UNAH
UNIVERSIDAD NACIONAL
AUTÓNOMA DE HONDURAS

IS-811 | Seguridad Informática

Primer Periodo 2022
Tarea 1-1

Elaborado por:

Tiffany Monique Matamoros Gonzalez

No. Cuenta:

20181002925

Docente:

Ing. Rafael E. Diaz del Valle O.

Índice General

1. Introducción

Las tecnologías evolucionan rápidamente, y esta carrera no deja atrás al malware. En el 2010 se dio a conocer un virus informático que marcó un hito por sus efectos que cruzan la línea entre lo virtual y el mundo real, y por conjugar además elementos tecnológicos y geopolíticos, dando luz de lo que podrían ser las próximas guerras. El virus StuxNet atacó con éxito infraestructura crítica de un país de Medio Oriente dejando rastros que describen un contexto geopolítico del que formó parte, y que ha dado origen a múltiples investigaciones las cuales han servido para la elaboración de esta investigación de la asignatura Seguridad Informática.

2. Objetivos

2.1 Objetivo General

- Conocer que hizo el virus Stuxnet, considerado la primera arma digital de la historia.

2.2 Objetivos Específicos

- Aprender sobre como un virus informático permitió causar estragos en el mundo físico
- Conocer cuáles fueron los efectos ocasionados por el virus, el método de infección y de propagación.
- Conocer un poco sobre la historia de este virus.

3. Marco Teórico

Aparición de Stuxnet.

En esta vorágine, en julio de 2010, un misterioso virus aparece de forma imponente, Stuxnet: la primera arma digital de la historia. Se trata de un enemigo tan eficaz como inquietante, pues su ataque puede llegar a ser devastador y, su atacante, absolutamente anónimo.

Una empresa de seguridad informática bielorrusa fue la primera en descubrir la amenaza. A raíz del hallazgo, los expertos de Symantec, empresa líder mundial en ciberseguridad, analizaron y desentrañaron el código, tardando más de tres meses en hacerlo. Teniendo en cuenta que Symantec emplean entre cinco y veinte minutos para analizar una amenaza convencional, podemos tener una idea de la complejidad de este código.

El virus aprovechaba hasta cuatro vulnerabilidades de día cero, algo absolutamente insólito y desconcertante. Una vulnerabilidad de día cero (ataque día cero) es una brecha -error de programación- en la seguridad del *software*, que puede afectar a un navegador, a un sistema operativo o a un programa cualquiera. Esta vulnerabilidad es aprovechada por el atacante para penetrar y ejecutar un código en dicho equipo o sistema de manera inadvertida para el usuario. Los *día cero* son muy valiosos al ser extraordinariamente inusuales.

Este *software* malicioso incluía además líneas de SCADA, una tecnología para ordenadores que permite controlar y supervisar procesos industriales a distancia: robots, sistemas automatizados, centrales eléctricas y un sinfín de infraestructuras industriales. Algo nunca visto antes por los expertos en ciberseguridad.

El virus también era capaz de dirigir los PLC, controladores lógicos programables,

computadoras usadas para automatizar procesos electromecánicos tales como máquinas de fábricas, sistemas de calefacción, atracciones mecánicas, cadenas de montaje, etcétera.

Es el primer virus informático que permite causar estragos en el mundo físico, los atacantes adquieren control total sobre el equipamiento que gestiona material crítico, lo cual lo hace extremadamente peligroso.

Requirió importantes fondos económicos para ser desarrollado y no existen actualmente muchos grupos que puedan crear una amenaza de este tipo.

Se trata de un complejísimo código que requiere el concurso de diversas tecnologías y la coordinación de equipos multidisciplinares. Los expertos estiman que se necesitaron entre cinco y diez personas, trabajando durante seis meses, para desarrollar este proyecto. Además, los involucrados debían tener conocimiento de sistemas de control industrial y acceso a dichos sistemas para realizar pruebas de calidad, con lo que el proyecto precisó grandes dosis de organización, infraestructura y fondos económicos. En base a esto, los investigadores dedujeron que se trataba de algo tutelado o dirigido por uno o varios Estados o empresas multinacionales.

