**Universidad Icesi**

Brayan Bejarano

Juan Camilo Jimenez

Juan Pablo Muñoz

Nicolas Taborda

**RESUMEN**

El impacto de internet en nuestras vidas ha llegado de forma abrupta, lo requerimos para todo y tiene solución para casi cualquier tipo de problema; con el internet también llegaron las botnets y por esta razón hablaremos más a fondo sobre ellas, su función y algunos ejemplos en los que han sido utilizadas; Una botnet es una red compuesta por dispositivos que están bajo el control de un nodo principal, conocido como el “botmaster”, éste administra los dispositivos que ha infectado por medio de los cuales puede realizar ataques DDoS, robar información o incluso propagarse y agrandar el alcance de su red. Se establecerán los objetivos alcanzables junto algunos mecanismos que existen para controlar y evitar ataques de Botnet, la implementación de una botnet para ser estudiada de manera práctica y las capturas de

con la muestra de tráfico para posteriormente identificar un ataque de la Botnet.

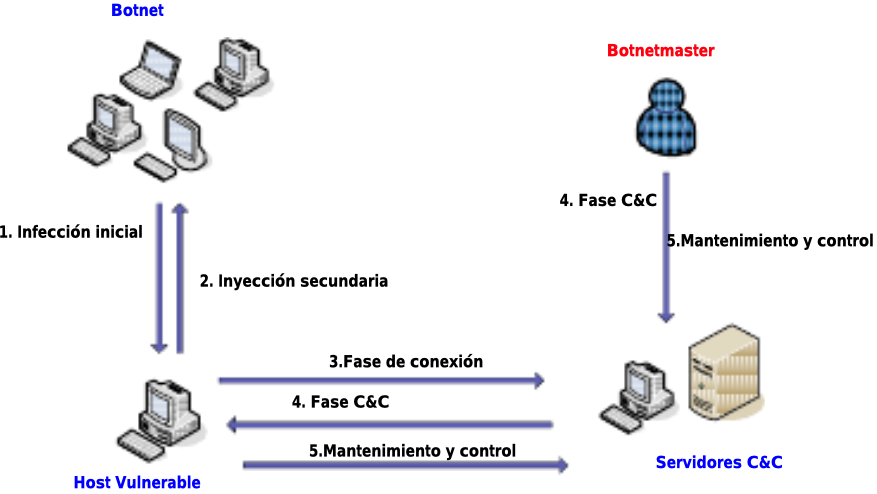
**ABSTRACT**

The impact of the internet on our lives has come abruptly, the requirements for everything and has a solution for almost any kind of problem; with the internet they also came to the botnets and for this reason we will talk more about them, their function and some examples in which they have been used; A network of networks is a network composed of devices that are under the control of a main node, known as the "botmaster", the latter manages the devices that it has infected by means of which it can carry out DDoS attacks, steal information or even spread and enlarge the reach of your network. You can establish the objectives of the network, the implementation of a bot network for the study of the practice and the catches of with the traffic sample to identify and not a Botnet attack.

**INTRODUCCIÓN**

Se hablará del concepto aplicativo de las Botnets y todo lo que ha implicado la búsqueda de información acerca de este tema. Además, se van a presentar situaciones en las cuales las Botnets son las protagonistas. También se dará el resultado acerca del proyecto investigativo y conclusiones del proyecto desarrollado. Por otro lado, se tendrá en cuenta como es el funcionamiento de las Botnets y qué implicaciones tienen en el internet de las cosas.

