Riesgos en la instalación de un sistema operativo Windows no auténtico

Ulises Manuel Cárdenas

Coordinación de los Servicios de Cómputo de la Facultad de Ciencias
ulises.ssb@ciencias.unam.mx

8 de julio de 2019

Introducción

Actualmente los sistemas operativos Windows son un enorme centro de atención para muchas empresas, organizaciones e individuos especializados en la Seguridad Informática, pues según una cuota de mercado realizada en el primer trimestre de 2018[1], más de un 75 % de computadoras en el mundo ejecutan alguna versión del sistema de Microsoft con el *núcleo NT*, es decir, tres cuartas partes de computadoras a nivel mundial funcionan con un sistema operativo de estructura y diseño muy similar por compartir el mismo núcleo, lo cual facilita que las piezas de Software Malicioso[1] (*Malware*) diseñadas para una versión de Windows específica sirvan para infectar a otras versiones del mismo sistema, provocando así que una enorme cantidad de usuarios del sistema, tanto los que lo usan a nivel personal como profesional, sean víctimas de alguna infección por Malware; aunado a esto tenemos que la práctica de realizar una instalación de Windows no auténtica, en la mayoría de los casos, expone al equipo de cómputo y por ende, a la información del usuario contra un potencial atacante. Estos hechos convierten a Windows en un objetivo común para *hackers* de todo tipo, desde los que buscan vulnerabilidades en el sistema para reportarlas con el fin de que sean corregidas (*hackers de sombrero blanco*), hasta los que buscan explotarlas y causar cuyos costos son de millones de dólares a nivel mundial (*hackers de sombrero negro*). Como ejemplo de estas infecciones en los sistemas Windows, se encuentra el ransomware[2] más llamativo de los últimos años y que se dió a conocer en 2017: ***Wanna Cry***, en el que México, según Kaspersky Lab, se posicionó en el onceavo lugar de los países más afectados a nivel mundial por este Malware[2].

Este artículo tiene como objetivo informar de algunos de los *Vectores de ataque*[3] y riesgos más comunes empleados contra usuarios promedio que realizan una instalación no auténtica de Windows. Este artículo se dividirá en dos secciones: en la primera se abordarán las acciones realizadas por el usuario que abren paso a un atacante para entrar en el sistema y los riesgos que esto conlleva; en la segunda sección se mencionan las repercusiones posinstalación de un sistema operativo infectado.

[1] Un programa cuyo fin es el de realizar alguna acción maliciosa
[2] Tipo de Malware que secuestra la información y recursos del sistema de la víctima, y pide un rescate por ellos.
[3] Pasos que el atacante sigue para materializar la amenaza[3]

Vectores de ataque más comunes

A continuación se mencionan algunas técnicas empleadas por los atacantes en las que los usuarios caen y realizan las acciones solicitadas por el atacante, normalmente éste les ofrece una licencia o un sistema operativo activado, a través de *Ingeniería Social*[4]. Algunas de las técnicas más empleadas por los atacantes consisten en engañar al usuario prometiéndole obtener una versión del sistema gratis y totalmente funcional.

Falsos activadores de Windows

Un *Falso activador* es un programa que promete que al ejecutarse en un sistema Windows sin licencia, hará que el sistema funcione como si tuviera una. Posiblemente el riesgo más común está en el momento de descarga del mismo, pues puede tratarse de un programa que no hace lo que dice (un *Troyano*[5]) e infectar el dispositivo donde se está descargando.

Algunos otros activadores podrían sí activar el sistema y durante la ejecución descargar Malware, crear *backdoors*[6] o llevar a cabo cualquier otra acción extra a sólo activar el sistema que pueda perjudicar al usuario, pues usualmente el Malware tiene acceso total a la computadora.

Descarga directa del sistema operativo creackeado[7]

En muchos casos los usuarios caen en sitios web que ofrecen la descarga de alguna versión de Windows *crackeada*, es decir, que ya contiene las modificaciones (también llamadas *parches*) necesarias para que se haga una instalación aparentemente legítima, algunos de los problemas que involucra esta descarga, aún suponiendo que el software efectivamente instala una versión de Windows válida, son:

- Infección del sistema Operativo local
  Se descarga un archivo que promete ser el sistema Operativo, pudiendo ser un *troyano*, tal como se mencionó en anteriormente.
- Instalación de certificados
  El sistema operativo descargado viene modificado con algunos certificados[8] instalados, normalmente creados por el atacante y no por una autoridad certificadora, de manera que ya no se puede confiar en que el sistema operativo verifique correctamente los programas instalados o los sitios web que se visitan, pues éste lo realiza haciendo uso de los certificados, ésta técnica se puede complementar con la redirección a sitios que aparentemente son auténticos (*Phishing*).

