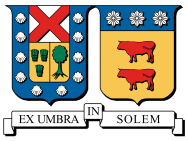
Gusanos de red

Daniel González Figueroa, *Rol 201404136-5*;
Felipe Díaz Otárola, *Rol 201321040-6*;
Leonardo Solis Zamora, *Rol 201104505-k*

17 de agosto de 2017



UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Redes de computadores I – ELO322, Grupo 7

1. Resumen

Un **malware** *(Malicious software)* es un término utilizado para referirse a cualquier software malicioso, es decir que que afecte negativamente al usuario, estos incluyen virus, troyanos, gusanos, etc...

Una forma de propagar un malware es mediante un gusano de red, que tiene la virtud de propagarse con bastante rapidez. Hoy en día, es necesario determinar si un usuario está siendo afectado por uno de estos gusanos y detenerlo a tiempo es la clave, ya que luego, se pueden utilizar diferentes formas de contención, hasta lograr canalizarlo.

2. Introducción: Historia de los gusanos de red

Gusano Morris

En un comienzo era un programa diseñado para medir los límites del internet, pero un error de programación lo convirtió en el primer gusano de computador. El error fue debido a que Morris creó el programa de modo que al momento de propagarse a un nuevo terminal preguntará si el programa ya se encontraba instalado. El error fue que incluso recibiendo una respuesta "Si" el programa se propagaba de igual manera, lo que traía como consecuencia tener más procesos abiertos y cada proceso ralentizaba el sistema. Esto es conocido como ataque **DoS (Denial of Service)**, ya que la red se encuentra ocupada mayormente con los procesos del virus y lo disponible para el usuario es cada vez menor.

Code Red

A diferencia de los anteriores, este gusano se propaga replicándose a direcciones IP que podrían estar conectadas al usuario (ya que no chequea si la dirección IP existe). Escanea el puerto 80 para encontrar algun host vulnerable y así poder realizar un ataque **DoS**. Posteriormente se descubre el **Code Red II** que instala un *back-door*[1] en los sistemas infectados.

Sasser

Gusano enfocado a *Windows XP* y *Windows 2000*. Se conocieron la primera notificaciones el 12 de abril de 2004 y se distribuye explotando un desbordamiento de búffer (se copia una cantidad superior a la establecida, por lo tanto se sobreescribe en zonas de memorias adyacentes).

[1]Tipo de troyano que permite el acceso al sistema infectado y su control remoto. El atacante puede entonces eliminar o modificar archivos, ejecutar programas, enviar correos masivamente o instalar herramientas maliciosas.

3. ¿Qué es un gusano informático?

Un **gusano informático** es una subclase de virus. La principal diferencia con estos últimos es que el virus necesita de acción humana para propagarse, ya que generalmente infectan archivos los cuales deben ser enviados a otros usuarios para infectarlos. Un gusano informático generalmente aprovecha vulnerabilidades de los mismos software para esparcirse entre sistemas y no necesariamente requieren intervención humana para lograr este esparcimiento lo cual los hace tan peligrosos. Por ejemplo un virus solo puede propagarse si un usuario envía un archivo infectado a otro y el receptor ejecute dicho archivo; mientras que un gusano podría esparcirse, por ejemplo, a todos los contactos de la lista de correos del usuario infectado sin siquiera este tener conocimiento. El gusano de red puede afectar casi todo lo relacionado con el computador. Puede provocar problemas tales como:

- Modificar/eliminar archivos dentro de un computador.
- Afectar el uso de la red del usuario (Enfoque dado en este trabajo)
- Crear un *back-door* en el computador, con lo cuál, el creador del virus podría manejar a gusto el computador del usuario.
- Obtener información privada.
- etc.

3.1. Funcionamiento de un gusano informático

Un gusano informático se propaga en 4 distintas fases: Encontrar un objetivo, Transferir el gusano, Activación, infección.

En la primera y segunda fase, el gusano se encuentra aún en la red. Este será el enfoque dado en este trabajo.

3.1.1. Encontrar el objetivo

Para encontrar un objetivo a infectar, el gusano de red puede usar distintas técnicas y así encontrar un objetivo vulnerable. Entre estas formas, se encuentras las siguientes:

Escaneo ciego

Consiste en probar direcciones IP (IPv4/IPv6) al azar. En general el escaneo ciego es el más fácil de implementar pero posee varias desventajas. Entre ellas está la opción de que la gran mayoría de *IP's* que intenten infectar no existirá, también no son tan rápidos respecto a otras estrategias utilizadas en IPv6. Existen 3 formas de usar este escaneo

- *Escaneo uniforme:* La forma más simple de implementación y es completamente al azar.

- *Escaneo secuencial:* Escanea las IP de manera secuencial después de elegir un punto de partida de forma aleatoria.
- *Escaneo de preferencia local:* Escanea preferentemente dentro de la misma subred. Se propagan más rápido que los 2 anteriores debido a que las *IP's* en el internet no se encuentran uniformemente distribuidas.

Pasivo

Este tipo de gusanos no buscará activamente a otras víctimas para infectar sino que esperará a que la víctima inicie una conexión con el usuario infectado y por medio de esta conexión intentará propagarse. Debido a que no generan conexiones adicionales son más difíciles de detectar.

Hit-List

Una *hit-list* es una lista de direcciones *IP's* conocidas a las que el gusano atacara. Esto lo hace un método efectivo, ya que su tasa de fallo no será muy alta, por lo que tendrán una alta velocidad de propagación.