Los malwares que, aunque parezca un tema del siglo XXI, ha estado presente por más de cuarenta años en el entorno del internet de las cosas y en la programación, pero cuando se habla de las botnets para atacar y robar información que no se encuentra mucha información al respecto, es algo muy reciente y que está tomando gran parte de la seguridad informática. Para entrar un poco más en contexto, como ya se ha tratado anteriormente una Botnet es un conjunto de sistemas que están programados para realizar operaciones en computadores o redes de computadores que están infectadas con estos *malware*, por esta razón se verá el ciclo de vida de una botnet, estas generalmente están definidas en 5 pasos:

1. **Fase de Infección inicial:** Durante este periodo el atacante busca vulnerabilidades en algún host de una subred particular e infecta a la víctima a través de algún método determinado.
2. **Fase de inyección secundaria:** En el host infectado se ejecuta un script llamado “Shell-code”. Éste script incluye una imagen del bot ejecutable (o binario), y se instala a sí mismo. Esto puede hacerlo vía FTP, HTTP o P2P.
3. **Fase de conexión:** Luego de establecer un canal de C&C, el programa se conecta al servidor C&C. Una vez establecida esta fase, el host infectado pasa a ser parte de la red zombie.
4. **Fase C&C**(Command & Control): En esta fase el botnet master utiliza el canal C&C ya establecido para controlar a su red zombi, así los bots reciben y ejecutan órdenes.
5. **Mantenimiento y actualización**: Se les ordena a los bots a descargar actualizaciones. También muchas veces se les ordena migrar a otros servidores C&C, de esta forma, mantiene indetectable a su red.

**HIPÓTESIS O PREGUNTA DE INVESTIGACIÓN.**

El grupo de investigación se da la tarea de desarrollar la hipótesis de que tan complejo puede ser desarrollar una botnet de cualquier tipo y cualquier escala (por motivos educativos y de tiempo será a pequeña escala).

**Objetivos específicos alcanzables y no alcanzables**

**Alcanzables**

* Describir algunos mecanismos que existen para controlar y evitar ataques de Botnet.
* Crear una Botnet centralizada.
* Realizar capturas con la muestra de tráfico para posteriormente identificar un ataque de la Botnet.

N**o alcanzables**

* Desarrollar o implementar un mecanismo para evitar el ataque de una Botnet.

A la hora de poner soluciones, los consejos para protegerse de las botnets y de cualquier amenaza de ciberseguridad se centran en un buen uso de Internet para lo que siempre debes tener en cuenta estas claves básicas:

1. Cambiar regularmente las contraseñas de las cuentas e incluso del acceso al router.
2. Las botnets se aprovechan de la vulnerabilidad de ciertas páginas web, evitar acceder a sitios cuya seguridad esté en entredicho o no estén bien valorados por parte de los internautas.
3. Tener siempre actualizado los sistemas operativos y los programas antivirus instalados en el equipo o dispositivo.
4. Evitar realizar descargas P2P o vía Torrent ya que, en muchas ocasiones, es la principal vía de entrada para las infecciones por botnets.
5. No acceder nunca a enlaces que remitan desde correo electrónico o a través de redes sociales sin tener la seguridad y la fiabilidad del remitente.

Existen varias soluciones que ayudan a mitigar el funcionamiento de las botnets, ya sea antes de su ejecución o durante el proceso, a continuación se mostrarán 4 tipos de soluciones al problema de las botnet y su funcionamiento.

* **HoneyPots:** El honeypot es una estrategia de ciberseguridad dirigida, entre otras cosas, a engañar a los posibles cibercriminales. Ya sea mediante software o a través de la acción humana, el honeypot hace que una empresa pueda simular tener algunas ‘puertas de entrada’ a sus sistemas que no han sido suficientemente protegidas.

De manera previa, una empresa decide habilitar una serie de servidores o sistemas cuyo aspecto parezca sensible. Aparentemente, esa empresa se ha dejado varios cabos sin atar y parece vulnerable. Una vez dejada la trampa, la intención es atraer al atacante, que acudirá a la llamada para intentar entrar. Sin embargo, lo que el cibercriminal no sabe es que, lejos de estar encontrando una puerta vulnerable, en realidad está siendo perfectamente controlado y monitorizado por la empresa en cuestión.

Además se logra obtener un beneficio triple: en primer lugar, contener posibles ataques verdaderamente peligrosos; en segundo, entretener y desgastar al atacante haciéndole perder el tiempo; y en tercero, analizar sus movimientos para detectar posibles nuevas formas de ataque que se estén llevando a cabo en el sector.

* **HoneyNets:** Es un tipo especial de Honeypots de alta interacción que actúan sobre una red entera, diseñada para ser atacada y recobrar así mucha más información sobre posibles atacantes. Se usan equipos reales con sistemas operativos reales y corriendo aplicaciones reales.

Este tipo de honeypots se usan principalmente para la investigación de nuevas técnicas de ataque y para comprobar el modus-operandi de los intrusos.

* **HoneyWall:** Es un mecanismo que posee dos capas : Una capa de control de datos que permite mitigar los ataques a los sistemas que se están colocando como señuelo y una capa de captura de datos, la cual monitorea la actividad de la red.

La capa de control de datos permite ponerle límite a la cantidad de datos que se puedan enviar, los límites utilizan las conexiones salientes en el caso de TCP y el número de paquetes para TCP y otros, pasan los datos por el cortafuegos y pasan por un sistema de prevención de intrusiones. Es capaz de tomar acciones contra el tráfico saliente que tenga ataques conocidos.

Para la captura de datos es requisito capturar toda la actividad del atacante minimizando las posibilidades de que se percate de ello. La actividad en la red trampa es registrada por varias herramientas diferentes. Primero, el cortafuegos registra todas las conexiones entrantes y salientes para proporcionar una perspectiva general de lo que está ocurriendo. Segundo, por defecto un proceso captura toda la actividad de red y todos los contenidos de los paquetes vistos por la interfaz de red interna es enviada mediante paquetes UDP. Tercero, una instancia adicional de Snort escucha en la interfaz interna y genera alertas IDS (Intrusion Detection System).

* **BotHunter:** Tiene como objetivo detectar la actividad de botnet dentro de una red. Lo hace analizando el tráfico de red y comparándolo con patrones característicos de procesos maliciosos. Están basados en un algoritmo llamado correlación de diálogo de red. Fueron desarrollados bajo el programa Cyber-TA en el laboratorio de ciencias computacionales en SRI international.

Monitorea flujos de comunicación entre host y la red. Esta herramienta clasifica los paquetes obtenidos como posibles pasos en el ciclo de vida de la botnet y realiza perfiles de infección que pueden ayudar al usuario a saber si el equipo ha sido comprometido o no.

**ANÁLISIS DE INVESTIGACIÓN, CREACIÓN DE LA BOTNET.**

**METODOLOGÍA**

Para dar paso al segundo objetivo alcanzable del proyecto de investigación se da la tarea de estudiar todo lo relacionado con la creación de una botnet, ya se había estudiado previamente de manera teórica cómo funcionaban las botnet, que tipo de botnet existían y cómo funcionaban, pero la teoría no era suficiente para la investigación de este proyecto así que se decidió desarrollar una botnet con simulación de un DDoS uno de los usos más comunes para las botnets.

Se procedió a investigar como se puede desarrollar y crear una botnet de cero y efectivamente aparecieron miles de videos y tutoriales de como crearlas y en distintos lenguajes, pudiendo ver que estas tecnologías están al alcance de todas las personas que les interese, no se debe de hacer una búsqueda relativamente profunda para poder crear una botnet propia.

La botnet se desarrolló en lenguaje Python v3 ya que es uno de los lenguajes más sencillos al momento de crear una botnet porque funciona con el comando de los equipos sin tener que abrir aplicaciones, siendo así más sigiloso al momento de querer ejecutarse, ahora el DDoS seleccionado fue el flood, éste consiste en enviar muchas solicitudes a una página saturando la de solicitudes hasta el punto se que pueda lograr dejar fuera de funcionamiento la página, todo esto con la suficiente cantidad de equipos infectados.

La Botnet funciona con un servidor y un cliente el cual sería el bot, mediante el comando del equipo se accede a la clase servidor y con comandos de Python se accede y empieza a correr, posterior a esto el servidor está esperando a un bot para poder empezar a hacer algo, así que de igual manera se inicia el bot para que el servidor esté listo para hacer lo que se desea, en este caso un flood, al correr el bot el servidor lo identifica y pide el código para empezar a hacer la inundación, el código s escribe y empieza a enviar solicitudes a la página.

**OBJETIVO DEL PROTOTIPO**

El objetivo de este prototipo es poder mostrar que tan sencillo o que tan complejo pueda ser la creación de una botnet dando cuenta así que cuál es el verdadero peligro que las personas se encuentran al estár en internet y más porque todas las cosas hoy en día tienen internet, y está en constante peligro la información de los usuarios que navegan en internet sin ser conscientes del peligro inminente que pueda estar a su alrededor ya que no son conscientes de estas tecnologías.

**INCONVENIENTES**

No había claridad de qué tipo de botnet se quería desarrollar, además no todas las personas del grupo sabían utilizar el lenguaje de Python, eso complicó las cosas al momento del desarrollo de la botnet, ya después de ver varios tutoriales se encontró una simulación que explicaba el funcionamiento del flood y en qué consiste, posterior a esto se empezó a desarrollar la botnet con este tipo de DDoS.

**CONCLUSIONES INVESTIGATIVAS**

Se puede concluir que la creación de una botnet es relativamente sencilla, sin tener mucho conocimiento o práctica en este tema se puede desarrollar una buena simulación de una botnet la cual permite la visualización de la magnitud de esta problemática mundial del día a día.

Se debe de concientizar a las personas que sean más cuidadosas cuando están navegando en internet ya que no se percatan de los peligros que están alrededor.

Es importante la implementación de los recursos que ayudan con la mitigación de las botnet, las empresas deben de seguir implementando estos seguros para protegerse a sí misma y la información de sus usuarios.

**RESULTADOS**

Después de ejecutar la botnet se procedió a capturar la información mediante la herramienta Wireshark la cual permite obtener capturas del tráfico de cualquier parte del computador, en este caso se analizó el puerto 80 del computador ya que mediante este se escucha el protocolo HTTP dando cuenta así de lo que estaba haciendo la botnet, al ver las capturas de primera instancia se logra ver las diversas solicitudes de HTTP por el método get lo cual nos permite saber que quiere acceder a una página con protocolo HTTP sabiendo así que es un servicio que está en internet y lo solicita repetidas veces en distintos instantes de tiempo como si mandara pulsaciones por intervalos de tiempo.

**CONCLUSIONES**

Se logra comprender el funcionamiento de la botnet y lo eficiente que puede ser entre más equipos infectados se tengan, seguir investigando de como poder crear una botnet P2P y analizar de igual manera su funcionamiento además para próximas investigaciones poder implementar algún método de mitigación para proteger los dispositivos de posibles ataques de las botnets.

**NOTICIA DE INTERÉS**

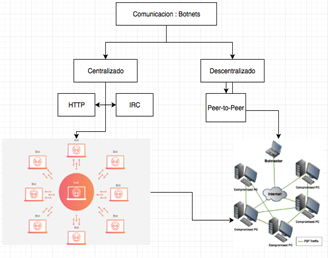
En octubre del 2018 salió una noticia acerca de que *hackers* por medio de Instagram, una reconocida red social, estaban vendiendo cuentas de *Fornite* y también se encontraban vendiendo Botnets, pero detrás de estas acciones que se estaban cometiendo hay una larga historia, ya que las personas que se encontraban comercializando estos “productos” afirmaban que dichas Botnets estaban asociadas con Mirai, un código de botnets que estaba destinado a la infección de equipos que eran parte del *Internet of Things* .

El internet de las cosas cada vez está más presente en todo lugar, ya todas las cosas pueden ser controladas por internet, un claro ejemplo de esto son las casas que todos los electrodomésticos son controlados por medio de internet, esto es el futuro que se veía venir hace tan solo treinta años. Pero, a pesar de que las cosas que nos ofrecen la posibilidad de manejarlas por internet son muy útiles, también se tiene que pensar en los riesgos que conlleva esto, y uno de estos riesgos son las Botnets cómo Mirai.

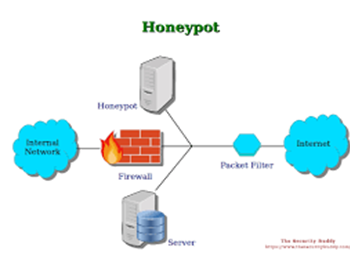
Entrando en contexto Mirai es muy conocida ya que en 2016 esta Botnet se desplegó a millones de dispositivos infectándolos y creando una red llamada Mirai. Velasco (2019) afirma que esta botnet estaba formada por millones de dispositivos, siendo una de las más grandes de toda la red de internet y que era controlada por piratas informáticos para su propio fin. Todos estos dispositivos estaban conformados por sistemas de vigilancia, cámaras IP, termostatos de casas y routers de internet. El mecanismo de infección de esta gran botnet era de que por medio de esta realizaba un proceso automático y con credenciales por defecto como “Administrador” y de tener otro tipo de contraseña se realizaba un ataque de fuerza bruta al dispositivo e ingresar e implantar el “software” malicioso y añadir ese dispositivo a la botnet.

Aunque se había pensado que después de 3 años había desaparecido la botnet después de que los implicados fueran capturados, una nueva botnet derivada de Mirai ha tomado control nuevamente de Mirai y representa una amenaza mayor ya que según Velasco (2019) esta nueva es capaz de realizar ataques DDoS de más de un terabyte por segundo.

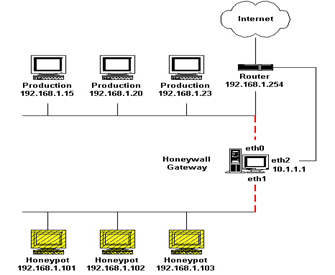
**ANEXOS**

****

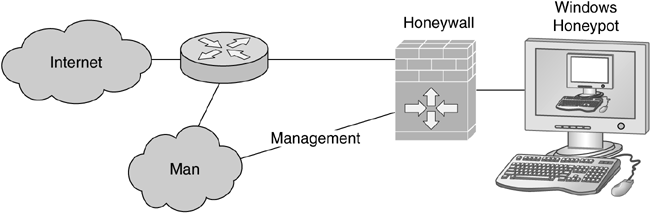
Botnet centralizada y descentralizada.

****

HoneyPot en una red.

