Malware-as-a-Service, el ciberdelito al alcance de cualquiera

Conocida como MaaS, esta modalidad dentro del cibercrimen democratiza la capacidad de realizar cibertataques, convirtiendo en *hacker* a cualquier delincuente aficionado.

El que piense que para convertirse en hacker hace falta tener profundos conocimientos de informática está equivocado. Hoy en día, todo internauta lo suficientemente inclinado hacia el lado del mal puede llevar a cabo una acción de *ransomware* –encriptar la información de los sistemas de la víctima y exigir un rescate- o poner en pie de guerra a un ejército de ordenadores zombis y atacar un objetivo, con las nociones más básicas sobre el uso de tecnología de redes. Y todo gracias a la tendencia *Malware-as-a-Service*.

Como su propio nombre indica, el "*malware* como servicio" o *Malware-as-a-Service* (MaaS) implica poner en manos de usuarios que carecen de destrezas digitales las herramientas y las instrucciones para que puedan poner en marcha ciberataques con éxito. Se trata de kits fáciles de usar que, a cambio de una cantidad de dinero que le pagas al delincuente que lo ha creado, te permiten crear tus propias ciberamenazas profesionales.

El MaaS no es sino una versión maliciosa del modelo de negocio "como servicio" (*as-a-service*), que se ha convertido en una forma de disponer de unos recursos digitales sin la necesidad de realizar inversiones elevadas. Básicamente, consiste en externalizar y contratar a terceros necesidades informáticas que antiguamente se llevaban en el seno de la empresa. Las ventajas que aporta este enfoque es que el cliente siempre dispone del *software* o los sistemas actualizados –sin tener que preocuparse de adquirir nuevas versiones-, y con la posibilidad de escalar cuando haga falta. De esta forma, aparecen conceptos como IaaS (infraestructuras), PaaS (plataformas) y SaaS (*software*), que suponen distintos niveles de prestación de los servicios. A pesar de que se trata de un planteamiento muy centrado en el mundo de la informática corporativa, el término ha dado el salto a otros sectores, como, por ejemplo, la movilidad urbana (*Mobility-as-a-Service*), en donde distintas soluciones de transporte urbano están integradas en una sola plataforma, a través de la cual los usuarios pueden determinar la mejor ruta al mejor precio, eligiendo distintas opciones entre distintos medios que unen dos puntos.

El Malware-as-a-Service (MaaS) implica poner en manos de usuarios que carecen de destrezas digitales las herramientas y las instrucciones para que puedan poner en marcha

ciberataques con éxito

Este formato de alquiler de *malware* bajo suscripción ha democratizado el uso de *botnets*, es decir, robots informáticos alojados en ordenadores infectados que son utilizados para llevar a cabo ciberataques, y ha contribuido a extender su número. Tradicionalmente, los criminales tenían que desarrollar una red de *bots*, primero, escribiendo el código malicioso, y después, intentando que se extendiese lo más posible infectando el mayor número de ordenadores. Era algo complicado y trabajoso, y solamente los ciberdelincuentes especialistas podían llevar a cabo este tipo de acciones delictivas. Hoy en día, el orquestar un ataque de denegación de servicio distribuido (DDoS) –consiste en obligar a miles de *bots* a efectuar simultáneamente solicitudes a un servidor con el fin de inhabilitarlo- es tan fácil y tan accesible como desplegar una campaña de publicidad en internet a través de Google o Facebook.

Un caso destacado de MaaS fue el troyano ZeuS llegó a infectar más de tres millones de equipos en Estados Unidos en el año 2009. El virus se introducía en los dispositivos a través de descargas voluntarias, aunque inintencionadas, mediante *pop-ups* o archivos anexados a correos electrónicos, y abría una puerta trasera, que era utilizada más tarde por el *hacker* para acceder al control total sobre el ordenador infectado. La administración de los equipos zombi se llevaba a cabo vía web por medio de una interfaz intuitiva y sencilla de manejar. Aunque la red que explotaba criminalmente ZeuS fue desmantelada en 2010, el *software* sigue circulando por la red y es utilizado y actualizado regularmente por los ciberdelincuentes.

Otro conocido ejemplo es la red de bots Mirai, un *software* desarrollado en 2016 por un estudiante para hacer dinero a través del juego Minecraft, pero que, tras publicar el código su autor fue utilizado para llevar a cabo ataques DDoS contra los servidores de Microsoft que albergan los juegos propiedad de la compañía.

Una peligrosa oferta de servicios

El auge que está conociendo esta modalidad de ciberamenaza está relacionado con el éxito actual del *Software-as-a-Service* (SaaS) general: rebaja las barreras de entrada al sector, tanto por la reducción de costes que acarrea, como porque elimina la necesidad de tener unos elevados conocimientos técnicos.

El *malware* como servicio puede adoptar distintas modalidades en función de las necesidades del usuario. Por una parte, existe la opción de recibir un producto personalizado, en el que el vendedor configura el software malicioso en función de las necesidades del cliente que va a hacer uso de él. Un ejemplo de este formato es Buer, en el que, a cambio del pago de una tarifa, los desarrolladores diseñan una versión de este *malware* adaptada, con un panel de control muy intuitivo, que describe dónde se están instalados los virus y los muestra por categorías, y permite al usuario gestionarlos cómodamente. Se trata de un servicio muy económico, puesto que en su forma más básica se puede adquirir desde 350 dólares.