Una vez conocido todo lo anterior, se concluyó que el virus estaba especialmente diseñado para atacar y sabotear sistemas de control industrial, más específicamente, centrales nucleares.

Ataque letal

Sin motivo aparente, de forma repentina y sin activación previa de alarma o sistema de emergencia alguno, en la central de Natanz, las centrifugadoras comenzaron a actuar de manera muy extraña.

El virus, oculto en el sistema, *observó* cómo trabajaban las centrifugadoras de la central,

registrando los datos generados de ese funcionamiento durante treinta días, como si se tratase de una cámara de vídeo. Luego, cuando su código atacó a dichas centrifugadoras, exhibió esa monitorización, reproduciendo los datos recogidos cuando todo era correcto en los paneles y sistemas de control, para que los técnicos no pudiesen detectar el comportamiento defectuoso que se estaba produciendo. Los treinta días no fueron un periodo elegido al azar, es lo que tardan en llenarse las centrifugadoras de uranio, se trata de un comportamiento notablemente perverso. El virus alteraba, por exceso o por defecto, su velocidad de giro, las reprogramaba. Los sistemas de aviso y el botón de parada de emergencia también estaban controlados y anulados por Stuxnet.

Incluso, cuando los operadores detectaron que la central estaba fuera de control, Stuxnet impidió el apagado de los sistemas.

Central y trabajadores estaban abocados a un final dantesco, a merced del enemigo más etéreo que ha surcado los anales de la historia.

Con el tiempo, la tensión provocada por las variaciones de velocidad provocó que las máquinas infectadas se colapsaran. Las centrifugadoras fueron destruidas sin que los ingenieros supiesen el motivo. La central cerró sus puertas.

Uno de los puntos más misteriosos de este ataque es la forma en la que Stuxnet penetró en la red informática de la central de Natanz, ya que esta no estaba conectada a Internet. Según Symantec, seguramente lo hizo a través de una memoria USB infectada. Esto implica que alguien introdujo, de forma deliberada o inconsciente, el virus en la central de uranio conectando una memoria a un ordenador de la misma: ¿Un ingeniero al que le infectaron el dispositivo de

forma secreta?,¿un técnico que realizó el *trabajo* a cambio de alguna gratificación?,¿alguien que accedió a la central sin ser visto? …nunca lo sabremos. La primera arma digital de la historia había destruido físicamente su objetivo.

Efectos

El objetivo de *Stuxnet.A* es llevar a cabo un ataque dirigido a empresas con sistemas SCADA (ver Nota) que utilicen WINCC de Siemens, con el objetivo de recopilar información.

Para instalarse en el ordenador, aprovecha la vulnerabilidad MS10-046 (CVE-2010-2568). Se trata de una vulnerabilidad de Windows que afecta a los accesos directos y que permite ejecutar código remoto.

Stuxnet.A realiza las siguientes acciones:

- La infección se inicia con varios accesos directos especialmente diseñados para explotar la vulnerabilidad ubicados en un dispositivo USB infectado.
- Los accesos directos maliciosos son los siguientes:

  Copy of Copy of Copy of Copy of Shortcut to.lnk

  Copy of Copy of Copy of Shortcut to.lnk

  Copy of Copy of Shortcut to.lnk

  Copy of Shortcut to.lnk
- Si el ordenador es vulnerable, se descarga y ejecuta automáticamente la librería ~WTR4141.TMP, sin tener que pulsar sobre el acceso directo, ya que dicha vulnerabilidad permite ejecutar código remoto.

- Esta librería se encarga de cargar y ejecutar otra librería, denominada ~WTR4132.TMP, que suelta varios rootkits en el ordenador. Estos rootkits permiten ocultar al gusano y así dificultar su detección.

