Si quieres saber que contraseñas son más vulnerables para los hackers a la hora de atacar un dispositivo tienes que leer este articulo.

Los hackers al desear atacar un dispositivo, lo primero que van a buscar son contraseñas débiles o predeterminadas.

La compañía de seguridad F-Secure tiene un conjunto de servidores 'honeypot' o trampas establecidos en países de todo el mundo para detectar patrones en los ataques cibernéticos. Esto se logra detectar cuando los hackers están buscando dispositivos para acceder.

Actualmente, estos ataques cibernéticos van en aumento. Hay un creciente número de amenazas a los dispositivos de Internet de las cosas (IoT).

Los hackers se valen de ciertos patrones para acceder a un dispositivo, esto es mediante el puerto SMB 445. Los hackers usan gusanos SMB y exploits como Eternal Blue, así como Trickbot.

Los hackers están a la vanguardia escaneando posibles dispositivos vulnerables, Una vez que lo descubren, lo siguiente que quieren hacer es intentar obtener acceso a él.

Pero, ahora veamos que contraseñas van usar los atacantes al momento de querer acceder al dispositivo:

'1. «admin», una contraseña que realmente no debería usarse para ningún dispositivo.

2. Otras contraseñas incorrectas en la lista incluyen '12345', 'predeterminado', 'contraseña' y 'root'.

3. Contraseñas más probadas, se encontraron los valores predeterminados de fábrica para grabadoras de vídeo digital y dispositivos integrados como enrutadores.

Para que se den una idea, el Centro Nacional de Seguridad Cibernética (NCSC) del Reino

Unido señaló que ‘123456’ una contraseña un poco más complicada se ha encontrado 23 millones de veces en las infracciones. Así que si pensamos en aquellas que no son complicadas, es mucho más fácil acceder a los dispositivos.

Para seguridad. el Reino Unido estableció pautas que sugieren que las contraseñas de dispositivos conectados a Internet del consumidor deben ser únicas y no restablecibles a ninguna configuración de fábrica universal.