El caballo de Troya de nuestra época: Botnets

*Julio Cesar Gaviria Jaramillo*

*Jaiver Andrés Orozco*

*Kevin Balanta*

***Resumen:***

En esta era donde todas las cosas están migrando hacia lo digital, se tiene que tener cada vez más cuidado cuando se navega en internet, ya que, los delincuentes no se han quedado atrás y cada vez sacan partido de las tecnologías y desarrollan nuevas modalidades de ataque para sacar provecho del poco conocimiento de sus víctimas. Es por esto que la investigación presentada a continuación será acerca de los “botnets”, el cual es una modalidad que busca utilizar a sus víctimas sin que ellos se den cuenta, tomando el control de sus dispositivos y utilizándolos para cometer sus delincuencias.

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. También se mencionará cuáles y en qué consisten algunas técnicas para la detección de botnes, tales como, los HoneyPots, HoneyNets, HoneyWall y los BotHunter. Además, por medio de la captura de algunos tráficos de red de un botnet se realizará un análisis para identificar algunos aspectos clave de cómo funciona el ataque de un botnet.

***Abstract:***

In this era, where all things are directed towards the digital, you can have more and more care when surfing the internet, they have been lost, they have been repeated and they have been given the times. An attack to extract the little knowledge of its victims. Thus, the research is translated below is the "botnets", which is a way that seeks to use their victims in your account, as the control of their devices and the use of their crimes. A network of networks is a network made up of devices that are under the control of a main node, known as the "botmaster", the latter manages the devices 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. Also mentioned are the technical characteristics of boots detection, stories like, HoneyPots, HoneyNets, HoneyWall and BotHunter. In addition, the means of capturing some bot network traffic is an analysis to identify some key aspects of how a botnet attack Works.

**INTRODUCCIÓN**

En la actualidad el desarrollo del internet ha traído consigo muchas ventajas para la sociedad y sirve como base de muchas tecnologías que mejoran la vida cotidiana de las personas, sin embargo, la delincuencia ha visto el alcance que el internet tiene sobre las personas y han migrado del mundo real al mundo digital, convirtiéndose en ciberdelincuentes. Estos ciberdelicuentes han mejorado cada vez más las modalidades y formas de cometer ciberdelitos, volviéndose cada vez más difíciles de detectar y evitar.

Una de las ciberamenazas que más ha tenido crecimiento han sido las botnets. Una botnet es una red de dispositivos administrados por un cibercriminal, denominado “botmaster”, el cual es el encargado de administrar el servidor C&C permitiendo realizar ataques DDoS, robo de información e incluso permitiéndole seguir incrementando su red. Las botnets han pasado de ser centralizadas, a ser descentralizadas. Una botnet centralizada es aquella que tiene un nodo maestro, el botmaster, la cual tiene una desventaja y es que, si se cae el nodo maestro, se cae la botnet, por lo que los ciberdelincuentes han desarrollado un nuevo mecanismo de operación aprovechando las redes P2P, la cual es una red descentralizada, donde no se puede saber cuál es el nodo maestro, por lo que es más difícil de que la botnet sea neutralizada.

**Ciclo de vida de una botnet**

La principal caracteristica de un botnet es el ciclo de vida de este. Generalmente se define en 4 pasos:

1. Formation
2. C&C
3. Attack
4. PostaAttack

**Formation**

Se realiza una “inbound scan o exploracion entrante”, donde se descubren las vulnerabilidades del target y se intentan explotar de manera que se pueda comprometer al objetivo, descargando un bot de un servidor administrado por el botmaster.

**C&C**

Comando y control es la jerarquia que define la botnet. Existen dos tipos de botnets :

1. **Centralizados :** Son aquellos botnets que manejan como protocolos principales IRC y HTTP para la comunicacion. Los bots o zombies se encuentran conectados a un solo servidor central. La desventaja es que si el servidor es encontrado, toda la botnet se puede ver comprometida
2. **Descentralizados :** Es un nuevo tipo de comunicación. Surgio cuando los cyber criminales se cansaron de ver que sus servidores estaban siendo atacados constantemente, asi que crearon esta nueva jerarquia, de forma tal que la comunicación fuese establecida entre los bots y uno de ellos tuviese la comunicación hacia el servidor central