Otra opción consiste en alquilar una "granja de *bots*" para fines propios. En este caso, los ciberdelincuentes le arrendan al usuario su propio ejército de dispositivos infectados para que este lleve a cabo acciones por su cuenta, como pueden ser campañas de *spam* o la propagación de archivos infecciosos. Finalmente, otro tipo muy común de ciberamenaza como servicio es el *Ransomware-as-a-Service*. Las acciones de *ransomware* consisten en encriptar mediante un código malicioso los archivos de la víctima y exigir un rescate para liberarlos. Uno de los ejemplos más conocidos es el del virus WannaCry, que en 2017 consiguió infectar más de 230 000 ordenadores en más de 150 países. En este caso, los *hackers* le venden al cliente para sus propios propósitos el acceso al *software* de encriptación, el código y el *back-end* para controlarlo. De esta forma, miles de pequeños delincuentes adquieren el poder de secuestrar y lucrarse con los rescates exigidos.

Las acciones de ransomware consisten en encriptar mediante un código malicioso los archivos de la víctima y exigir un rescate para liberarlos

Para el *hacker* aficionado el *Malware-as-a-Service* no presenta más que ventajas: pone a su disposición unos recursos y una capacidad de ataque que de otra forma no podría tener, proporcionándole además una vía para obtener algunos ingresos procedentes de los ciberdelitos.

Un negocio atractivo

También presenta el MaaS numerosas ventajas para el proveedor del servicio, el *hacker* experto o la organización criminal responsables del costoso y trabajoso desarrollo de *software* malicioso. La más obvia son los ingresos económicos derivados del alquiler del *malware*, y, en su caso, de una posible participación en las cantidades monetarias que reciba el cliente fruto de sus acciones de *ransomware*. A modo de ejemplo, en 2019 se produjo un ataque de ransomware contra la empresa Virtual Care Providers, a la que se exigía una cantidad equivalente a catorce millones de dólares en bitcoins por desencriptar su información. Aunque esta no pagó el rescate, el mismo tipo de *malware* Ryuk que fue utilizado en esa ocasión había generado a los delincuentes casi cuatro millones de dólares en los tres últimos meses de 2018.

Aparte del tema económico, los cibercriminales se benefician de otras cuestiones al alquilar sus recursos, como el poder ejecutar acciones a mucha mayor escala, gracias a todos los usuarios que ponen en marcha campañas con su *software*, y, también, el que la autoría del delito quede diluida ante la proliferación de pequeños delincuentes que hacen uso del mismo software infeccioso.

Una de las principales plataformas de distribución de *malware* como servicio es Emotet, desde donde se lanzan ataques de *ransomware* o troyanos como TrickBot y QBot. Durante la crisis de la COVID-19 han partido desde allí numerosas campañas de *spam*. Emotet –considerado como uno de los troyanos más peligrosos del mundo- roba credenciales de acceso a cuentas de correo en los ordenadores infectados, que luego utiliza para acciones de envíos masivos de correos lanzadas desde robots.

Emotet hace además de nodriza para otro *malware*, facilitando su difusión y la infección por su código maligno. Es el caso TrickBot, que ha evolucionado de ser un conocido troyano especializado en hacer daño en el sector financiero a convertirse en una pieza de *malware-as-a-service*, que ahora es utilizado por numerosos agentes. Como está articulado en distintos módulos, puede ser utilizado de distintas maneras en función de las necesidades del cliente, desde robar datos financieros y credenciales personales, hasta lanzar ataques de *ransomware*. Las campañas de TrickBot se suelen basar en el envío de correos electrónicos maliciosos que contienen anexos infecciosos de programas de Microsoft Office que, al ser abiertos por la víctima, instalan la carga útil del virus en el dispositivo en cuestión. Este *malware* ataca a empresas y particulares, especialmente en Estados Unidos y Europa, y se calcula que puede haber llegado a infectar hasta un millón de ordenadores desde su descubrimiento.

Las campañas de TrickBot se suelen basar en el envío de correos electrónicos maliciosos que contienen anexos infecciosos de programas de Microsoft Office

Por su parte, Qbot es otro troyano, descubierto en 2008, que ha estado especialmente activo entre marzo y agosto de 2020 a través de Emotet, de forma que se calcula que ha afectado al 5% de las empresas del mundo en julio del pasado año. Este *malware* es capaz de robar información de los equipos a los que infecta, incluyendo contraseñas, correos electrónicos, números de tarjetas de crédito y otra información sensible. Entre sus funciones destaca la capacidad para secuestrar los correos electrónicos de los usuarios desde su cliente de Outlook, y usar las direcciones para intentar infectar los ordenadores de los contactos de estos.

Foto de **Markus Spiske** en **Pexels**

Cyberint (2020) "Trickbot Malware-as-a-service". Disponible en: https://blog.cyberint.com/trickbot-malware-as-a-service

Derecho en la Red (2020) "La Botnet ZeuS". Disponible en: https://derechodelared.com/botnet-zeus/

Fink, B. (2018) "Hackers for Hire: The Continued Rise of Malware-as-a-Service" en White Ops. Disponible en: https://www.whiteops.com/blog/hackers-for-hire-the-continued-rise-of-malware-as-a-service

Gooding, M. (2020) "How malware as a service is turning novice hackers into cyber criminals" en Techmonitor. Disponible en: https://techmonitor.ai/cybersecurity/malware-as-a-service-emotet-buer-covid-19

Herranz, A. (2020) "Emotet: un malware de 2014 que está causando estragos en 2020 y sobre el que están alertando las agencias de seguridad de muchos países" en Xataca. Disponible en: https://www.xataka.com/pro/emotet-malware-2014-que-esta-causando-estragos-2020-que-estan-alertando-agencias-seguridad-muchos-paises

Posey, B. (2020) "Malware Is Taking on a New Shape: Malware as a Service" en ITProToday. Disponible en: https://www.itprotoday.com/cloud-security/malware-taking-new-shape-malware-service