Botnets: un peligro latente

La red de dispositivos "zombies" que puede afectar a la seguridad electrónica

Por definición, botnet es un término que hace referencia a "un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática". Esta red maliciosa puede poner en peligro toda una instalación de dispositivos de seguridad si éstos no están debidamente protegidos.

Lic. Damián Colaneri
Socio Gerente
T3 Tic Ingeniería SRL

Continuando con nuestra primera nota y para poner en foco la relevancia del conjunto de la seguridad informática y la seguridad electrónica, abordaremos en esta ocasión un tema desde hace muchos años conocido por los expertos en seguridad informática y que desde hace unos meses es motivo de preocupación para la seguridad electrónica: las botnet.

Dado que el propósito de estas notas es el de mejorar la confiablidad de los dispositivos de seguridad electrónica, hablaremos de las botnet sin abordar detalles técnicos ya que es un tema muy amplio. Sin embargo, para lograr comprender cómo esto afecta a los sistemas, ofreceremos algunos conceptos básicos.

¿QUÉ ES UNA BOTNET?

En palabras simples, una botnet es una red de dispositivos (entiéndase como dispositivo a cualquier equipo que pueda conectarse a una red TPC/IP) controlada mediante un software diseñado para tal fin, con el objeto de que todos los dispositivos de esa red ejecuten en conjunto una orden determinada, sumando así la potencia de todos como en un trabajo en equipo.

¿Para qué hacer esto? Tiene muchas utilidades no éticas, entre ellas hacer "caer" los servicios de una empresa. Imaginemos la web del home banking del banco X. Esta web está montada sobre un hardware y software calculado para poder atender, simultáneamente, a mil clientes. Si a este servidor le llegaran dos mil conexiones simultáneas, el servidor colapsaría (mientras las 2000 peticiones estén activas) y no podría atender ningún cliente, por lo cual las personas que quieran operar a través del home banking de ese banco X no podrían hacerlo, generando una gran pérdida de dinero para el mismo.

Ahora, si en la casa del atacante solo hay una PC, que generaría solo una conexión con el banco X, ¿cómo podría éste generar dos mil conexiones simultáneas? Usando una botnet.

Existen botnets de todo tipo y tamaño, desde cientos hasta miles de dispositivos conformándolas. Para poder generar una botnet, primero deben infectarse los dispositivos "víctima" para transformarlos en equipos "zombies" de la red y así hacer que ejecuten nuestras órdenes cuando lo solicitemos. Por ejemplo, atacar al banco X.

Hasta no hace mucho las botnets estaban formadas por PCs infectadas, aunque esto comenzó a cambiar, incluyendo entre los infectados a los dispositivos de seguridad electrónica. Esto se debe a que, al igual que IdC (Internet de las cosas o Internet of things) estos dispositivos con conexión TCP/IP tienen escasa o prácticamente nula seguridad. Por ello es que resulta más sencillo infectar dispositivos como cámaras IP, DVR, NVR y todo dispositivo que estuviera conectado a internet.

TESTEO DE BOTNETS

Para probar estas nuevas botnet basadas en IdC, donde entran los dispositivos de seguridad electrónica, el 21 de octubre de 2016 se hizo público un capítulo de una botnet IdC llamada "Mirai" (1) (futuro en japonés), la que utilizando menos del 10% de su potencia paralizó la costa este de Estados Unidos realizando millones de peticiones al servidor DNS de la empresa DYN, lo cual generó la caída, entre otras webs, de las redes Twitter, Facebook, Github y Spotify.

Según lo explicado en los párrafos anteriores, debemos tomar conciencia de lo peligroso que es una botnet formada con dispositivos IdC y, más aún, cuando estas botnets pueden alquilarse por la cantidad de horas que uno desee en la "deep web" (web profunda) usando una plataforma de ataque diseñada para ser operada por personas que no sean del sector informático y abonando el costo de la misma de forma anónima con bitcoins (moneda virtual). Imaginemos, entonces, el caos que puede generar un empleado descontento realizando un ataque contra su empresa con solo unos clicks.

Es por esto que la seguridad informática de los dispositivos de seguridad electrónica debe ser mejorada. El implementador es responsable de mantener todos los dispositivos actualizados con el último firmware, realizar auditorías sobre los equipos, estar al tanto de nuevas vulnerabilidades del modelo y marca de dispositivos que usa y, en caso de ser necesario, reclamar al distribuidor de la misma para que desde la fábrica se genere un parche. Y es en este último punto donde notaremos una diferencia entre la respuesta de dispositivos de marcas reconocidas con respecto a marcas genéricas. Empresa, rubros y edificios importantes deben comprender que no solo el costo financiero a la hora de adquirir sus dispositivos de seguridad es lo que importa, sino también las pérdidas que pueden generarse por bajar costos sin medir consecuencias, ya sea con productos genéricos y/o integradores no idóneos o certificados.

Como dice el dicho, "en seguridad lo barato puede resultar muy caro".

Para cerrar esta entrega les dejo una pregunta: ¿saben ustedes si en este momento sus PCs y/o dispositivos de seguridad electrónica son parte de una botnet? ■

(1) Si desea conocer más sobre Mirai, el malware realizado para botnet de IdC, el código fuente del mismo es público y está disponible en la web: https://github.com/jgamblin/Mirai-Source-Code.