
IOT
Internet of things

Gusano RapperBot lanzando ataques DDOS

Un equipo de investigadores ha descubierto una variante del gusano Rapperbot, que se basa en la botnet Mirai para infectar dispositivos IoT con el fin de lanzar ataques de denegación de servicio mediante una fuerza bruta "inteligente".

En junio de 2022, se encontró por primera vez con Rapperbot, que tenía como objetivo el protocolo Secure Shell (SSH). Se enfoca en Telnet, un protocolo de red para acceder y controlar en remoto otra máquina.

Un grupo de expertos de Kaspersky ha determinado que, esta vez, el gusano basado en la botnet Mirai busca infectar dispositivos IoT utilizando "una fuerza bruta inteligente". El gusano comienza comprobando el "prompt" y eligiendo las credenciales adecuadas en función de él, acelerando el ataque y evitando tener que revisar grandes listados de credenciales.

La última iteración de este gusano fue interceptada en octubre de 2022 e integra un minero propio llamado Watcher que monitoriza los sistemas y dispositivos de la víctima, mientras que esta utiliza programas pesados.

Se difundían a través de un troyano crackeado que se descarga a través de BitTorrent y a través de redes basadas en OneDrive. Finalmente, los expertos de Kaspersky mencionan a Rhadamanthys, un ladrón de información que utiliza Google Advertising para propagar malware.

Apps de streaming convierten Android TV Boxes en Zombies

Una nueva variante de la famosa botnet Mirai, Pandora, apuntó a Latinoamérica, provocó más de 2000 ataques distribuidos de denegación de servicio usando dispositivos esclavizados por malware.

La búsqueda de ampliar el catálogo de películas y series, para ver en esos dispositivos, lleva a algunas personas a no mirar con detenimiento qué aplicación están bajando, o qué página visitan.

Pandora, una nueva botnet emparentada a Mirai

Según se detalla en último ESET Threat Report, estos dispositivos fueron blanco de un malware de tipo troyano emparentado con Mirai, una muy conocida botnet —red de equipos secuestrada por los

atacantes que toman el control y pueden enviarle órdenes diversas, como enviar spam, robar datos o lanzar ataques DdoS.

Su distribución fue principalmente fue mediante las aplicaciones de streaming en sitios web como Tele Latino, You Cine y Magis TV, entre otras. Estas aplicaciones están disponibles no solo para Android Tv Boxes, sino también muchos otros dispositivos, entre ellos, TV Sticks como los de Amazon o Xiaomi. Otra forma detectada es mediante actualizaciones maliciosas de firmware que pueden estar preinstaladas por un revendedor, o que pueden ser instaladas por el usuario desprevenido.

Una vez infectados los dispositivos, los atacantes toman el control y los utilizan para orquestar ataques distribuidos de denegación de servicio (DDoS), es decir, usar cada uno de los miles de zombies que logra infectar para que estos envíen solicitudes dirigidas a un mismo destino y así inhabilitar los servidores del objetivo.

VENENO EN LA CIUDAD

En febrero de 2021, la ciudad de Oldsmar, en Florida, reconoció que una de sus plantas de agua que abastece a los vecinos había sido atacada. Un ciberdelincuente había conseguido acceder a los sistemas de la planta y alterar los niveles de químicos en el agua, con lo que durante unos minutos el abastecimiento pudo llegar a ser de agua envenenada. Afortunadamente, los sistemas de defensa reaccionaron rápido.

No era la primera vez que ocurría. A finales de marzo, el Departamento de Justicia estadounidense acusaba formalmente a un hombre de Kansas de haber intentado atacar a una planta de aguas de su ciudad.

Noticias

GUSANO
TV ZOMBIES
AGUA ENVENENADA