Ingeniería social y detección de intrusos en *hacking* ético.

Bots.

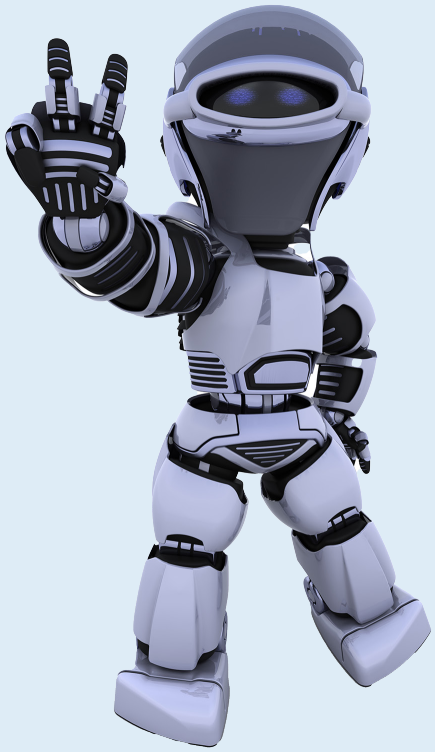
Servicio Nacional de Aprendizaje SENA

Bots.

Las redes de *bots* también se están convirtiendo en una parte importante de los debates culturales sobre la seguridad cibernética. La controversia sobre los anuncios falsos de Facebook y el fracaso del *bot* de Twitter durante las elecciones presidenciales de EEUU en 2016 preocupan a muchos políticos y ciudadanos sobre el potencial perturbador de las redes de *bots*. Estudios publicados recientemente por el MIT han concluido que los *bots* de los medios sociales y las cuentas automatizadas desempeñan un papel importante en la difusión de noticias falsas.

El uso de *botnets* para extraer criptodivisas como Bitcoin es un negocio creciente para los ciberdelincuentes. Se predice que la tendencia continuará, lo que resultará en más ordenadores infectados con *software* de minería y más carteras digitales robadas.

Para entender mejor cómo funcionan las *botnets*, considere que el nombre en sí mismo es una mezcla de las palabras "robot" y "red". En un sentido amplio, eso es exactamente lo que son las redes de bots: una red de robots utilizados para cometer delitos cibernéticos. Los ciberdelincuentes que los controlan se llaman *"botmasters"* o "*bot herders*".



Para construir una red de robots, los maestros de robots necesitan tantos dispositivos en línea infectados o *"bots"* bajo su mando como sea posible. Cuantos más *bots* estén conectados, más grande será la red de bots. Cuanto más grande sea la red de robots, mayor será el impacto. Así que el tamaño importa. El objetivo final del criminal suele ser el beneficio económico, la propagación de *malware* o simplemente la interrupción general de Internet.

Los ciberdelincuentes usan *botnets* para crear una interrupción similar en Internet, ordenan a su ejército de bots infectados que sobrecarguen un sitio web hasta el punto de que deje de funcionar y/o se le niegue el acceso. Este tipo de ataque se llama denegación de servicio o DDoS.

Ataques de botnets

Además de los ataques DDoS, los maestros de los bots también emplean los botnets para otros propósitos maliciosos.

Fraude publicitario

Los ciberdelincuentes pueden utilizar el poder de procesamiento combinado de las redes de *bots* para ejecutar planes fraudulentos; por ejemplo, los responsables de los *botnets* crean esquemas de fraude publicitario ordenando a miles de dispositivos infectados que visiten sitios web fraudulentos y hagan "clic" en los anuncios que allí se publican, por cada clic, el pirata informático obtiene un porcentaje de las tarifas publicitarias.

Venta y alquiler de redes zombies

Los *botnets* pueden ser vendidos o alquilados en Internet. Después de infectar miles de dispositivos, los maestros de los *bots* buscan a otros ciberdelincuentes interesados en usarlos para propagar *malware*. Los compradores de *botnets* luego llevan a cabo ciberataques, propagan rescates o roban información personal.

Las leyes que rodean a los *botnets* y al cibercrimen continúan evolucionando. A medida que los *botnets* se convierten en amenazas más grandes para la infraestructura de Internet, los sistemas de comunicaciones y las redes eléctricas, los usuarios deberán asegurarse de que sus dispositivos estén adecuadamente protegidos de las infecciones. Es probable que las leyes cibernéticas comiencen a responsabilizar más a los usuarios por los delitos cometidos con sus propios dispositivos.