La policía alemana cateó ayer la casa del desarrollador de OmniRAT y se apoderó de su computadora portátil, de escritorio y teléfonos móviles, como parte de una investigación sobre un reciente ataque cibernético, según informó THN.

OmniRAT llegó a los medios en noviembre de 2015, cuando su desarrollador lo lanzó como una herramienta de administración remota legítima para que los expertos de TI y las compañías administren sus dispositivos con permisos explícitos.

Disponible entre 25 y 100 dólares, OmniRAT se convirtió rápidamente en una de las herramientas de administración remota más populares, permitiendo a los usuarios monitorear dispositivos Android, Windows, Linux y Mac de forma remota, además de acceder a toda la información disponible en ellos.

Sin embargo, como cualquier otra herramienta de administración remota, como DroidJack, DarkComet, AndroRAT y njRAT, algunos clientes de OmniRAT también utilizaron la herramienta para fines ilícitos, especialmente porque estaba disponible a un precio mucho más bajo que otros RAT en el mercado.

En uno de los eventos a inicios de este año, un grupo de hackers intentó atacar varias industrias explotando una antigua vulnerabilidad de ejecución remota de código (CVE-2016-7262) en Microsoft Excel, que finalmente instaló OmniRAT en las computadoras seleccionadas.

Según un investigador de seguridad que informó acerca del incidente en enero, los atacantes utilizaron una hoja de Excel con formato incorrecto, que se disfrazaba como perfil empresarial de *«Kuwuait Petroleum Corporation (KPC)»*, para atraer a sus víctimas a abrir el archivo adjunto.

Aunque KPC no fue atacada por el malware, otra fuente anónima dijo que hace casi dos meses, los abogados que representan a la compañía petrolera comenzaron a enviar un correo electrónico al registrador de dominios desde donde estaba registrado el dominio oficial de OmniRAT y les exigió que revelaran la identidad del propietario del dominio, citando

las reglas GDPR e ICANN relacionadas con Whois.

El contenido en el sitio web oficial de OmniRAT no ha estado disponible desde los últimos días, lo que probablemente ha sido eliminado por su desarrollador para evitar que su registrador de dominio revele su identidad a la empresa.

Parece que el desarrollador de OmniRAT reside en Alemania, pero su identidad aún es desconocida para el público. En este momento no está claro si la redada policíaca alemana está relacionada con los esfuerzos por la Compañía Petrolera de Kuwuait o si involucra algún caso penal separado en su contra.

También es posible que la policía alemana esté detrás de la lista y la identidad de todos los clientes que compraron OmniRAT en los últimos cuatro años para acabar con los ciberdelincuentes que abusan de la herramienta.

En una operación similar en 2015, las agencias de aplicación de la ley en varios países, allanaron los hogares y arrestaron a presuntos usuarios de malware de teléfonos inteligentes DroidJack.

Al igual que las herramientas de prueba de penetración, las herramientas de administración remota también son una espada de dos filos y se pueden usar para fines legales e ilegales.

En un caso, se informó que hace dos años un grupo de piratas informáticos estaba usando OmniRAT para espiar a los miembros y simpatizantes de ISIS, distribuyendo su versión de Android por medio de la popular aplicación de mensajería Telegram.

Una disolución de responsabilidad, como se observa a continuación, se publicó en el sitio web oficial de OmniRAT, y dice que la herramienta no es para piratería y que los clientes son responsables de cualquier mal uso.

> *«OmniRAT es creado por autores alemanes y los servidores también están ubicados*

> *en Alemania. Por lo tanto, la ley alemana se aplica a nosotros. OmniRAT es una herramienta de administración remota (RAT). No es, como muchos creen, un troyano creado para piratería informática. Por lo tanto, no es ilegal y no viola la ley. Sin embargo, el uso es únicamente lícito en los dispositivos que posee o tiene permiso. Esto también se establece en nuestros términos de servicio. Al comprar y usar OmniRAT, usted cumple con lo anterior».*

Aunque el desarrollador de OmninRAT no parecía haber alentado de forma directa a los usuarios para utilizar la herramienta con fines de espionaje, a finales del año pasado, se publicó una descripción y nuevas características de la herramienta en un foro de hacking, un sitio web famoso entre los novatos para encontrar herramientas de hacking en el mercado.

En el mismo foro de piratería, en abril de este año, anunció el cierre de OmniRAT y dijo que *«desafortunadamente, debido a la presión del gobierno y la división de delitos cibernéticos, OmniRAT debe cerrarse. Esto tendrá efecto inmediato».*

Sin embargo, ya que el funcionamiento de la herramienta no confía directamente ni comparte los datos del dispositivo recopilados con el servidor OmniRAT, los usuarios que ya tienen acceso a la herramienta de administración remota pueden seguir usándola para cualquier propósito.