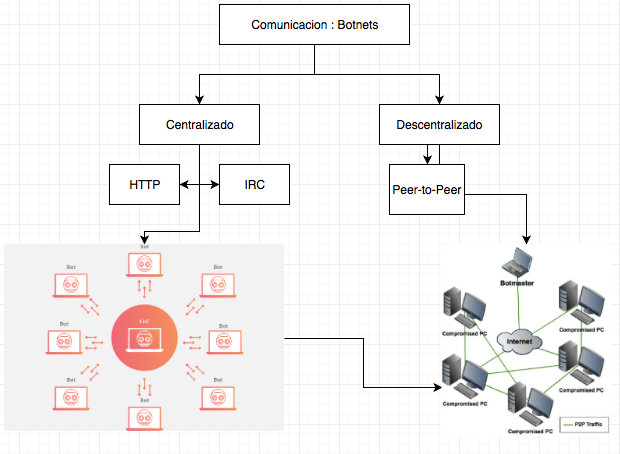


Ilustración 1. botnet centralizada vs descentralizada

**Hipótesis o pregunta de investigación**

La hipótesis sobre el cual se trabajó la investigación radico en cómo detectar un ataque botnet por medio del análisis de trafico de red.

**Objetivos específicos alcanzables y no alcanzables**

**Alcanzables**

1. Describir mecanismos que existen para controlar o evitar ataques de botnets
2. Obtener muestras de tráfico de red aplicaciones de botnet
3. Describir muestras de tráfico de red para tratar de evidenciar un ataque Botnet

**No alcanzables**

1. Llevar a cabo la implementación de un Botnet P2P

**objetivo alcanzable 1**

**Mecanismos de mitigacion y control de botnets**

* **Honeypots :** Son recursos informaticos estrechamente monitoreados cuyo objetivo es tentar al atacante a realizar un ataque, para poder realizar investigaciones sobre sistemas de seguridad en la actualidad. El unico problema esque en algunos paises tienen un uso no autorizado o es ilegal usar esta clase de mecanismos

Estos sistemas pueden ejecutar ciertos componentes y de alli depende su tipo de interaccion de ellos , las cuales pueden ser :

1. **alta interaccion :** Utilizan recursos reales como sistemas operativos y aplicaciones
2. **Baja interaccion :** Permiten emular servicios

****

Ilustración 2. La Honeypot en una red

* **Honeynets :** Es una red de seguridad utilizada para capturar actividad maliciosa y pueden poseer 2 o mas honeypots. Cualquier interaccion con una honeynet puede ser maliciosa.

****

Ilustración 3. La Honeynet

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

****

Ilustración 4. La Honeywall

* **Bothunter :** Son sistemas diseñados para la deteccion de botnets. Estan basados en un algoritmo llamado correlacion de dialogo de red. Fueron desarollados bajo el programa Cyber-TA en el laboratorio de ciencias computacionales en SRI internacional.

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

**Analisis investigacion “botnet command detection using virtual honeynet”**

Uno de los principales logros de esta investigacion, fue que encontraron los comandos mas utilizados por los atacantes a la hora de manipular su red, entre ellos tenemos :

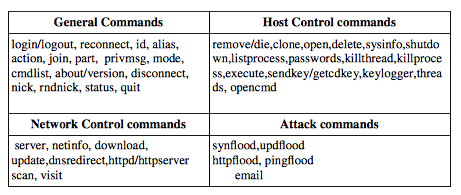


Ilustración 5. Lista de comandos

* **General Commands :** Son comandos generales utilizados por el atacante. Pueden tener diferentes usos
* **Host Control commands :** Son comandos de manejos de host utilizado generalmente por el cyber criminal
* **Network Control commands :** Son comandos utilizados por el atacante para obtener informacion de la red
* **Attack commands :** Son comandos utilizados para realizar ataques syncronizados a servidores u targets primordiales, de los cuales el atacante requiere algun servicio.

Ellos en esa investigacion desarollaron un algoritmo basado en el comportamiento de la red en tiempo de ejecucion de los bots y en la secuencia utilizada en la conversacion entre el bot y el servidor de C&C. A su vez desarollaron un prototipo de recoleccion de malware. El objetivo de ese prototipo era recoger la mayor cantidad de binarios como sea posible

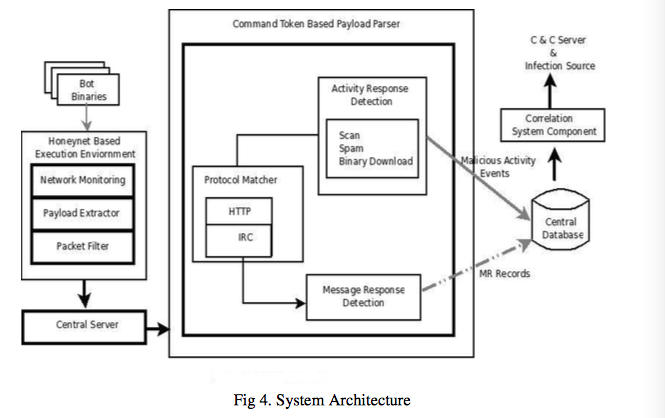


Ilustración 6. Arquitectura utilizada para la recolección de malware

En la entrada de su sistema permitian el ingreso de codigos binarios de bots que se recopilaban a travez del sistema de la red señuelo o honeynet. Su sistema se componia de 3 entes principales :

1. Ejecucion basada en una honeynet
2. Analizador de carga util
3. Componente del sistema de correlacion

Una vez recopilaban el malware , lo pasaban al motor de Symantec Anti-Virus para clasificarlos como ejemplos de bots y no bots. Luego estos binarios los pasaban automaticamente a un entorno de analisis abierto basado en una honeynet.

**Funcionamiento**

Aquellos investigadores ejecutaban codigos binarios durante 30 minutos utilizando diferentes marcas de tiempo. Configuraron un entorno Vmware ejecutando una instancia de windows XP. Asiggaron una direccion IP publica y estatica e infectaron un bot durante media hora.

El entorno de ejecucion basado en la Honeynet les permitia inyectar una muestra de bots maliciosos en un sistema y volver a conectarlo a su destino original. Lo anterior les permitia aislar el bot de la red y monitorear su trafico de una manera controlada en lugar a esperar a que se infecte , para luego poder monitorear el trafico de forma pasiva

Se utilizo un HoneyWall para capturar todo el trafico de red y poderlo combinar en un archivo PCAP para poderlos enviar al servidor central para su posterior analisis

**Extractor de carga util**

Luego de la ejecucion del bot binario, se extrae la carga util y se envia al servidor central para poderlo analizar, permitiendole al investigador extraer las firmas de token de comandos con respecto a la comunicación IRC o HTTP

**Filtro de paquetes**

Un primer filtro que los investigadores hicieron fue seleccionar los paquetes basados en TCP ( ya que muchas de las botnets atacan puertos dedicados a TCP)

El segundo filtro fue eliminar el paquete que contenia los indicadores o banderas SYN y RST, debido a que estos podian indicar que la comunicación nunca se establecion y no proporcionarian informacion util.

**Objetivo del prototipo**

El objetivo de su prototipo era recolectar la mayor cantidad de codigos binarios cambiando los servicios y configuraciones de los honeypots. Propusieron un sistema de recoleccion que recopila malwares para ser analizados dinamicamente. Ademas , su sistema proporcionaba proteccion contra la participacion significativa en ataques. Para ello utilizaba el firewall y tecnicas de prevencion de intrusiones

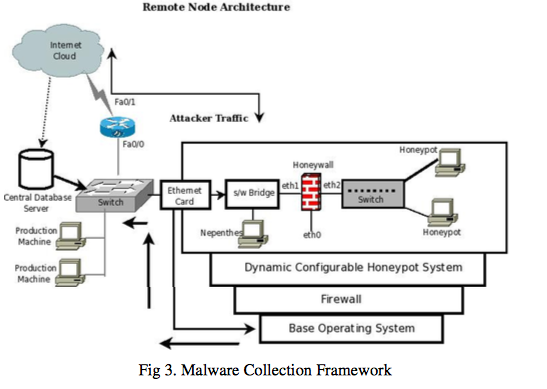
****

Ilustración 7. Arquitectura de la red para la recolección de malware

**Inconvenientes**

En esta investigacion proponian seguir realizando estudios acerca de como implementar esto a una escala mas robusta y de mayor dimension, ya que para ellos fue dificil implementar uno a escala reducida.

**Conclusion de esta investigacion**

Por una parte obtuvieron que la comunicación IRC es con direciones ip especificas. Las secuencias de seguimiento de TCP incluyen el USUARIO, NICK , MODO, UNIR

En el caso de las botnets HTTP, se observaron que la comunicación entre bots con el server C&C era basado en parametros GET, HEAD y POST. En algunos casos se descargaban algunos ejecutables.

**otras noticias de interes**

En Panama , un grupo de investigadores realizaron una investigacion para saber que tantos servidores de botnets se encontraban en esta ciudad. Su hipotesis se basaba en que como Panama se basa principalmente en un sistema economico movido mayoritariamente por sistemas informaticos, podria ser muy propenso a ataques de cyber criminales

Realizaron dos prototipos, uno basado en una Honeynet colocada en una red universitaria al cual le anexaron unm BotHunter y el otro, una Honeypot colocado en una red residencial

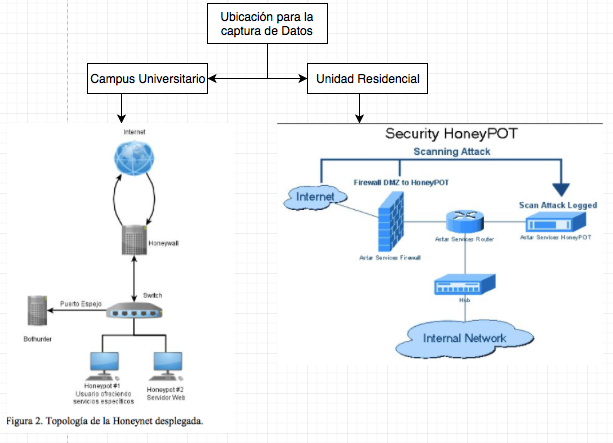


Ilustración 8. Plataformas de captura

Pudieron evidenciar que el numero de conexiones era extremadamente alto y la prioridad se daba en el puerto 445 que era de tipo TCP

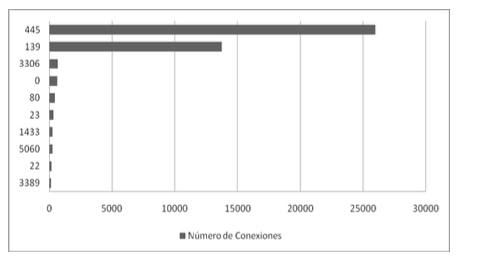
****

Ilustración 9. Número de conexiones

En esa investigacion proveen diferentes tablas con informacion valiosa para el lector. Se dejaran como anexos para no saturar el documento de imágenes.

**objetivo alcanzable 2 y 3**

**Metodología**

Para lograr el objetivo 2 propuesto con anterioridad, se ingresó a páginas como “Malware-Traffic-Analysis” y a “Contagiominidump” las cuales sirvieron como fuentes para obtener las capturas de tráfico de red de diferentes tipos de botnet en diversas situaciones y fechas.

Durante la investigación, se logró obtener 4 capturas de tráfico de red, estas capturas eran de bots tipo nercus. Nercus es una red de bots que distribuye malware, por medio del correo no deseado, al revisar cada una de estas capturas logramos evidencias que a pesar de que todas eran ataque de bots por medio de Spam, y que tenían lugar en diferentes fechas, estaban utilizando distintos protocolos, por ejemplo: en la captura que se realizó el 3 de abril del 2018 se estaba utilizando un protocolo snb2 el cual es un protocolo la inyección y ejecución de código remoto, mientras que en otras capturas se utilizaba protocolos como TCP o HTTP.

Para lograr el objetivo 3, lo que se realizó fue organizar y seleccionar las captura de botnets obtenidas, y utilizar la herramienta WireShark el cual permite ver o analizar el tráfico que ocurre en la red, para observar las 4 capturas obtenidas, y así seleccionar dos sobre las cuales se iba a analizar más exhaustivamente.

**Resultados**

Después de obtener las capturas se seleccionaron dos, la primera que se analizó fue la captura del 13 de junio del 2018. Esta captura era de botnets tipo Necurs, y utilizaban archivos “.IQY” estos archivos son normalmente archivos de Excel, lo cuales contienen grandes listas de parámetros para realizar consultas a internet, Además como grupo inferimos que por medio de los macros que se ejecutan en Excel, es que se propaga el software “Ammy”, el cual es un software que se utiliza para acceder al escritorio de un pc de forma remota, utilizado así por ciberdelincuentes como un RAT (Remote Acces Trojan).

Al analizar las capturas de tráfico, como grupo lo que inferimos que ocurre es que después de que alguien descarga el archivo del correo no deseado, se ejecutan lo archivos IQY lo cuales por medio de los macros se encargan de esparcir un software malicioso. En un principio en la captura se realiza una solicitud a un Servidor DNS, preguntando por la página brtt7, seguidamente el servidor DNS le responde con la dirección ip 47.74.153.72, una vez tiene la dirección ip de la página web, se establece una conexión utilizando el acuerdo de 3 vías, todo este proceso se logra evidenciar en la Ilustración 1. Análisis tráfico, después de establecer dicha conexión, la fuente empieza a enviar solicitudes a la página web, la cual acepta las solicitudes, sin embargo le dice que no hay contenido así como se logra apreciar en la Ilustración 2 Análisis tráfico, hasta que la fuente le solicita la ruta específica /preload.gif, en este momento la página web acepta la solicitud así como se logra evidenciar en la Ilustración 3 Análisis tráfico, y por medio de la ejecución de los macros de Excel solicita que se salga de la hoja de Excel y ejecute la consola, y por medio de esta abre el PowerShell y crea un objeto de tipo WebClient, sobre el cual invoca unos métodos para descargar un archivo infectado (Ammy admin) de una página web, la cual es “http://brtt7.com/load.gif\”)” esto se puede observar en la Ilustración 4. Ejecución código, al revisar esta página efectivamente se encontraba fuera de servicio, por lo tanto, decidimos investigar si había sido reportada por algún antivirus, para esto utilizamos la página virusTotal y efectivamente había sido reportada por 7 antivirus como se observa en la Ilustración 5. VirusTotal.

**Conclusiones**

Como trabajos que quedan a futuro, tenemos no solo seguir investigando más sobre la nueva tendencia de botnets descentralizados P2P, sino también llegar a la implementación de un botnet P2P en phyton.

**Referencias**

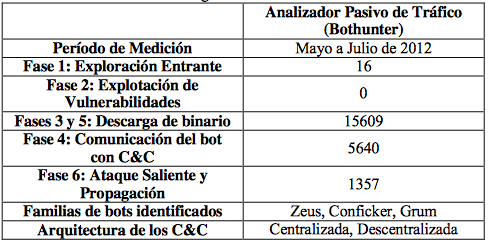
[1]https://www.researchgate.net/profile/Mario\_Gongora\_Blandon/publication/268196271\_Estudio\_de\_Medicion\_de\_la\_Actividad\_de\_Botnets\_en\_la\_Republica\_de\_Panama/links/54636f520cf2837efdb30889/Estudio-de-Medicion-de-la-Actividad-de-Botnets-en-la-Republica-de-Panama.pdf

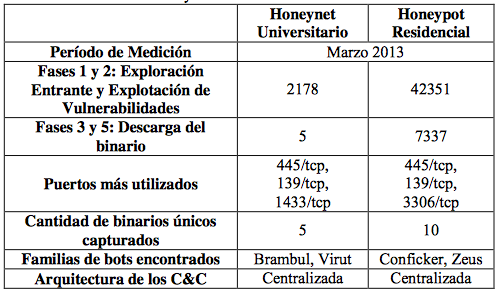
[2] Detecting P2P Botnets through Network Behavior and Machine Learning (2011)

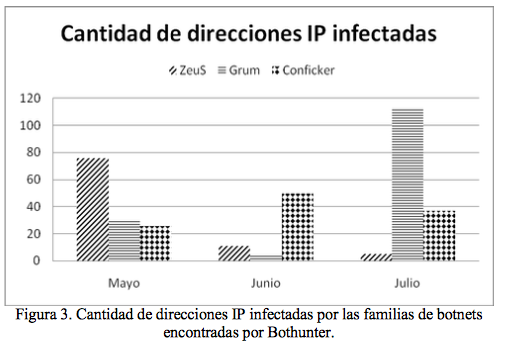
[3]https://pdfs.semanticscholar.org/d8a4/f03eac099a35ec90f6b2eb0b1259c7a15178.pdf

