PARA | PIENSA | CONÉCTATE® | ARGENTINA

Ministerio de Seguridad
Argentina

DATOS Y CONSEJOS SOBRE BOTS Y REDES DE BOTS

¿QUÉ SON LOS BOTS Y LAS REDES DE BOTS?

No hay duda de que Internet nos facilita la vida y nos conecta con el resto del mundo. Por desgracia, existen ciberdelincuentes que aprovechan la comodidad que la red nos brinda para cometer delitos. Una de las modalidades más comunes de ciberdelincuencia tiene por objetivo infectar a uno o varios dispositivos, convirtiéndolos en lo que se conoce como bots. El origen de la palabra proviene de inglés, (Robot Network), donde la palabra robot indica la capacidad de control inteligente que se puede realizar a distancia.

Una vez que un dispositivo se convierte en bot, puede formar parte de una botnet, es decir una red más amplia de otros dispositivos infectados y controlados remotamente por ciberdelincuentes, quienes la utilizan para obtener beneficios económicos, infectar más dispositivos y/o atacar sitios e infraestructuras. Una botnet puede tener desde unos cientos hasta muchos miles de dispositivos a su disposición.

¿QUE PODÉS HACER?

Protegéte a vos mismo y a los demás, siguiendo estos consejos:

MANTENÉ TUS DISPOSITIVOS LIMPIOS: Procurá mantener actualizado el software en todos los dispositivos conectados a Internet. Todo el software crítico, incluidos los sistemas operativos de computadoras y dispositivos móviles, el software de seguridad y otros programas y aplicaciones de uso frecuente, deben ejecutarse en sus versiones más recientes.

REALIZÁ UNA COPIA DE SEGURIDAD: Protegé tu trabajo, música, fotografías y otra información digital realizando periódicamente una copia de respaldo y almacenándola de forma segura. Tené en cuenta que esta copia puede ser hecha en frío (Cuando se detiene la operatoria del sistema o dispositivo para realizar la copia de respaldo) o en caliente (Continua la operatoria del sistema o dispositivo al realizarse la copia de respaldo)

MEJORÁ TUS CONTRASEÑAS: Si tus contraseñas son débiles, fortalecélas añadiendo mayúsculas, números y símbolos, y utilizando contraseñas diferentes para cada cuenta.

SI TENÉS DUDAS, NO LO ABRAS: Los enlaces enviados a través de correos electrónicos, mensajes y mensajes de texto son, a menudo, la forma en que los ciberdelincuentes intentan robar tu información o infectar tus dispositivos. Incluso si conoces la fuente, si algo parece sospechoso, no lo abras.

CONECTÁ Y ANALIZÁ: Los dispositivos USB y otros dispositivos externos pueden infectarse con facilidad. Por ello, usa tu software de seguridad para realizar un escaneo cuando conectes un dispositivo externo a tus equipos.