Publicado en Madrid el 24/04/2023

RapperBot: el gusano dirigido a dispositivos IoT mediante ‘fuerza bruta inteligente’

Los ciberdelincuentes están en constante evolución, buscando nuevas formas de comprometer personas y empresas. Kaspersky ha descubierto una variante de Rapperbot, un gusano basado en la botnet Mirai que infecta dispositivos IoT para lanzar ataques de denegación de servicio (DDoS). Kaspersky también analizó Rhadamanthys, un sistema centrado en el robo de información, y CUEMiner, malware de código abierto distribuido presumiblemente a través de BitTorrent y One Drive

RapperBot se observó por primera vez en junio de 2022, cuando tenía como objetivo el protocolo Secure Shell (SSH), un sistema seguro de transferencia de archivos mediante encriptación. Sin embargo, la última versión del malware se enfoca exclusivamente, y con bastante éxito, a Telnet, protocolo de red para acceder y manejar en remoto otra máquina. En el cuarto trimestre de 2022, los intentos de infección afectaron a 112.000 usuarios de más de 2.000 direcciones IP únicas. Basado en la botnet Mirai, busca infectar dispositivos IoT para realizar ataques masivos de denegación de servicio.

Lo que diferencia a RapperBot de otros gusanos es la manera en que realiza los ataques de fuerza bruta. Lo hace de una forma muy inteligente: comprueba el prompt y, en función del mismo, elige las credenciales adecuadas. Se trata de un formato que acelera el ataque, ya que no ha de revisar grandes listados de credenciales. En diciembre de 2022, los países con mayor cantidad de dispositivos infectados por RapperBot fueron Taiwán, Corea del Sur y Estados Unidos.

Otra nueva familia de malware descubierta por Kaspersky tiene como fuente inicial CUEMiner, un malware open source descubierto por primera vez en Github en 2021. La última versión apareció en octubre de 2022 e incluye un minero propio denominado ‘Watcher’. Este programa monitoriza sistemas y dispositivos de la víctima mientras el usuario inicia programas de cierto peso, como puede ser un videojuego.

Durante las investigaciones realizadas sobre CUEMiner, Kaspersky descubrió dos métodos de propagación del malware. El primero de ellos consiste en su difusión a través de un troyano crackeado que se descarga a través de BitTorrent. El segundo es a través de redes basadas en OneDrive. Como hasta ahora no se han descubierto enlaces directos, se desconoce cuál es el cebo para que las víctimas se descarguen el software. El análisis de los expertos de Kaspersky apunta a técnicas de ingeniería social a través de la plataforma Discord.

El malware es muy popular entre los ciberdelincuentes tanto cualificados como primerizos, ya que permite ejecutar con relativa facilidad campañas masivas. CUEMiner ha dejado víctimas por todo el mundo, también en empresas. La mayoría de ellas, según las métricas que maneja Kaspersky Security Network (KSN), se encuentran en Brasil, India y Turquía.

En cuanto a Rhadamanthys, se trata de un ladrón de información que hace uso de Google Advertising para distribuir malware. Kaspersky ya habló sobre ello en marzo de 2023 y, desde entonces, se ha descubierto una fuerte conexión con Hidden Bee, software orientado a la minería de criptomonedas. Ambos malwares utilizan imágenes para esconderse y tienen códigos de tipo shell similares para activarse. Los dos usan sistemas de archivos virtuales en memoria y el lenguaje de programación Lua para cargar módulos y complementos.

"El malware, su reutilización y el cambio de nombre son técnicas muy utilizadas por los ciberdelincuentes. Los menos avezados pueden ahora ejecutar campañas a gran escala y sobre víctimas de cualquier lugar del mundo. Además, la publicidad maliciosa se está convirtiendo en una tendencia al alza, con una gran demanda entre los grupos de malware. Para evitar este tipo de ataques y proteger a las empresas, es importante conocer lo que sucede en el ámbito de la ciberseguridad y usar las últimas herramientas de protección", explica Jornt van der Wiel, analista sénior de seguridad de GReAT en Kaspersky.

Para protegerse de ataques de ransomware, Kaspersky ofrece estos consejos a usuarios y empresas:

No exponer servicios de escritorio remoto (como RDP) en redes públicas si no es estrictamente necesario. Es importante utilizar contraseñas fuertes en estos servicios.
Instalar siempre que sea posible los parches para las soluciones comerciales VPN que dan acceso remoto a empleados y actúan como puertas de entrada a la red.
Centrar la estrategia defensiva en la detección de movimientos laterales y filtraciones de datos. Se debe poner especial atención al tráfico saliente para detectar las conexiones de los cibercriminales.
Es importante realizar copias de seguridad regularmente y tener un acceso a las mismas en caso de emergencia.
Usar soluciones de seguridad de confianza como Kaspersky Endpoint Detection and Response Expert y Kaspersky Managed Detection and Response, que ayudan a identificar y detener ataques en estado inicial, antes de que los ciberdelincuentes hayan conseguido sus objetivos.
Disponer de la información de amenazas (Threat Intelligence) más reciente para conocer las Tácticas, Técnicas y Procedimientos (TTPs) usadas por los ciberdelincuentes. Kaspersky Threat Intelligence Portal proporciona información y datos sobre ciberataques recopilados en los últimos 25 años. Para que las empresas dispongan de sistemas defensivos efectivos, Kaspersky permite ahora acceder sin cargo alguno a información independiente, actualizada y de todo el mundo sobre los ciberataques y amenazas más recientes. El acceso se puede solicitar aquí.

Aprender más acerca de los nuevos métodos y técnicas de infección utilizados por los cibercriminales en Securelist.

Datos de contacto:
Mónica Iglesias
690 196 537

Nota de prensa publicada en: Madrid

Categorías: Nacional Madrid Software Ciberseguridad Dispositivos móviles