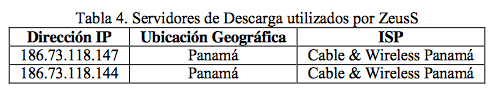
**Anexos**

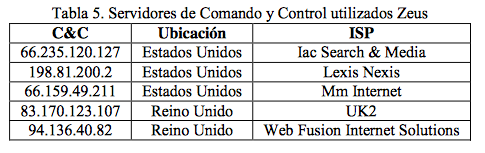
**Respecto a la investigacion de Panama**

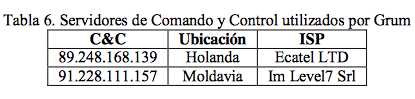
****

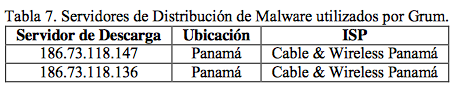
****

****

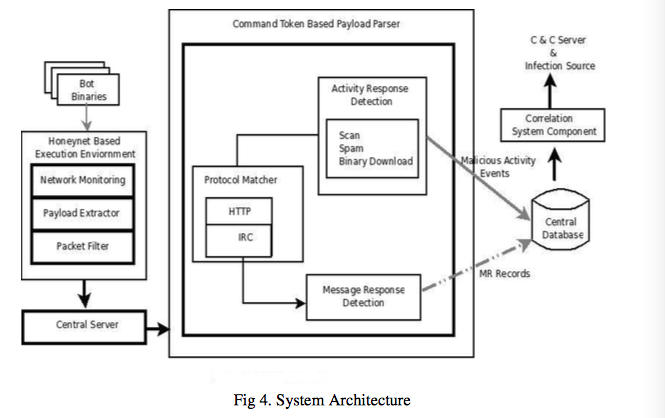
****

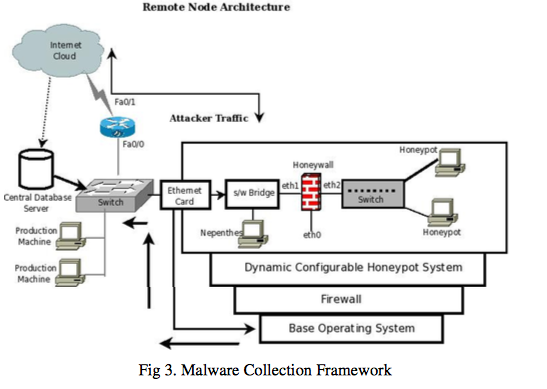
****

****

****

**Respecto a la investigacion “botnet command detection using virtual honeynet”**

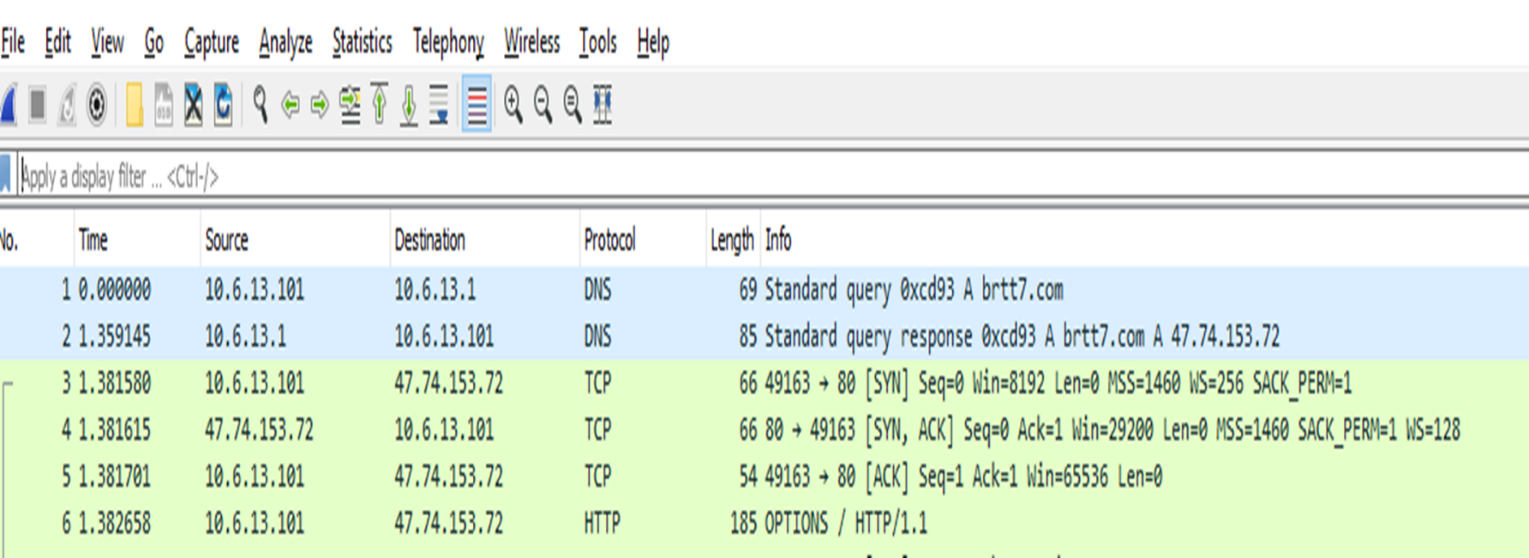
****

****

**Respecto a el analisis de trafico de red realizado por**

**nosotros**

Ilustración 1. Análisis trafico



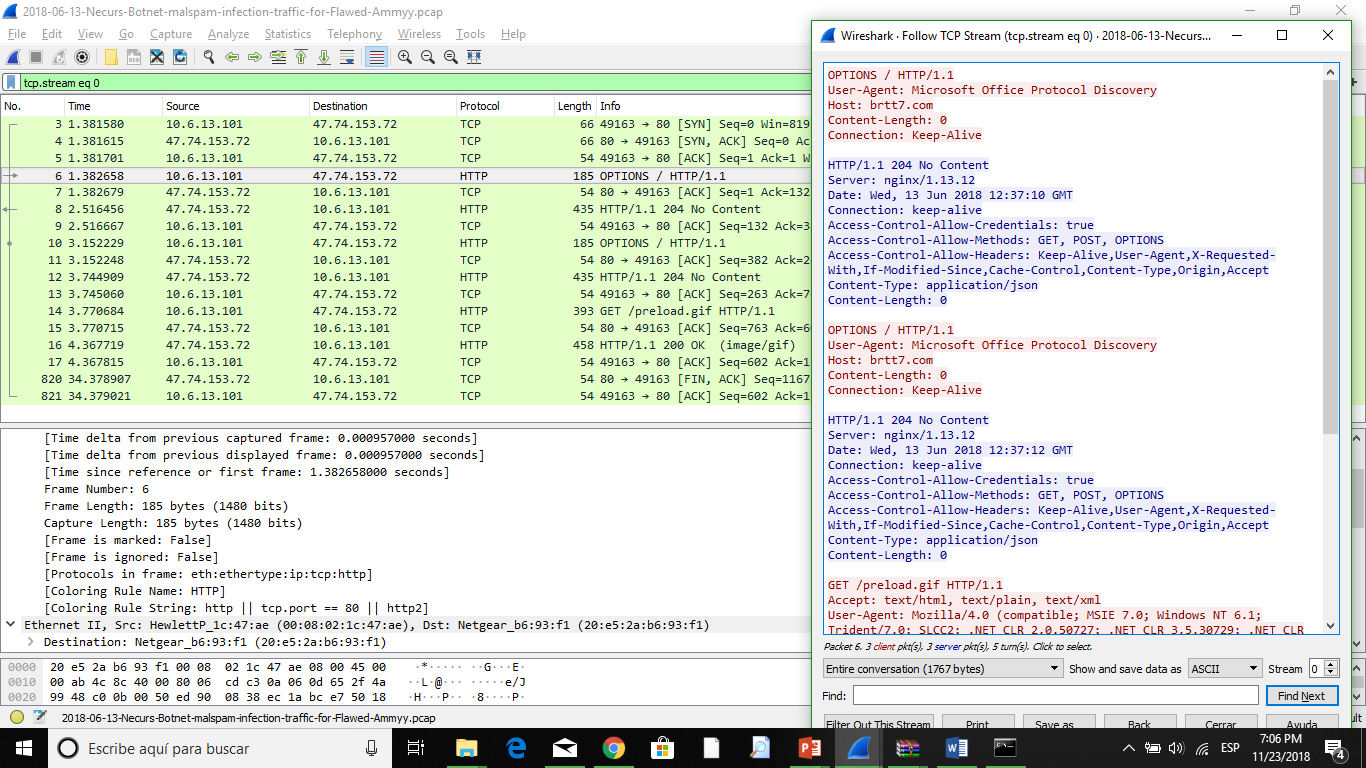


Ilustración 2. Análisis trafico

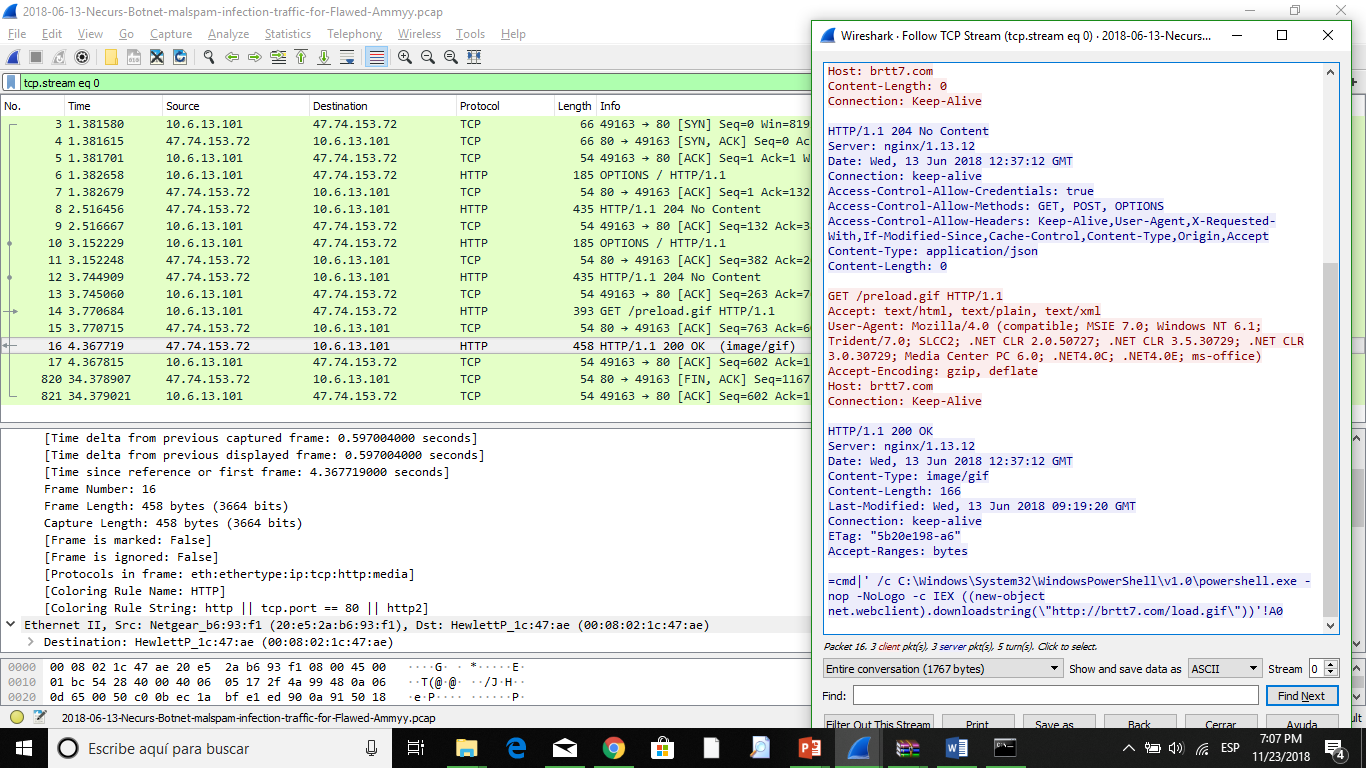


Ilustración 3. Análisis trafico

Imagen que contiene captura de pantalla

Descripción generada con confianza muy alta

Ilustración 4.Ejecución código

Imagen que contiene captura de pantalla

Descripción generada con confianza muy alta

Ilustración 5. VirusTotal