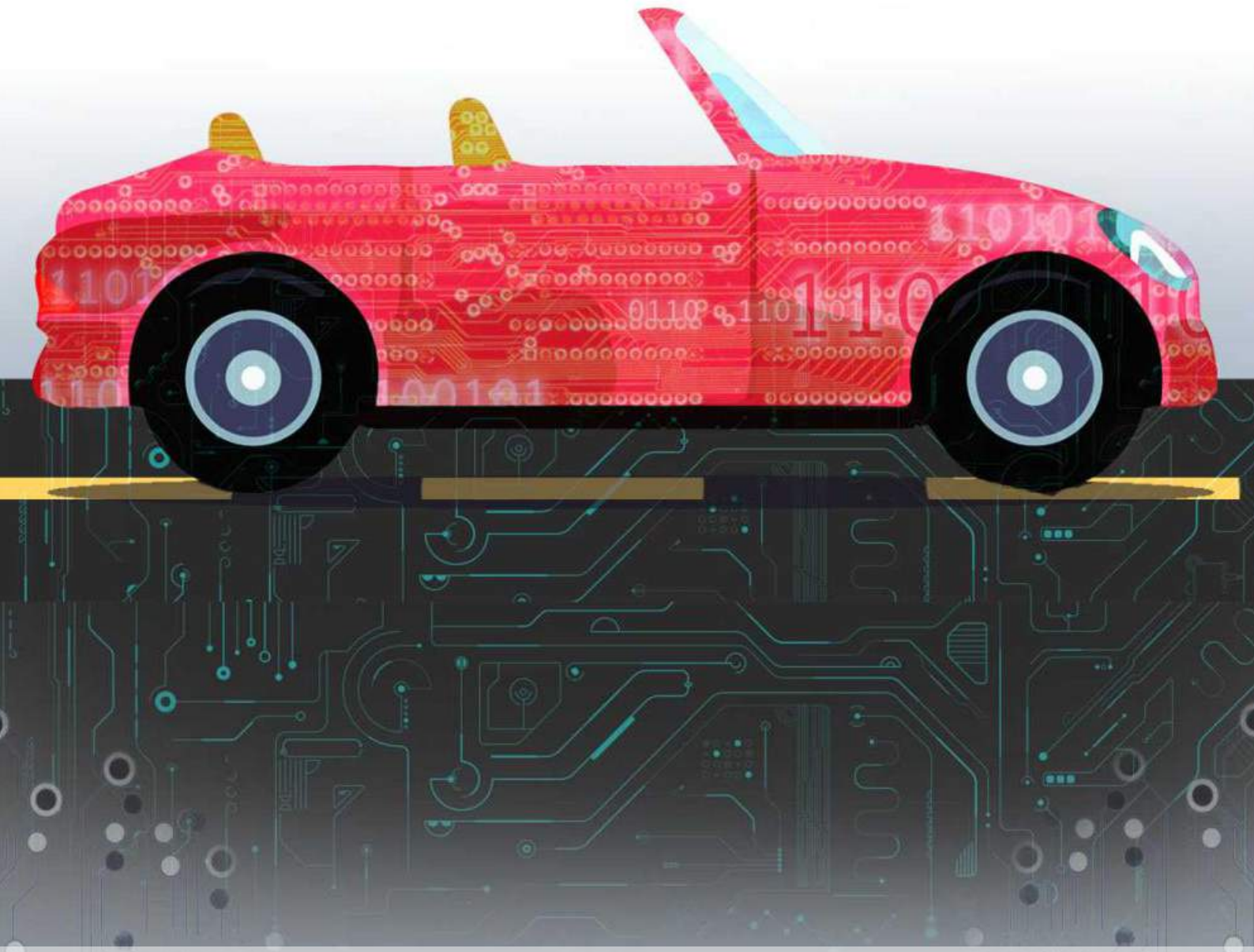
No.25 / agosto-septiembre 2015 ISSN: 1251478, 1251477

.Seguridad

Cultura de prevención para TI

25

Monitoreo y detección



Protección de datos en movimiento

Data Loss Prevention | Frameworks para monitoreo | Honeypot Glastopf | Botnet Liberpy | Likejacking | TIC y ciberterrorismo

Contenido

.Seguridad
Cultura de prevención para TI

Universidad Nacional Autónoma de México. Dirección General de Cómputo y Tecnologías de Información y Comunicación. Coordinación de Seguridad de la Información/UNAM-CERT. Revista .Seguridad Cultura de prevención para TI M.R., revista especializada en temas de seguridad del UNAM-CERT.

Editorial

Monitoreo y detección

Protección de datos en movimiento

La información que generamos cada día se ha vuelto "nómada". Me atrevo a decir esto porque en nuestros días es muy común enviar archivos por correo electrónico, subirlos a la nube, pasar documentos al teléfono o a la tableta, trabajar en aplicaciones basadas en la web y muchas otras tareas que vuelven a la información que generamos un viajero incansable.

Entre este flujo de datos se encuentran nuestras fotografías, las contraseñas de acceso a todos los servicios que consumimos, nuestras conversciones en línea, la comunicación por correo y en algunos casos hasta datos bancarios, llamadas telefónicas y mucha, mucha más información.

Proteger los datos en movimiento nos motivó a presentar en este número tecnologías relacionadas al monitoreo del tráfico de red y al análisis de esa información; herramientas que son útiles para conocer y ajustar los parámetros de red a las necesidades de cada organización, para la detección de intrusiones y continuidad de operaciones. Pues bien, las propuestas de nuestros autores son un apoyo para evitar que estos viajeros digitales pierdan el camino o se "crucen con el lobo" a mitad de su destino.

Invitamos a todos nuestros lectores, especialmente a aquellos administradores de red o responsables de TI en cada nivel, a conocer los contenidos que preparamos en esta ocasión, esperamos que sean de utilidad.

Feliz y seguro viaje, información.

Jazmín López Sánchez
Editora
Coordinación de Seguridad de la Información

.Seguridad
Cultura de prevención para TI

.Seguridad Cultura de prevención TI M.R. / Número 25 / agosto-septiembre 2015 / ISSN No. 1251478, 1251477 / Revista Bimestral, Registro de Marca 129829

DLP: Tecnologías para la prevención de la fuga de información

Israel Andrade Canales

No cabe duda que la facilidad para procesar, almacenar y transmitir la información que las TIC nos brinda a su vez dificulta el control sobre la misma, para muestra de lo anterior: la fuga de información en medios digitales. Dicho problema se ha colocado dentro de las primeras cuatro tendencias sobre delitos informáticos en este año [1] y además, es una noticia común en los medios de comunicación, desde la fuga de los primeros cuatro capítulos de la nueva temporada de “Game of Thrones” [2] hasta el robo de datos personales en una de las tiendas departamentales más populares de México [3].

Parece que si las condiciones son propicias, alguien extrae o pierde información que incluye documentos laborales, bases de datos con información sensible, fotografías o videos que en cuestión de horas el público puede descargar desde la comodidad de su dispositivo personal.

La fuga de información

El problema principal de la fuga de información es que las amenazas, las vulnerabilidades y las malas prácticas de seguridad que la propician se presentan en una gran variedad de escenarios durante el ciclo de vida de la información: creación, procesamiento, almacenamiento, transmisión y deposición.

Durante la creación o la adquisición de la información olvidamos definir cuáles van a ser las reglas del uso de la misma, comenzando así los problemas de control. ¿Quiénes tendrán acceso? ¿En cuáles dispositivos se podrá almacenar? ¿A quiénes se podrá transferir? ¿Se puede publicar? ¿Durante cuánto tiempo será útil? Son preguntas que podríamos plantearnos

justo en el momento de adquirir o crear dichos medios, no sólo para información laboral, también para la personal.

El descontrol de la información empeora en el siguiente estado de la información: el almacenamiento. Hoy contamos con una extensa variedad de dispositivos en donde podemos almacenar archivos y la mala práctica es no tener un control de dónde se resguardan. Es por esto que en el ámbito laboral están en boga los inventarios de información, prácticas que eran exclusivas para los bienes materiales.

Cuando transferimos, compartimos o publicamos la información perdemos por completo su control, es aquí donde comienza la pesadilla, porque otras personas pueden hacer mal uso de los contenidos: copias y accesos no autorizados a personas, correos personales, almacenamiento en dispositivos móviles, en la nube, redes sociales, etcétera.

En último lugar se encuentra el estado final de la información (la cual olvidamos frecuentemente): la eliminación. Por una parte está la práctica poco realizada del borrado seguro: ¿qué información podría obtenerse de nuestras viejas memorias USB, de los teléfonos celulares o de los servidores que se dan de baja en las empresas?; y por el otro, la dificultad de eliminar la información una vez que ha salido de nuestro ambiente de control, por ejemplo, cuando se almacena en Internet.

Figura 1. Ciclo de vida de la información

El problema es demasiado grande para una solución definitiva, involucra gente, tecnología, aspectos legales, de gestión, y a su vez, que las medidas precautorias no desfavorezcan el uso ágil de la información.

¿Qué es un DLP?

Una de las estrategias que las empresas están adoptando con más fuerza es el uso de sistemas de Prevención de Pérdida de Información (traducción propia de *Data Loss Prevention*, DLP). Se trata de un sistema porque son un conjunto de tecnologías que previenen la fuga de información.

El principio fundamental de esta serie de técnicas se basa en una herramienta más que conocida en el mundo de la seguridad informática: el antivirus; sólo que en lugar de buscar todas las formas reconocibles de una pieza de *malware*, éste sistema busca patrones y firmas de la información que nosotros consideremos sensible.

Adicionalmente, otras herramientas del DLP se distribuyen en toda la infraestructura informática (principalmente en los equipos de escritorio y en los dispositivos de red) para cubrir todos los estados de la información y los puntos de fuga.

El dueño de la información puede definir si algún archivo, base de datos o algún tipo de dato en particular (como el número de una tarjeta de crédito) debe ser analizado y, en su caso, bloqueado si es transmitido por algún medio. Estas herramientas pueden ser configuradas desde la forma más sencilla y ágil de clasificación (pública o privada) hasta el esquema más complejo.

Mientras la información se encuentra almacenada en uno o más equipos, el dueño puede realizar una búsqueda exhaustiva (justo como lo haría un antivirus en la búsqueda de *malware* en el equipo) y descubrir cuántas copias de la información o del mismo dato se encuentran distribuidas sobre la infraestructura tecnológica y así proceder a su organización, control o eliminación. ¿Te imaginas en cuántos docu-

mentos, dispositivos de almacenamiento y correos viejos has abandonado algún archivo con datos sensibles?

Quizá la funcionalidad más interesante es la del monitoreo y bloqueo de cualquier intento de transferencia no autorizada de los datos en resguardo. Esto funciona con la misma tecnología que un *firewall*, que detiene un patrón de ataque, pero en este caso se evita que la información sensible salga si no lo está permitido. Por ejemplo, un usuario apunto de mandarse una copia del reporte de finanzas a su correo personal (para revisarlo en casa) será detenido desde el cliente de correo o navegador, también será detenido al momento de subirlo a la nube y su sistema operativo no le permitirá almacenarlo en su memoria USB, si así fue establecido.

Pues bien, para el usuario no especializado en informática, un DLP podrá parecerle un medio de control más. Por eso es necesario que este tipo de mecanismos sean acompañados de un aspecto importante: una sensibilización informada del porqué cierto tipo de datos serán resguardados de esta manera, sea por implicaciones legales (como en el caso de la Ley Federal de Protección de Datos Personales) o por su criticidad para el negocio (como en el caso de los capítulos filtrados de "Game of Thrones").

También es importante recalcar que este tipo de sistemas requieren mantenimiento por parte de personal especializado y no son infalibles, pues pueden presentar "falsas alarmas" debido a la configuración imprecisa de políticas o la definición de patrones de búsqueda incorrectos que generarán más de un dolor de cabeza.

Sin embargo, como mencioné al principio de este artículo, la fuga de información es una de las tendencias más importantes en materia de seguridad. Con el perfeccionamiento de estas tecnologías y su integración con otras como los DRM[1], deberá disminuir considerablemente el problema. ¿Crees que algún día esta tecnología será utilizada comúnmente por los usuarios caseros en sus computadoras y dispositivos móviles como lo hizo el antivirus o el *firewall* personal?

Figura 2. Funcionamiento de un DLP

Notas al pie

[1] La gestión digital de derechos o DRM (por sus siglas en inglés) son un conjunto de tecnologías de hardware y software que controlan el acceso a contenidos digitales, principalmente películas y música, que permiten controlar la ejecución, vista o la impresión de información. La diferencia principal con un DLP es que los candados de seguridad están embebidos en el contenido y el software o dispositivo debe validar el derecho sobre el mismo; sin embargo, esta característica no permite tener un control sobre bases de datos o datos crudos como números de tarjetas de crédito, números de seguridad social, etcétera.

Referencias

[1] ESET. (2015). "Tendencias 2015 El mundo corporativo en la mira" Obtenido de ESET Latinoamérica,http://www.welivesecurity.com/wp-content/uploads/2015/01/tendencias_2015_eset_mundo_corporativo.pdf, consultado el 01 de junio de 2015.

[2] NOTIMEX. (2015). "Se filtran los primeros capítulos de Game of Thrones" Obtenido de El Economista,http://eleconomista.com.mx/entretenimiento/2015/04/12/se-filtran-primeros-capitulos-game-of-thrones, consultado el 01 de junio de 2015.

[3] Alberto García Álvarez. (2015). "¿Qué hacer después de una fuga de datos?" Obtenido de Forbes México,http://www.forbes.com.mx/que-hacer-despues-de-una-fuga-de-datos/, consultado el 01 de junio de 2015.

Si quieres saber más consulta:

- Recomendaciones al Elegir una Suite de Seguridad
- Dispositivos móviles: un riesgo de seguridad en las redes corporativas
- Normatividad en las organizaciones: Políticas de seguridad de la información - Parte I

Israel Andrade Canales

Ingeniero en computación de la Universidad Nacional Autónoma de México, Maestro en Investigación de Operaciones del Posgrado de Ingeniería de la misma institución. También fue miembro de la cuarta generación del Plan de Becarios de Seguridad en Cómputo del UNAM-CERT. Se ha desempeñado como auditor, analista de riesgos y consultor de seguridad de la información en el sector público, privado y bancario desde 2010.

Ha publicado artículos en la revista “.Seguridad” y colaboró como traductor técnico para el boletín de seguridad OUCH! del SANS Institute.

Frameworks para monitoreo, forense y auditoría de tráfico de red-II (POC)

Javier Ulises Santillán Arenas

En el artículo anterior se presentó una introducción general sobre tres *frameworks* de monitoreo de tráfico de red: NSM (Network Security Monitoring), SIEM (Security Information and Event Management) y PNA (Passive Network Audit). Recapitulando, tanto el objetivo del análisis como los recursos técnicos (software y hardware) con que se cuente, definen el modelo de análisis que puede ser más conveniente para el analista de tráfico. Para mayor referencia se puede consultar la Figura 1. “Panorama General de los modelos de monitoreo y análisis” del artículo anterior.

El actual trabajo tiene como objetivo presentar una prueba de concepto de Passive Network Audit Framework (PNAF), implementación de un *framework* basado en PNA el cual puede ser utilizado como herramienta de análisis pasivo de tráfico de red, aprovechando ventajas de otras herramientas. El alcance de este artículo incluye la instalación, configuración y modelos de ejecución para extracción de datos e interpretación de información. Para una mejor referencia del modelo teórico, puede consultarse el artículo anterior y la fuente original[1] de dicho *framework*.