Nota: SCADA es una aplicación de software especialmente diseñada para funcionar sobre ordenadores en el control de producción, proporcionando comunicación con los dispositivos de campo y controlando el proceso de forma automática desde la pantalla del ordenador.

Método de Infección

Stuxnet.A crea los siguientes archivos:

- MRXCLS.SYS y MRXNET.SYS, en la carpeta *drivers* del directorio de sistema de Windows. Estos archivos corresponden al malware detectado como *Rootkit/TmpHider*. Estos archivos tienen las firmas digitales, supuestamente robadas, de ciertas empresas. El objetivo no es otro que hacerse pasar por archivos legítimos.
- MDMCPQ3.PNF, MDMERIC3.PNF, OEM6C.PNF y OEM7A.PNF, en la carpeta *Inf* del directorio de Windows. Los archivos con extensión PNF son archivos de datos encriptados.

Stuxnet.A crea las siguientes entradas en el *Registro de Windows*:

- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_MRXCLS
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_MRXCLS\0000
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_MRXCLS\0000\Control
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_MRXNET

- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_MRXNET\0000
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_MRXNET\0000\Control
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxCls
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxCls\Enum
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxNet
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MRxNet\Enum
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXCLS
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXCLS\0000
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXCLS\0000\Control
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXNET
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXNET\0000
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MRXNET\0000\Control
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls\Enum
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet\Enum

Mediante estas entradas, los rootkits consiguen registrarse como servicio y ejecutarse en cada arranque del sistema. Además, se inyectan en los procesos LSASS.EXE, SERVICES.EXE, EXPLORER.EXE y SVCHOST.EXE para que no se puedan ver a simple vista.

Método de Propagación

Stuxnet.A se propaga a través de dispositivos extraíbles, como llaves USB, copiando los accesos directos maliciosos en las llaves USB que se conecten a un ordenador infectado. Estos accesos directos se aprovecha de la vulnerabilidad denominada MS10-046 (CVE-2010-2568), que afecta a los archivos con extensión LNK.

4. Conclusiones

Aunque a fecha de hoy no se tengan datos empíricos reales sobre los efectos de las ciberarmas, solo algunos hechos como los de Estonia (2007) y Stuxnet (2010), se cree que no es ciencia ficción y que sus posibilidades pueden ir más allá de una denegación de servicio. Definitivamente Stuxnet llegó a convertirse en una celebridad tecnológica en la geopolítica de los ataques cibernéticos. No se puede negar que el software malicioso se ha perfeccionado progresivamente hasta llegar a la relevancia del célebre Stuxnet, pionero en ataques dirigidos contra importantes instalaciones industriales El dominio del ciberespacio debe considerarse como una dimensión transversal a los otros cuatro dominios reconocidos por los gobiernos (tierra, mar, aire, espacio). A diferencia de los otros cuatro dominios, el ciberespacio fue creado por el ser humano y no debe mezclarse, no son de naturaleza homóloga, de hecho el dominio del ciberespacio es vulnerable a la interrupción generalizada producida por el ser humano. Adicionalmente el dominio del ciberespacio es multidimensional, es decir, no posee límites o fronteras, en su dimensión virtual, sin embargo la infraestructura tecnológica que constituye su dimensión física está sujeta a leyes que enmarcan una soberanía. Cualquiera de estas dimensiones vulneradas pueden afectar no solo a infraestructuras críticas o servicios militares, sino también a los servicios gubernamentales, civiles o comerciales.

5. Referencias

Romero G. (2018). STUXNET: La primera ciberarma de la historia. Recuperado el 27 de enero de 2022, de https://cronicaseguridad.com/2018/05/16/stuxnet-primera-ciberarma-historia/

Panda. Stuxnet.A. Recueperado el 27 de enero de 2002, de https://www.pandasecurity.com/es/security-info/222123/information/Stuxnet.A/

6. Anexos