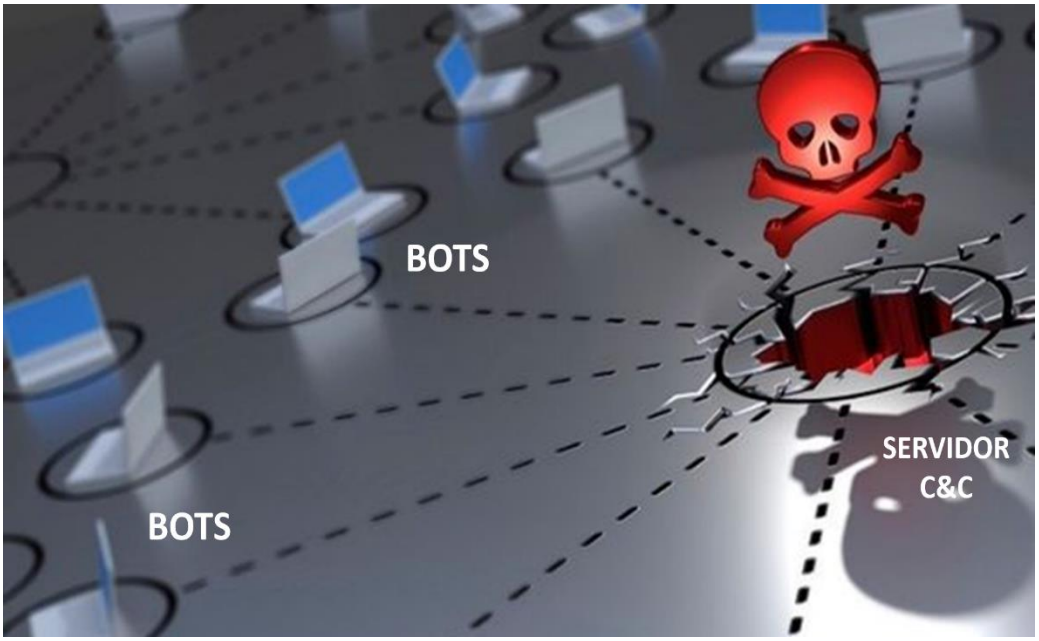
Academia de Ingeniería México

BOTNETS

Botnet es un término que se refiere a una red o conjunto de robots informáticos conocidos como bots.
Los bots (Zombies) son equipos de usuarios infectados con algún tipo de malware, que permite sean controlados de manera remota a través de servidores de comando y control (C&C), los cuales son utilizados por usuarios mal intencionados para enviar instrucciones a los equipos comprometidos.



A continuación, se listan algunas de las actividades de los equipos comprometidos (bots):

1. Robo de información confidencial de equipo infectado.
2. Envío de correo Spam.
3. Publicación de software ilegal, pornografía, repositorios malintencionados, noticias falsas, entre otros.

4. Generación de ataques de Negación de Servicio (DDoS).
5. Publicación de sitios fraudulentos (Phishing).
6. Propagación de ataques (Infección) hacia otros equipos de la red.

De acuerdo con el reporte del CERT (Equipo de respuesta a incidentes de seguridad en computo) de la empresa especialista en seguridad MNEMO, para el mes de abril se detectaron casi 4 millones de eventos relacionados con botnets que afectaron a México.

El reporte se basa en el análisis de los intentos de conexión realizados por bots a servidores de Comando y Control (C&C), a través de la identificación de direcciones IP (Protocolo de internet).
La información obtenida indica los siguientes orígenes de los servidores de comando y control:

Polonia
Estados Unidos
Alemania
Países bajos
Japón
Canadá

Según este reporte el mayor trafico en el mes de abril proviene de USA, también se tiene la información de las direcciones IP de origen (C&C) y los tipos de puerto utilizado, con esta información se puede apoyar las fases de identificación y contención de actividad maliciosa, que permitirá reducir cualquier afectación al respecto.

Recomendaciones

Una vez que se han analizado las direcciones IP de los servidores C&C en conjunto con los puertos utilizados por los bots, se recomienda realizar algunas de las siguientes actividades:

- Generar listas negras que eviten comunicación hacia los servidores C&C.
- Identificar equipos en su infraestructura que presenten comunicación con los C&C listados.
- Implementar dispositivos de seguridad que permitan identificar y bloquear peticiones maliciosas hacia o desde los equipos de su infraestructura.
- Verificar la eficacia de los controles de ciberseguridad implementados.
- Implementar procedimientos para la identificación y gestión de vulnerabilidades en la infraestructura de TI.
- Implementar campañas de información y de concientización de la seguridad de la información dentro su organización.
- Gestionar el apoyo de un equipo de respuesta a incidentes de ciberseguridad, si detectan equipos con actividad maliciosa en su infraestructura.

Es muy importante que los usuarios lleven a cabo las acciones preventivas aquí recomendadas y además que las autoridades mexicanas generen las leyes y normas necesarias en esta materia, para poder contrarrestar el uso de los botnets.

Para cualquier pregunta o comentario, a mi me ubican en Twitter @jfniembro

Y para seguir a Pedro Ferriz de Con háganlo en centralfmonline.com