¿Estáis preparados?

Solución del Reto 5: botnet

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL

Índice

R.5 Solución al RETO 5: formar parte de una botnet y atacar a otra empresa sin saberlo

Este es el material que se ha de entregar al equipo cuando hayan debatido sobre el incidente.

1.1 ¿Qué puedes hacer?

- Desactivar inmediatamente de la red el equipo o servicio vulnerable, si es posible.
- Contactar con personal especializado en ciberseguridad.
- Poneros en contacto con la policía y con Incibe para ver si era algo que hubiera pasado a más gente.
- Realizar una copia cifrada de los ficheros logs (ficheros de registro) de los servidores para aportarlos como prueba en caso de denuncia. Esto nos servirá para alegar que nuestros servidores estaban respondiendo legítimamente a las consultas realizadas por el demandante.
- Preventivamente y antes de restablecer el servicio:
  - realizar una auditoria de seguridad para detectar errores de configuración y vulnerabilidades que pongan en peligro la red;
  - configurar correctamente el servidor DNS para permitir el acceso únicamente desde la red interna;
  - configurar el cortafuegos para separar los servicios internos de los externos, filtrando el tráfico de red.

1.2 ¿Qué no debes hacer?

- Destruir las pruebas del problema. Pueden servirnos como evidencias ante una posible denuncia.
- Cuando hay algo sospechoso o cometo algún error, lo oculto para que no se note y no me echen las culpas.
- Intentar resolverlo yo sólo, sin buscar ayuda. Soy un «manitas».
- Echarle la culpa a otro a ver si cuela.
- No denunciar para evitar que se sepa que he sido objeto de un ataque.

1.3 Lecciones aprendidas: ¿cómo podrías evitarlo?

- Es importante estar preparado por si ocurre un incidente, es decir tener un procedimiento de gestión de incidencias que todo el mundo conozca para saber cómo actuar.
- Utilizar un servicio externo o personal especializado en ciberseguridad para el diseño y mantenimiento de la red y de los servidores de la empresa.
- Realizar auditorías de seguridad periódicas para aseguramos que los servicios web están bien configurados y que no tienen vulnerabilidades.
- Disponer de una política de copias de seguridad que incluya los logs de los sistemas y redes. Hay que hacerlas regularmente, conservarlas en un lugar externo y separado (no conectado) y probar que funcionan y sabemos recuperarlas.
- Tener a mano la lista de contactos de apoyo y de denuncia para estos casos.
- Utilizar el servicio antibotnet de Incibe para averiguar si nuestros equipos forman parte de alguna botnet.

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL