arma cibernética plantea importantes cuestiones éticas y legales sobre el uso de malware para fines militares y de inteligencia. Algunos argumentaron que el ataque era una medida necesaria para prevenir la proliferación nuclear, mientras que otros lo condenaron como un acto de agresión cibernética que violaba la soberanía nacional de Irán.

Conclusiones

El caso de Stuxnet es un ejemplo claro de cómo el ciberespacio se ha convertido en un nuevo campo de batalla. Este ataque cibernético, que tuvo un impacto significativo en la infraestructura nuclear de Irán, demostró que las ciberarmas pueden ser tan destructivas como las armas físicas tradicionales.

En este contexto, la decisión del presidente Barack Obama en 2011 de considerar el ciberespacio como otro tipo de espacio de guerra fue un reconocimiento de esta nueva realidad. Esta decisión marcó un cambio en la política de seguridad de Estados Unidos, reconociendo que las amenazas cibernéticas representan un riesgo real y significativo para la seguridad nacional y global.

Respuesta a las consignas

1. ¿Por qué es importante?
   El caso Stuxnet fue importante por varias razones:
   - **Primera ciberarma destructiva**: Stuxnet es considerado por muchos como la primera ciberarma verdaderamente destructiva. Fue diseñado para causar daño físico a la infraestructura nuclear de Irán, lo que demostró que el software malicioso puede tener efectos físicos reales y destructivos.
   - **Cambio en la guerra cibernética**: Antes de Stuxnet, la mayoría de los ataques cibernéticos se centraban en el robo de información o la interrupción de los servicios. Stuxnet representó un cambio hacia una nueva forma de guerra cibernética, donde los ataques pueden causar daño físico.
   - **Implicaciones geopolíticas**: El ataque a la infraestructura nuclear de Irán tuvo importantes implicaciones geopolíticas. Aunque nunca se ha confirmado oficialmente, se cree ampliamente que Stuxnet fue desarrollado por los Estados Unidos e Israel para retrasar el programa nuclear de Irán.
   - **Despertar sobre la seguridad cibernética**: El éxito de Stuxnet en dañar una instalación nuclear bien protegida sirvió como un despertar para el mundo sobre la importancia de la seguridad cibernética. Destacó la necesidad de proteger las infraestructuras críticas contra los ataques cibernéticos.

   Por todas estas razones, el caso Stuxnet es un hito importante en la historia de la ciberseguridad y la guerra cibernética.

2. ¿Qué pilar y componente fue afectado?

   El virus Stuxnet afectó principalmente dos componentes en las instalaciones nucleares de Irán:

   - Controladores lógicos programables (PLC): Stuxnet se infiltró en los ordenadores conectados a los PLC que controlaban las centrifugadoras y otra maquinaria industrial involucrada en la producción de material nuclear.
   - Centrifugadoras: El objetivo principal de Stuxnet eran las centrifugadoras nucleares iraníes. Estas máquinas, que son esenciales para el enriquecimiento de uranio, fueron manipuladas para autodestruirse. El diseño de las centrifugadoras tenía dos puntos débiles: la resonancia en los rotores y las válvulas de escape.

Estos componentes forman parte del pilar fundamental de la infraestructura nuclear, y su daño causó una interrupción significativa en el programa nuclear de Irán

3. ¿Estuvo involucrado alguno de los elementos que vimos en el encuentro? (ransomware, organización delictiva, etc.)

   El caso Stuxnet es un ejemplo de cómo el ciberespacio se ha convertido en un nuevo campo de batalla, y está directamente relacionado en la clase con la decisión de Barack Obama en 2011 al declarar el ciberespacio como un espacio de guerra.

4. Es posible estimar el monto asociado al evento?

   El virus Stuxnet, conocido por ser uno de los malwares más sofisticados y desarrollados hasta la fecha, causó un daño significativo a la infraestructura nuclear de Irán. Este virus tomó el control de 1.000 máquinas que participaban en la producción de materiales nucleares y les dio instrucciones de autodestruirse. Los expertos afirman que Stuxnet retrasó el programa nuclear iraní provocando grandes daños físicos.

   Sin embargo, los datos exactos sobre el impacto económico del ataque de Stuxnet no se han revelado oficialmente. Dada la naturaleza del ataque y su objetivo, es difícil estimar con precisión las pérdidas económicas. Estas podrían incluir el costo de reemplazar el equipo dañado, la pérdida de productividad durante el tiempo de inactividad y los costos asociados con la investigación y la mitigación del ataque. Además, el impacto a largo plazo en el programa nuclear de Irán podría tener implicaciones económicas significativas. Sin embargo, estos son solo posibles factores y no proporcionan una cifra exacta.

Referencias

- El virus que tomó control de mil máquinas y les ordenó ... - BBC. https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet.
- Los 5 mayores ciberataques de la historia | Deloitte España. https://www2.deloitte.com/es/es/pages/risk/articles/los-cinco-mayores-ciberataques-de-la-historia.html.
- El virus que tomó control de mil máquinas y les ordenó autodestruirse. https://www.latercera.com/noticia/el-virus-que-tomo-control-de-mil-maquinas-y-les-ordeno-autodestruirse/.