[4] Acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas.[4]

[5] Tipo de malware que aparenta hacer algo y que en realidad realiza otra acción

[6] Puntos de acceso silenciosos al sistema por donde un atacante puede conectarse para obtener información.

[7] Crackear: Técnica en que se modifica el comportamiento de un programa con el fin de saltar validaciones.

[8] Un certificado, en computación, es un componente el cual sirve para verificar la autenticidad de una página web o un programa a instalar.

Riesgos posinstalación

Pérdida de soporte por parte de Microsoft (actualizaciones de seguridad)

Al recurrir a una versión crackeada de Windows, en muchas ocasiones, se impiden las actualizaciones automáticas que éste lleva a cabo de manera periódica, bloqueando así parches que protegen al equipo contra vulnerabilidades de seguridad, de ciertas piezas de malware, o bien, de correción de errores de funcinalidad; terminando una experiencia de usuario pobre y dejando al equipo aún más expuesto a un ataque.

Redirección a sitios controlados por atacantes

Si se utilizan técnicas como las antes mencionadas para la instalación de certificados y redirección a páginas no auténticas, un usuario podría intentar acceder, por ejemplo, a su sitio de banca en línea, correo electrónico o redes sociales y ser redirigido a una dirección controlada por el atacante sin notar lo que está sucediendo, pues los certificados en el navegador creerán que el sitio malicioso es auténtico y facilitarán la extracción de información personal o confidencial que el usuario posee.

Control total de la máquina del usuario

Minar Criptomonedas

Minar Criptomonedas consiste en emplear recursos de procesamiento de una computadora para resolver operaciones matemáticas difíciles en una red distribuída y obtener una recompensa (Criptomoneda) que tiene algún valor económico. Si se tiene control total de una máquina es sencillo utilizar sus recursos para minar mientras el usuario sufre de un bajo rendimiento de su propia computadora.

Adware

El Adware es una categoría de programas diseñados para mostrar publicidad y recopilar datos de marketing sobre los usuarios, por ejemplo, qué tipo de sitios web visita, con el fin de mostrarles una publicidad personalizada.

Usualmente el Adware se instala de manera silenciosa, es decir, no es tan evidente su localización en los archivos del sistema; y se ejecutan en segundo plano, haciendo su detección y erradicación más complicada. Normalmente hacen que el usuario tenga bastantes molestias mientras usa su computadora, y por cada publicidad mostrada, el atacante gana una pequeña cantidad de dinero[5].

Ataques colaterales

Los equipos infectados pueden estar organizados para enviar correo basura (spam) a miles de direcciones de correo que han sido recopiladas previamente. Estos correos pueden contener archivos que descargen malware en el equipo del remitente o incluir phishing, también podrían extender su ataque a través de Gusanos[9] a las computadoras en una red hogareña o formar parte de un ataque en masa a una entidad específica.

Botnets

Una Botnet es una red de computadoras con una estructura específica en donde hay una entidad que envía órdenes al resto y éstas últimas obedecen. Las botnets permiten que los cibercriminales centralicen el control de todos los equipos infectados sin que los usuarios lo sepan. También se pueden usar para realizar ataques masivos de SPAM y DDoS[10][6].

Spyware

El Spyware es un término para denominar al software malicioso que recopila información sobre el usuario de una computadora.
Este tipo de malware se ejecuta silenciosamente en segundo plano y recopila información o supervisa la actividad para llevar a cabo acciones maliciosas que afectan al equipo y a su uso, entre los principales tipos de Spyware se encuentran:

- KeyLoggers

  Son aplicaciones que llevan el registro de las pulsaciones de teclas, mediante este método se realiza un seguimiento de cada tecla que el usuario pulsa en el teclado. Normalmente estos programas se utilizan para recopilar información confidencial, como contraseñas o datos financieros, que posteriormente se envían a programas externos para su uso.

- Capturadores de pantalla

  Graban toda la actividad del usuario y ofrecen capturas de pantalla bajo demanda o programadas al atacante. El objetivo es conocer a la víctima para robar su información o para una extorsión que suele buscar beneficios económicos.

- Control total de las cuentas en internet.

  Se hace un seguimiento de todos los movimientos a través de internet de manera silenciosa, obteniendo información sin el consentimiento del usuario, aquí se busca atacar principalmente cuentas personales como las de correo o redes sociales y cuentas financieras, como los portales de banco, desde los que se podría vaciar cuentas o utilizarlas como pivotes y hacer movimientos poco llamativos para una institución.

[9] Malware que se esparce a través de la red

[10] Distributed Denial of Service: Consiste en enviar una cantidad muy grande de peticiones a una misma entidad con el fin de saturarla y afectar así su disponibilidad.

Conclusión

Llevar a cabo la infección a un usuario promedio es una tarea relativamente sencilla para un atacante con experiencia. En la mayoría de casos el Malware tiene la confianza ganada por parte de los usuarios, éstos al creer que el software les dará lo que buscan y cuando el malware solicita Permisos de Administrador[11], el usuario los cede en la mayoría de casos y sin dudar.

Es poco probable que exista un Sistema perfectamente seguro y esto no es un secreto, lo que se busca es mejorar la cultura de la Seguridad de la Información de la población en general, pues al menos en el área de Computación ha habido pérdidas económicas enormes tanto para grandes empresas como para usuarios comunes, por ejemplo, algunas de las cifras obtenidas en 2018 son: el 43 % de los ciberataques son dirigidos a pequeños negocios[7], Windows es el sistema operativo más atacado por hackers y Android es el segundo; 230,000 nuevos malware son producidos cada día, y se predice que este número crecerá[8]. Esto nos muestra la importancia de saber cuidar nuestra información al utilizar una computadora y al estar conectados a Internet y una buena práctica es comenzar asegurándonos que las herramientas que utilizamos, tales como el sistema operativo, es confiable.

Aunque Windows es el sistema operativo más utilizado en el mundo, no todos lo pueden adquirir, sin embargo, esto no significa que la única manera de poseer un sistema operativo es utilizar uno no auténtico, pues existen alternativas que son gratuitas y seguras, por ejemplo, los sistemas basados en GNU/Linux, que tienen muchos beneficios, entre ellos que poseen licencia de código abierto y variantes como Ubuntu son una buena opción para un usuario promedio, por su sencillez de uso.

[11] Permisos solicitados por Windows y que deben ser confirmados por el usuario cuando algún programa requiere hacer una modificación a los archivos del sistema.

Referencias

[1] "*Cuota de mercado de los principales sistemas operativos a nivel mundial en el primer semestre de 2018*", statista.com, https://es.statista.com/estadisticas/576870/cuota-de-mercado-mundial-de-los-sistemas-operativos/

[2] "*México, entre los países más afectados por Wanna Cry a nivel mundial*", Forbes.com, https://www.forbes.com.mx/mexico-entre-los-paises-mas-afectados-por-wanna-cry-a-nivel-mundial/

[3] "*¿Qué es un vector de ataque en ciberseguridad?*", Tecnofor, https://tecnofor.es/que-es-un-vector-ataque-ciberseguridad

[4] "*Ingeniería Social: Corrompiendo la mente humana*", .Seguridad, https://revista.seguridad.unam.mx/numero-10/ingenieri-social-corrompiendo-la-mente-humana

[5] "*Adware*", Karspersky, https://encyclopedia.kaspersky.es/knowledge/adware/

[6] "*Clasificaciones Alternativas*", Karspersky, https://encyclopedia.kaspersky.es/knowledge/riskware/

[7] "*Cyber Security Statistics: Numbers Small Businesses Need to Know*", Small Business Trends, https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html

[8] "24 Estadísticas de Seguridad Informática que Importan en el 2019",Prey Nation, https://preyproject.com/blog/es/24-estadisticas-seguridad-informatica-2019/

[9] "*Spyware*", Malwarebytes.com, https://es.malwarebytes.com/spyware/

[10] "*Falsos activadores de Windows y sus consecuencias en el sistema*", Welivesecurity.com, https://www.welivesecurity.com/la-es/2015/07/24/falsos-activadores-windows-consecuencias-sistema/

[11] "*Categorías de aplicaciones legítimas que pueden ser usadas por ciberdelincuentes*", Karspersky, https://support.kaspersky.com/sp/664#block2