Modelo general de PNAF

El modelo general de PNAF (Figura 1) define el funcionamiento y flujo de datos a través del cual PNAF decodifica, filtra e interpreta información a partir del tráfico de red.

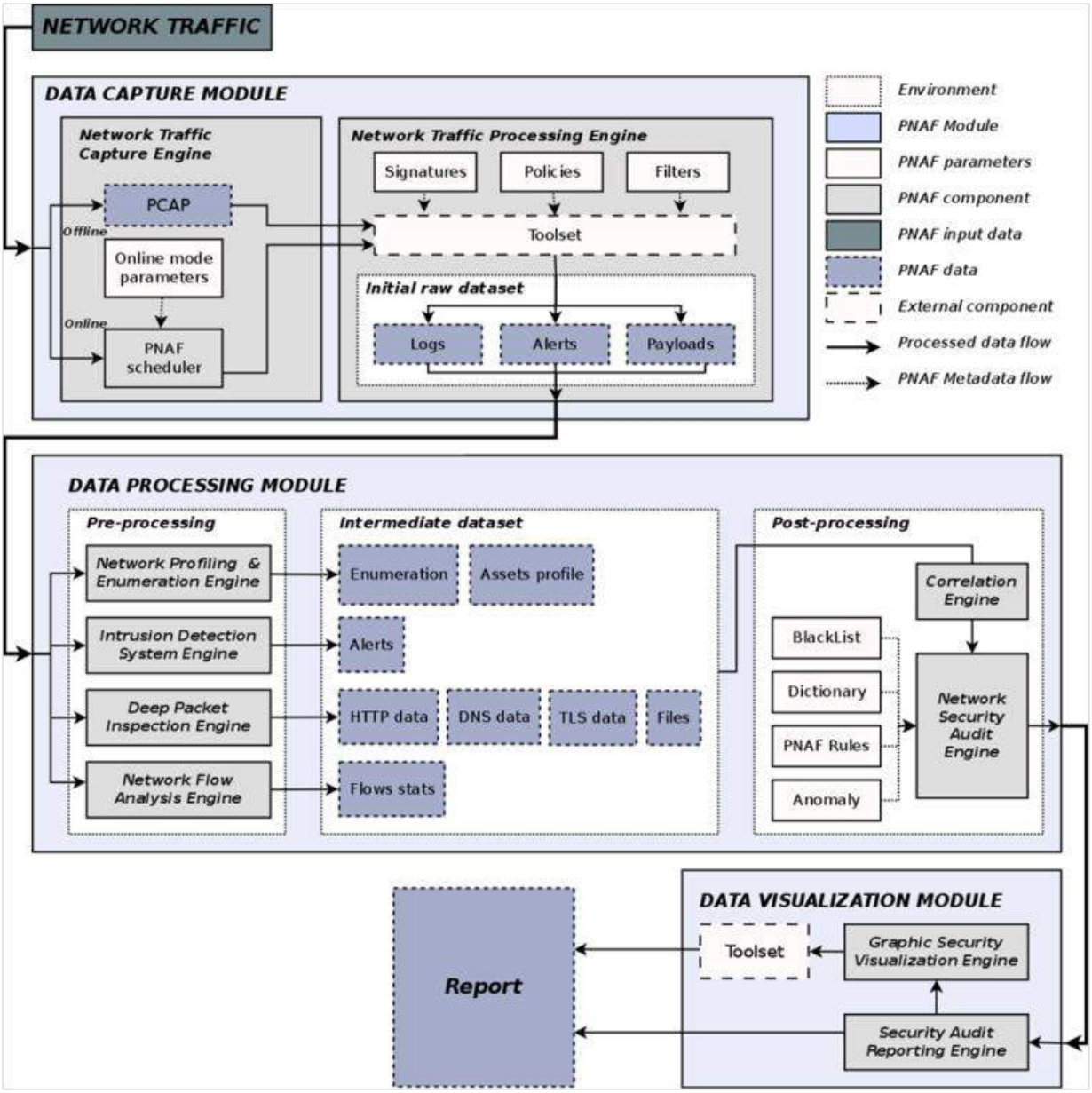


Figura 1. Modelo de análisis de Passive Network Audit Framework (PNAF)

Modos de instalación

PNAF incluye una serie de herramientas[2] para captura y análisis de tráfico de red. Debido a sus características y capacidades, algunas de estas herramientas por sí mismas pueden involucrar complejos procesos de instalación y configuración. Por esta razón, PNAF está diseñado para proveer modos de instalación que faciliten y automaticen el proceso de manera que el analista pueda hacer uso del *framework* sin mayor problema. Existen cuatro modos de instalación explicados a continuación.

Instalación mediante instalador

PNAF incluye un instalador que automatiza la descarga, compilación y configuración de todas las herramientas. Este instalador incluye un *wizard* (asistente de instalación) basado en *dialog*. Para poder utilizar este modo de instalación es necesario cumplir los siguientes requerimientos:

Es posible su funcionamiento en Ubuntu u otra distribución basada en Debian, sin embargo implica verificar las equivalencias en paquetes instalados por Apt. Asimismo, es posible usar el instalador

en otros sistemas no basados en Debian siempre y cuando se instalen manualmente todas las dependencias necesarias para la compilación de las herramientas. Para esto se puede consultar el archivo README e instalar las dependencias equivalentes de la lista de Apt/emerge.

Debido a que PNAF instala una gran cantidad de dependencias, se recomienda instalar el *framework* en un ambiente *chroot* para evitar cualquier problema de compatibilidad de dependencias en el sistema nativo. En esta prueba de concepto el proceso se hará de esa manera y se explicará a continuación.

Asumiendo que se cuenta con un sistema *Debian* 8 de 64 bits (*amd64*):

1. Creación del ambiente chroot (vía *debootstrap*):

```
# aptitude install debootstrap
# debootstrap --arch amd64 jessie chroot_pnaf
http://ftp.mx.debian.org/debian
# mount -t sysfs sysfs   chroot_pnaf/sys
# mount -t proc proc     chroot_pnaf/proc
# mount -o bind /dev     chroot_pnaf/dev
# mount -o bind /dev/pts chroot_pnaf/dev/pts
```

Ahora se cambia al ambiente *chroot*:

```
# chroot chroot_pnaf
# cd ~/
```

2. Descarga de PNAF

Opción 1: Desde el repositorio oficial del proyecto:

```
# aptitude install git
# git clone
https://dev.honeynet.org.mx/traffic-analysis/pnaf.git
```

Opción 2: Desde el *mirror* en github:

```
# git clone https://github.com/jusafing/pnaf
```

Una vez descargado, ingresar al directorio y ejecutar el instalador:

```
# cd pnaf
# ./install.sh
```

Esto ejecutará el asistente. Primero se deberá confirmar que se desea instalar PNAF. Posteriormente se pueden seleccionar las herramientas que se incluirán en el *framework*. A pesar de que no todas las herramientas se utilizan en esta versión de PNAF (v0.1.2) se recomienda seleccionar todas para utilizarlas de manera independiente. Visto de este modo, PNAF es también un asistente para la instalación de herramientas de análisis de tráfico de red.

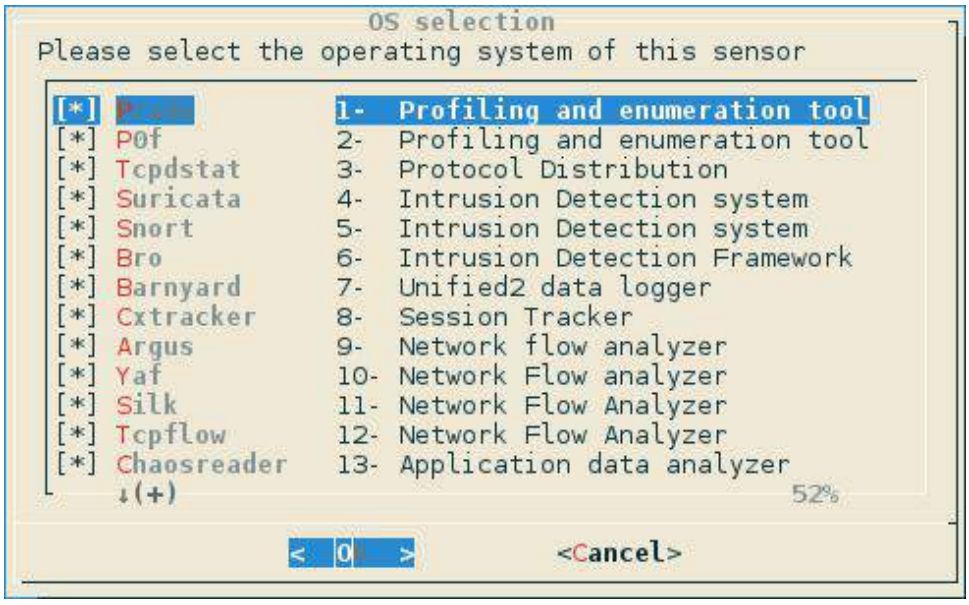


Figura 2. Selección de herramientas en la instalación de PNAF

Si es la primera vez que se instala PNAF se debe seleccionar una instalación limpia, *"clean installation"*. En caso de que exista una instalación previa, la instalación limpia eliminará cualquier herramienta y archivos instalados por PNAF. Si sólo se desea agregar o reinstalar ciertas herramientas, se debe seleccionar "NO" en este paso.

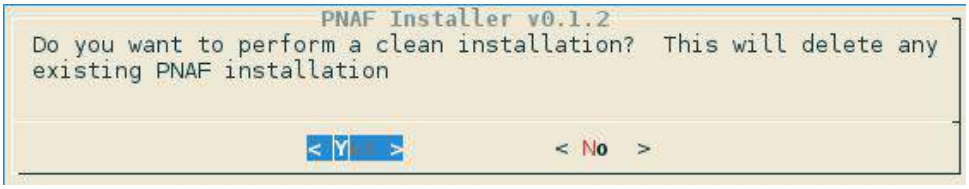


Figura 3. Selección del tipo de instalación

A partir de ese momento el instalador comenzará a compilar y configurar todas las herramientas. Este proceso puede durar aproximadamente 30 minutos, dependiendo de las capacidades del equipo. En caso de que exista un error en el proceso, el instalador mostrará el mensaje correspondiente y se podrán verificar los archivos *install.log* e *install.log.exec* para identificar el problema. De lo contrario, si el proceso terminó correctamente, PNAF habrá quedado instalado y listo para usarse.

Como recomendación, para actualizar las variables de ambiente hay que salir del ambiente *chroot* y volver a entrar. Asimismo, para identificar cuándo se esté dentro del directorio de *chroot* es conveniente agregar una etiqueta al *shell*:

```
# echo 'PS1="(PNAF) $PS1"' >> ~/.bashrc
# exit
# chroot chroot_pnaf
```

Para verificar que PNAF se ha instalado correctamente:

```
# pnaf_auditor --help
```

```
root@debian:~# pnaf_auditor --help

=======================================
 Passive Network Audit Framework (PNAF)
 Version 0.1.0
=======================================

Usage:
        $ pnaf_auditor [options]

        OPTIONS:
        ================================================================================

        Execution:
        --debug                 : Enable debug mode
        --conf                  : Specify configuration file (yaml)
        --help                  : Show this
        --version               : Show tools versions
        --parser arg1[,arg2]    : Specify parsers to be loaded
            'p0f'               : Process enumeration data
            'prads'             : Process enumeration data
            'argusFlow'         : Process NFA data (flow analysis)
            'snortAppId'        : Process enumeration data (App identification)
            'httpry'            : DPI over HTTP (URL's, UA, etc)
            'tcpdstat'          : Process enumeration data (protocol dist)
            'suricataEve'       : Process IDS data (alerts and payloads)
            'bro'               : DPI over different protocols
            'tcpflow'           : Process NFA data (session tracking)
        --out_dataset           : Specify the kind of output data to generate
            'all'               : Generate all datasets
            'audit'             : Generate only audit dataset
        --home_net              : Specify the 'homenet' in CIDR format
        --payload               : Flag to enable payload decoding (IDS data)

        Inputs:
        --cap_file              : Set input capture file (pcap)
        --audit_dict            : Path to vulnerability dictionary
        --instance_dir          : Path to directory with 'initial raw dataset'

        Logging:
        --log_dir           : Path to log directory
        --log_file          : Path to output directory
```

Figura 4. Opciones de ejecución de PNAF

Instalación mediante Debian *chroot* preconfigurado

El segundo modo de instalación corresponde al uso de un directorio *chroot* con todas las herramientas precompiladas y preconfiguradas. Esta alternativa básicamente evita todo el proceso de compilación y creación del directorio raíz con *debootstrap* (herramienta presentada en el modo anterior). Por otro lado, facilita tener una plantilla con un directorio preparado para usarse con *chroot*. Con este modo sólo es necesario descargar el archivo empaquetado *.tar.bz2* (aproximadamente 1.3 GB) y desempaquetarlo en el sistema de archivos local.

Es importante mencionar que este modo funciona sólo si el sistema local en el que se planea instalar es Debian 8 amd64 (la compilación de todas las herramientas depende de la arquitectura y de las versiones de las dependencias usadas por Apt).

```
# wget http://pnaf.honeynet.org.mx/download/chroot_pnaf.tar.bz2
# tar -jxvf chroot_pnaf.tar.bz2
# mount -t sysfs sysfs   chroot_pnaf/sys
# mount -t proc proc     chroot_pnaf/proc
# mount -o bind /dev     chroot_pnaf/dev
# mount -o bind /dev/pts chroot_pnaf/dev/pts
# chroot chroot_pnaf
```

Igualmente se puede verificar que PNAF se ha instalado correctamente:

```
# pnaf_auditor -help
```

Instalación (uso) mediante una máquina virtual

En este modo de instalación es necesario descargar una imagen de máquina virtual en formato OVA para ser importando con VirtualBox o Vmware.

1. Descargar la imagen en http://pnaf.honeynet.org.mx/download/pnaf-0.1.2.ova

2. En VirtualBox:

En el menú *File/Import appliance/* seleccionar el archivo OVA y crear la máquina virtual.

Esta máquina virtual tiene instalado PNAF con todas las opciones mostradas en el instalador. Las credenciales de acceso para el usuario *root* se muestran en el mensaje de bienvenida una vez que se inicia la máquina virtual.