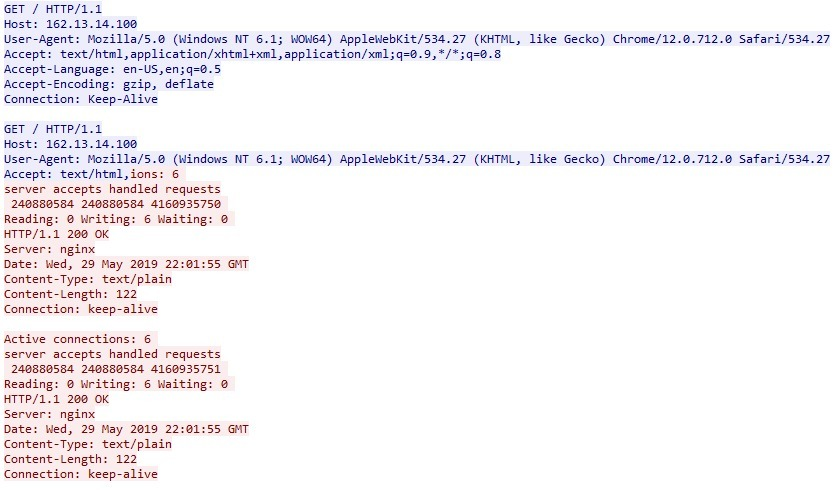
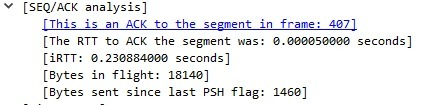
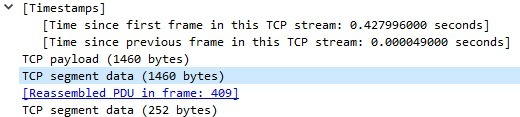
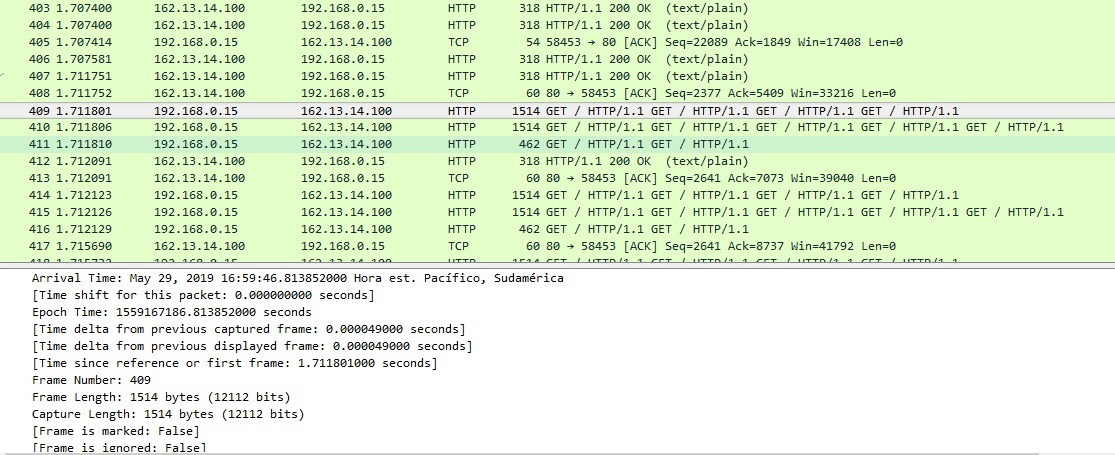
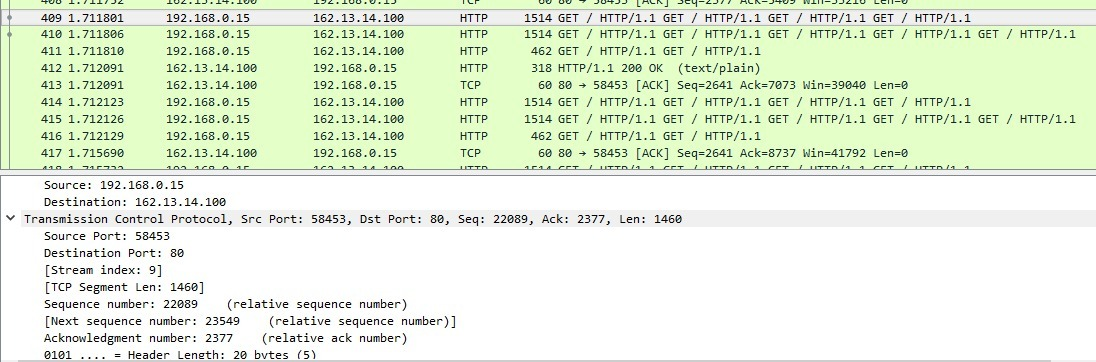


HoneyNet.



HoneyWall.

**Capturas Wireshark**

1. 
2. 
3. 
4. 
5. 
6. 

**Bibliografía**

[1] PandaSecurity (2018, Sept 12) *¿En qué se diferencian el sandboxing y los honeypots?* [En línea]. Disponible en: <https://bit.ly/2QBPa2Z>

[2] Wikipedia (2013, Julio 13). *Honeynet.* [En línea]. Disponible en: <https://bit.ly/30SdaUB>

[3] SorfeForget (2004, May 14). *Conoce a tu enemigo: Honeywall CDROM.* [En línea]. Disponible en: <https://bit.ly/2HMzdED>