BOTNETS

1. INTRODUCCIÓN

Una botnet es un conjunto de hosts, conectados a internet, que interactúan con el fin de cumplir una tarea distribuida. Aunque un conjunto de computadores puede ser usado para aplicaciones útiles y constructivas, el término botnet típicamente se refiere a un sistema utilizado para fines ilícitos. Estos sistemas están compuestos por hosts comprometidos que son controladas sin el conocimiento ni consentimiento de sus propietarios.

Los hosts comprometidos comúnmente son conocidos como drones o zombies, y el software malicioso que se ejecuta se conoce como bot.

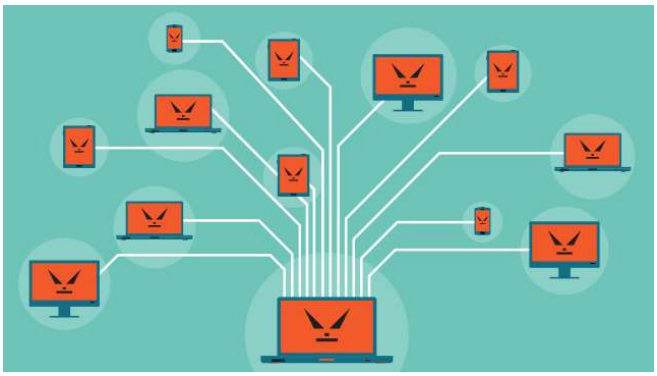

Figura No. 1[1]

2. RIESGO

La propia naturaleza de una botnet da a los criminales mucho poder en internet. Con el control de tantos drones, los *hearders* pueden involucrarse en actividades muy perjudiciales a usuarios de internet, como:

a) Click Fraud

[1] **Fuente:** https://www.kaspersky.com/blog/botnet/1742/

Las botnets pueden ser usadas en *Click Fraud*, donde el software bot puede ser usado para visitar páginas web y automáticamente dar "click" en anuncios publicitarios. Los *herders* han estado usando este mecanismo para robar grandes sumas de dinero a empresas de publicidad en internet, que pagan una recomepensa por cada página visitada. Debido a que los "clicks" provienen de diferentes máquinas alrededor del mundo, aparenta ser tráfico legítimo para un investigador sin experiencia.

b) DDoS

Las botnets pueden ser usadas para causar mucho daño a otros equipos en internet saturando completamente su ancho de banda u otros recursos. Tales ataques de DDoS (Denegación de Servicio Distribuido) pueden impedir el acceso a una página web en particular por largos períodos de tiempo. Esto supone una enorme carga para las operaciones financieras de muchas empresas que no pueden llegar a sus clientes. También ocurren ataques de extorsión, cuando los atacantes demandan un pago a las organizaciones para poner fin al ataque DDoS y permitir el tráfico normal nuevamente.

Los ataques de DDoS son posibles debido a que una botnet otorga recursos de red inimaginables a los criminales. Con la capacidad de establecer muchas conexiones desde miles de máquinas diferentes, su mitigación se hace difícil.

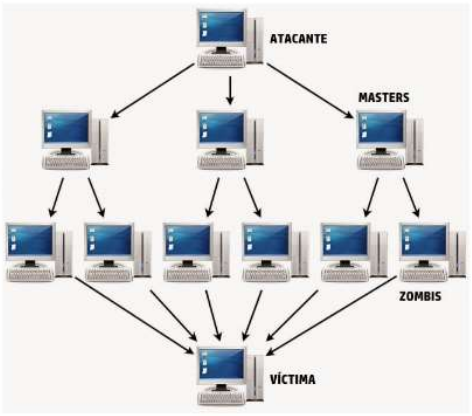

Figura No.2 Ataque DDoS mediante Botnet[2]

c) Keylogging

El keylogging es probablemente la mayor amenaza de una botnet a la privacidad individual. Muchos bots escuchan la actividad del teclado y la reportan lo que la

[2] **Fuente:** http://luisarizmendi.blogspot.com/2014/03/ataques-dos-y-ddos-prevencion-deteccion.html

víctima ha escrito de vuelta al atacante (herder). Algunos bots incluyen software que informa al atacante cuando se ha visitado una página que requiere del ingreso de un password. Esto da al Herder la capacidad de obtener acceso a información personal y cuentas bancarias que pertenecen a miles de personas.