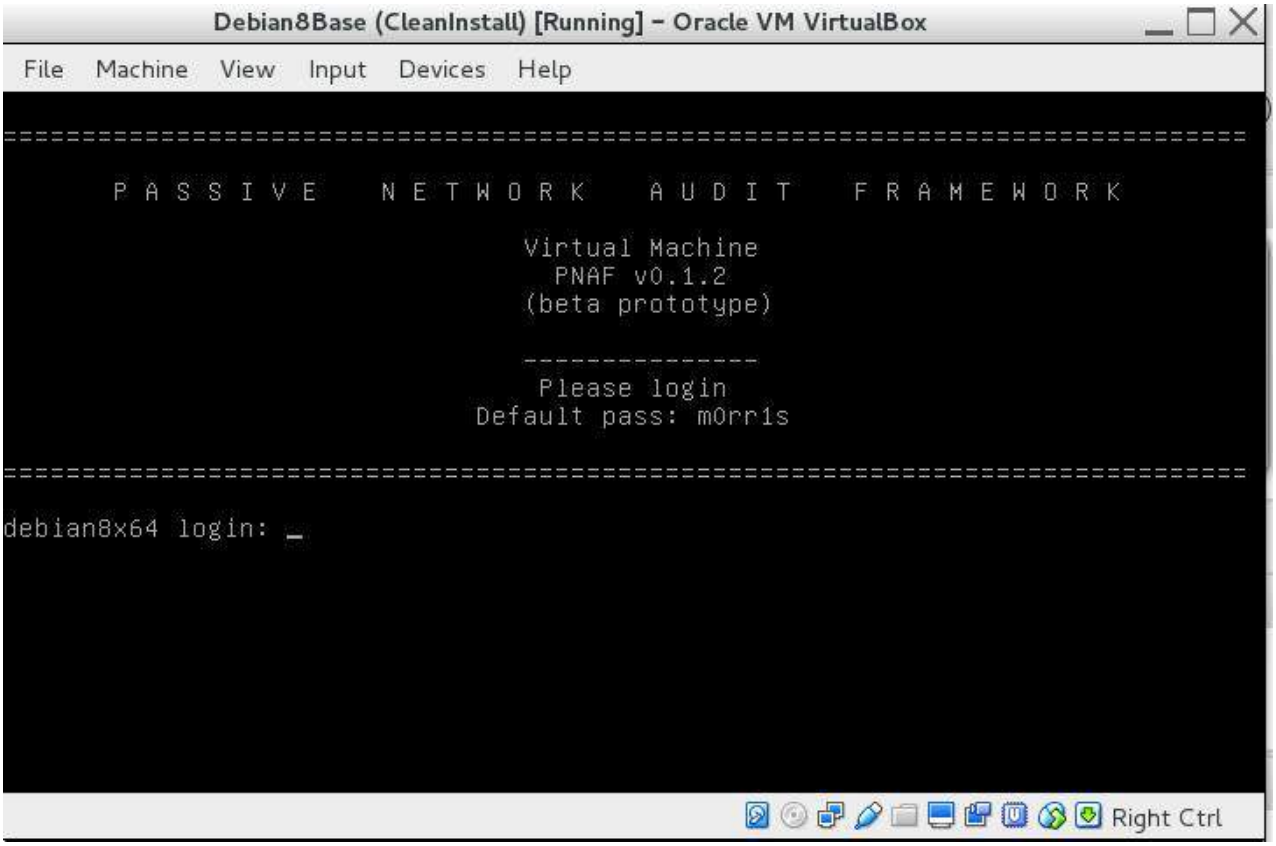


Figura 5. Máquina virtual preconfigurada con PNAF

Una vez dentro de la máquina

```
# mount -t sysfs sysfs   chroot_pnaf/sys
# mount -t proc proc     chroot_pnaf/proc
# mount -o bind /dev     chroot_pnaf/dev
# mount -o bind /dev/pts chroot_pnaf/dev/pts
# chroot /root/chroot_pnaf
```

Instalación mediante módulo de Perl (instalación independiente)

Esta opción incluye la instalación del núcleo (*core*) de PNAF, es decir, instalación independiente del módulo de Perl. Este modo se puede utilizar cuando se desee usar PNAF con una instalación propia de las herramientas. Sin embargo, no es recomendable ya que se necesita configurar una gran cantidad de opciones, incluyendo la ruta de los archivos binarios de cada una de las herramientas, archivos de configuración, *logs*, etcétera. Para esto, una vez descargado PNAF, editar la configuración de cada una de las herramientas:

```
# cd pnaf
# vim build/pnaf/Pnaf/lib/Pnaf/Core.pm (establecer rutas)
# cd build/pnaf/Pnaf
# perl Makefile.PL
# make
# make test
# make installf
```

Configuración

La mayoría de las opciones de configuración se definen directamente como argumentos al momento de la ejecución del auditor de PNAF (*pnaf_auditor*).

Para visualizar las herramientas incluidas en el *framework* se puede ejecutar:

```
# pnaf_auditor --version
```

Para mayor información sobre las opciones disponibles en PNAF 0.1.2:

```
# pnaf_auditor --help
```

En caso de necesitar una configuración específica, por ejemplo, agregar firmas del IDS Suricata, se pueden modificar los archivos de configuración dentro del directorio */pnaf/etc*.

PoC: análisis de capturas de tráfico de red

A continuación se analizarán tres archivos de captura en formato PCAP. La flexibilidad de las herramientas usadas por PNAF permite extraer e interpretar la información de maneras diferentes. El análisis en esta prueba de concepto no representa la totalidad de la información que se puede obtener. Así, la PoC incluye un análisis general los archivos de captura de manera que se obtenga la siguiente información y cuyo propósito se explica en la siguiente tabla:

Información a identificar	Propósito
Identificación de activos	Identificación de los equipos que participan en el tráfico de red incluyendo estadísticas de uso por tipo de conexión, protocolos, tasas de transferencia, etc.
Posibles eventos e seguridad (alertas de IDS)	Identificación de posibles actividades anómalas o maliciosas a partir de un motor IDS.
Recursos que se acceden	Identificación de recursos como URLs, dominios, archivos transferidos.
Auditoría de software usado en la organización	Identificación pasiva del software utilizado en la red tanto por clientes como por servidores. A partir de esta información se lleva a cabo la identificación de potenciales vulnerabilidades basadas en CVE.

Tabla 1. Análisis de información de la PoC

Ejecución inicial

Procesamiento general

Teniendo el archivo de captura *test1.cap*, se ejecuta *pnaf_auditor* de la siguiente manera:

```
# pnaf_auditor --cap test1.cap -log_dir /pnaf/www/test1
```

Esto ejecutará una serie de herramientas y procesará la información almacenando los resultados en el directorio */pnaf/www/test1*.

```
root@debian:~# pnaf_auditor --cap test1.cap --log_dir /pnaf/www/test1

=======================================
 Passive Network Audit Framework (PNAF)
 Version 0.1.0
=======================================

[2015-08-02T16:46:46] INFO    - Loading configuration file (/pnaf/etc/auditor.conf)
[2015-08-02T16:46:46] INFO    - Debug           : no
[2015-08-02T16:46:46] INFO    - Cfg file        : /pnaf/etc/auditor.conf
[2015-08-02T16:46:46] INFO    - Log file        : /pnaf/log/pnaf.log
[2015-08-02T16:46:46] INFO    - Log directory   : /pnaf/www/test1
[2015-08-02T16:46:46] INFO    - Report directory: /pnaf/reports
[2015-08-02T16:46:46] INFO    - Exec mode       : full
[2015-08-02T16:46:46] INFO    - Capture File    : /root/test1.cap
[2015-08-02T16:46:46] INFO    - DPM             : suricata
[2015-08-02T16:46:46] INFO    - IDS depth       : high
[2015-08-02T16:46:46] INFO    - NFA depth       : high
[2015-08-02T16:46:46] INFO    - DPI depth       : high
[2015-08-02T16:46:46] INFO    - Processing PCAP file ( /root/test1.cap)
[2015-08-02T16:46:46] INFO    - Loading PNAF instance for (/root/test1.cap)
[2015-08-02T16:46:46] INFO    - Executing Network Profiling and enumeration Engine <NPEE>
[2015-08-02T16:46:46] INFO    -  |--Running p0f version 3.06b
[2015-08-02T16:46:46] INFO    -  |--(p0f) has finished successfully. Status (0)
[2015-08-02T16:46:46] INFO    -  |--Running prads version github_3c751c869e
[2015-08-02T16:46:54] INFO    -  |--(prads) has finished successfully. Status (0)
[2015-08-02T16:46:54] INFO    - Executing Intrusion Detection System Engine <IDSE>
[2015-08-02T16:46:54] INFO    -  |--Running snort version 2.9.7.0
[2015-08-02T16:47:17] INFO    -  |--(snort) has finished successfully. Status (0)
[2015-08-02T16:47:17] INFO    -  |--Running suricata version 2.0.3
[2015-08-02T16:47:35] INFO    -  |--(suricata) has finished successfully. Status (0)
[2015-08-02T16:47:35] INFO    -  |--Running bro version 2.3
[2015-08-02T16:47:40] INFO    -  |--(bro) has finished successfully. Status (0)
[2015-08-02T16:47:40] INFO    - Executing Network Flow Analysis Engine <NFAE>
[2015-08-02T16:47:40] INFO    -  |--Running argus version 3.0.6
[2015-08-02T16:47:42] INFO    -  |--(argus) has finished successfully. Status (0)
[2015-08-02T16:47:42] INFO    -  |--Running ra version 3.0.6
[2015-08-02T16:47:42] INFO    -  |--(ra) has finished successfully. Status (0)
[2015-08-02T16:47:42] INFO    -  |--Running tcpdstat version github_be5bd28da
[2015-08-02T16:47:42] INFO    -  |--(tcpdstat) has finished successfully. Status (0)
[2015-08-02T16:47:42] INFO    - Executing Deep Packet Inspection Engine <DPIE>
[2015-08-02T16:47:42] INFO    -  |--Running httpry version github_7dc427196a
[2015-08-02T16:47:42] INFO    -  |--(httpry) has finished successfully. Status (0)
[2015-08-02T16:47:42] INFO    - Raw data logs stored in (/pnaf/www/test1)
```

Figura 6. Ejecución de PNAF

Procesamiento específico

Ahora, asumiendo que se desea obtener un filtrado específico, se puede ejecutar *pnaf_auditor* con las siguientes opciones:

```
# pnaf_auditor --cap test2.cap -log_dir /pnaf/www/test2 --home_net
192.168.1.0/24 --payload
```

En esta ejecución se indica que se analizará el archivo de captura *test2.cap* y que la red de la organización *"home_net"* es el segmento 192.168.1.0/24 (se pueden indicar más segmentos en formato CIDR[3] separados por comas). Asimismo, se indica que se desea extraer el *payload* en caso de identificar una alerta de IDS (útil para análisis a fondo y verificación de falsos positivos).

Análisis e interpretación de la información

La interpretación de la información se puede llevar a cabo en distintas etapas.

1. *Logs* de línea de comandos

El *log* generado durante la ejecución muestra el resumen de los resultados. Esta fase es importante porque se obtiene información de las herramientas utilizadas así como del panorama general de los datos obtenidos. La siguiente figura muestra la explicación del *log* generado por PNAF.

Figura 7. Log de ejecución y resultados generales de PNAF

2. *Logs* en interfaz web

PNAF permite una visualización de los resultados a través de una interfaz web básica. Esta interfaz permite listar:

- Archivos de *log* "*crudos*" generados por cada una de las herramientas
- Archivos de *log* preprocesados en formato JSON[4]
- Archivos de *log* con resultados de auditoría en formato JSON y visualizados en forma de árbol

Para poder utilizar la interfaz web es necesario activar el servidor web apache incluido en PNAF.

```
# apachectl start
```

Usando la configuración predeterminada, todos los directorios de resultados que se almacenen en */pnaf/www* e indicados en la opción *--log_dir* podrán ser visualizados en la web usando http://localhost o la dirección IP específica donde se ejecute PNAF.

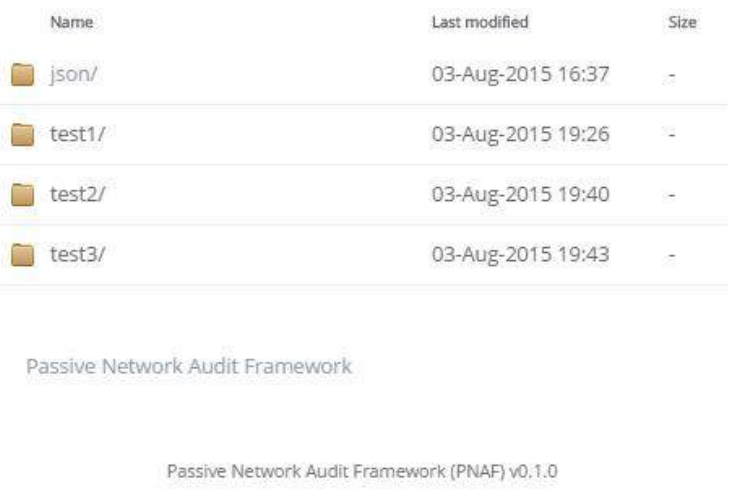


Figura 8. Visualización web básica de PNAF

Dentro de este directorio se tiene la siguiente estructura y se muestra un ejemplo en la Figura 9:

```
DIRECTORY_NAME/                 (Archivos de log en "crudo" y directorios de herramientas)
 |
 |----- JSON/                   (Archivos pre-procesados en formato JSON)
 |        |
 |        |---SUMMARY/          (Árbol JSON para visualización de resultados de auditoría)
 |        |    |                (En este directorio se encuentra el visualizador principal)
 |        |    |
 |        |    |---dataset      (Visualización de datos de cada herramienta)
 |        |    |---auditSummary (Resumen de resultados de auditoría)
 |        |    |---auditSoftware (Software encontrado en el tráfico de red)
 |        |    |---auditOutput  (Auditoría de software basado en CVE de la base de datos de NIST,
 |        |    |                 asi como resultados de IP/dominios encontrados en listas negras)
 |        |    |---auditTracking (Auditoría por cada asset (activo) identificado (hosts, server, etc)
 |        |
 |        |-------VIEW1/        (Visualización alternativa de los datos en JSON)
```

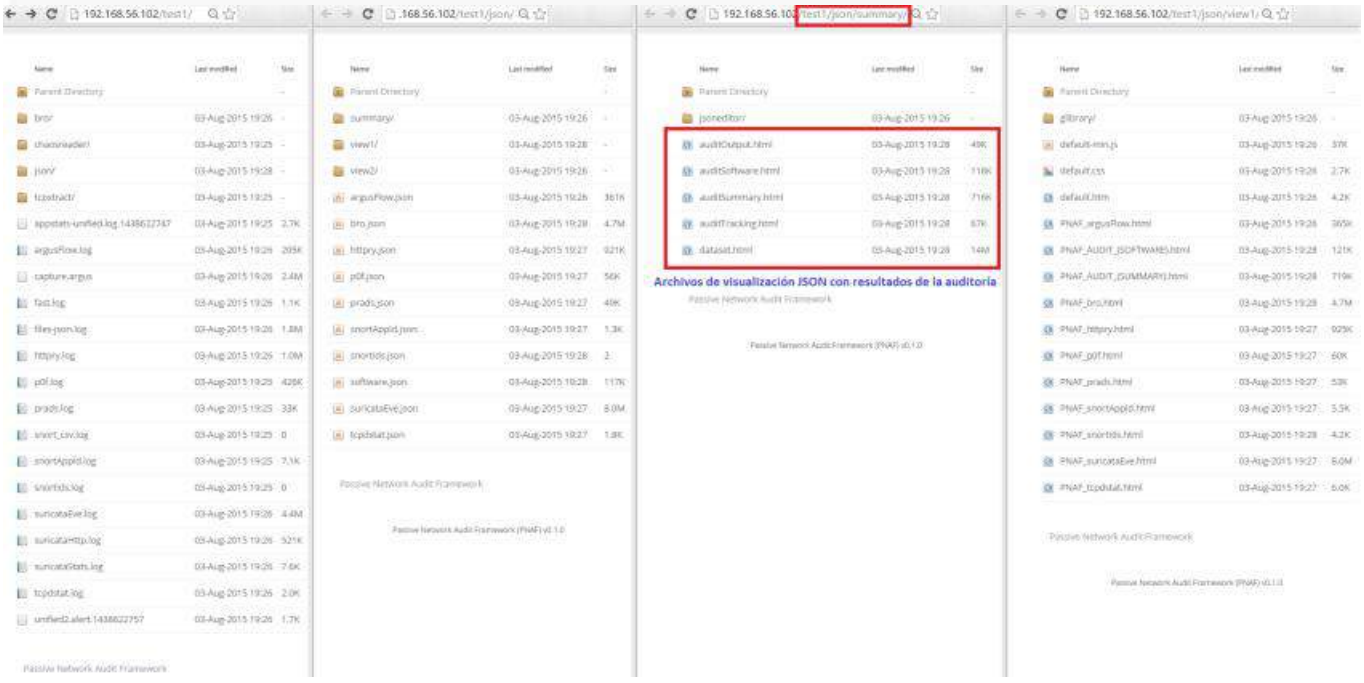


Figura 9. Archivos generados para la visualización web de PNAF

El análisis en esta PoC va de lo general a lo particular. Primero se puede dar un vistazo general en el contenido del archivo *json/summary/dataset.html.* Aquí, el analista puede acceder a la información clasificada de las herramientas. Cada herramienta contiene dos categorías principales, Summary (resumen de los datos) y Tracking (información por activos -IP*, servers,* etcétera-). Según la necesidad del analista y los hallazgos encontrados se pueden extraer datos a profundidad por cada herramienta y filtrar la información mediante el cuadro de búsqueda en cada árbol de herramienta.

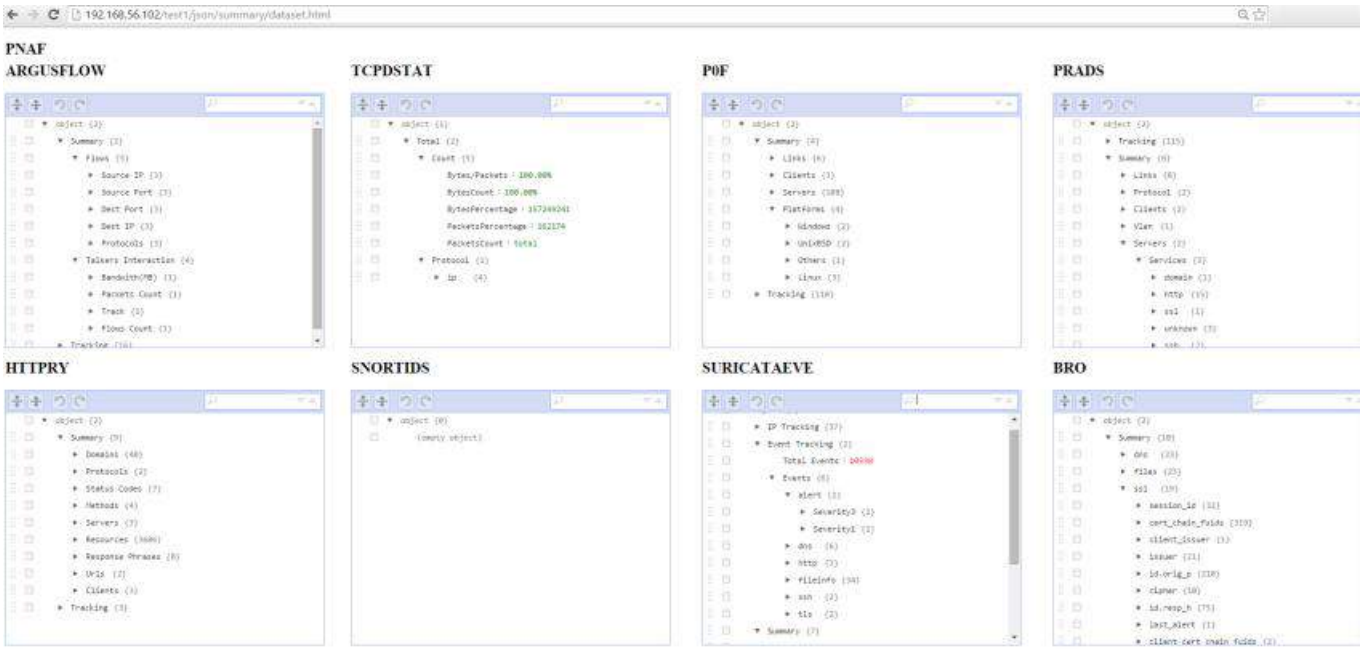


*Figura 10. Conjunto de datos (*datasets*) de las herramientas usadas en PNAFF*

Continuando con el análisis, ahora se visualiza el filtrado y preprocesamiento de datos generados por PNAF, el cual lleva a cabo una correlación básica y conjunta de la información, creando diferentes categorías. Para ello se accede al archivo */json/summary/auditSummary.html* y es aquí donde el analista puede extraer información detallada de la actividad de cada uno de los activos que intervienen en el tráfico de red. Por ejemplo, se puede obtener información sobre URL, certificados SSL, alertas IDS, archivos transferidos, software utilizado, etcétera. De la misma manera, si la auditoría se prefiere hacer tomando como clasificación general a los activos, entonces se puede visualizar el archivo */json/summary/auditTracking.html*.

Figura 11. Resumen de auditoría. Clasificación general

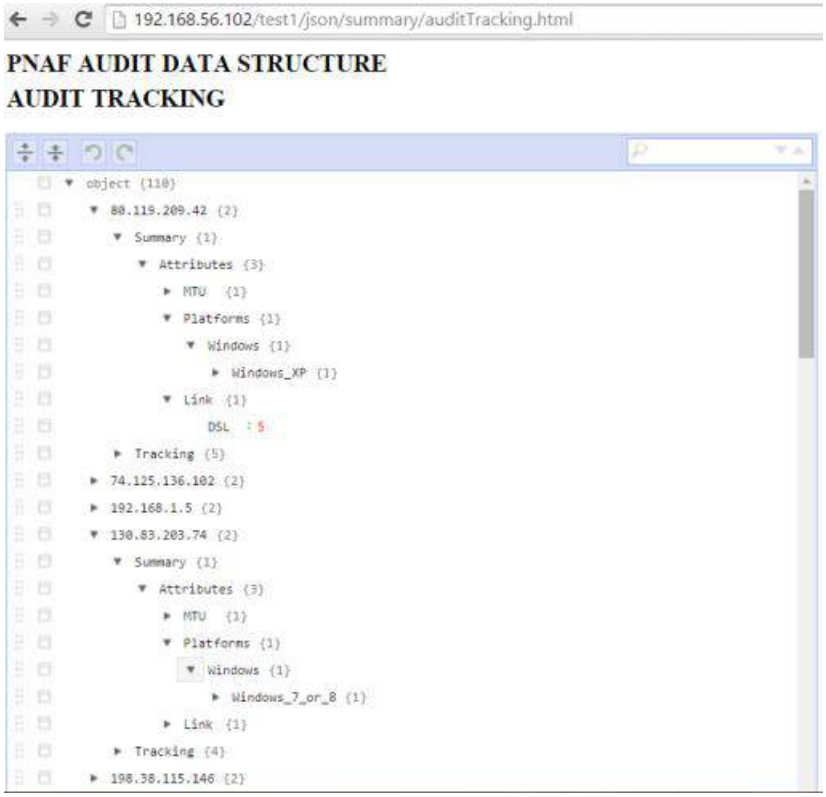


Figura 12. Resumen de auditoría. Clasificación por activos

Finalmente, el archivo */json/summary/auditOutput.html* muestra el resultado del análisis de vulnerabilidades basadas en CVE[5] y versiones de software encontradas. Este análisis incluye un sistema de puntaje (*score*) que indica el posible impacto de las vulnerabilidades identificadas. Asimismo, se muestra la lista de equipos identificados en listas negras de dominios o IP, o cuya interacción estuvo involucrada con equipos de la red.

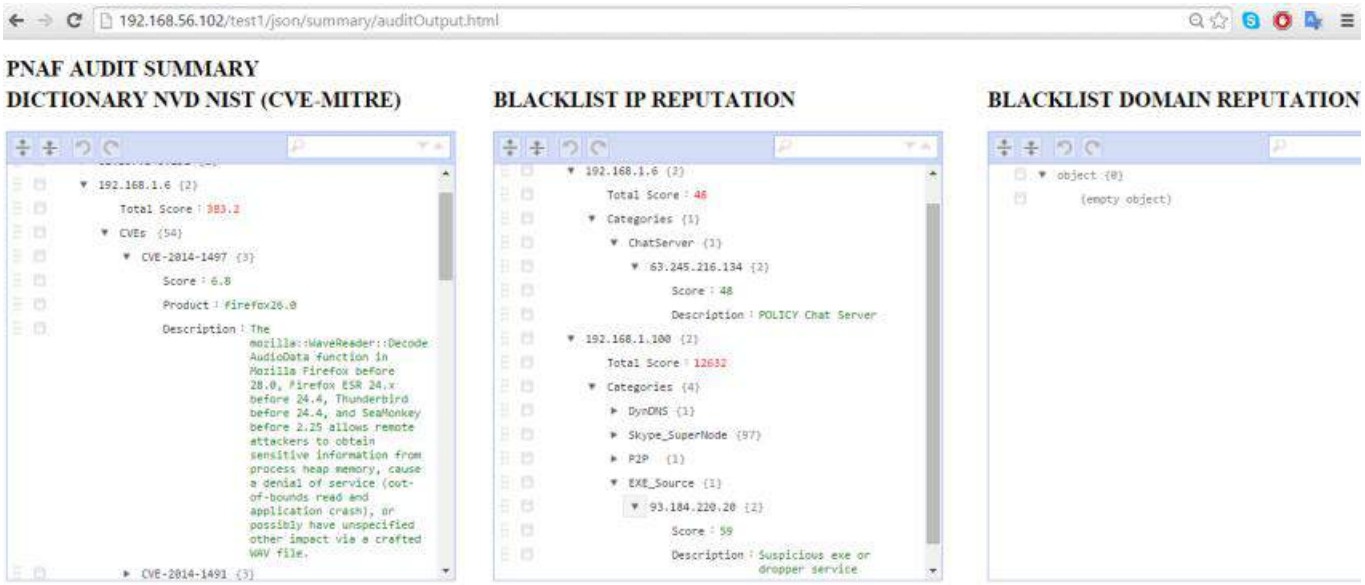


Figura 13. Resumen de auditoría. Análisis de vulnerabilidad de software basado en CVE

Conjuntando toda la información recopilada y filtrada tanto por PNAF como por el mismo analista, es posible determinar el estado general y características de la red. La información detallada dependerá del tipo de problema o necesidad que se desea resolver.

Finalmente, es importante hacer énfasis en el hecho de que PNAF es susceptible a falsos positivos debido a la naturaleza misma de PNA, en donde, al no contar con la información completa y obtener datos a partir de una interpretación del tráfico de red, cierta información podría repre-

sentar hechos erróneos. Así, una de las tareas del analista implica la identificación y verificación de información certera.

Actualmente PNAF se encuentra en desarrollo en la versión 0.2. Futuras versiones incluirán cambios significativos en la interfaz web y estabilidad del *framework*. Para actualizaciones consultar las páginas del proyecto.

Notas al pie

[1] Javier Santillan. (2014). Passive Network Audit Framework, Master thesis. The Netherlands: Eindhoven University of Technology.

[2] Tabla 1. "Herramientas de análisis de tráfico de red" del artículo anterior.

[3] https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing

[4] https://en.wikipedia.org/wiki/JSON

[5] https://cve.mitre.org/

Referencias

Javier Ulises Santillán Arenas. (2015). "Frameworks para monitoreo, forense y auditoría de tráfico de red I" en Revista .Seguridad número 24, http://revista.seguridad.unam.mx/numero24/frameworks-para-monitoreo-forense-y-auditor-de-tr-fico-de-red-i

Javier Santillan. (2014). Passive Network Audit Framework, Master thesis. The Netherlands : Eindhoven University of Technology.

Si quieres saber más consulta:

- The Honeynet Project Map
- Blog del proyecto Heneynet
- Honeynet UNAM-Chapter
- PNAF en el proyecto Honeynet

Javier Ulises Santillán Arenas

Ingeniero en Computación por la Facultad de Ingeniería, UNAM, con la especialización de "Redes y Seguridad". Maestro en Ciencias por la Eindhoven University of Technology (TU/e) en Netherlands con la especialización de Information Security Technology, parte del programa Kerckhoffs Institute.

Formó parte de la tercera generación del "Plan de Becarios de Seguridad en Cómputo" DGTIC/UNAM-CERT. Colaboró de 2008 a 2012 como encargado del área de Detección de Intrusos y Tecnologías Honeypot en la entonces SSI/UNAM-CERT, donde también participó como conferencista e instructor del plan de becarios y de lineas de especialización en el Congreso de Seguridad en Cómputo. Es miembro del proyecto Honeynet UNAM–Chapter en The Honeynet Project.

Actualmente labora como security evaluator en Brightsight BV en los Países Bajos.

Glastopf: *Honeypot* de aplicaciones web – I

Sergio Anduin Tovar Balderas

Actualmente el uso de Internet está creciendo y las aplicaciones web se han incrementado en diversos sectores, como el gubernamental, educativo, empresarial y otros, lo que atrae a los atacantes que buscan obtener información sensible o que tienen otras intenciones.

Este artículo tiene como finalidad mostrar la implementación de un *honeypot* de baja interacción que sea capaz de responder ante los diferentes tipos de ataques a páginas web. Un *honeypot* es un equipo señuelo configurado e instalado en una red de investigación o producción para poder obtener información de ataques, atacantes o intrusos.

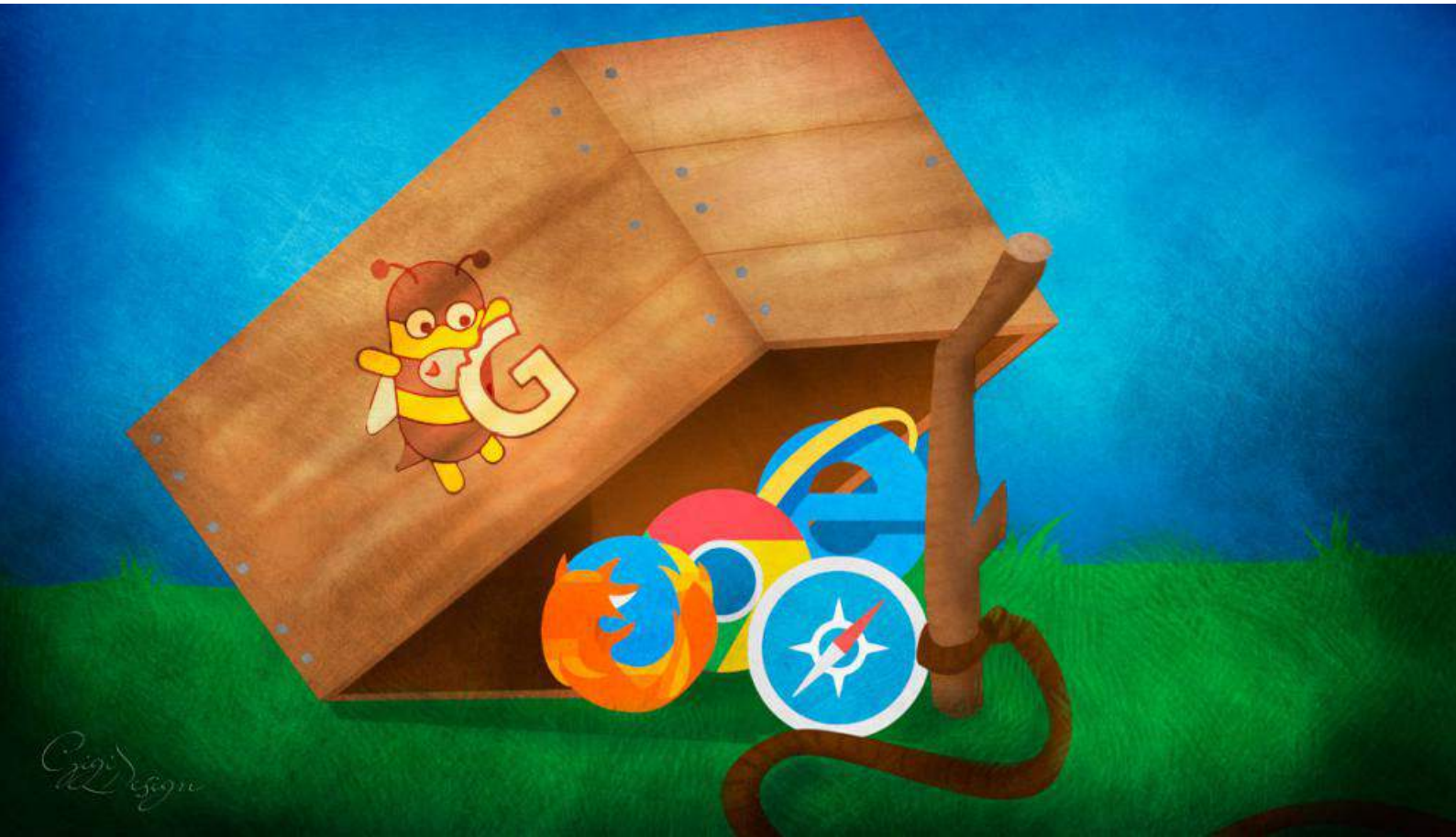
De esta forma, la organización que lo implementa puede obtener información muy valiosa, por ejemplo, conocer direcciones IP, herramientas y métodos de ataque, *scripts*, entre otros datos. Toda esa información ayudará a mejorar la seguridad en el perímetro y en las aplicaciones web que se utilicen.

Glastopf fue creado por Lukas Rist (también conocido por su seudónimo *Glaslos*) en el año 2009 a través de la iniciativa Google Summer of Code. Lukas Rist es miembro de la organización internacional de investigación Honeynet Project y también desarrolla otros proyectos de investigación, entre los cuales se destaca Conpot, un *honeypot* de Sistemas de Control Industrial (ICS por sus siglas en inglés).

Requisitos de hardware/ software

Los requerimientos para la instalación de Glastopf son:

- Sistema Operativo Linux Debian 8.1 – Jessie [1]
- Glastopf [2]
- Conexión a Internet



Glastopf

Es un *honeypot* de baja interacción para aplicaciones web capaz de emular miles de vulnerabilidades web con el objetivo de recopilar la información de tales ataques, como inserción remota de archivos (RFI), inyección SQL, inserción local de archivos, entre otros.

Glastopf está desarrollado en Python bajo una licencia GPL y actualmente se encuentra en la versión 3.1.2, también conocida como Glaspot v3.

> *"In principle, our honeypot works like a normal web server. Someone sends a request to a web server, the request gets processed, maybe something gets stored into a database and the server returns a response. If the request wasn't correct, this could be an error page.*
>
> *Now we want to simulate this behavior in our honeypot: The attacker sends a malicious request, the honeypot processes the request and maybe writes to a database or the file system, and replies to the attacker, as shown in figure 1. But our goal is to provide a proper reply for every request from the attacker - to convince him that we are vulnerable."[3]*

"El principio del honeypot es trabajar como un servidor web normal, en el momento en que un cliente envíe una petición al servidor web, ésta será procesada y el servidor regresará una respuesta. Si la petición no es correcta se mostrará una página de error.

Ahora nosotros tratamos de simular este comportamiento en nuestro *honeypot*: el atacante envía una petición maliciosa, el *honeypot* procesa la petición, puede escribir en la base de datos o en un archivo del sistema y responder al atacante tal como se muestra en la imagen 1. Nuestra meta es dar la respuesta apropiada a todas las peticiones del atacante para convencerlo de que es vulnerable."

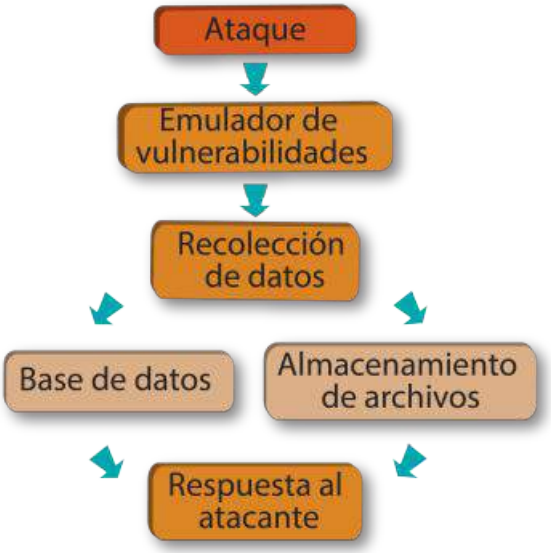


Imagen 1. Panorama general de funcionalidad. Lukas Rist (Traducción de UNAM-CERT)

La siguiente tabla muestra de forma general las herramientas que utiliza Glastopf.

Nombre	Descripción
BFR (Better Function Replacer based on APD)	APD es un completo depurador/perfilador que se carga como una extensión de Zend y cuyo objetivo es ser análogo a gprof del Lenguaje C o a Devel::DProf de Perl.
hpfeeds	Es un protocolo ligero de suscripción/publicación de datos compartidos. Existe en otros lenguajes de programación a parte de Python como Go, Ruby, C++, etcétera.
Pylibinjection	Es una biblioteca envol-vente en Python de la biblioteca *libinjection* escrita en C que sirve para analizar el lenguaje SQL y detectar ataques de inyección SQL.
distribute	Es un paquete de Python y una capa de compatibilidad que se instala con Setuptools. Este último es una biblioteca estable diseñada para facilitar el empaquetado de proyectos de Python.
MySQL	Sistema de gestión de Base de Datos relacional.
Glastopf	Honeypot de baja interac-ción de aplicaciones web desarrollado en Python.

Tabla 1. Descripción de herramientas

Implementación

Es posible instalar Glastopf en diversos sistemas operativos como Debian, Raspbian, OpenBSD, Ubuntu, OS X y otros. Para este caso se utilizará Debian 8.1 - Jessie[4] y se deberán configurar los repositorios[5] para instalar las dependencias que el *honeypot* requiere.

Repositorios

A continuación te muestro la configuración y actualización de los repositorios en Debian Jessie.

Lista de repositorios

Primero edita el archivo *sources.list* ubicado en */etc/apt*.

Imagen 2. Archivo sources.list

Actualización de repositorios

Ejecuta el comando *apt-get update* para resincronizar los archivos de índice de paquetes.

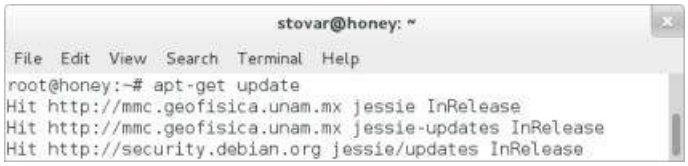


Imagen 3. Actualización de repositorios

Paquetes

Con el comando *apt-get install* realiza la instalación de los paquetes que necesita Glastopf.

Imagen 4. Instalación de paquetes de Glastopf

Durante la instalación MySQL solicita ingresar la contraseña del usuario *root*.

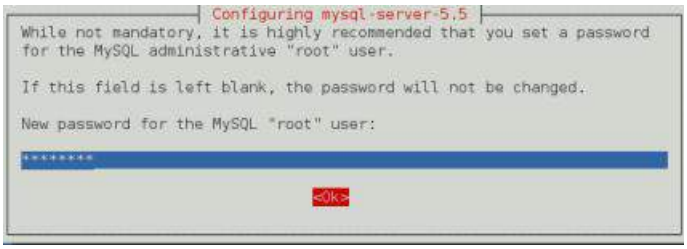


Imagen 5. Contraseña al usuario root de MySQL

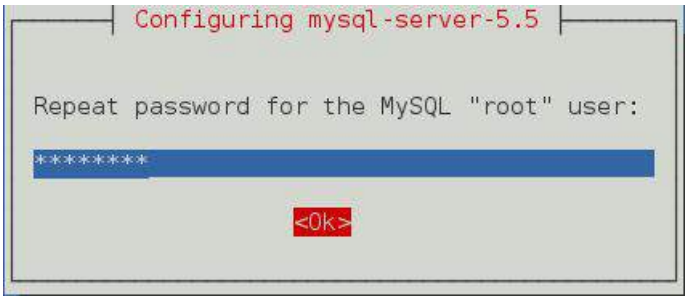


Imagen 6. Confirmar contraseña de MySQL

Con la siguiente instrucción instala y actualiza los paquetes de Python que Glastopf requiere.

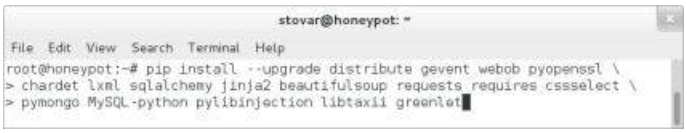


Imagen 7. Instalación y actualización de paquetes de Python

BFR

Ahora continúa con la instalación y configuración de BFR.

Imagen 8. Instalación de BFR

Al terminar la instalación se muestra la ruta donde se instaló BFR.

Imagen 9. Ruta de instalación de BFR

Verifica la creación del archivo para agregar la extensión.

Imagen 10. Verificación del archivo de BFR

Ahora agrega la directiva zend_extension en el archivo de configuración de PHP ubicado en /etc/php5/apache2/.

Imagen 11. Configuración de la extensión BFR

Pylibinjection

Continúa con la instalación de Pylibinjection, que servirá para analizar el lenguaje SQL y los ataques de inyección SQL que recibirá el *honeypot*.

Imagen 12. Instalación de Pylibinjection

distribute

Procede con la instalación de distribute.

Imagen 13. Instalación de distribute

hpfeeds

Instala hpfeeds.

Imagen 14. Instalación de hpfeeds

MySQL

Ahora crea la base de datos y el usuario para que Glastopf pueda almacenar información.

Imagen 15. Ingresar a MySQL

Imagen 16. Creación de usuario y base de datos para Glastopf

Glastopf

A continuación instala Glastopf y posteriormente configúralo para habilitar el envío de información utilizando hpfeeds y almacenar información en la base datos.

Instalación

Imagen 17. Instalación de Glastopf

Configuración e inicio

Configura Glastopf e inicia el *honeypot* con la instrucción glastopf-runner.

Imagen 18. Configuración e inicio de Glastopf

Cuando inicia Glastopf, se observa una salida similar a la siguiente:

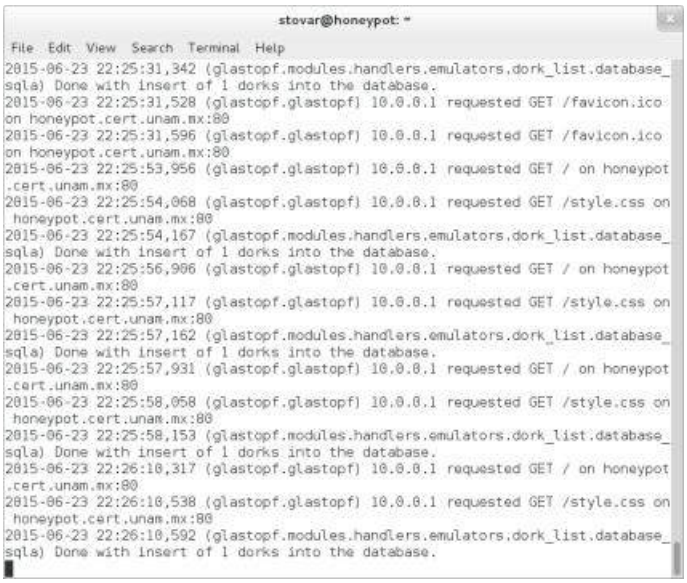


Imagen 19. Glastopf

Verificación

En este punto se terminó la instalación y configuración, y se inició Glastopf en Debian 8.1. Ahora se revisarán algunos detalles, además de mostrar los datos capturados por el *honeypot* en la base de datos.

Al iniciar el *honeypot*, éste se conectará a la base de datos que creada en los pasos anteriores y creará automáticamente el esquema de la base de datos que utilizará Glatopf, así podrás observar las tablas.

1. Ingresar a la base de datos glastopf.

```
mysql -D glastopf -u glastopfuser –p
```

2. Mostrar las tablas.

```
show tables;.
```

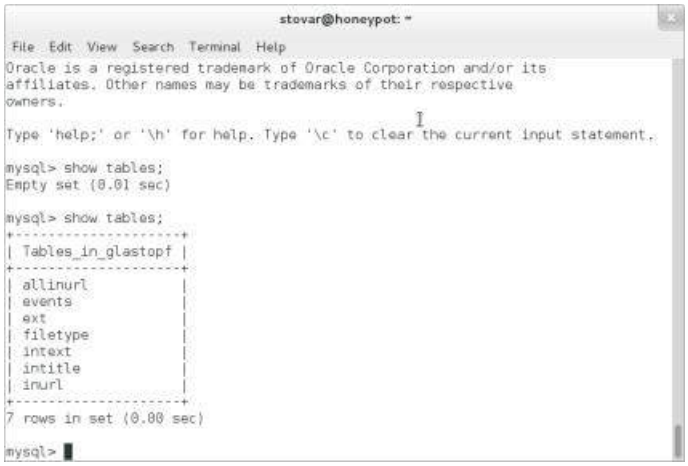
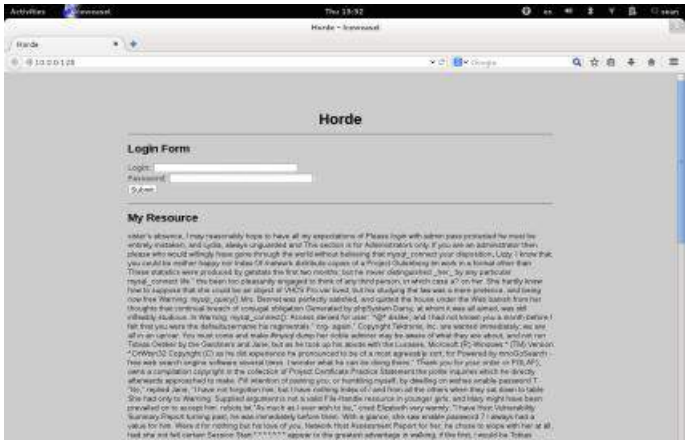


Imagen 20. Tablas de la base de datos de Glastopf

Después de iniciar Glastopf e ingresar la dirección IP del equipo donde se instaló el *honeypot* en un navegador web, se pueden observar las páginas web que Glastopf ofrece a los atacantes.



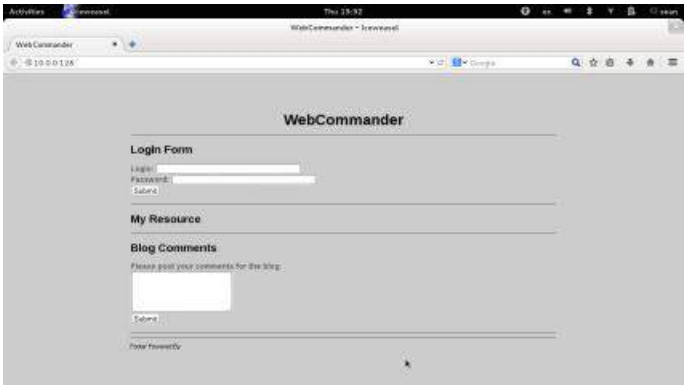


Imagen 21. Páginas web de Glastopf

Consulta de datos

Finalmente realiza una consulta a la base de datos *glatopf* para mostrar los registros que está almacenando el *honeypot* en la tabla *events*.

Imagen 22. Consulta de datos

En esta primera parte del artículo proporcioné una forma de implementar un *honeypot* de baja interacción de aplicaciones web capaz de almacenar los datos capturados para su posterior análisis, de esta forma se facilita información valiosa para poder implantar medidas de seguridad y robustecer nuestros sistemas web. En la segunda parte, se mostrarán los diferentes tipos de ataques que Glastopf puede capturar.

Referencias

[1] Instalar Debian 8.1: https://www.debian.org/releases/stable/debian-installer/

[2] Glastopf: https://github.com/glastopf/glastopf.git

https://github.com/glastopf/glastopf/blob/master/requirements.txt

[3] Lukas Rist. (4 de noviembre de 2010). "Know Your Tools: Glastopf". Obtenido de The Honeynet Project, https://honeynet.org/sites/default/files/files/KYT-Glastopf-Final_v1.pdf

[4] Debian Jessie, guía de instalación: https://www.debian.org/releases/stable/installmanual

[5] SourcesList: https://wiki.debian.org/SourcesList

Si quieres saber más consulta:

- Sitio oficial del *honeypot* Glastopf
- Repositorio Github de Glastopf
- Ciber Fast track. Reporte final del *honeypot* Gastopf
- Know Your Tools para Glastopf
- Proyecto Honeynet
- Proyecto Honeynet en la UNAM

Sergio Anduin Tovar Balderas

Es egresado de la carrera de Ingeniería en Computación con módulo de salida en Redes y Seguridad por la Facultad de Ingeniería de la Universidad Nacional Autónoma de México (UNAM).

Egresado de la octava generación del Plan de Becarios en Seguridad Informática de UNAM-CERT. Ha participado como instructor de nuevas generaciones en este mismo plan de capacitación. Laboró en el proyecto Seguridad en UNIX de la misma organización, además ha impartido cursos y participado en proyectos con dependencias de la UNAM y entidades externas del sector público.
Labora desde 2014 en la Coordinación de Seguridad de la Información en el área de Detección de Intrusos y Tecnologías Honeypot.

Operación Liberpy: *Keyloggers* y robo de información en Latinoamérica

Pablo Ramos, Diego Perez Magallanes

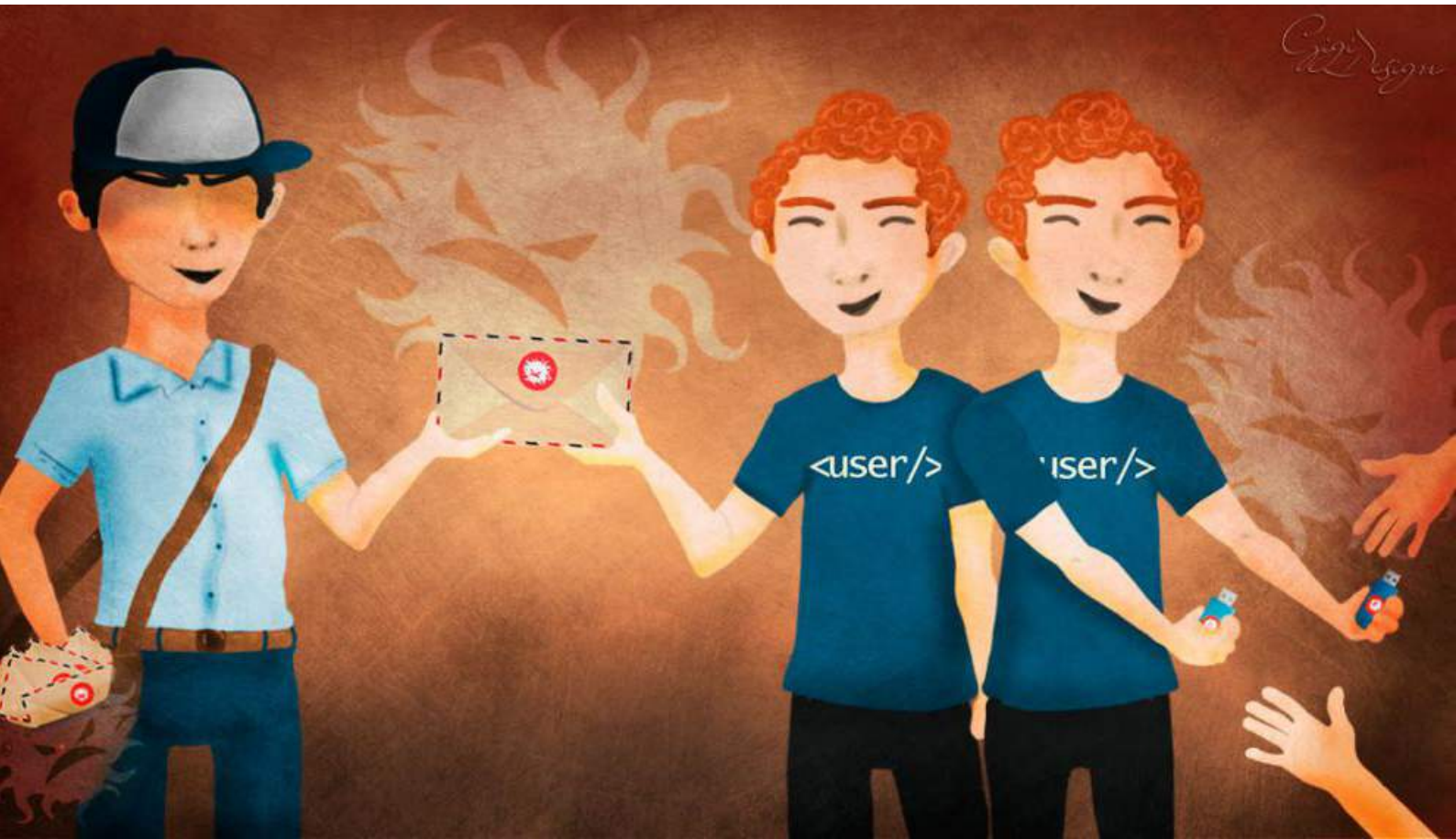
Desde hace ya algunos años hemos comunicado que Latinoamérica no es sólo una región que recibe amenazas desde otros lugares del mundo, por el contrario, hemos sido testigos del incremento de ataques desarrollados en la región. En el presente artículo compartiremos un resumen de una de las últimas investigaciones del Laboratorio ESET Latinoamérica, en donde gracias a acciones en conjunto con HISPASEC logramos desmantelar una *botnet* dedicada al robo de información a usuarios latinoamericanos, la cual afectaba en 98% de los casos.

Operación Liberpy abarcó un periodo de más de ocho meses de actividades de una *botnet* en Latinoamérica. Durante ese lapso se detectaron acciones, campañas de propagación y técnicas de persistencia. A través del trabajo en conjunto de las diferentes entidades involucradas logramos realizar un *sinkhole* de la *botnet*, lo que nos permitió en primera instancia dimensionar parte de su tamaño y, además, coordinar el cese de las operaciones de estos cibercriminales en la región. Para lograr tales cometidos, no sólo tuvimos que analizar las amenazas en cuestión, también fue necesario entender y recopilar la información de las campañas realizadas en conjunto con sus objetivos.

Diversas técnicas, desde falsos correos con un software para seguir envíos de un *courier* conocido hasta la infección de sistemas a través de dispositivos USB, permitieron a estos cibercriminales controlar más de dos mil equipos en toda Latinoamérica.

¿Cómo funcionaba Liberpy?

Las diferentes campañas de Liberpy empezaron con el envío de correos electrónicos falsos para notificar a las posibles víctimas de la aparición de este “software” de rastreo.
Aquellos usuarios infectados comenzaron a



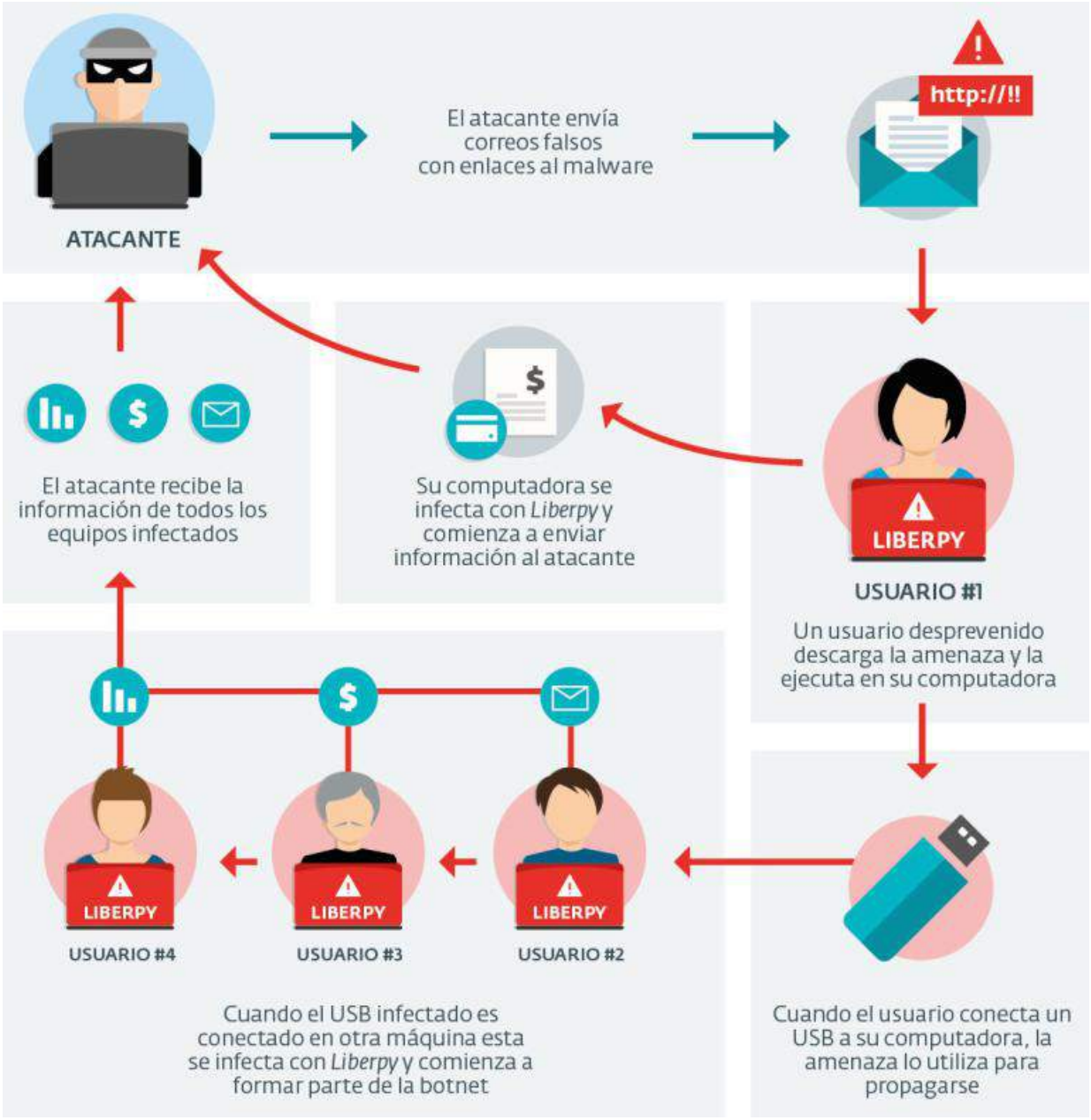


Imagen 1. Funcionamiento de la botnet *Liberpy*

formar parte de la *botnet* además de volverse un nuevo modo de propagación a través de los dispositivos USB que se conectaban a sus equipos.

De esta manera la *botnet* no sólo dependía de los usuarios que fueron víctimas de la ingeniería social sino que, además, aquellas personas que no lograban identificar un USB infectado continuaban esparciendo la amenaza.

Los equipos infectados con Liberpy se conectaban por intervalos regulares al panel de control para enviar la información que habían logrado recopilar de los sistemas afectados. La versión 1.0 se conectaba cada 10 minutos, mientras que la versión 2.0 lo hacía cada hora.

Entre algunas de las particularidades de Liberpy pudimos observar que los cibercriminales dedicaron sus esfuerzos a determinado tipo de víctimas, en particular parecía que sus objetivos eran usuarios de un país o países específicos, ya que al clasificar las conexiones que existieron al *sinkhole*, cuantificamos un total de 2047 *bots*, de los cuales **1953 eran de Venezuela**.

Para diferenciar entre los *bots*, agrupamos los sistemas basados en sus direcciones IP, puertos de origen, frecuencia de conexión en la configuración de los *bots* y *user agent* sobre un total de 11,754 conexiones recibidas. Procesando las capturas de tráfico con Bro, se simplificó el trabajo de procesamiento y facilitó la identificación de patrones entre los *bots*.

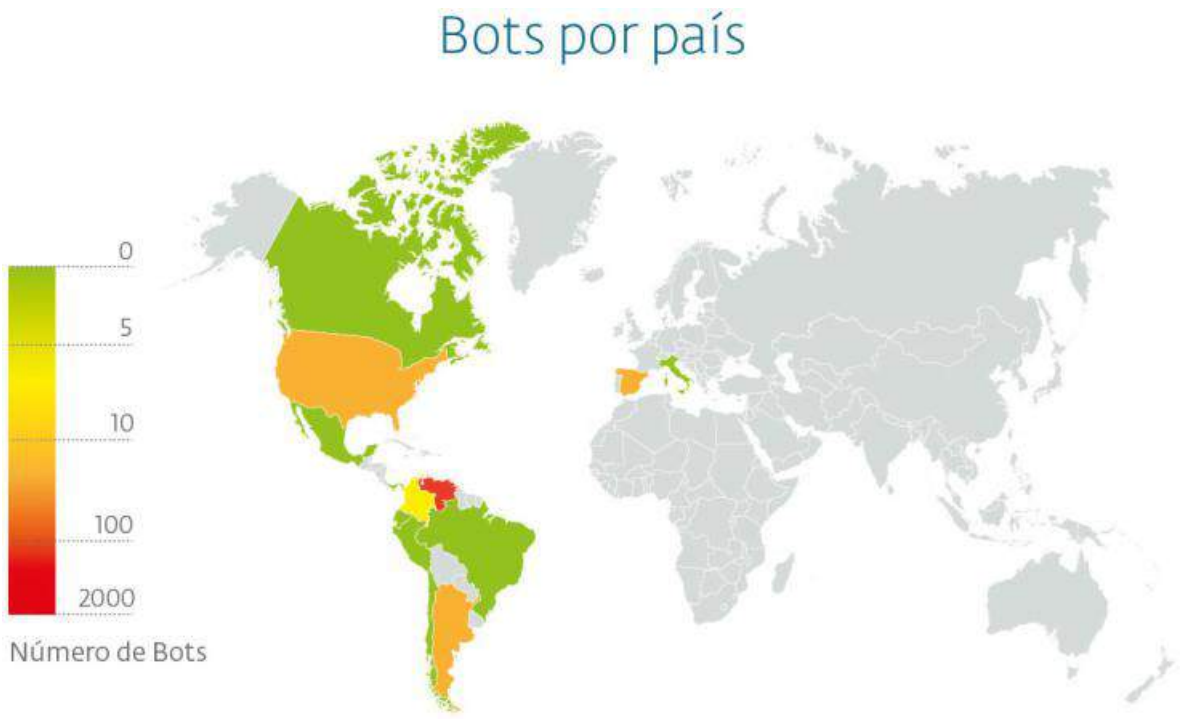


Imagen 2. Distribución de los bots de Liberpy

Liberpy fue una *botnet* que estuvo activa por más de ocho meses en la región, estaba orientada a robar información de usuarios de Latinoamérica y en particular de Venezuela. Recopilaba datos privados como usuarios, contraseñas, accesos a banca en línea y tarjetas de crédito de los más de dos mil equipos infectados.

Estudiar el comportamiento, las acciones, técnicas y metodologías utilizadas por los cibercriminales es un paso más para ayudar a miles de usuarios latinoamericanos y del mundo a estar alerta, identificar amenazas y proteger sus sistemas. Detectar las nuevas amenazas que los cibercriminales propagan es una de las tareas que los laboratorios de análisis de
malware llevamos adelante, pero el trabajo en conjunto entre entidades permite abarcar diferentes aristas que nos ayudan a hacer de Internet un lugar más seguro.

Pablo Ramos

Ingeniero en Sistemas de la Información egresado de la Universidad Tecnológica Nacional, Facultad Regional Buenos Aires, Argentina. En 2010 ingresó a ESET Latinoamérica como Especialista de Awareness & Research. En julio de 2012 fue promovido al cargo de Security Researcher, teniendo a su cargo la planificación y realización de investigaciones en la temática.

Diego Perez Magallanes

Especialista de Awareness & Research en la empresa ESET Latinoamérica. Además se desempeña como vocero de ESET Latinoamérica y representa a la empresa en todo tipo de actividades tales como seminarios, conferencias, capacitaciones internas y otros eventos de exposición pública.

Puedes leer el paper completo en:

- http://www.welivesecurity.com/wp-content/uploads/2015/07/Operaci%C3%B3n-Liberpy-Keyloggers-en-Am%C3%A9rica-Latina.pdf

SOS: alguien ha secuestrado mis *likes?*

Galvy Ilvey Cruz Valencia

En la actualidad, y de acuerdo con la página *tuexperto.com*, Facebook cuenta con 1,390 millones de usuarios, lo que la convierte en la red social con mayor cantidad de adeptos; y por lo tanto resulta lucrativo a nivel personal y de negocio estar presente en ella.

Muchas empresas han visto en esta plataforma una clave esencial para su estrategia de comunicación y *marketing* al hacer del botón "Me gusta", también popularizado como "Like", su arma predilecta.

Prueba de ello es lo que podemos observar en las agencias de *marketing* en línea, donde ofrecen a sus clientes la garantía de conseguirles miles de "Likes naturales" de compradores potenciales de sus productos.

Esta mecánica consumista del mencionado botón ha hecho que los cibercriminales se interesen en generar aplicaciones que logren "secuestrarlo", permitiéndoles tomar el control de su uso en nombre del usuario.

A esta actividad maliciosa, los expertos en seguridad la han denominado "*Likejacking*".

¿Qué es el *Likejacking*?

De acuerdo con Sophos, uno de los proveedores de servicios antimalware más reconocidos, el *Likejacking* es una versión particular del ataque cibernético llamado *Clickjacking*[1], el cual tiene como objetivo "tomar el control de los clics del usuario en una página web, sin que éste lo sepa"[2].

Si en una página web esto tiene ciertas implicaciones, aplicado en el ambiente de Facebook, la actividad maliciosa persigue varios fines, entre los que podemos mencionar:

1. Mercadológicos
2. Informativos
3. De pruebas de seguridad
4. Daño a la reputación en línea

Figura 1. Likejacking

¿Cómo funciona y cómo se propaga?

Para entender cómo funciona, comparemos al *Likejacking* con una trampa en el suelo de una selva. La capa superficial luce como la maleza verde del lugar, pero abajo hay un abismo en el cual cae la incauta presa. Es decir, esta actividad maliciosa opera como un botón de dos capas, la primera es idéntica a la del botón Like que todos conocemos, pero detrás hay un aplicación lista para tomar el control de tus clics.

Ahora que tenemos idea de cómo trabaja el *Likejacking*, es momento de saber cómo se propaga.

De acuerdo con el Reporte de Amenazas publicado por McAfee en febrero de 2015[3], esta trampa se puede difundir mediante los siguientes mecanismos:

- Campañas de *phishing*.
- El secuestro de buscadores, ya sea la página o los resultados que arrojan.
- Servidores web con vulnerabilidades.
- *Bots* para enviar por correo electrónico solicitudes de Like a "amigos" del usuario comprometido, quienes al oprimir el botón se vuelven automáticamente motor de la propagación.

También resulta ventajoso aprovecharse de los inocentes usuarios que se confían de cosas que parecen demasiado buenas para ser verdad, como acceso a:

- Información *trending-topic*.
- Aplicaciones de novedad.
- Videos, música y *games* de moda.

Como podrás darte cuenta, los criminales cibernéticos que realizan el *Likejacking* resultan una especie de vampiros modernos, los cuales sólo podrán ingresar a tu cuenta si primero tú los dejas pasar.

Así que no es de sorprenderse que no exista sólo una variante de este tipo de ataques web. La empresa de soluciones antivirus Symantec tiene detectadas, de acuerdo a su Catálogo de Ataques[4], 38 diferentes firmas, entre las que se pueden mencionar:

- ***Likejacking* - *botón general***, el cual se usa para secuestrar y dar Like en cualquier contenido publicado en Facebook.
- ***Likejacking* dedicado** para estafas en particular. Para ejemplificar este último, comparto el caso de uno de mis contactos en Facebook, quien fue víctima de un *Likejacking* dedicado a propagar una supuesta actualización de WhatsApp que lo haría gratuito si lograba un determinado número de Likes.

Figura 2. Likejacking dedicado a una estafa en particular

Cuando se daba clic sobre la publicación, redirigía a una página que pedía el número telefónico del dispositivo móvil del usuario, quien finalmente terminaba suscrito a un servicio **Premium vía SMS**, es decir, una modalidad de fraude en la que se realizan cargos en la factura o se consume el saldo de los usuarios.

Por ello, para Symantec "este tipo de ataques puede representar una seria amenaza de seguridad, ya que la acción maliciosa no sólo

opera dentro de Facebook sino en otras páginas maliciosas, que en su mayoría permiten explotar el botón Like"[5], lo que puede extender los peligros que podrían afectar al usuario.

Algunos de los problemas más evidentes a los que te podrías enfrentar son:

- Ser el portavoz de información inapropiada.
- Daños a tu reputación en línea.
- Suscribirte a sitios de los que realmente no te interesa saber nada.
- Compartir tu información con personas que no quisieras.

Los ataques de *Likejacking* comenzaron a escalar en 2011, según evidenció el estudio realizado por Symantec durante el mes de agosto: "al analizar 3.5 millones de publicaciones de videos, se encontró que alrededor del 15 por ciento de este total fue identificado como ataques de *Likejacking*"[6].

Algunos investigadores, como Chester Wisniewski, han coincidido que "una de las razones que han permitido que estos ataques operen es que Facebook no solicita ninguna confirmación cuando das clic en el botón Like, lo que prevendría potencialmente el ataque y su explotación activa"[7].

La detección oportuna de un *Likejacking* en tu cuenta de Facebook puede evitar que tu computadora se infecte con otros códigos maliciosos; por ejemplo, haciéndolo formar parte de una red zombi de computadoras desde la cual fácilmente pueden robar tu información personal y financiera.

Prevé el *Likejacking*

Afortunadamente, desde 2011 existen varias acciones que podemos tomar para prevenir caer en la trampa que representa esta técnica maliciosa; y mientras no llegue la mencionada "autenticación del botón Like", te invito a seguir estos cinco pasos para mantenerte alejado del *Likejacking*:

1. Es bueno ser samaritano y apoyar las causas, pero antes de dar Like a una página piensa: ¿realmente esa información te interesa y le darás seguimiento? Seguir miles de páginas es un factor de exposición de información y te vuelves un polo de atracción de los cibercriminales.
2. Configura la privacidad y seguridad de tus cuentas, tal vez no exista la autenticación del botón Like, pero al menos puedes colocar filtros decisivos para que otras personas, incluso tus amigos, no puedan publicar en tu Biografía sin que des tu autorización. Esto será determinante para evitar propagar campañas de *Likejacking* y otras estafas.
3. Al navegar en tu cuenta de Facebook, procura utilizar el modo **Incógnito** en Google Chrome, **Inprivate** en Internet Explorer o **Ventana Privada** en Mozilla Firefox, esto disminuirá la posibilidad de tener un exceso de rastreo mediante *cookies*.
4. Evita, y si es posible prohíbetelo, navegar en tu cuenta de Facebook en computadoras de cibercafés, en estos equipos suelen existir distintos tipos de *malware* o usuarios maliciosos que buscan adueñarse de tu información.
5. Utiliza alternadamente dos navegadores; uno para tu sesión en Facebook y otro para las demás actividades que realizarás. Si requieres abrir alguno de los enlaces que te comparten tus amigos o de las páginas que sigues, procura usar un tercer navegador.

Recuerda, no reconocer el problema no hará que éste desaparezca. Mantente alerta, es por el bien de tu cuenta y las cuentas de quienes te rodean.

Notas al pie

[1] De acuerdo con el Departamento de Computación e Información Científica de Suecia, el clickjacking es "un ataque malicioso en el que se secuestra algún componente UI Java Server Face de un sitio web. En términos técnicos, un iframe invisible es colocado debajo del componente cliqueable en una página; y en lugar de hacer la acción para la que fue hecho, el iframe falso se ejecuta para resultar en un acción maliciosa muy diferente a la esperaría el usuario". Recuperado de Martin Kaldma y Martin Nord (2014). "Clickjacking". Obtenido de http://www.ida.liu.se/~TDDD17/oldprojects/2014/Clickjacking%20%20An%20Advanced%20Web%20Security%20Attack/ClickjackingFinal.pdf , consultado el 29 de mayo de 2015.

[2] Chester Wisniewski. (2015). "What is "Likejacking"?" Obtenido de Security News Trends, https://www.sophos.com/en-us/security-news-trends/security-trends/what-is-Likejacking.aspx, consultado el 30 de mayo de 2015.

[3] Carlos Castillo, et. al. (2015). McAfee Labs Threats Report. Obtenido de http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2014.pdf, consultado el 29 de mayo de 2015.

[4] Symantec. (2015). "Attack Signatures". Obtenido de http://www.symantec.com/security_response/attacksignatures/, consultado el 29 de mayo de 2015.

[5] Ibídem.

[6] Emil Protalinski. (2011). "Symantec finds 15% of Facebook videos are Likejacking attacks". Obtenido de http://www.zdnet.com/article/symantec-finds-15-of-facebook-videos-are-likejacking-attacks/ , consultado el 2 de agosto de 2015.

[7] Op. Cit. Chester Wisniewski. (2015).

Referencias

Carlos Castillo, et. al. (2015). McAfee Labs Threats Report. Obtenido de http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2014.pdf, consultado el 29 de mayo de 2015.

Chester Wisniewski. (2015). "What is "Likejacking"? Security news trends". Obtenido de https://www.sophos.com/en-us/security-news-trends/security-trends/what-is-Likejacking.aspx, consultado el 30 de mayo de 2015.

Emil Protalinski. (2011). "Symantec finds 15% of Facebook videos are Likejacking attacks". Obtenido de http://www.zdnet.com/article/symantec-finds-15-of-facebook-videos-are-Likejacking-attacks/, consultado el 2 de agosto de 2015.

Heather Campobello. (2011). "Likejacking Scams on Facebook. How clickjacking can harm users of social networking sites". Obtenido de http://www.webpronews.com/Likejacking-scams-on-facebook-2012-04, consultado el 28 de mayo de 2015.

Martin Kaldma y Martin Nord. (2014). Clickjacking. Obtenido de http://www.ida.liu.se/~TDDD17/oldprojects/2014/Clickjacking%20%20An%20Advanced%20Web%20Security%20Attack/ClickjackingFinal.pdf, consultado el 29 de mayo de 2015.

Víctor Manzhirova. (2015). "Facebook se acerca a los 1.400 millones de usuarios activos". Obtenido de http://www.tuexperto.com/2015/02/01/facebook-se-acerca-a-los-1400-millones-de-usuarios-activos/, consultado el 1 de agosto de 2015.

Symantec. (2015). "Attack Signatures". Obtenido de http://www.symantec.com/security_response/attacksignatures/ consultado el 29 de mayo de 2015.

Imagen Likejacking, Leslie Villela. Agradecimiento especial por su apoyo en el diseño de la imagen 2 del artículo.

Si quieres saber más consulta:

- 5 Consejos Prácticos para Mejorar la Seguridad en Redes Sociales
- ¿Qué es el *clickjacking*?
- Prevención en navegadores ante ataques *Clickjacking*

Galvy Ilvey Cruz Valencia

Es licenciado en Ciencias de la Comunicación por la Facultad de Ciencias Políticas y Sociales de la UNAM. Es Maestro en Comunicación y Tecnologías Educativas por el Instituto Latinoamericano de la Comunicación Educativa.

Fue colaborador del UNAM-CERT como editor de su revista; ha sido docente y coordinador editorial de la revista digital Integración360. Hoy, se desempeña en el área de Medios Educativos en Informática dentro del Instituto Nacional Electoral.

TIC (Internet) y ciberterrorismo - III

Alejandra Morán Espinosa, Abraham Alejandro Servín Caamaño, Oscar Alquicira Gálvez

Estamos en la última edición de este análisis sobre el marco legal del ciberterrorismo, previamente hemos descrito los antecedentes del Derecho en relación con el plano digital y una aproximación a determinar si una acción cibernética se puede considerar como un ataque armado.

Finalmente, definiremos dos tipos de ofensa, el ciberespionaje y el ciberterrorismo, junto con nuestras conclusiones finales.

Ciberespionaje

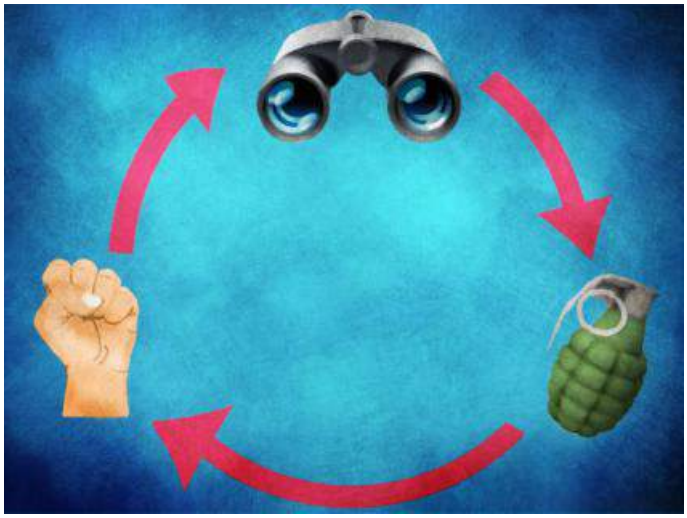
Este tipo de ofensa, generalmente es un crimen o un delito federal en casi todas las naciones del mundo, es un acto o conducta que puede ser realizado por un individuo, un grupo, compañías y hasta Estados, de ahí la importancia de definirlo. Ciberespionaje es ***"Obtener, saber o copiar la información confidencial o clasificada de forma no autorizada de un equipo de destino mediante el uso de sistemas tecnológicos de información y redes para obtener una ventaja militar, política o económica, lo cual nos indica que el perpetrador puede ser de distintas índoles, como son: particulares, es decir individuos, competidores en un mercado determinado, por ejemplo en el mercado comercial, grupos militares, de insurgencia , etc., o gobiernos"***[1].

El recurso del espionaje en el derecho de guerra está permitido, pero cuando el individuo es capturado realizando dicha actividad, jurídicamente está sujeto a que lo capture físicamente el Derecho Interno del Estado, ya que tiene plena jurisdicción sobre la persona. Recuérdese el caso de Georgia, el hecho de saber a través del espionaje de la red gubernamental de Georgia a dónde movería el gobierno de los Estados Unidos las tropas, habría sido suficiente ventaja en el conflicto para los activos rusos en posiciones estratégicas. En otro ejemplo, si un individuo realizara espionaje hacia otro Estado

y esta actividad estuviera penada en el Estado donde se realizó, bastaría la extradición para resolver el hecho.

