Source:
Computer World

En la actualidad, se estima que un 96% de las redes han sufrido una infiltración; aunque son necesarias diferentes herramientas para detectar un atacante, hay formas sencillas para percibir actividad sospechosa; esta es la lista de señales que te advierten de que hay hackers en tu red:
Control de equipos y dispositivos

Lo primero que hay que realizar es un análisis de los puertos, fallos continuos de login y otras señales sospechosas. Para ello, lo mejor es controlar qué dispositivos conectas en tu red habitualmente y en qué puertos.

Lo primero es investigar las funciones de administración que parezcan normales; los ciberatacantes han aprendido, y ahora emplean herramientas no sospechosas que no son detectadas por los antivirus. Mediante buenas prácticas de Active Directory, puede investigarse quienes son administradores en el ordenador (u ordenadores en el caso de las compañías) y que herramientas suelen utilizar en cada dispositivo. Con esto, puede detectarse cuando un atacante está controlando una máquina y lleva a cabo tareas administrativas de una manera inesperada.

En la actualidad, no hay ninguna fuente de información que te informe exactamente quién está haciendo labores de administrador y qué está gestionando. Sin embargo, un buen sitio por dónde empezar es la monitorización del uso de las RPC o del protocolo SSH, aunque en algunos casos puedas encontrar falsos positivos.

Diversas cuentas de usuario

Los hackers suelen crearse usuarios para moverse en las redes que quieren; así pues, analiza el uso de las credenciales para encontrar este cambio continuo que podría ser sinónimo de ataque. Para ello lo mejor es analizar el tráfico de la red o analizar la infraestructura de autorización o autentificación. Con ello puede verse con cuantos sistemas interactúa cada usuario.

Rastrea a los usuarios con movimientos sospechosos
Un típico movimiento de hacker es descubrir qué archivos son accesibles fácilmente e intentar encontrar información valiosa o directamente encriptar información de forma remota para poder realizar prácticas de ransomware. Encontrar anomalías en la compartición de archivos es una señal de alerta.

Una buena forma de controlar esto es exigir el login para poder acceder a los servidores de archivos, pero también requiere especialistas que sean capaces de ver anomalías en las historias de los usuarios que acceden.

Analiza la actividad y conexiones

Los hackers necesitan comunicarse desde internet con los endpoints del entorno del ordenador. Aunque ya no es tan común como antes, todavía pueden darse RAT (Remote Access Trojans) por lo que lo mejor es examinar las comunicaciones de entrada y salida. A veces, el malware tiene como objetivo contactar con servicios alojados en la nube como AWS, Azure, o servidores nuevos, por lo que los servicios anti amenaza tradicionales no los pueden reconocer.

Para mejorar la seguridad se puede analizar los logins de DNS para encontrar los patrones de búsqueda de los servidores que indicarían el malware que busca los servidores de control y comando. Las solicitudes incorrectas de acceso continuo son un claro signo de ataque.

Disponible en:

http://cso.computerworld.es/alertas/cinco-senales-que-alertan-de-la-presencia-de-un-hacker-en-tu-red#cxrecs_s [1]

Links
[1] http://cso.computerworld.es/alertas/cinco-senales-que-alertan-de-la-presencia-de-un-hacker-en-tu-red#cxrecs_s