d) Warez

Las botnets pueden ser usadas para robar, almacenar o propagar warez. Warez constituye cualquier software obtenido ilegalmente y/o software pirata. Los bots pueden buscar por software o licencias instaladas en la máquina víctima, y el *Herder* puede fácilmente transferirlo para su duplicación o distribución ilegal. Por otra parte, los drones se utilizan para almacenar copias de warez encontrados en otras fuentes. Como un todo, una botnet tiene una gran capacidad de almacenamiento.

e) Spam

Las botnets a menudo se utilizan como mecanismo para propagar spam. Los drones pueden enviar spam o sitios de phishing, además a través de cuentas de mensajería instantánea se pueden enviar enlaces de malware a todos los contactos en la libreta de direcciones de la víctima. Mediante la difusión de spam a través de una botnet, un *Herder* puede mitigar la amenaza de ser capturado, ya que está usando miles de computadores individuales que hacen el trabajo sucio.

3. DETECCIÓN

Este reporte es una lista de PC's, drones y host zombies que han sido detectados mediante el monitoreo de Controles y Comandos IRC, capturando conexiones IP a botnets HTTP. Muchas de las direcciones IP de este reporte tienen un tipo de infección que serán aprovechadas únicamente para fines de la botnet.

INFORMACIÓN DE LOS CAMPOS DEL REPORTE

Campo	Descripción
Vulnerabilidad	Hace referencia al nombre de la vulnerabilidad
Dirección IP	Dirección IP del dispositivo en cuestión
Puerto	Puerto que responde a la vulnerabilidad
timestamp_EcuCERT	Tiempo en que la IP fue probada por el ECUCERT en GMT -5
AS_name	Nombre del ASN
status_ EcuCERT	Estado de la vulnerabilidad

timestamp	Fecha y hora de reporte de Shadowserver en UTC+0
ip	Dirección IP del host involucrado
port	Puerto desde donde se obtiene la respuesta SSL
asn	ASN donde se encuentra el host involucrado
geo	País donde se encuentra el host involucrado
region	Provincia donde se encuentra el host involucrado
city	Ciudad donde se encuentra el host involucrado
hostname	DNS reverso del host involucrado
type	Protocolo de capa transporte (udp / tcp)
Infection	Nombre de la infección si es conocida
url	URL de conexión (si aplica)
agent	Agente de conexión HTTP (si aplica)
cc	El host de Comando y Control (C&C) que controla esta dirección IP
cc_port	Puerto en el servidor al que la dirección IP se conecta.
cc_asn	ASN del host de C&C
cc_geo	País del host de C&C
cc_dns	DNS reverso del host de C&C
count	Número de conexiones desde esta IP drone o zombie
proxy	Indica si la conexión usa un sistema proxy conocido
application	Nombre de la aplicación o protocolo de capa 7
p0f_genre	Familia de sistema operativo
p0f_detail	Versión de sistema operativo
machine_name	Nombre de host de la pc comprometida
id	Bot ID

4. ACCIONES RECOMENDADAS

- Tener un programa antivirus actualizado instalado en su computadora.
- Permite las actualizaciones automáticas para el sistema operativo.
- Crea contraseñas fuertes y no utilizar la misma o dos contraseñas para todo.
- Solo bajar software gratuito de sitios confiables y oficiales.

- No abrir anexos de correos electrónicos sospechosos, aún si vienen de personas en su lista de contactos.
- Nunca hacer clic en enlaces incluidos en un correo electrónico; mejor cerrar el correo electrónico e ir directamente al sitio de internet de la organización u empresa.

5. REFERENCIAS

- https://www.shadowserver.org/wiki/pmwiki.php/Information/Botnets
- https://www.shadowserver.org/wiki/pmwiki.php/Information/BotnetDetection
- https://www.shadowserver.org/wiki/pmwiki.php/Services/Botnet-Drone-Hadoop
- https://www.fbi.gov/news/espanol/como-proteger-tu-computadora-de-los-botnets