Ingeniería

Algoritmos Maliciosos

ICS202-01

Ing. Harold Marzán

Informe “Minion Time”

Víctor Toribio

1098632

Santo Domingo, 23 de julio de 2022

Introducción

La proliferación de malware ha sido una realidad de los últimos años a medida que se desarrollan nuevas tecnologías y se mejoran las existentes. Toda esta evolución ha permitido que personas puedan explotar las debilidades, así como modificar o manipular el funcionamiento de los dispositivos que utilizamos diariamente.

Con el propósito de entender el funcionamiento y proceso detrás de la creación de malware es necesario comprender los aspectos claves del desarrollo de estos elementos mediante la realización de un virus para entender las implicaciones y detalles que involucren para luego identificarlos y proteger a los dispositivos de estos.

El presente documento recopila elementos de la creación de un virus con fines académicos

Concepto

Antes que nada, es importante aclarar un concepto fundamental para analizar el virus. El malware desarrollado es un Troyano.

Un virus de caballo de Troya es un tipo de malware que se descarga en una computadora disfrazado como un programa legítimo. Un troyano está diseñado para dañar, interrumpir, robar o, en general, infligir alguna otra acción dañina en sus datos o red.

Un troyano actúa como una aplicación o archivo de buena fe para engañar para ser ejecutado en su dispositivo. Una vez instalado, un troyano puede realizar la acción para la que fue diseñado. Estas acciones pueden incluir:

- Eliminación de datos
- Bloqueo de datos
- Modificación de datos
- Copiando datos
- Interrumpir el rendimiento de las computadoras o redes informáticas

Antecedentes

Los ataques troyanos se han encargado de causar grandes daños al infectar equipos y robar datos de los usuarios. Ejemplos bien conocidos de troyanos incluyen:

- Tiny Banker: Tiny Banker permite a los piratas informáticos robar los datos financieros de los usuarios. Se descubrió cuando infectó al menos a 20 bancos estadounidenses.
- Zeus o Zbot: es un troyano que es bien conocido por propagarse rápidamente y por copiar pulsaciones de teclas, lo que lo llevó a ser ampliamente utilizado en casos de robo de credenciales y contraseñas. Los ataques de Zeus afectaron a grandes empresas como Amazon, Bank of America y Cisco. Los daños causados por Zeus y sus variaciones se estiman en más de 100 millones de dólares desde su creación en 2007.
- Emotet es un troyano que se hizo famoso en 2018 después de que el Departamento de Seguridad Nacional de EE. UU. lo definiera como uno de los

malware más peligrosos y destructivos ya que roba información financiera. 2 ejemplos llamativos son el caso del banco chileno Consorcio, con daños por USD 2 millones, y el caso de la ciudad de Allentown, Pensilvania, con pérdidas por USD 1 millón.

Descripción

El malware diseñado se llama “Minion Time” y consiste en un troyano para Windows, disfrazado de archivo PDF. El resultado del virus es la eliminación ya sea parcial o completa de los archivos encontrados en la carpeta donde se aloja el ejecutable dentro de dispositivo.

El nombre y acciones del virus provienen de la actitud malvada y bromista de alterar el dispositivo infectado, así como lo hacen los Minions.

Cabe destacar que el virus tiene repercusiones variables en función de la criticidad de los archivos que sean contenidos en la carpeta que albergue al virus, haciendo que sea una amenaza indeterminable y variable según el caso.

Detalle

El programa funciona de manera sencilla y clara. El ejecutable ubica el PDF que la víctima pretende utilizar dentro de una carpeta temporal que genera el ejecutable y lo abre para el usuario.

Pasado un tiempo prudente de haber sido abierto el archivo se ejecuta el “happy pack”. Esta función inicia ubicando la carpeta en la cual fue ejecutado el archivo, así como busca una imagen que también está en la carpeta temporal. Luego, se define la estructura de la interfaz de usuario que carga el virus, que consta de un título, una imagen y una barra de progreso que muestra los archivos que va eliminando el virus.

Con esto se pasa a la parte principal, un bucle recorre el listado de archivos del directorio presente y revisa si es un archivo o una carpeta ya que existen métodos distintos para la eliminación de ambos recursos. Si no es posible la eliminación del archivo, se envía un mensaje, de lo contrario el sistema continúa con el siguiente.

Al final de este análisis, se entra un fragmento de código para actualizar y refrescar el progreso de la barra de la interfaz.

Una vez recorrida la carpeta, el sistema muestra un mensaje de la finalización de los archivos y se cierra la interfaz 5 segundos después.

Conclusión

Con la creación de malware es comprensible la facilidad de encontrar puntos de inflexión y debilidad en los programas y que estos, especialmente, se encuentran en la parte de la víctima.

Con esta actividad, es mucho más claro la importancia que tiene el manejo de los aparatos digitales, así como su uso adecuado para procurar la integridad de los mismos y la información que contienen.