3.1.2. Transferencia/Propagación

La transferencia o propagación puede ser realizada mediante conexiones TCP o UDP teniendo en este último caso, una velocidad de propagación mayor. Los gusanos se transmiten generalmente explotando vulnerabilidades de software oficial. En general tiene 2 métodos de propagación:

Self-Carried

Consiste en enviar un paquete compuesto de 2 partes: **Exploit**, la cual permite utilizar la vulnerabilidad del sistema para así poder modificarlo y **payload**, que es el código del gusano en sí.

Second Channel

Consiste en enviar pequeños trozos de código malicioso al objetivo mediante un *back-door* creado por alguna aplicación. Con ese código, se descarga el resto del gusano desde algún servidor externo. Esto permite juntar el código del gusano junto a tráfico de red legítimo, lo que hace difícil la detección.

3.2. Defensa ante un gusano informático

Para encontrar actividad de gusanos en la red a nivel general, es necesario observar las diferentes anomalías que se puedan generar mediante los intentos de conexión, tráfico ilegal y anomalía de carga útil.

Intentos de conexión

Para propagarse rápidamente, los gusanos de red envían un gran número de paquetes TCP SYN o paquetes UDP para poder encontrar víctimas en un periodo corto de tiempo. Algunas estrategias para poder detener esto son:

- *Contador de intentos de conexión:* Si el número de paquetes SYN enviados desde cierto host excede el límite definido dentro de un periodo de tiempo, entonces el host se considera infectado.
- *Correlación entre Fuente-Destino:* Los gusanos de red se mueven a través de los host que son vulnerables. O sea, si el host está infectado en dentro de una subred, pronto, intentará infectar a otro host que sea parte de la misma subred. Por lo tanto, la correlación entre paquetes de entrada y de salida entre host pueden dejar al descubierto un gusano de red.

Tráfico ilegal

Hay una gran cantidad de direcciones no utilizadas en la internet. Las máquinas normales rara vez envían paquetes a esas direcciones, sin embargo, los gusanos lo hacen y caen en el envío de paquetes a estas direcciones. El tráfico ilegal se podría interpretar entonces como trafico de paquetes a direcciones no utilizadas. Es así como se pueden detectar gusanos de red que se basan en tráfico ilegal.

Un Método para combatir esto es:

- *Darknet:* Una *darknet* es un espacio asignado de IP donde no hay actividad de servicios. Aparentemente, dentro de esas redes no existe nada. Cualquier tráfico de paquetes hacia esas redes es probablemente producto de gusanos de red, por lo que la darknet se considera un señuelo para gusanos de red.

4. Resultados: Detección de gusanos mediante Wireshark

El uso de whireshark permite detectar conexiones sospechosas que pueda estar realizando el malware hacia direcciones remotas para poder obtener archivos de diferente tipo. Una forma de prevenir o detectar que existen gusanos de red interfiriendo con el host, es mediante los siguientes métodos:

4.1. Uso de filtros

Utilizar filtros en el detector de tráfico de red, ayuda a poder analizar los diferentes paquetes obtenidos con ayuda de los diferentes protocolos.

4.2. DNS

Es importante saber a que servidores podemos estar conectados. Esto se puede realizar a través del filtro **DNS**. Para el caso del malware, es necesario saber a que servidores éste se conecta.

4.3. Peticiones realizadas

A través del filtro *http.request* es posible obtener todos los **GET** y **POST** realizados durante el periodo de captura de paquetes. Cuando existe un malware, estas peticiones son muy utilizadas para enviar información sobre el sistema utilizado.

4.4. Protocolo SMTP

Una forma de propagación del malware es a través del correo electrónico. Para esto es necesario analizar los paquetes con ayuda del filtro **SMTP**, incluso filtrando estos paquetes es util conocer el remitente del correo. Con el filtro *smtp.data.fragment*, es posible obtener los paquetes que contienen el cuerpo del mensaje.

4.5. Secuencia de paquetes

Se puede obtener dicha secuencia, seleccionando a través del paquete la opción *follow tcp stream*. Esto para poder visualizar el paquete completamente.

5. Conclusiones

Este trabajo dio a entender que la labor de un software como Wireshark proporciona un apoyo a la seguridad del usuario, debido a que puede dejar en evidencia algún gusano de red que esté interfiriendo con las labores del usuario. Es fundamental reconocer cuando la anomalía se puede estar produciendo por un malware de este estilo, sabiendo su forma de actuar y reconociendo los patrones que este tiene para atacar. Una vez que un equipo se encuentra infectado, resulta vital actuar con rapidez para minimizar el impacto que pueda tener en el propio sistema o en el resto de los host conectados dentro de la misma subred, por lo que es crucial identificar de qué espécimen se trata y eliminarlo. Hoy en día, este tipo verificación de paquetes a dado paso a la detección temprana de este tipo de malware, lo que obliga a que el método de propagación de estos se deba realizar de mejor manera y más de forma más persuasiva, pudiendo así eludir esta forma de prevención. Con ayuda de wireshark, es posible abarcar un gran rango de gusanos de red y poder canalizarlos a tiempo. La utilización efectiva de este software hace posible que gran parte de estos malwares no tengan una labor efectiva.

Referencias

[1] http://www.albany.edu/iasymposium/proceedings/2012/12-Misra&Uneojo.pdf

[2] http://www.lovemytool.com/blog/2016/05/how-to-detect-worm-with-a-network-analyzer-the-most-potent-threats-to-network-and-computer-security-are-worms-as-they-hav.html

[3] http://www.solucionavirus.com/2013/02/wireshark-uso-de-filtros-para-detectar.html

[4] http://www4.comp.polyu.edu.hk/ csbxiao/paper/2009/IEICE-2009-worm.pdf

[5] https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf