Un hacker publicó una lista masiva de credenciales de Telnet para más de 515 mil servidores, enrutadores domésticos y dispositivos inteligentes de Internet de las Cosas (IoT).

La lista se publicó en un foro de piratería popular, incluye la dirección IP de cada dispositivos, junto con un nombre de usuario y contraseña para el servicio Telnet, un protocolo de acceso remoto que se puede usar para controlar dispositivos por medio de Internet.

Según los expertos y una declaración del mismo pirata informático, la lista se compiló escaneando toda la Internet en busca de dispositivos que estuvieran exponiendo su puerto Telnet.

Estos tipos de listas, llamadas *«listas de bots»*, son un componente común de una operación de botnet de IoT. Los hackers escanean Internet para crear dichas listas y luego las usan para conectarse a los dispositivos e instalar malware.

Estas listas por lo general se mantienen privadas, aunque algunas se filtraron en línea en el pasado, como el caso de 33,000 credenciales Telnet de routers domésticos que se filtraron en agosto de 2017.

Se cree que la lista fue publicada en línea por el responsable del servicio DDoS-for-hire (DDoS booter). Cuando se le cuestionó por la lista masiva, el filtrador dijo que actualizó su servicio DDoS, de trabajar encima de las botnets IoT a un nuevo modelo que se basa en alquilar servidores de alto rendimiento de proveedores de servicios en la nube.

Todas las listas que el pirata informático filtró, tienen fecha de octubre a noviembre de 2019. Algunos de los dispositivos ahora pueden ejecutarse en una dirección IP diferente o utilizar diferentes credenciales de inicio de sesión.

ZDNet identificó dispositivos en todo el mundo utilizando los motores de búsqueda IoT BinaryEdge y Shodan. Algunos de los dispositivos estaban ubicados en las redes de proveedores de servicios de Internet conocidos, pero otros dispositivos estaban ubicados en las redes de los principales proveedores de servicios en la nube.

Un experto en seguridad de IoT anónimo, dijo que incluso si algunas entradas en la lista ya no son válidas porque los dispositivos podrían haber cambiado su dirección IP o contraseñas, las listas siguen siendo increíblemente útiles para un atacante experto.

Los dispositivos mal configurados no se distribuyen de forma uniforme en Internet, pero por lo general están agrupados en la red de un solo ISP debido a que el personal del ISP configura mal los dispositivos al implementarlos en sus respectivas bases de clientes.

Un hacker podría usar las direcciones IP incluidas en las listas, determinar el proveedor de servicios y luego volver a escanear la red del ISP para actualizar la lista con las últimas direcciones IP.