INTERNET SEGURIDAD INFORMÁTICA

Hackers de sombrero blanco: los detectives de la web

19 de febrero de 2017

Los hackers éticos son una especie de detectives digitales. Indagan los sistemas informáticos para encontrar cómo podría haber entrado un intruso con las pruebas que puede haber dejado y tratan de determinar qué puede haber robado.

Los hackers éticos cavan profundamente en los sistemas digitales, examinan los archivos de registro de actividad de los usuarios y deconstruyen el software malicioso. A veces se reúnen con expertos legales, comerciales y en seguridad que añaden contexto a lo que se puede encontrar en el registro electrónico.

La detección de una intrusión

Una investigación comienza cuando se detecta una intromisión no autorizada. La mayoría de los administradores de red configuran los sistemas de detección de intrusos para ayudarles a mantener un ojo en las cosas. Al igual que la alarma de una casa, este software observa áreas específicas de una red, por ejemplo, donde se almacenan datos sensibles.

Cuando ve una actividad inusual (un usuario no autorizado o un alto tráfico de datos), el sistema alerta a los administradores de red. Ellos dan la primera respuesta en ciberseguridad. Reaccionan a la alerta y tratan de averiguar qué hizo que se activara. Esto puede incluir ataques al azar por parte de individuos y grupos pequeños hasta ataques de precisión orientados y bien organizados por hackers respaldados por agencias gubernamentales.

La respuesta inmediata

Las redes y servidores mantienen registros de quién se conecta, de dónde viene la conexión y lo qué hace el usuario en el sistema. La investigación inicial tiende a centrarse en la recopilación, organización y análisis de estos datos. Dependiendo de lo que muestra ese análisis, el administrador puede solucionar el problema de inmediato, por ejemplo, mediante la prevención de que determinado usuario pueda iniciar sesión o el bloqueo de todo el tráfico procedente de un lugar. Pero una cuestión más compleja podría requerir llamar a un equipo de respuesta para incidentes sofisticados.

Lo ideal sería que cada empresa u organización tenga su propio equipo interno o acceso rápido a un equipo externo. Estos equipos son grupos de hackers éticos capacitados para investigar las intrusiones más desafiantes. Por lo general, trabajan para detener el ataque, prevenir futuros episodios y, a veces, dar caza a los atacantes.

La atribución de un ataque

Determinar la identidad o ubicación de un atacante es muy difícil porque no hay evidencia física para recoger u observar. Los hackers profesionales pueden cubrir sus huellas. Las técnicas de atribución de identidad incluyen observar los datos dejados o robados y publicados por los atacantes.

Los programadores se dejan notas entre sí. Los equipos de respuesta pueden analizar la gramática utilizada en esos comentarios. Pueden ver si el texto fue traducido de un idioma a otro. Por ejemplo, en el hackeo al Comité Nacional Demócrata (CND) de Estados Unidos, los metadatos en los archivos indicaron que algunos de ellos contenían texto convertido de los caracteres cirílicos del alfabeto ruso a los caracteres latinos.

Los investigadores pueden incluso identificar las referencias socioculturales que dan pistas sobre quién llevó a cabo el ataque. La persona o grupo que se atribuyó el ataque al CND –usando el nombre Guccifer 2.0– afirmaba ser rumano, pero tenía dificultad para hablar rumano con fluidez, lo que sugiere que no era en realidad un nativo. Además, Guccifer 2.0 utilizaba ")" como emoticon de sonrisa, en vez de ":)", dando a entender que era de Europa del Este.

Las "amenazas avanzadas persistentes" son ataques con tácticas muy sofisticadas desplegadas durante periodos de tiempo. A menudo, los atacantes personalizan el diseño de las intrusiones para explotar las debilidades de sus objetivos. La personalización puede revelar pistas, como el estilo y el lenguaje de programación, aportando datos sobre quién podría ser responsable.

Colaboración

Mientras que los atacantes suelen trabajar solos o en grupos pequeños y en secreto, los hackers éticos operan juntos en todo el mundo. Cuando surge una pista en una investigación, es común compartir esa información, ya sea públicamente en un blog o en un artículo científico, o simplemente con otros investigadores conocidos.

Los hackers más hábiles pueden escribir código de auto-borrado, direcciones web falsas, dirigir sus ataques a través de dispositivos de personas inocentes y hacer que parezca que se encuentran en varios países a la vez. Esto hace que arrestarlos sea muy difícil.

Cuando el ataque es más avanzado, coordinado a través de múltiples plataformas, lo más probable es que sea un esfuerzo patrocinado por un gobierno, lo que hace poco probables las detenciones.

Por supuesto, las sanciones diplomáticas son una opción. Pero señalarse con el dedo entre potencias mundiales es siempre un juego peligroso.

Fuente: Timothy Summers / The Conversation