¿Estáis preparados?

Descripción del Reto 5: botnet

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL

Índice

Botnet

R.5 Descripción del incidente de formar parte de una botnet y atacar a otra empresa sin saberlo

Este es el material que se ha de entregar al equipo para debatir sobre el incidente con ayuda de la presentación.

1.1 Escenario

- Trabajáis en una mediana empresa que tiene varias oficinas con ordenadores, red wifi y conexión a internet.
- En vuestra empresa, la información se emplea para las actividades de producción y para contactar con clientes y proveedores, mantener la página web de la tienda online, elaborar las facturas, intercambiar datos con la gestoría (RRHH, impuestos,...).
- Para vuestra actividad tenéis contratada una conexión a internet y disponéis en vuestras instalaciones de un CPD con:
  - el servidor de la página web;
  - el servidor de bases de datos (de ventas y clientes);
  - el servidor de correo electrónico corporativo;
  - el servidor de resolución de nombres interno (DNS) que es el que permite que al escribir la dirección de la intranet y otros servicios de la empresa accedan a ellos;
  - el servidor de cuentas de usuario (LDAP) con el que se validan los usuarios de la empresa cuando acceden a sus puestos.
- Aunque dispones de una persona que se ocupa de algunas tareas informáticas, tienes contratado un servicio externo de mantenimiento.
- Los empleados tienen un horario comercial.

1.2 ¿Qúe ha pasado?

- Recibís una llamada del gerente de una gran corporación que os informa de que está recibiendo grandes cantidades de «tráfico de red» procedente de los servidores de vuestra empresa, entre otras. Este tráfico, está sobrecargando su servidor web colapsándolo y dejándolo inoperativa la web de la corporación.
- Sin saber cómo, les estáis realizando un ataque por denegación de servicio.
- Con la ayuda del soporte externo os dais de cuenta de que tenéis varios errores en la configuración de la red de servidores:
  - Hay un problema en la configuración del servidor de nombres DNS. Está abierto públicamente en internet, aunque está pensado como un servicio interno de la empresa.
  - La red interna y los servidores corporativos no disponen de ninguna protección del exterior (internet), por ejemplo un cortafuegos que pueda servir de defensa.
- Con estos errores de configuración, un ciberdelincuente utilizó los recursos de nuestra empresa para atacar la corporación, enviando tráfico hacia ella.
- Posiblemente el ciberdelincuente habrá instalado un malware para hacernos pertenecer a una botnet, que controla a distancia para enviar tráfico, desde muchas empresas infectadas como la nuestra, a esa corporación y así colapsarla.

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL