CINCO PASOS PARA PROTEGERSE CONTRA LAS BOTNETS

por El Procurador General Greg Abbott

REDES ROBÓTICAS Y REDES DE ZOMBIS parece un cuento de ciencia ficción, pero no lo es. Desafortunadamente, estos nombres identifican amenazas reales a los sistemas de información en Texas y en todo el mundo.

Invadiendo secretamente las conexiones de Internet, los hackers y spammers pueden descargar programas dañinos, incluyendo spyware y viruses, a las computadoras particulares. Estos programas maliciosos vuelven computadoras comunes y corrientes en robots que pueden ser controlados remotamente. Al establecer una red de computadora robótica, o botnet, los delincuentes cibernéticos pueden espiar a los usuarios, recolectar información confidencial y enviar millones de correos electrónicos basura.

El año pasado, la Procuraduría General le puso fin a la operación de un spammer de Texas que "rentaba" una botnet a distribuidores de correo electrónico basura ilegal. También tomamos acción legal en contra de dos sospechosos que usaron botnets para crear campañas de correo electrónico basura vendiendo activos casi sin valor.

Los expertos en seguridad cibernética estiman que hasta una cuarta parte de todas las computadoras conectadas a la Internet podrían haber sido secuestradas por botnets. Señales de una infección incluyen un funcionamiento lento, fallos frecuentes y una bandeja de salida llena de correos electrónicos que el usuario no envió. Los virus de la botnet y el spyware usualmente no inutilizan las computadoras, porque tienen que estar funcionando y conectadas a la Internet para que la botnet pueda funcionar.

A pesar de esta creciente amenaza, los texanos pueden tomar cinco pasos sencillos para evitar que su computadora sea parte de una red zombi.

Primero, se deben instalar programas antivirus y antispyware. Muchos proveedores de Internet y empresas de software ofrecen programas de protección. La mayoría de los sistemas operativos emiten parches de seguridad periódicamente para corregir problemas en sus programas.

Segundo, los usuarios deben colocar un cortafuegos para bloquear acceso no autorizado mientras la computadora esté conectada a la Internet. Las computadoras sin protección son extremamente vulnerables a invasiones de programas dañinos.

Tercero, los consumidores nunca deben abrir anexos a correos electrónicos o descargar archivos enviados por desconocidos ya que pueden contener programas escondidos para colocar la computadora en una botnet. Además, los usuarios deben saber que los spammers a menudo solicitan información personal por medio de correos fraudulentos que parecen provenir de una fuente legítima, como un banco. Para evitar el robo de identidad y acceso no autorizado a la computadora, los texanos siempre deben tener precaución al descargar o abrir anexos a correos electrónicos.

Los usuarios de computadoras también deben cambiar frecuentemente su contraseña para su cuenta de correo electrónico, cuentas bancarias y demás páginas Internet seguras. Los expertos en seguridad cibernética sugieren usar contraseñas que contengan una serie de caracteres al azar y mezclen letras en mayúsculas y minúsculas con números y símbolos. No se deben usar fechas de cumpleaños o aniversarios en la contraseña o usar la misma contraseña repetidamente.

Por último, los usuarios siempre deben desconectarse de la Internet cuando no están frente a la computadora para evitar acceso a su información y recursos privados.

Los texanos que crean que sus computadoras han sido secuestradas o infectadas por spyware o un virus deben desconectarse inmediatamente de la Internet y usar un programa antivirus o antispyware para revisar completamente la computadora. Los usuarios deben reportar acceso no autorizado a su computadora a su proveedor de servicio de Internet al igual que al Centro del FBI de Quejas de Delitos Cibernéticos en www.ic3.gov.

PUNTOS PARA RECORDAR

PROTÉJASE DE LAS BOTNETS

- Instale programas actualizados antivirus y antispyware.
- Coloque un cortafuegos para proteger contra acceso cibernético no autorizado.
- Nunca abra anexos a correos electrónicos o descargue archivos de fuentes desconocidas.
- Cambie las contraseñas con frecuencia.
- Desconéctese de la Internet cuando no esté usando la computadora.

Reporte acceso no autorizado a su computadora al proveedor de servicios de Internet y al FBI :

Centro del FBI de Quejas de Delitos Cibernéticos
www.ic3.gov

Para más información sobre este y otros temas del consumidor, visite la página Internet de la Procuraduría General en
www.texasattorneygeneral.gov

ATTORNEY GENERAL OF TEXAS
GREG ABBOTT