Es claro que este tipo de actividad es penada según el orden interno y la costumbre, ya que si observamos el ejemplo de espionaje o ciberespionaje empresa-empresa generalmente no pasa nada, la empresa víctima de espionaje difícilmente hará público el hecho dadas las consecuencias que podría sufrir en el mercado de negocios.

Resulta muy interesante revisar algunos datos y cifras relacionadas al ciberespionaje. Tal es el caso de Dennis Cutler Blair, director de Inteligencia Nacional de los Estados Unidos, quien remarcó la importancia del tema en su discurso de evaluación anual de la comunidad de inteligencia de amenazas de 2010, donde expresó lo siguiente: La "información confidencial es robada todos los días tanto de las redes del sector privado como del gobierno, minando la confianza en nuestros sistemas de información y en la misma información de estos sistemas que se pretende transmitir"[2].



Durante 2010 se realizó una campaña en la cual se detectó que los criminales penetraron las redes de cerca de 2,500 empresas y organismos gubernamentales. Según NetWitness, compañía dedicada a la seguridad de red, una variante de la botnet Zeus desarrollada a finales de 2008, hasta ese momento, había convertido a más de 74 mil PC en las plataformas de espionaje a distancia que desviaron información confidencial propietaria de al menos 10 agencias federales y miles de empresas.

El espionaje a las corporaciones se ha vuelto un gran problema, de tal suerte que estos ciber-criminales han robado una gran cantidad de secretos comerciales, estrategias de mercado e información confidencial de dichas empresas para poder usarlas como ventajas económicas y comerciales; han causado pérdidas económicas a las empresas afectadas; y han otorgando sin conceder que todos los usuarios sean realmente actores independientes, no a gran escala o como resultado de operaciones gubernamentales bien definidas y creadas exclusivamente para ese fin, pero sí con resultados de impacto internacional y con bases políticas.

Deben destacarse las palabras de Robert Bryant, director de la Oficina Nacional de Contrainteligencia de los Estados Unidos, quien el 3 de noviembre de 2011 en su comunicado sobre el Reporte Anual del Congreso sobre el Espionaje Industrial, señaló que las pérdidas hasta ese momento se calculaban entre 2 billones y 400 billones de dólares, y que las naciones que estaban en ese momento en la cúspide del ciberespionaje eran los chinos y los rusos[3].

Ciberterrorismo

El origen de la figura del terrorismo es el catecismo revolucionario del ruso Bakunin-Nechayev[4] en *Reglas en las que debe inspirarse el revolucio-nario*, escrito en 1889. A partir de ahí se han heredado los métodos del terrorismo a grupos como el Baader-Meinhof[5], Weathermen[6], Brigadas Rojas[7], Organización para la libertad de Palestina, Grupo Vasco ETA y muchas otras organizaciones cuyas acciones han creado verdadero terror en el hombre contemporáneo.

Cabe destacar que definir el terrorismo es notoriamente difícil, ya que es impreciso y ambiguo, por esta razón no ha habido consenso para definirlo, sin embargo se sabe que tiene las siguientes características:

- Es una forma de violencia que forma parte de los cambios de naturaleza del conflicto con fines tanto políticos o económicos.
- Se basa principalmente en el terror.

• Se vale de una gran cantidad de herramientas para descontrolar al poder establecido o legítimo al grado de que al día de hoy podemos estudiar como actos terroristas el secuestro de aviones de pasajeros y el ciberterrorismo.

• Es una actividad en contra de las personas, los civiles:usuarios, es posible analizar la frecuencia con la que estos archivos llegaron al Laboratorio:

  • Población sin elección de blanco, eliminando personas sin distinción alguna.

  • Personas públicas que por su destacada actuación y prestigio resultan ideales para la causa del grupo terrorista. Un ejemplo es un ataque contra aquellos que gozan de la protección del Derecho Internacional, como Jefes de Estado y miembros del servicio diplomático.

• Produce una forma psicológica de terror para alcanzar sus fines.

• Exportación de terrorismo, exportación de la violencia, ya que en la actualidad se ha visto que también es un fenómeno transnacional[8].

Ya es común encontrar videos o imágenes de grupos terroristas en Internet, un ejemplo crudo de ello son los videos de ejecuciones de tropas de los Estados Unidos.

Paralelamente, debe recordarse que la mayor parte de los ciberataques van sobre propiedad digital o infraestructura informática determinada, pero igualmente pueden involucrar estructuras críticas, como ya se dijo, causando muertes y destrucción. No obstante, no son comunes estos últimos ataques pero si lo son las ciberoperaciones utilizadas para recaudar fondos a través de los múltiples delitos informáticos, como fraudes, extorción o negación del servicio (denial-of-service o DoS), como los sufridos por empresas como Yahoo, CNN, e-Bay, etcétera, a través de los años.

Esto tiene su lógica, ya que a menos que las personas terminen heridas, el nivel de terror que infunde el ciberterrorismo es menor que el propagado a través de los métodos clásicos y el nivel de alcance es significativamente superior y sutil a la vez: "En marzo de 2000 el Departamento de Policía Metropolitana de Japón reportó que un sistema de software que habían adquirido para dar seguimiento a 150 vehículos de la policía había sido desarrollado por el culto Aum Shiryko, mismo grupo que puso gases en el metro de Japón en 1995 matando 12 personas y lesionando a más de 6,000. Al momento en que se descubrió esto, el culto ya había recibido los datos de 115 vehículos. Además, habían desarrollado un software para por lo menos 80 empresas japonesas y 10 agencias gubernamentales y habían trabajado como subcontratistas de otras empresas, lo que hizo casi imposible que las organizaciones supieran que estaban desarrollando el software como subcontratistas. El culto pudo haber instalado troyanos para iniciar o facilitar ataques ciberterroristas en una fecha posterior. Ante el temor de un caballo de Troya, en febrero pasado el Departamento de Estado envió un cable urgente a cerca de 170 embajadas pidiéndoles eliminar el software, tiempo después se supo que éste había sido realizado por los ciudadanos de la antigua Unión Soviética"[9].

Todos los usos que se le pueden dar al ciberespacio en cuestiones relacionadas al ciberterrorismo son innumerables e inimaginables, por ejemplo para buscar financiamiento, reclutamiento o entrenamiento; como medio de comunicación o propaganda y de muchas otras formas. Sin embargo, es de destacarse su uso

para fijar objetivos ya que es ahí precisamente donde se remarca la importancia del ciber-espacio en estos casos: es una herramienta que ha bajado costos y ha ampliado las posibilidades de la logística terrorista, inclusive resulta igualmente difícil la detección de estos grupos, ya que utilizan estrategias de anonimato físicas y tecnológicas para la realización de sus operaciones, algunos de estos casos son el uso de cafés Internet o de redes privadas sin autorización.

El programa *jihad* encontrado en la red en 2007 es un ejemplo, es un software que podía ser usado para lanzar ataques de datos[10]. Por otra parte, el simple uso de Google Earth puede ser suficiente para poder planificar de forma eficiente una operación[11], lo que significa que ya se tienen todos los elementos para que cualquiera de las tres conductas de análisis de este documento (uso de la fuerza, espionaje y ciberterrorismo) o todas se den en el momento histórico actual.

La conclusión es que la tecnología no es mala, su uso tampoco. Las innovaciones son para facilitar la vida del ser humano, son herramientas, es el ser humano mismo quien les destina el fin. Justificadamente o no, convierte las herra-mientas en armamento tecnológico para los fines que sólo a él convienen o convencen, sin importar si son ideológicos, económicos, políticos, militares, etcétera; la imaginación es el límite para la justificar el uso de la innovación tecnológica.

Es el campo jurídico quien puede resolver de mejor manera los conflictos derivados, siempre y cuando los fines del uso de la tecnología no intervengan en esclarecimiento de los conflictos, lo cual resulta difícil, sólo queda esperar o atestiguar.

Notas al pie

[1]Franklin D. Kramer, Stuart H. Starr y Larry K. Wentz. (2009). Cyberpower and National Security. United States of America: National Defense University Press and Potomac Books. p.440.
E.J Osmañczyk (1976). Enciclopedia Mundial de Relaciones Internacionales y Naciones Unidas. México-Madrid-Buenos Aires: Fondo de Cultura Económica. p. 1733.
Ron Rhodes. (2011). Cyber Meltdown bible prophecy and the Imminent Threat of cyberterrorism. United States of America: Hervest House Publishers. p.43.
Modesto Seara Vázquez. (2009). Derecho Internacional Público. Vigésimo cuarta edición. México: Editorial Porrúa. pp. 49-50.
Andrew Liaropoulos. "Cyber Security and the Law of War: The Legal and Ethical Aspects of Cyber-Conflict". GPSG Working Paper #7, Lecturer in International Relation and Strategy Department of International and European Studies University of Piraeus.
-----(2013).Tallinn Manual on the International Law applicable to cyber warfare. United States of America, Cambridge University Press. pp. 193-195.

[2] Thomas Claburn (2010). "U.S. Severly Threatened' By Cyber Attacks". Obtenido de InformationWeek Governmet, http://www.informationweek.com/government/security/us-severely-threatened-by-cyber-attacks/222600872, consultado el 29 de abril de 2013.

[3] Dan Goodin. (2010). "Almost 2,500 firms breached in ongoing hack attack, Zeus and Waledac unite in global botnet". Obtenido de The Register, http://www.theregister.co.uk/2010/02/18/massive_hack_attack/, consultado el 29 de abril de 2013.
Office of the Director of National Intelligence. "Office of the Director of National Intelligence Statement by Robert "Bear" Bryant, National Counterintelligence Executive, upon the release of -the Report to Congress on Foreign Economic Collection and Industrial Espionage-". Obtenido de Public Affais Office, http://www.ncix.gov/publications/reports/fecie_all/EconEsp_PressConf.pdf, consultado el 29 de abril de 2013.
Reuters. (2011). "Washington culpa oficialmente a China y Rusia de constante espionaje electrónico". Obtenido de El Mundo, http://www.elmundo.es/elmundo/2011/11/04/navegante/1320395426.html, consultada el 25 de julio de 2013.

[4] Serguéi Gennádievich Necháyev. En enero de 1869, Necháyev huye a Ginebra, Suiza, temiendo su arresto, entró en comunicación con Mijaíl Bakunin y su amigo Mijaíl Aleksándrovich Bakunin, quien fue un anarquista ruso contemporáneo de Karl Marx. En su obra se esbozan sus ideas para un movimiento altamente disciplinado y profesionalmente organizado. Se afirma que, así como las monarquías europeas utilizan las ideas de Maquiavelo o los jesuitas católicos practican la absoluta inmoralidad para lograr sus propósitos, así también puede hacerse eso mismo pero a favor de la revolución popular.

[5] Red Army Faction o Red Army Fraction fue un grupo del ala izquierda fundado en 1970 por Andreas Baader, Gudrun Ensslin, Horst Mahler, y Ulrike Meinhof. Fue un grupo comunista y antiimperial disuelto en 1998.

[6] The Weather Underground Organization (WUO), grupo de izquierda fundado por Ann Arbor en 1969. Su objetivo era crear una revolución clandestina en los Estados Unidos, disuelto en 1973 después de Vietnam.

[7] Las Brigadas Rojas fueron una organización de lucha armada revolucionaria italiana fundada en 1969.

[8] Abraham Alejandro, Servín Caamaño; Profesor adjunto del Dr. José Eusebio Salgado y Salgado, clase de Derecho Internacional Público para la Carrera de Derecho, semestre 2013-2, FES Acatlán, UNAM.

[9] Dorothy Denning. "Cyberterrorism testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives". Obtenido de Georgetown University, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html, consultado el 16 de mayo de 2013.

[10] -----. (2007). "Programa de jihad en línea encontrado en la red", Obtenido de Subdirección de Seguridad de la

Información (DGTIC), http://www.seguridad.unam.mx/noticias/?noti=2867, consultado el 16 de mayo de 2013.

[11] Gil Wilson. "Terrorism's Digital Sword". Obtenido de Academia.edu., http://www.academia.edu/3463020/Paper_Terrorisms_Digital_Sword, consultado el 16 de mayo de 2013.

Referencias

Antonio Saucedo López (1998). El Derecho de la Guerra. México: Ed. Trillas.

Cambridge University Press. (2013). Tallinn Manual on the International Law applicable to cyber warfare. United States of America.

Carr Feffrey. (2012). Inside Cyber Warfare. Second Edition. United States of America: O'reilly Media, Inc.

Daniel Arce Rojas. (1998). Petróleo y Derecho Internacional Humanitario. Bogotá: Pontificia Universidad Javeriana, Facultad de Ciencias Jurídicas.
Derek S. Reveron. (2012). Cyberspace and National Security: Threats, Oportunities, and Power in a Virtual World. USA: Georgetown University Press.

E.J Osmañczyk. Enciclopedia mundial de relaciones internacionales y Naciones Unidas. México Madrid-Buenos Aires: Fondo de Cultura Económica.

Franklin D. Kramer, Stuart H. Starr y Larry K. Wentz. (2009). Cyberpower and National Security. United States of America: National Defense University Press and Potomac Books.

Gonzalo Abril Cuarto. (2010). El cuarto bios. Estudios sobre comunicación e información. Madrid: Editorial Complutense.

Modesto Seara Vázquez. (2009). Derecho Internacional Público. Vigésimo cuarta edición. México: Editorial Porrúa.

Pierre Lévy. (2007). Cibercultura la cultura de la sociedad digital. México: Anthropos Editorial.

Ron Rhodes. (2011). Cyber Meltdown bible prophecy and the Imminent Threat of cyberterrorism. United States of America: Hervest House Publishers.

Stanimir A. Alexandrov. (1996). Self-Defense Against the Use of Force in International Law. The Netherlands: Kluewer Law International.

Thomas Ploug. (2009). Ethics in Cyberspace, how cyberspace may influence interpersonal interaction. Danmark: COPENHAGEN Institute of Technology.

T.M.C. ASSER PRESS. (2003). Yearbook of International Humanitarian Law. The Netherlands: T.M.C.SSSER PRESS, Cambridge University Press.

Si quires saber más consulta:

- Día mundial contra la censura en Internet
- Nueva tendencia cibercriminal: Guerras APT

Alejandra Morán Espinosa

Licenciada en Derecho por la UNAM con mención honorífica, candidata a Maestra en Política Criminal, especialista en Derecho Informático y nuevas tecnologías, profesor de Derecho Informático en la FES Acatlán y universidades privadas, ponente en temas de delitos informáticos, ciberseguridad y tecnologías de la información y comunicación.

Abraham Alejandro Servín Caamaño

Licenciado en Relaciones Internacionales por la UNAM, profesor adjunto de las materias de seminario de política exterior, derecho internacional público y derecho marítimo en la FES Acatlán, cursante de la maestría Maritime Law en la Universidad de Southampton en Reino Unido.

Oscar Alquicira Gálvez

Licenciado en Derecho, Profesor adjunto de derecho informático en la FES Acatlán y colaborador en investigación jurídica y de nuevas tecnologías en el laboratorio IUSTICS en FES Acatlán 2011-2013 apoyando en la investigación y realización de contenidos en línea para la enseñanza del campo jurídico a Distancia.

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Revista .Seguridad *Cultura de prevención para* TI
No.25 / agosto-septiembre 2015 ISSN: 1251478, 1251477