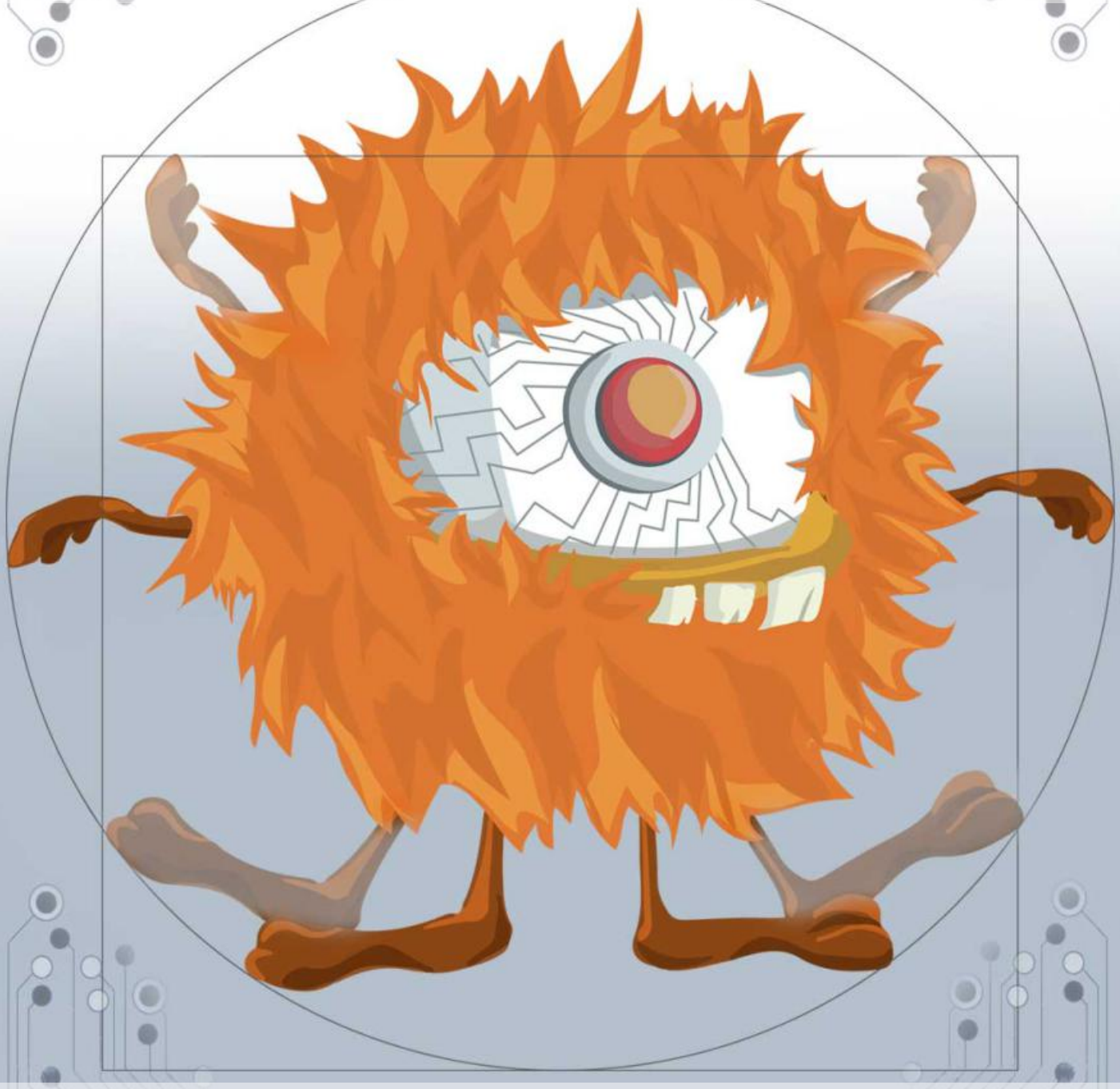
No.24 / junio-julio 2015 ISSN: 1251478, 1251477

.Seguridad 24

Cultura de prevención para TI

Aproximación al malware



De la detección al aprendizaje

Malware PoC II | MAAGTICSI | Frameworks para monitoreo | TICs y ciberterrorismo | ¿Quién te conoce? | CPL Malware

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

Aproximación al *malware*

De la detección al aprendizaje

Hace tiempo publicamos sobre una amenaza que se propagaba a través de videos en las redes sociales, en uno de los comentarios se leía: "Éstos no son atacantes, eres tú mismo quien se infecta por no tomar precauciones", dicho comentario trataba de explicar a la comunidad que una infección por software malicioso no siempre es responsabilidad de terceros sino que puede ser producto de un error en las acciones de los usuarios. Si bien había cierta razón en esas ideas, nos hizo reflexionar en lo siguiente: **Detrás de cada muestra maliciosa, hay un atacante al acecho.**

Es decir, existen piezas de malware que necesitan muy poca interacción de los usuarios para infectar los sistemas. Pero hay otras que requieren de mucho trabajo "creativo" de ingeniería social para llevar al usuario a descargar, ejecutar, aprobar o realizar acciones que resulten en una infección.

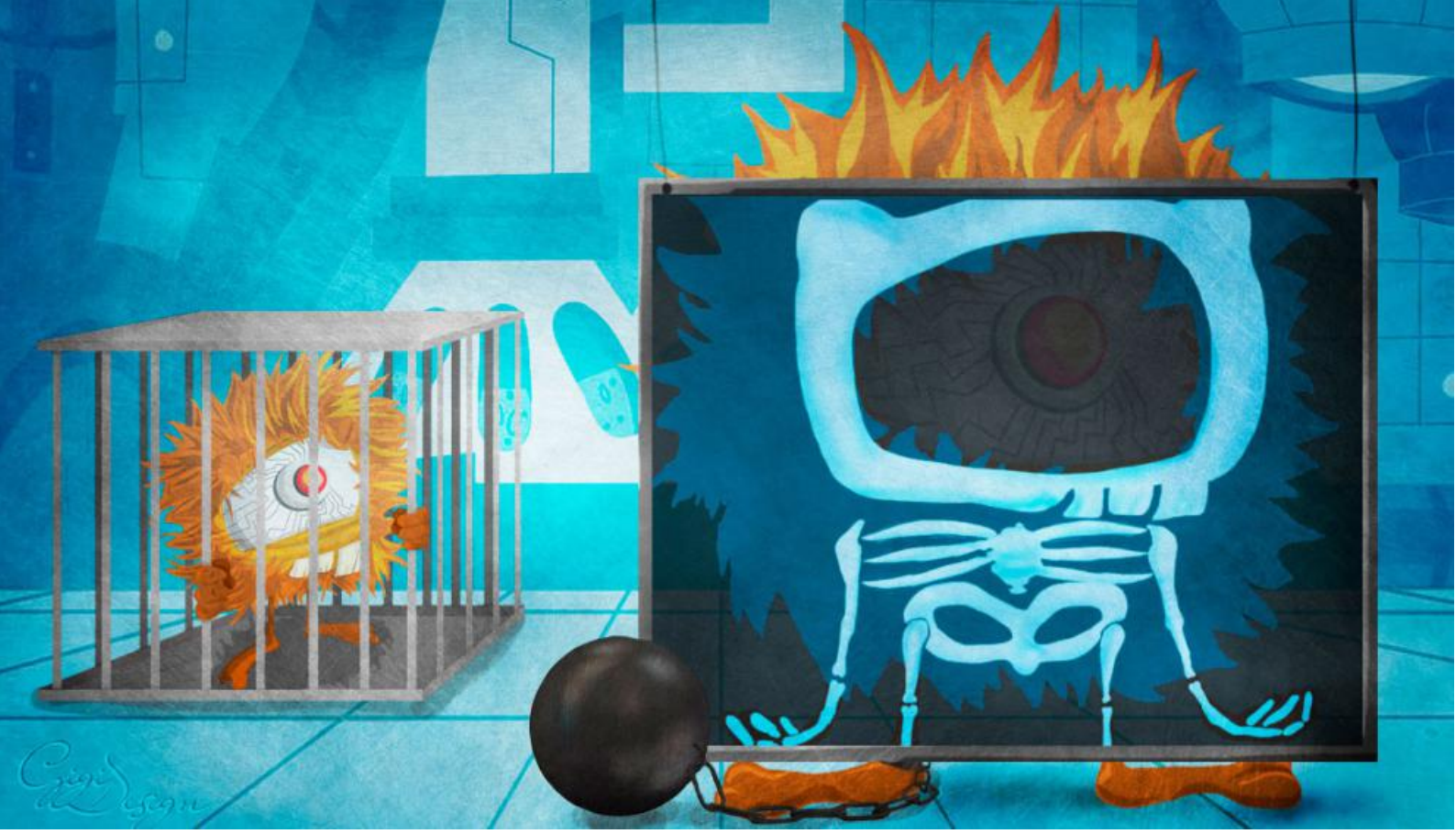
A primera vista parece que somos nosotros mismos quienes provocamos la infección, pero no hay que olvidar que es un atacante (al menos) quien **desarrolla, distribuye** y se **beneficia** del software malicioso. Y para conocer más sobre estos tres aspectos queremos ofrecerte un panorama de los actores principales en el desarrollo de los códigos maliciosos: El malware, los atacantes que lo crean y los analistas que lo estudian.

Creemos que es importante aprender sobre el comportamiento y las nuevas amenazas para poder prevenir ataques similares en el futuro y contrarrestar, en alguna medida, la proliferación del *malware*; pensamos que detrás de cada muestra maliciosa no sólo hay un atacante: **detrás de cada muestra maliciosa, también hay un analista de malware en su laboratorio.**

Jazmín López Sánchez
Editora
Coordinación de Seguridad de la Información

.Seguridad
Cultura de prevención para TI

.Seguridad Cultura de prevención TI M.R. / Número 24 / junio-julio 2015 / ISSN No. 1251478, 1251477 / Revista Bimestral, Registro de Marca 129829



PoC: Captura de *malware* con el *honeypot* Dionaea - Parte II

Jonathan Banfi Vázquez

En el artículo anterior se describió una forma de instalar Dionaea y algunas de sus características, en esta ocasión, se explicará cómo se configura el laboratorio virtual para ver paso a paso la captura de una muestra de *malware*.

El objetivo del *honeypot* Dionaea es obtener una copia del *malware* que intenta propagarse por la red al brindar servicios que pretenden ser vulnerables. En este artículo se describirá el proceso de dicha captura.

Los servicios que proporciona el *honeypot* Dionaea son los siguientes:

- SMB (*Server Message Block*): 445
- HTTP (*Hypertext Transfer Protocol*): 80
- HTTPS (*Hypertext Transfer Protocol Secure*): 443
- FTP (*File Transfer Protocol*): 21
- TFTP (*Trivial File Transfer Protocol*): 69
- MySQL (*Structured Query Language*): 3306
- MSSQL (*Microsoft Structured Query Language Server*): 1433
- EPMAP (*Endpoint Mapper*): 135
- SIP (*Session Initiation Protocol*): 5060/5061
- Nameserver (*Host Name Server*): 42

Para esta prueba de concepto se empleará un gusano informático que ataca el servicio SMB de Windows, este último es un protocolo de red que permite compartir recursos, como archivos e impresoras, entre equipos de cómputo.

Configuración del laboratorio virtual

El laboratorio consistirá de dos máquinas virtuales generadas en la plataforma VMware (aunque se puede utilizar cualquier otro software de virtualización), una con sistema operativo

Windows XP y otra con GNU/Linux Debian 7. Además, estará en una red interna que permitirá establecer un segmento de red dentro del rango propuesto 192.168.1.X/24.

Imagen 1. Laboratorio de análisis

Las interfaces de red en ambos equipos deberán configurarse en modo “Host-Only”, por lo que solamente tendrán comunicación entre ellas.

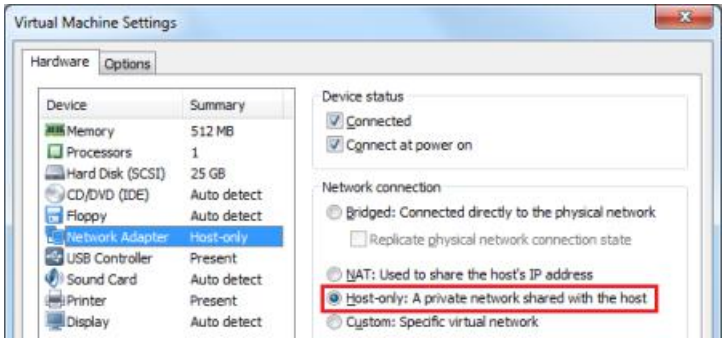


Imagen 2. Adaptadores de red en modo "Host-only"

La interfaz de red del equipo Windows debe configurarse de acuerdo a los siguientes parámetros para garantizar que todo el tráfico sea redirigido a la máquina Debian:

- **Dirección IP:** 192.168.1.5
- **Máscara de subred:** 255.255.255.0
- **Puerta de enlace predeterminada:** 192.168.1.30
- **Servidor DNS preferido:** 192.168.1.30

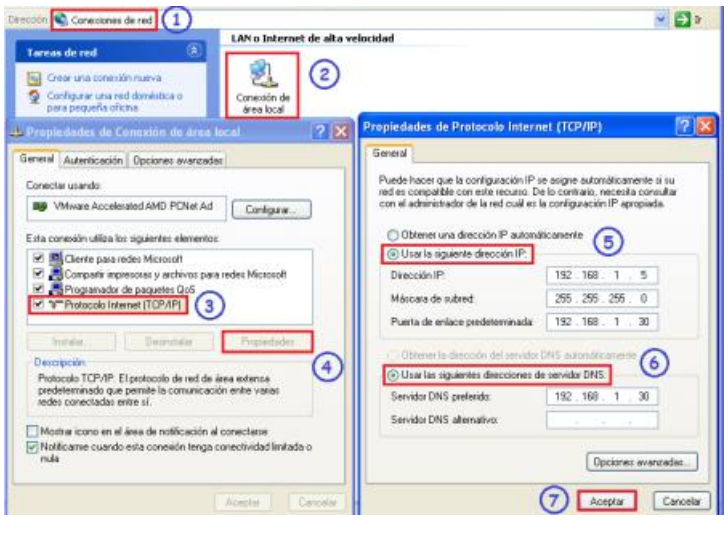


Imagen 3. Configuración de la interfaz de red en Windows

También se debe deshabilitar el **Firewall de Windows** para probar conectividad entre los equipos mediante el protocolo ICMP.

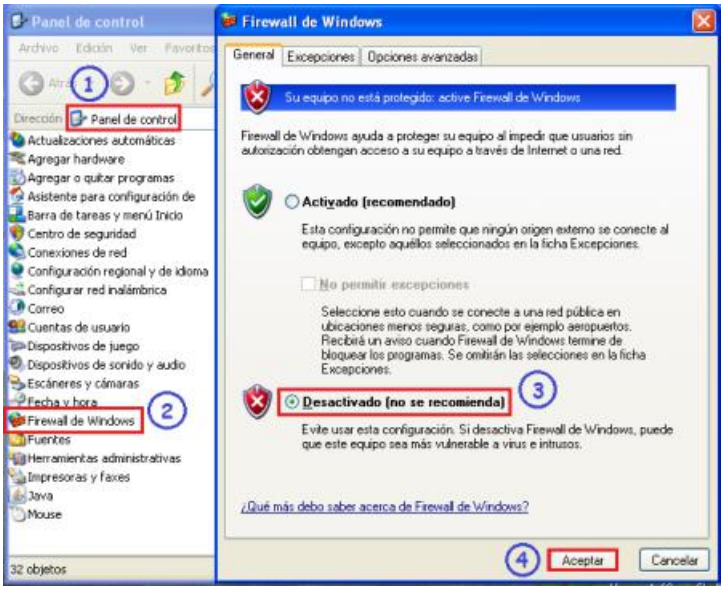


Imagen 4. Firewall de Windows desactivado

La interfaz de red del equipo Debian debe configurarse de forma estática de acuerdo a los siguientes parámetros:

- **Dirección IP:** 192.168.1.30
- **Máscara de subred:** 255.255.255.0

```
root@MalwareAnalysisLab:/home/malware# more /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
#auto eth0
#iface eth0 inet dhcp

auto eth0
iface eth0 inet static
        address 192.168.1.30
        netmask 255.255.255.0

root@MalwareAnalysisLab:/home/malware# /etc/init.d/networking restart
```

Imagen 5. Configuración de la interfaz de red en Debian

Para verificar que los equipos virtuales tienen comunicación, se puede utilizar el comando *ping* entre ambos.

```
root@MalwareAnalysisLab:/home/malware# ping 192.168.1.5 -c 4
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data.
64 bytes from 192.168.1.5: icmp_req=1 ttl=128 time=0.968 ms
64 bytes from 192.168.1.5: icmp_req=2 ttl=128 time=0.517 ms
64 bytes from 192.168.1.5: icmp_req=3 ttl=128 time=0.605 ms
64 bytes from 192.168.1.5: icmp_req=4 ttl=128 time=0.630 ms

--- 192.168.1.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3015ms
rtt min/avg/max/mdev = 0.517/0.680/0.968/0.171 ms
root@MalwareAnalysisLab:/home/malware#
```

Imagen 6. Conectividad correcta desde Debian a Windows

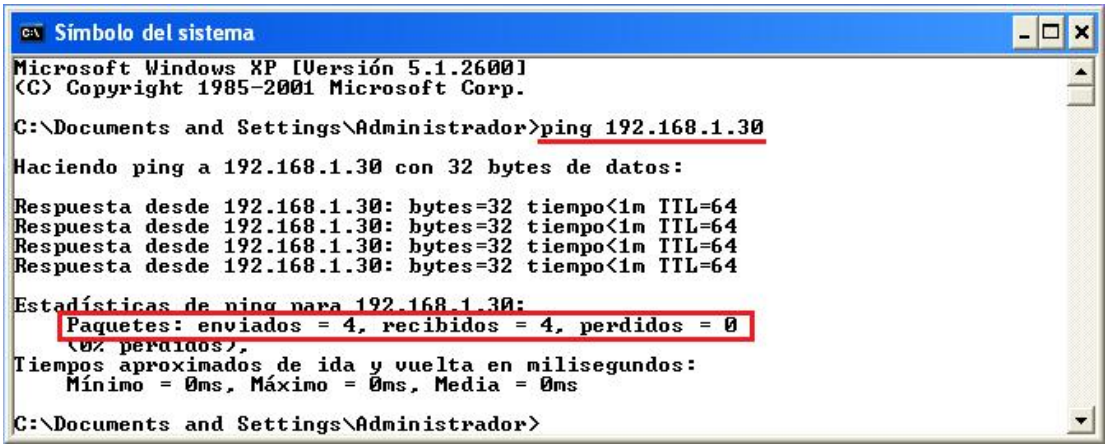


Imagen 7. Conectividad correcta desde Windows a Debian

Actividad de red de la muestra gusano445.exe

Abrir las herramientas de monitoreo Process Explorer y TCPView en el equipo Windows. Posteriormente, ejecutar la muestra y observar su actividad de red.

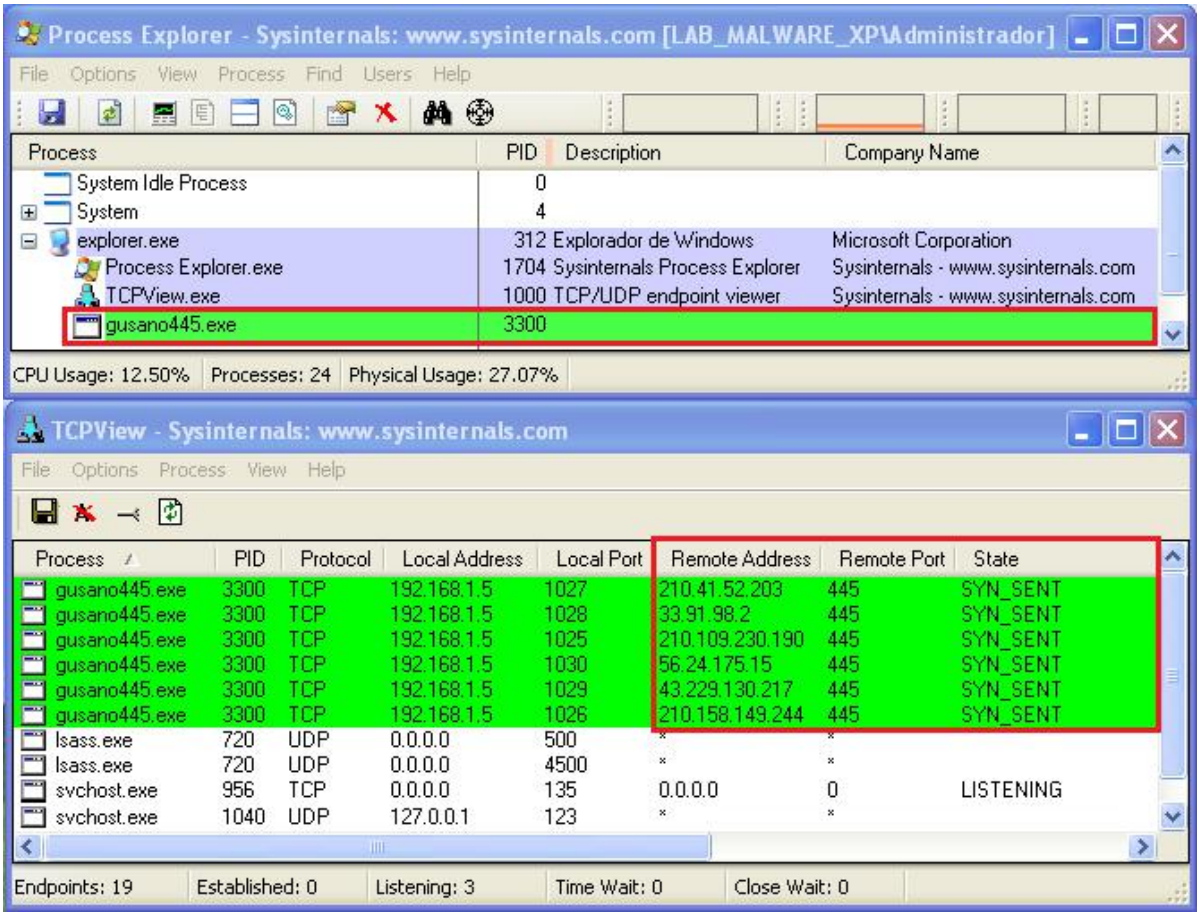


Imagen 8. Actividad de red del gusano informático

En TCPView se observan peticiones de sincronización a direcciones IP púbicas al puerto 445 asociado al servicio SMB. Después, terminar el proceso malicioso desde Process Explorer.

Con Honeyd se proporcionarán los *host* que solicita el *malware* bajo demanda, y con Dionaea se proporcionará el servicio SMB, por lo que ambas herramientas deben trabajar de manera conjunta.

Archivo de configuración de Honeyd

Si la instalación de Honeyd se realizó desde código fuente, es necesario crear el archivo de configuración con el siguiente contenido:

```
root@MalwareAnalysisLab:/home/malware# more /opt/honeyd/share/honeyd/honeyd.conf
create default
set default default tcp action block
set default default udp action block
set default default icmp action open
add default tcp port 445 proxy 127.0.0.1:445
root@MalwareAnalysisLab:/home/malware#
```

Imagen 9. Reglas de configuración en Honeyd

Las primeras cuatro líneas definen el comportamiento al cual responderá Honeyd. Fue configurado para no redireccionar tráfico UDP y TCP, pero sí el tráfico ICMP, debido a que se deben realizar pruebas de conectividad mediante el uso del comando *ping* desde el equipo Windows.

El puerto definido en la última línea del archivo no estará bloqueado, de esta manera Honeyd escuchará en todas las direcciones IP posibles por la interfaz eth0 (en nuestro caso) y reenviará las conexiones del puerto 445 a *listeners* o servidores locales, en nuestro caso es el servicio SMB proporcionado por Dionaea.

Ahora verificaremos la conectividad desde el equipo Windows hacia la máquina Debian donde Honeyd responderá a las peticiones ICMP.

- Iniciar Honeyd

```
root@MalwareAnalysisLab:/home/malware# /opt/honeyd/bin/honeyd -f /opt/honeyd/sha
re/honeyd/honeyd.conf &
[1] 4509
root@MalwareAnalysisLab:/home/malware# Honeyd V1.6d Copyright (c) 2002-2007 Niel
s Provos
honeyd[4509]: started with -f /opt/honeyd/share/honeyd/honeyd.conf
honeyd[4509]: listening promiscuously on eth0: (arp or ip proto 47 or (udp and s
rc port 67 and dst port 68) or (ip )) and not ether src 00:0c:29:c0:a9:9d
Honeyd starting as background process
[1]+  Hecho     /opt/honeyd/bin/honeyd -f /opt/honeyd/share/honeyd/honeyd.conf
root@MalwareAnalysisLab:/home/malware#
```

Imagen 10. Uso del archivo de configuración para iniciar Honeyd

- Probar la conectividad con direcciones IP públicas

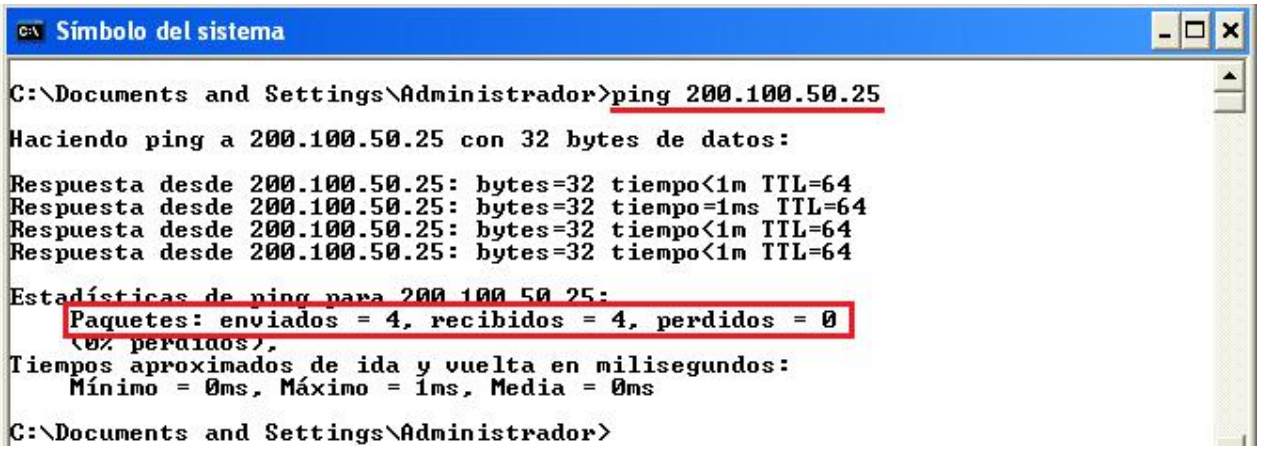


Imagen 11. Respuesta satisfactoria de Honeyd al equipo Windows

Servicios proporcionados por Dionaea

Hasta este momento debemos recordar que la muestra de *malware* no está en ejecución en el equipo Windows y que Honeyd está activo en la máquina Debian. Ahora, es momento de iniciar Dionaea y verificar los servicios que proporciona.

```
root@MalwareAnalysisLab:/home/malware# /opt/dionaea/bin/dionaea -D -r /opt/diona
ea -w /opt/dionaea -p /opt/dionaea/var/dionaea.pid -l all,-debug -L '*'

Dionaea Version 0.1.0
Compiled on Linux/x86 at Oct  1 2013 05:07:14 with gcc 4.7.2
Started on MalwareAnalysisLab running Linux/i686 release 3.2.0-4-686-pae

root@MalwareAnalysisLab:/home/malware#
```

Imagen 12. Comando para iniciar Dionaea

A continuación se muestran los servicios proporcionados por Dionaea.

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@MalwareAnalysisLab:/home/malware# netstat -natup | grep dionaea
tcp        0      0 192.168.1.30:3306       0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 192.168.1.30:42         0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 127.0.0.1:42            0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 192.168.1.30:80         0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 127.0.0.1:80            0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 192.168.1.30:21         0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 127.0.0.1:21            0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 192.168.1.30:1433       0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 127.0.0.1:1433          0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 192.168.1.30:443        0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 127.0.0.1:443           0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 192.168.1.30:445        0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 127.0.0.1:445           0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 192.168.1.30:5060       0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 127.0.0.1:5060          0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 192.168.1.30:5061       0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 127.0.0.1:5061          0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 192.168.1.30:135        0.0.0.0:*               LISTEN      4523/dionaea
tcp        0      0 127.0.0.1:135           0.0.0.0:*               LISTEN      4523/dionaea
tcp6       0      0 fe80::20c:29ff:fec:3306 :::*                    LISTEN      4523/dionaea
tcp6       0      0 fe80::20c:29ff:fec0::42 :::*                    LISTEN      4523/dionaea
tcp6       0      0 fe80::20c:29ff:fec0::80 :::*                    LISTEN      4523/dionaea
tcp6       0      0 fe80::20c:29ff:fec0::21 :::*                    LISTEN      4523/dionaea
tcp6       0      0 fe80::20c:29ff:fec:1433 :::*                    LISTEN      4523/dionaea
tcp6       0      0 fe80::20c:29ff:fec0:443 :::*                    LISTEN      4523/dionaea
tcp6       0      0 fe80::20c:29ff:fec0:445 :::*                    LISTEN      4523/dionaea
tcp6       0      0 fe80::20c:29ff:fec:5060 :::*                    LISTEN      4523/dionaea
tcp6       0      0 fe80::20c:29ff:fec:5061 :::*                    LISTEN      4523/dionaea
tcp6       0      0 fe80::20c:29ff:fec0:135 :::*                    LISTEN      4523/dionaea
udp        0      0 192.168.1.30:69         0.0.0.0:*                           4523/dionaea
udp        0      0 127.0.0.1:69            0.0.0.0:*                           4523/dionaea
udp        0      0 192.168.1.30:5060       0.0.0.0:*                           4523/dionaea
udp        0      0 127.0.0.1:5060          0.0.0.0:*                           4523/dionaea
udp6       0      0 fe80::20c:29ff:fec0::69 :::*                                4523/dionaea
udp6       0      0 fe80::20c:29ff:fec:5060 :::*                                4523/dionaea
root@MalwareAnalysisLab:/home/malware#
```

Imagen 13. Servicios que ofrece Dionaea

En la máquina Debian, cambiarse al directorio “binaries” de Dionaea, que es donde se almacenarán las muestras de *malware* capturadas y se monitorizará la actividad de la carpeta con el comando *watch*, este último para ejecutar el comando *ls* cada determinado intervalo de tiempo, en nuestro caso cada dos segundos.

```
root@MalwareAnalysisLab:/home/malware# cd /opt/dionaea/var/dionaea/binaries
root@MalwareAnalysisLab:/opt/dionaea/var/dionaea/binaries#
root@MalwareAnalysisLab:/opt/dionaea/var/dionaea/binaries# pwd
/opt/dionaea/var/dionaea/binaries
root@MalwareAnalysisLab:/opt/dionaea/var/dionaea/binaries# ls
root@MalwareAnalysisLab:/opt/dionaea/var/dionaea/binaries#
root@MalwareAnalysisLab:/opt/dionaea/var/dionaea/binaries# watch -n 2 ls
```

Imagen 14. Directorio de muestras de malware capturadas

Captura del gusano informático

En este momento, ya estamos listos para infectar el equipo Windows con la muestra de *malware*, puesto que tenemos Honeyd activo para proporcionar, bajo demanda, las direcciones IP públicas que solicite el gusano informático; y Dionaea proporcionando el servicio SMB.

Ejecutar por segunda ocasión la muestra gusano445.exe y observar que se han establecido conexiones hacia diferentes direcciones IP públicas en el puerto 445.

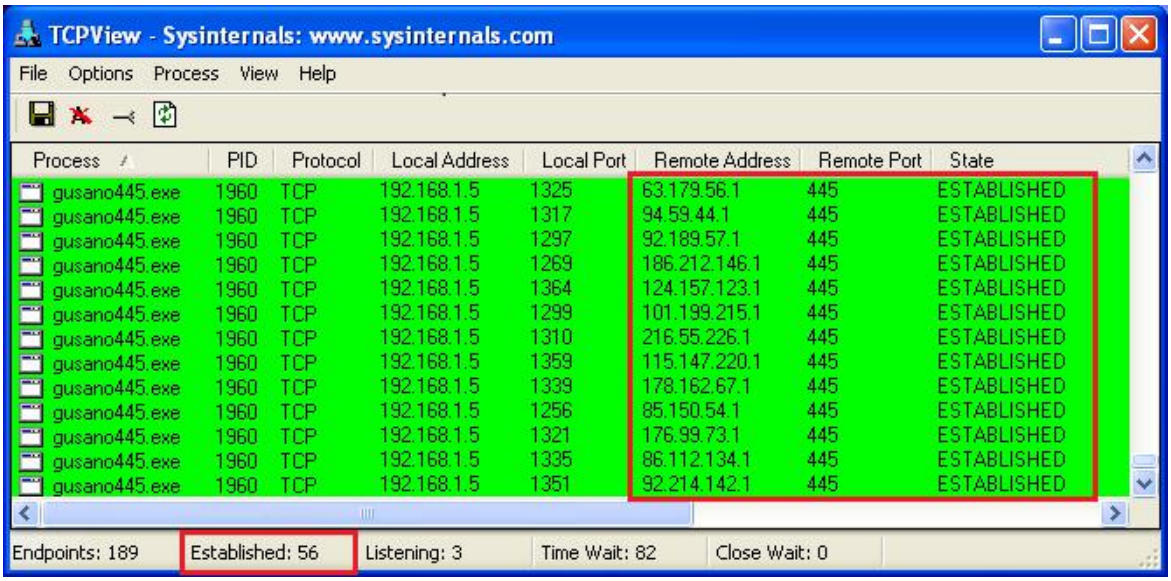


Imagen 15. Conexiones establecidas al equipo Debian

Después de unos minutos, en la carpeta */opt/dionaea/var/dionaea/binaries/* se guarda un archivo nombrado con su firma md5 y otros con extensión "tmp".

```
Every 2.0s: ls

786ab616239814616642ba4438df78a9
smb-3ape40.tmp
smb-dqfbrp.tmp
smb-g8ph0e.tmp
smb-gizmw4.tmp
smb-i2wlwd.tmp
smb-jcv6fl.tmp
smb-kln6nb.tmp
smb-mp5ozr.tmp
smb-trkmfl.tmp
smb-_ubf42.tmp
```

Imagen 16. Archivos guardados en la carpeta binaries

Detener el comando *watch* con las teclas CTRL+C; detener Dionaea, Honeyd y el proceso malicioso desde Process Explorer.

Cuando Dionaea obtiene una "copia" del *malware*, lo nombra con el valor de su firma md5, mientras la consigue genera archivos temporales.

Verificar el tipo de archivo con el comando *file*.

```
root@MalwareAnalysisLab:/opt/dionaea/var/dionaea/binaries# ls
786ab616239814616642ba4438df78a9
root@MalwareAnalysisLab:/opt/dionaea/var/dionaea/binaries# file 786ab61623981461
6642ba4438df78a9
786ab616239814616642ba4438df78a9: data
root@MalwareAnalysisLab:/opt/dionaea/var/dionaea/binaries#
```

Imagen 17. Tipo de archivo de la muestra capturada

El resultado muestra que es tipo *data* y no un ejecutable de Windows, por lo que debemos revisar el archivo capturado. Usar la herramienta Hexdump con la opción -C para que muestre el archivo en formato hexadecimal y en ASCII.

```
root@MalwareAnalysisLab:/opt/dionaea/var/dionaea/binaries# hexdump -C 786ab61623
9814616642ba4438df78a9 | head
00000000  00 4d 5a 4b 45 52 4e 45  4c 33 32 2e 44 4c 4c 00  |.MZKERNEL32.DLL.|
00000010  00 50 45 00 00 4c 01 03  00 be b0 11 40 00 ad 50  |.PE..L......@..P|
00000020  ff 76 34 eb 7c 48 01 0f  01 0b 01 4c 6f 61 64 4c  |.v4.|H.....LoadL|
00000030  69 62 72 61 72 79 41 00  00 18 10 00 00 10 00 00  |ibraryA.........|
00000040  00 00 80 00 00 00 00 40  00 00 10 00 00 00 02 00  |.......@........|
00000050  00 04 00 00 00 00 00 39  00 04 00 00 00 00 00 00  |.......9........|
00000060  00 00 30 02 00 00 02 00  00 00 00 00 00 02 00 00  |..0.............|
00000070  00 00 00 10 00 00 10 00  00 00 00 10 00 00 10 00  |................|
00000080  00 00 00 00 00 0a 00 00  00 00 00 00 00 00 00 00  |................|
00000090  00 ee 21 02 00 14 00 00  00 00 20 01 00 62 00 00  |..!....... ..b..|
root@MalwareAnalysisLab:/opt/dionaea/var/dionaea/binaries#
```

Imagen 18. Formato hexadecimal y ASCII del archivo binario capturado

Se observa que tiene un byte de más al inicio, por lo cual se usará el comando *dd* para quitarlo, aunque también se puede abrir con un editor hexadecimal como Ghex y realizar el cambio. Posteriormente se revisa el tipo de archivo con el comando *file*, se observa que es un ejecutable para Windows. Por último obtenemos su firma sha1 para compararla con la que inicialmente se ejecutó en el equipo Windows.

```
root@MalwareAnalysisLab:/opt/dionaea/var/dionaea/binaries# dd if=786ab6162398146
16642ba4438df78a9 of=gusano445.exe bs=1 skip=1
33128+0 registros leídos
33128+0 registros escritos
33128 bytes (33 kB) copiados, 0.0894087 s, 371 kB/s
root@MalwareAnalysisLab:/opt/dionaea/var/dionaea/binaries# file gusano445.exe
gusano445.exe: MS-DOS executable, MZ for MS-DOS
root@MalwareAnalysisLab:/opt/dionaea/var/dionaea/binaries# sha1sum gusano445.exe
42e56d72982ac04edba2ce7fb9f4e5048766aa94  gusano445.exe
root@MalwareAnalysisLab:/opt/dionaea/var/dionaea/binaries#
```

Imagen 19. Formato hexadecimal y ASCII del binario capturado

Parámetros del comando *dd*:

- if ; archivo de entrada
- of ; archivo de salida
- bs ; tamaño del bloque en bytes que se quiere retirar
- skip ; número de veces que se requiere hacer el salto del bloque

Cabe mencionar que no todos los archivos capturados por Dionaea tienen un byte de más, pero se debe considerar en caso de que se envíen las muestras a sistemas automatizados de análisis de *malware* o se realice de forma manual. En UNAM-CERT se han detectado los siguientes inicios de archivos capturados por Dionaea:

- 4D 5A ; inicio correcto de los archivos ejecutables de Windows
- 00 4D 5A ; quitar el byte 00 que está de más en la cabecera
- 5A ; agregar el byte 4D al inicio
- 00 00 5A ; quitar el primer byte 00 y reemplazar el segundo byte 00 por 4D

Posteriormente, obtener la firma sha1 de la muestra gusano445.exe en Windows para verificar que se trata del mismo archivo.

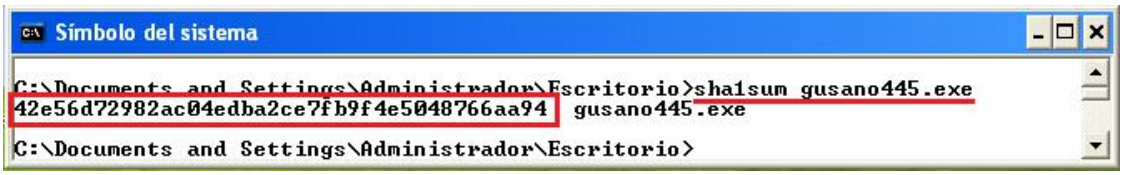


Imagen 20. Firma sha1 de la muestra localizada en Windows

Finalmente, se recomienda crear los *scripts* que inicien, como cualquier otro servicio en sistemas Linux, las herramientas Honeyd (para entornos locales de prueba) y Dionaea (en entornos de producción para capturar *malware* que se propaga por Internet). Además de un *script* de sanitización que procese las muestras capturadas por nuestro *honeypot* para que, al ser enviadas a firmas antivirus o *sandbox* públicas, puedan ejecutarse correctamente. A continuación se propone una lista de cambios:

- Agregar o quitar bytes de la cabecera del ejecutable según se requiera.
- Renombrar, con la nueva firma md5, el ejecutable que fue modificado.
- Agregar la extensión ".exe" a los ejecutables para Windows.
- Comprimir las muestras con contraseña para evitar infecciones accidentales (varios sitios de seguridad que recopilan *malware* recomiendan usar: "*infected*" o "*malware*").

Tener en cuenta que Dionaea podría tener vulnerabilidades, por lo que, para minimizar el impacto, debería ejecutarse con permisos de usuario que no sean de administración.

Ahora, el lector ya cuenta con las herramientas necesarias para montar un laboratorio de captura de *malware* y comenzar con el trabajo de análisis. Este primer acercamiento al uso de las tecnologías *honeypots* es una buena entrada para quienes se interesan en el análisis de software malicioso. Si te interesa conocer más de este tema, puedes dar el siguiente paso con los artículos seleccionados más adelante.

Si quieres saber más consulta:

- Impacto de las Amenazas, El Caso de "Iloveyou"
- The Honeynet Project Map
- HoneyPots Parte 3 - Configuración y análisis de malware con Dionaea
- Dionaea - A Malware Capturing Honeypot

Jonathan Banfi Vázquez

Ingeniero en Computación por la Facultad de Ingeniería de la UNAM, con módulo de salida Redes y Seguridad.

Formó parte de la 3ra generación del Programa de Certificación Cisco CCNA Exploration, impartido en la Facultad de Ingeniería de la UNAM. Fue miembro de la 6ta generación del Programa de Becas de Formación en Seguridad Informática de CSI/UNAM-CERT.

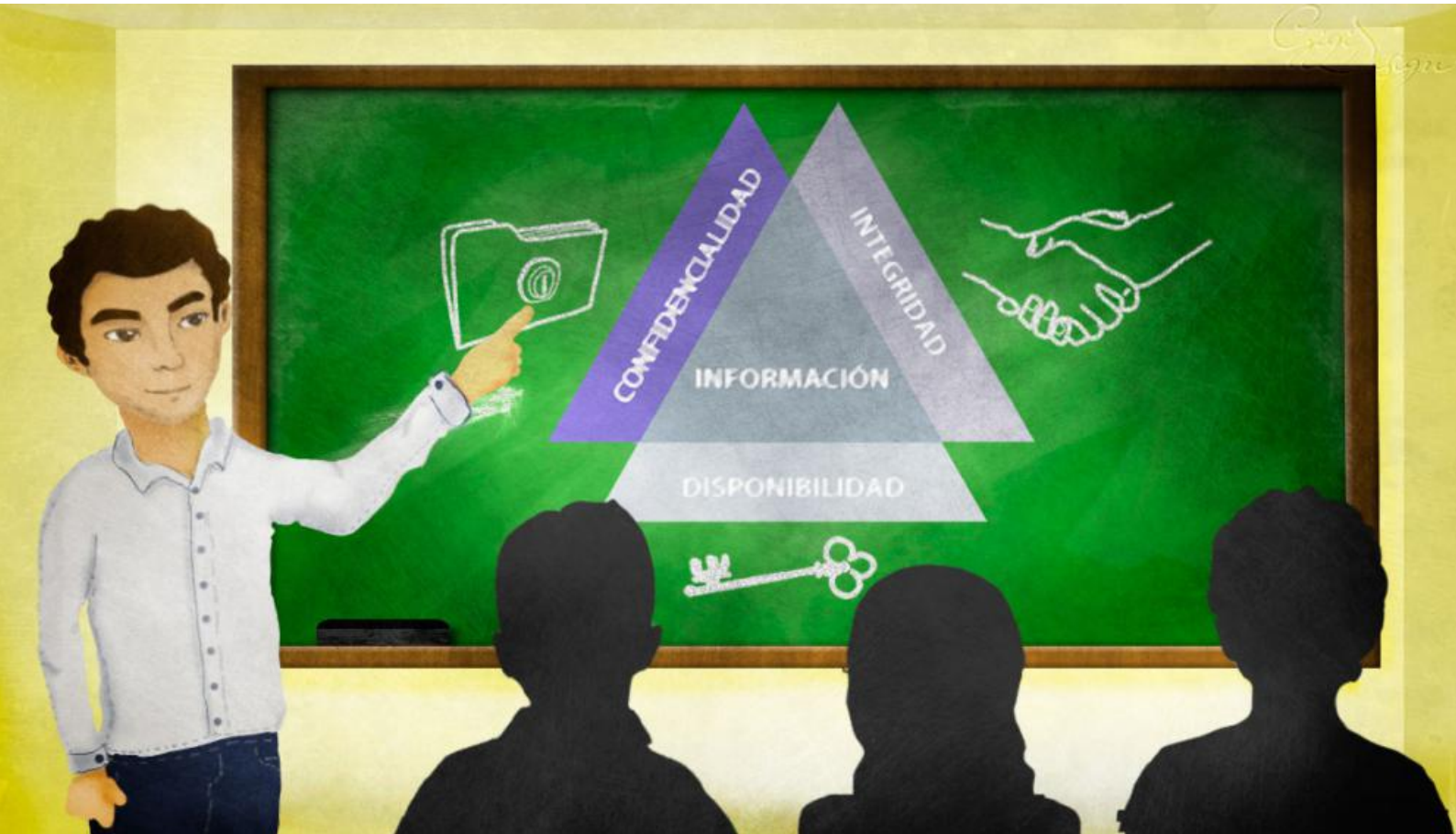
Gestión de seguridad de la información basado en el MAAGTICSI para programas académicos en Instituciones de Educación Superior

Lidia Prudente Tixteco, Gabriel Sánchez Pérez, José de Jesús Vázquez Gómez

Los ataques e incidentes de seguridad de la información no sólo ocurren en instituciones relacionadas con los sectores de seguridad nacional, financieros, productivos o de infraestructuras críticas. Las entidades académicas también se han convertido en blancos de éstos, como lo reporta el informe de la OEA (OEA y Symantec, 2014) en donde presentan que, en México, las entidades de ámbito académico son las más afectadas, con un 39% de delitos informáticos reportados al CERT-MX.

Particularmente se presenta esta situación en aquellas instituciones en las que se cuenta con programas avanzados de investigación, donde, con frecuencia, se maneja información de carácter reservado o confidencial relacionada a desarrollos científicos y tecnológicos financiados por organizaciones para resolver problemas o necesidades complejas, asimismo, se manejan datos personales de su comunidad (alumnos, profesores, investigadores y directivos), datos de su programa académico, entre otros; y ocupan activos de TI para su almacenamiento y procesamiento.

En este artículo se presenta un estudio sobre este tema partiendo de la estructura y misión de una Institución de Educación Superior Pública en México, para la cual se propone establecer un **SGSI (Sistema de Gestión de Seguridad de la Información)** basado en el **MAAGTICSI (Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información)**. Al ser el esquema de



gestión adoptado por la Administración Pública Federal, permitirá desarrollar sus procesos con una estrategia de seguridad de la información alineada a la misión y visión planteadas para un Programa Académico, tomando en consideración que este manual puede ser aplicado a procesos de diferente índole y tamaño.

Gestión de Seguridad de la Información

Un SGSI comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de seguridad de la información en una organización (Gómez Vieites & Suárez Rey, 2012), que permita tratar los riesgos a los que está expuesta la información.

Un Sistema de Gestión de Seguridad de la Información toma como fundamento el garantizar que la seguridad de la información sea gestionada correctamente, identificando inicialmente su ciclo de vida y los aspectos relevantes para asegurar su *confidencialidad, integridad y disponibilidad* (CID) (ISO/IEC 27001:2005), teniendo en cuenta que los riesgos no se pueden eliminar totalmente, pero sí se pueden gestionar.

En este proceso es necesario contemplar un modelo que tome en cuenta los componentes tecnológicos, organizativos, de marco legal y factor humano, tal y como se presenta en la Figura 1 (Gómez Vieites & Suárez Rey, 2012).

Figura 1. Componentes de un SGSI

Gestión y análisis de riesgos

En el proceso de gestión de riesgos se define un plan para la implantación de controles de seguridad en los sistemas de información que permita, como se presenta en la Figura 2, disminuir la probabilidad de que se materialice una amenaza, reducir la vulnerabilidad del sistema o el posible impacto en la organización, y posibilite la recuperación del sistema en caso de una afectación grave. Pero para esto se debe de emprender una etapa de evaluación previa de los riesgos del sistema de información, misma que se debe realizar con rigor y objetividad para que se cumpla su función con garantías; esta etapa es denominada análisis de riesgos.

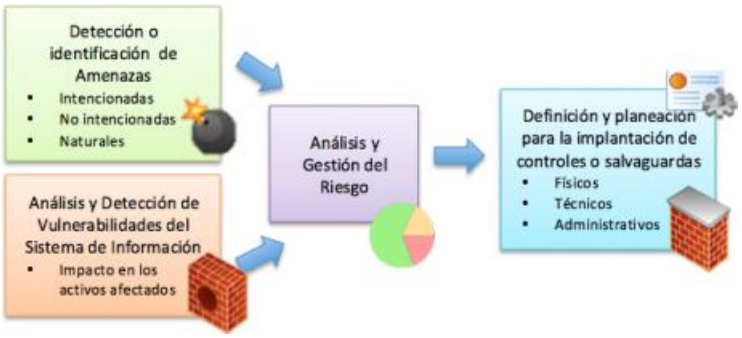


Figura 2. Análisis y gestión de riesgos en una organización

MAAGTICSI

El Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI) fue publicado en el año 2011 y es una actualización del MAAGTIC.

Más tarde, en mayo de 2014 fue publicado en el Diario Oficial de la Federación por la Secretaría de la Función Pública una actualización del MAAGTICSI, en el Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional en México, definiendo los procesos con los que, en las materias de TIC y de seguridad de la información, las instituciones públicas en México deberán regular su operación, independientemente de su estructura organizacional y las metodologías de operación con las que cuenten.

El manual ahora contiene, en tres grupos, los procesos necesarios para propiciar la operación ágil y oportuna de las actividades de las TIC (Secretaría de la Función Pública, 2014). Los tres grupos se refieren a gobernanza, organización y entrega, como se muestra en la Figura 3. Para los propósitos del presente trabajo, sólo se instrumentará el proceso de Administración de la Seguridad de la Información (ASI) ubicado en el grupo de Organización.

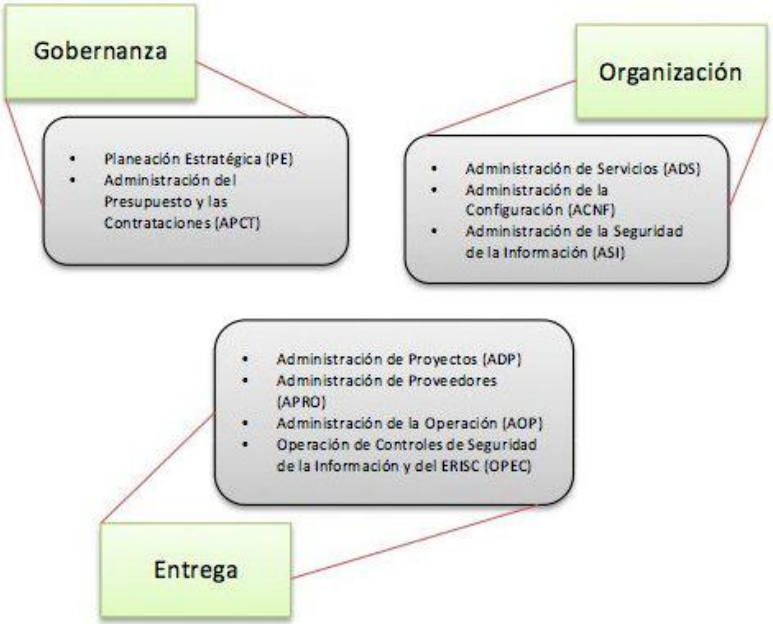


Figura 3. Marco rector del MAAGTICSI (Secretaría de la Función Pública, 2014)

Enfoque de un SGSI para un Programa Académico

Un *Programa Académico* consiste en un "conjunto organizado de elementos necesarios para generar, adquirir y aplicar el conocimiento en un campo específico; así como para desarrollar habilidades, actitudes y valores en alumnos, en diferentes áreas de conocimiento" (Instituto Politécnico Nacional, 2011).

Como se mencionó en la sección anterior, este trabajo se basará en el proceso de **Administración y Seguridad de la Información (ASI)** del MAAGTICSI. Uno de los objetivos específicos del ASI es establecer un SGSI que proteja los activos de información de la Institución, con la finalidad de preservar su confidencialidad, integridad y disponibilidad. Las actividades del ASI desarrolladas se muestran en la Figura 4 y están enfocadas al alcance de gestionar la seguridad de la información que se emplea en un Programa Académico.

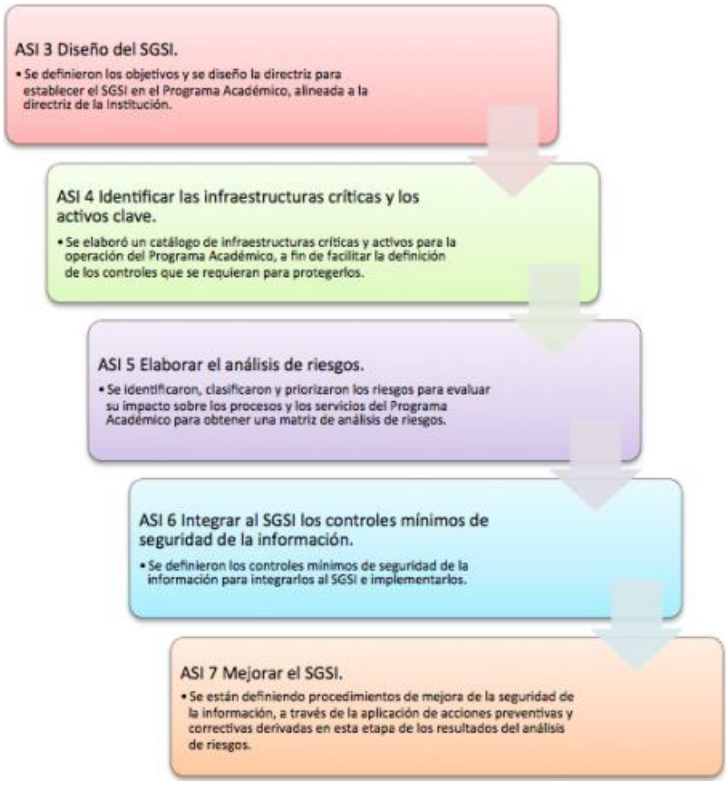


Figura 4. Actividades ASI enfocadas a un SGSI en un Programa Académico

Para lograr sus misiones y objetivos, la mayoría de las organizaciones dependen de la ejecución de varios procesos. Se encontró en el presente estudio que un aspecto importante como punto de partida para ello es conocer a la organización desde su misión hasta sus procesos, profundizando en cuáles de éstos son críticos para su operación. Los pasos importantes en el diseño del SGSI para el Programa Académico se muestran en la Figura 5 y se describen a continuación.

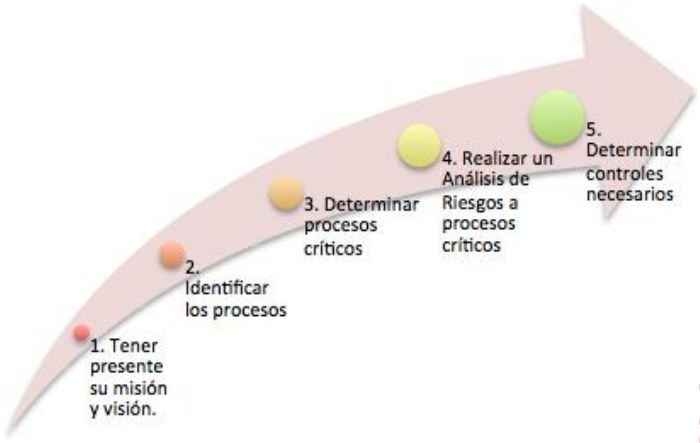


Figura 5. Pasos para el diseño del SGSI para el Programa Académicos

1. Tener presente su misión y visión (ASI 3). Como primer paso es fundamental el revisar la misión y visión del Programa Académico, ya que la directriz del SGSI debe estar alineada para fortalecerlas y no para ir en contra.

2. Identificar los procesos (ASI 4). Consiste en identificar los diferentes procesos que se llevan a cabo en el Programa Académico, situación que a veces no es tan sencilla debido a que muchos de esos procesos se llevan a cabo de manera rutinaria y no hay documentación sobre ellos, cuando se está en esta situación se dice que hay nivel de madurez cero en seguridad de la información.

3. Determinar procesos críticos (ASI 4). Se sugiere realizar una evaluación de los procesos para determinar aquellos críticos para el Programa Académico, por ejemplo: pidiendo la opinión a los directivos y comunidad respecto a las actividades que se realizan en cada proceso; asociando los activos de información que participan en ellos; y si se quiere ser más específico, asociando también aspectos de confidencialidad, integridad y disponibilidad de los activos. La participación de los directivos en esta etapa es esencial, ya que son los que conocen las expectativas que se tienen del Programa Académico y son los encargados de presentar resultados positivos.

4. Realizar un análisis de riesgos a los procesos críticos (ASI 5). El realizar un análisis de riesgos es esencial para la implementación de un SGSI; aunque existen diferentes metodologías para realizarlo, el MAAGTICSI sugiere una, que entre otras cosas consiste en:

• Utilizar un catálogo de amenazas con base en activos de información.

• Seguir una guía de identificación y evaluación de escenarios de riesgo, en la que se utilizan las escalas alta, media y baja para determinar la probabilidad y el impacto de una manera sencilla. MAAGTICSI también cuenta con otras estrategias para obtener una mayor precisión en los valores de riesgo que se calculen; por ejemplo, para la probabilidad se pueden incluir factores adicionales que ejercen influencia en la probabilidad de ocurrencia, como:

• *Existencia* de un agente-amenaza desde la perspectiva de un activo de información particular (existir),

• *Interés* del agente-amenaza para atacar al activo de información (querer),

• *Capacidad* del agente-amenaza para atacar al activo de información (poder), y

• *Vulnerabilidad* del activo de información.

•Y para el impacto también se incrementa la cantidad de valores a considerar, como los aspectos: *humano, material, financiero, operativo y de imagen*.

5. Determinar controles necesarios (ASI 6). El MAAGTICSI deja libre la selección de controles de seguridad después de un análisis costo-beneficio; para este caso es práctico auxiliarse en la lista de controles que tiene el ISO/IEC 27001 en su anexo para elegir los más convenientes.

En la siguiente tabla se presentan dos de las vulnerabilidades con un riesgo alto, encontradas después del Análisis de Riesgos a los activos de los procesos críticos del Programa Académico; también muestra el tratamiento del riesgo que se eligió, los controles relacionados y la recomendación que se realizó para tratar dicho riesgo.

Vulnerabilidad	Probabilidad	Impacto	Riesgo	Nivel	Tratamiento	ID Control	Nombre del control	Recomendación
Los usuarios del activo necesitan reforzar su conocimiento, capacitación y actualización, enfocadas a su función laboral para evitar realizar funciones inadecuadas y que puedan provocar deterioro de las operaciones del servidor.	0.8	10	8.00	ALTO	MITIGAR	A.6.1.1	Funciones y responsabilidades de seguridad de la información	Se sugirió capacitar al personal en las políticas de seguridad de la información aplicadas a su función laboral, así como asignar responsabilidades de los procedimientos aplicadas al activo y tenerlos disponibles para evitar que se pueda comprometer el activo
						A.7.2.2	Capacitación y educación en la seguridad de la información	
El activo no cuenta con procedimientos documentados de operación del servidor, lo que podría causar el deterioro de sus operaciones por parte de personal inexperto.	0.8	10	8.00	ALTO	MITIGAR	A.8.1.1	Inventarios de activos	Se sugirió establecer la responsabilidad y uso del activo para evitar comprometer el equipo o deteriorar su operación, así como, elaborar y mantener los procedimientos de operación y eliminación del activo y mantenerlos al alcance del usuario.
						A.8.1.2	Propiedad de los activos	
						A.8.1.3	Uso aceptable de los activos	
						A.8.1.4	Devolución de los activos	
						A.11.2.5	Eliminación de activos	
						A.11.2.7	Eliminación segura o re-uso de equipo	
						A.11.2.8	Equipo de usuario desatendido	
						A.12.1.1	Documentación de procedimientos operacionales	

Tabla 1. Tratamiento de riesgos

El proceso completo descrito en los cinco pasos se ejemplifica en el diagrama de la Figura 6.

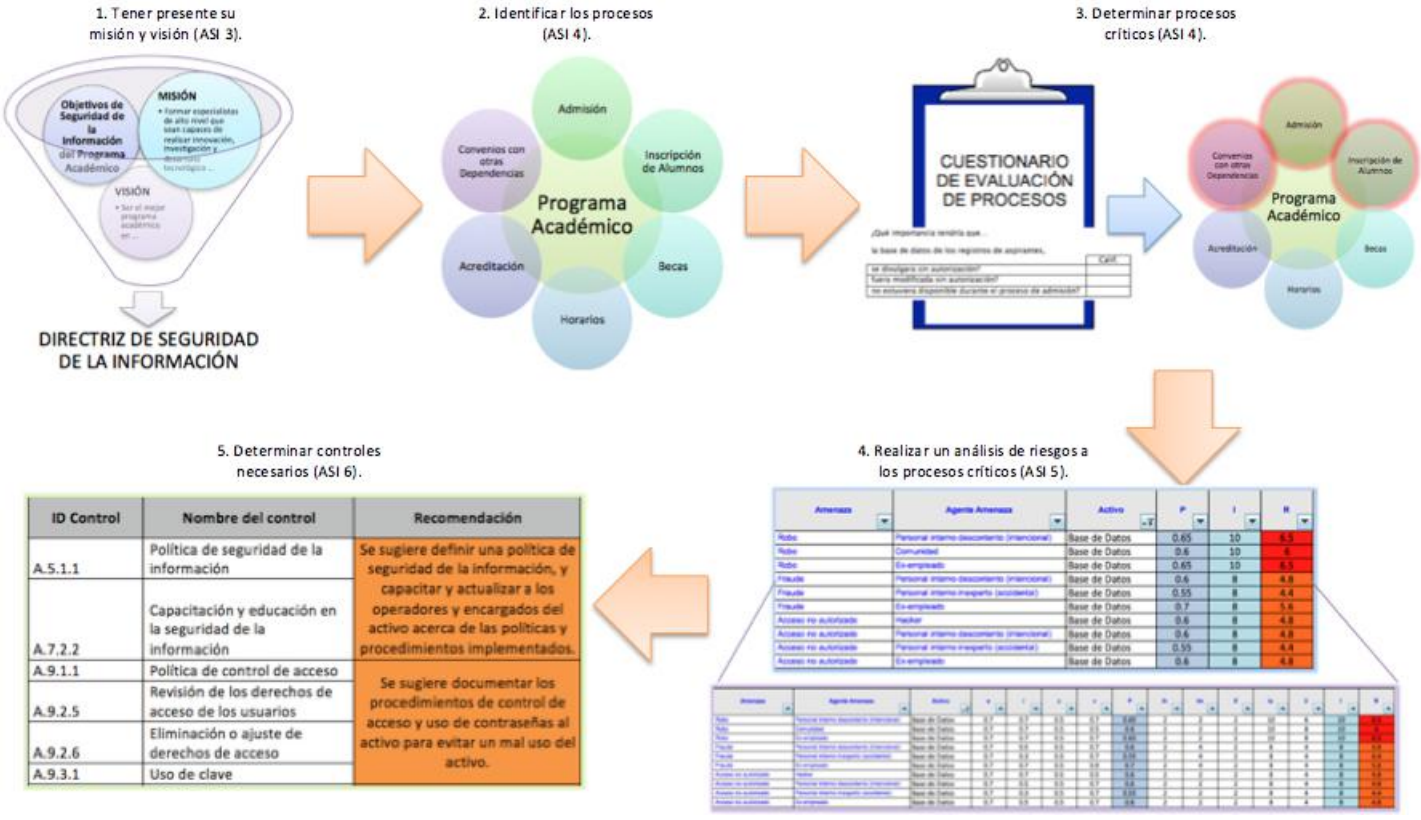


Figura 6. Proceso para el diseño de un SGSI para un Programa Académico

Recomendaciones

Dos puntos clave que podemos recomendar durante este proceso son:

- Construir una tabla de dependencias de activos y
- Generar una matriz de riesgos en donde se posicione a cada activo.

Ambos ayudan a tener una mejor perspectiva de la seguridad de la información en la organización y, por consiguiente, mejoran la definición de estrategias que apoyan la toma de decisiones.

Si bien en algunos Programas Académicos u otras instancias similares no es común que cuenten o puedan contar con un departamento de seguridad dentro de su organigrama, dedicado a gestionar los aspectos de protección de la información que manejan; lo anterior generalmente se debe a las restricciones de recursos humanos y materiales que pudieran estar destinados al propósito de asegurar sus procesos. Sin embargo, esto no debería ser una excusa para no proteger sus activos de información críticos, tan relevantes para instituciones de los sectores al inicio mencionados (las cuales sí cuentan con los recursos que permiten proteger su información), y que esperan es que una institución educativa, que les está realizando un estudio clave para sus misiones y objetivos, cuente con una gestión de seguridad similar o más estricta para confiarle sus estrategias y planes de desarrollo; y esto se puede conseguir a través de un SGSI basado en el MAAGTICSI.

Referencias

Secretaría de la Función Pública. (2014). Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información. Secretaría de la Función Pública. Diario Oficial de la Federación.

Gómez Vieites, Á., & Suárez Rey, C. (2012). Sistemas de Información - Herramientas prácticas para la gestión empresarial (4ª edición ed.). México: Alfaomega.

ISO/IEC 27001. (2005). Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos. Estándar, Organización Internacional para la Estandarización y Comisión Electrotécnica Internacional.

Instituto Politécnico Nacional. (2011). Reglamento General de Estudios. Gaceta Politécnica, 13 (86), p 8.

OEA y Symantec. (2014). Tendencias de Seguridad Cibernética en América Latina y el Caribe. Organización de Estados Americanos y Symantec, Seguridad Multidimensional Organización de los Estados Americanos y de Asuntos Gubernamentales y Políticas Globales de Seguridad Cibernética.

Si quieres saber más consulta:

- Lo que no debes pasar por alto para gestionar la seguridad de la información
- Normatividad en las organizaciones: Políticas de seguridad de la información - Parte I
- Riesgo tecnológico y su impacto para las organizaciones parte II Gobierno de TI y riesgos

Lidia Prudente Tixteco

Ingeniera en Computación y Especialista en Seguridad Informática y Tecnologías de la Información por el Instituto Politécnico Nacional. Profesora en la Carrera de Ingeniería en Computación en la ESIME Unidad Culhuacán del IPN desde 2008.

Gabriel Sánchez Pérez

Es Ingeniero en Computación y Doctor en Comunicaciones y Electrónica por el IPN. Realizó una estancia de investigación en 2001 en la Universidad de Electro-comunicaciones de Tokio, Japón (UEC). Tiene estudios de Pos-doctorado en el Instituto Nacional de Astrofísica, Óptica y Electrónica de 2008 a 2009.

José de Jesús Vázquez Gómez

Es especialista en TI para la Dirección de Sistemas de Banco de México. Ha sido profesor invitado en la MISTI de la ESIME Unidad Culhuacán, desde el año 2008, donde ha apoyado en el asesoramiento de tesis y proyectos de investigación.

Frameworks para monitoreo, forense y auditoría de tráfico de red - I

Javier Ulises Santillán Arenas

Actualmente existen diversas técnicas y tecnologías para el monitoreo del tráfico de red. Las redes de datos manejan información con protocolos y aplicaciones cada vez más complejas. Esto, combinado con la gran cantidad de información que se transfiere y la migración paulatina a modelos de comunicación codificados o cifrados, ha hecho también del monitoreo una tarea cada vez más compleja.

En los últimos años se han desarrollado tecnologías de análisis de datos como los SIEM (Security Information and Event Management), SIM (Security Information Management), SEM (Security Event Management), NSM (Network Security Monitoring), PNA (Passive Network Audit), etcétera. Estas tecnologías han ido madurando a través de la adición de nuevos modelos de análisis de información e incluso de nuevos mecanismos de detección e identificación de patrones, usando aprendizaje de máquina o *machine learning*. En este contexto, existen también diversas técnicas y herramientas que pueden ayudar a los administradores a desarrollar o elegir un modelo de monitoreo, detección y auditoría que mejore el nivel de seguridad de sus organizaciones.

Frameworks de monitoreo

Ciertas técnicas podrían ser más efectivas, dependiendo del contexto del monitoreo y tomando en cuenta sus características, ventajas y enfoque. La Figura 1 presenta un panorama general sobre la relación entre los modelos de monitoreo y detección que se abordan en este artículo y que proveen lineamientos para desarrollar o implementar *frameworks* usando diversas tecnologías.

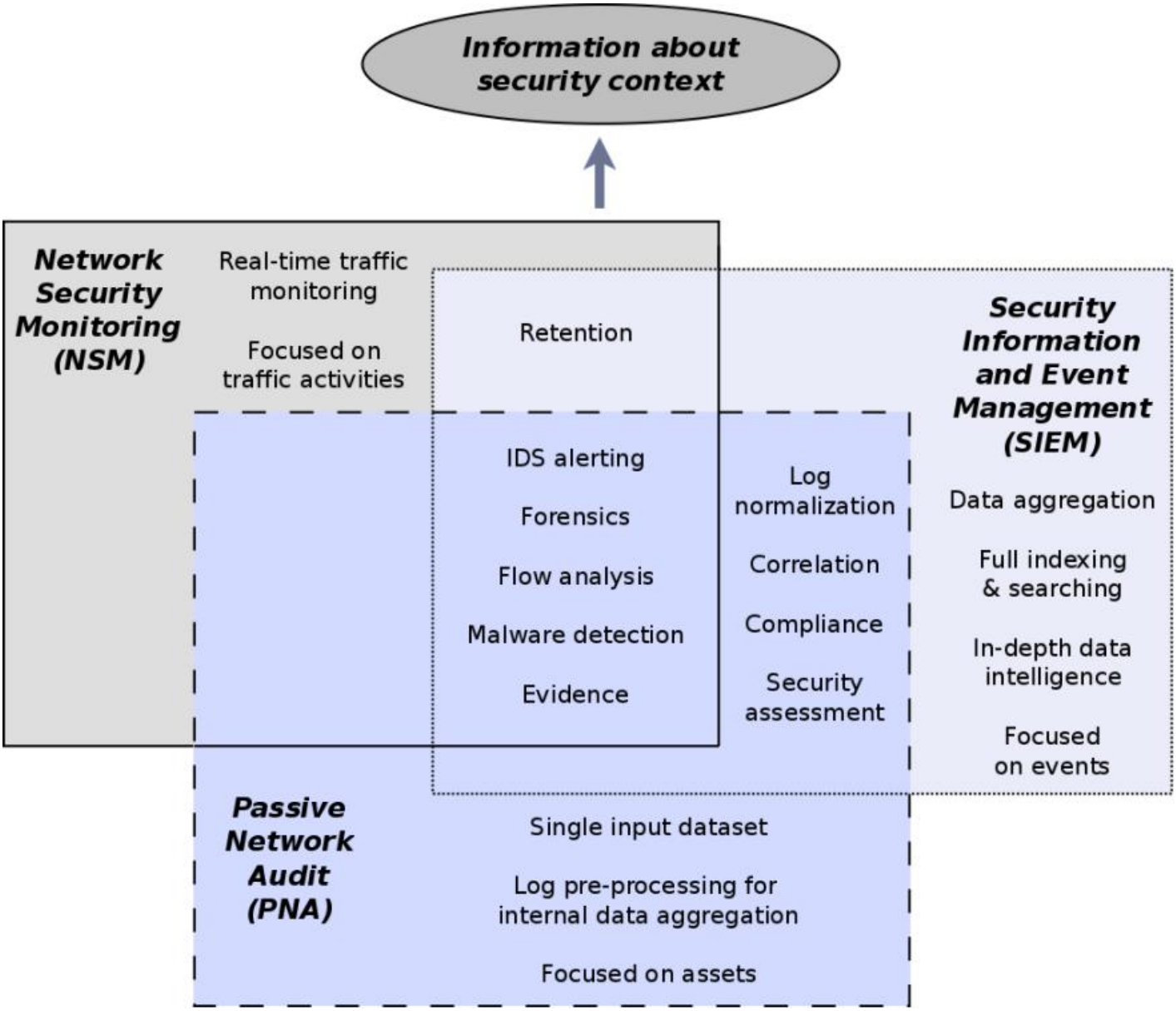


Figura 1. Panorama general de los modelos de monitoreo y análisis (Santillan, 2014)

Network Security Monitoring (NSM)

Es un modelo de análisis de tráfico de red que proporciona lineamientos para desarrollar un *framework* que incluya técnicas y herramientas para monitoreo, detección y retención de evidencia sobre incidentes de seguridad. Este modelo está basado en el análisis de datos generados por herramientas de seguridad como los IDS (Intrusion Detection Systems), analizadores de flujos, entre otros. NSM hace énfasis en las técnicas a seguir para poder alcanzar una mejor detección, es decir, no solamente describe qué herramientas pueden ser utilizadas, también cómo, cuándo y dónde utilizarlas dentro del contexto de la red, así como las consideraciones de implementación, zonas y puntos de monitoreo. Una de las herramientas más conocidas y utilizadas en este tipo de *framework* es Sguil[1], un *front-end* para el análisis de datos extraídos del IDS Snort[2] y el analizador de flujos Argus[3], entre otras herramientas.

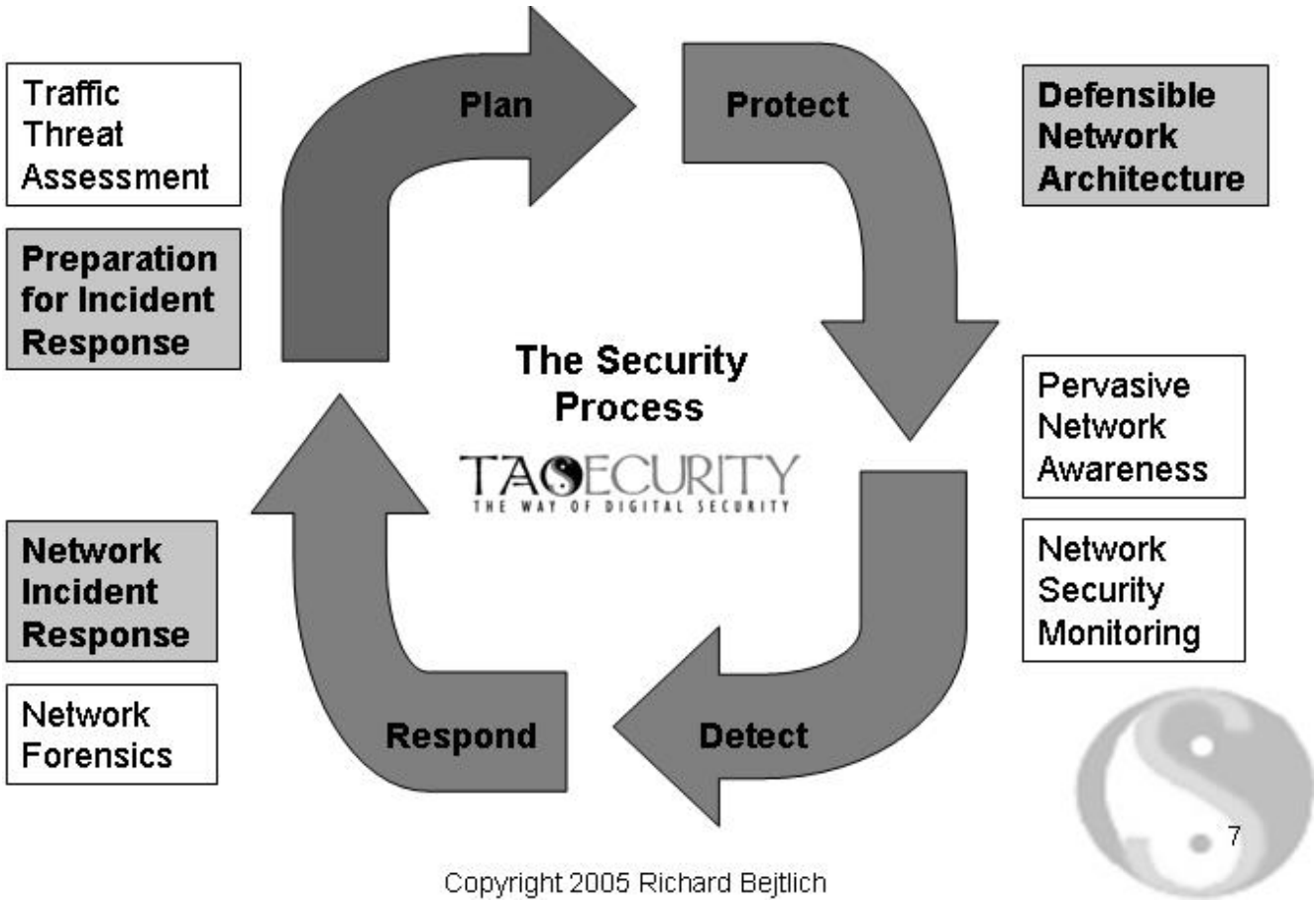


Figura 2. Proceso de atención de incidentes de red (Network Incident Response Process)[4]

Dentro del proceso de atención a incidentes de red (Network Incident Response Process) mostrado en la Figura 2, NSM está involucrado en la fase de Detección (Detect), específcamente en dos de sus procesos: Contención Pronta del Incidente (Short Term Incident Containment), donde se tiene información sobre el incidente detectado; y en Emergencia (Emergency), donde se identifica y provee evidencia del incidente. Asimismo, NSM describe el llamado *Modelo de Referencia de Intrusiones (Reference Intrusion Model)[5]* el cual define cuatro tipos de datos:

- Datos de contenido completo: captura *bit-a-bit.*
- Datos de sesión: Distribución de protocolos y acumulación de tráfico.
- Datos estadísticos: Registro de conversaciones entre dispositivos.
- Datos de alerta: Información extraída de IDS.

En relación a NSM y la detección de intrusos, algunos debates[6] mencionan que los desarrolladores de IDS buscan una "detección inmaculada", es decir, detección precisa; mientras que los practicantes de NSM buscan una "colección de datos inmaculada", es decir, captura de evidencia tanto como sea posible.

Security Information and Event Management (SIEM)

La *minería de datos* es un proceso de extración de modelos descriptivos a partir de grandes cantidades de datos, mediante el uso de modelos de análisis estadísticos, *machine learning*, entre otros. En el contexto de la seguridad en TI, la minería de datos se aplica en los llamados SIEM (Security Information and Event Management) para la identificación de patrones con propósitos de detección, auditoría e interpretación de información. Las fuentes de datos a analizar pueden ser herramientas como IPS (Intrusion Prevention Systems o Sistemas de Prevención de Intrusiones), IDS, *firewalls, routers,* bitácoras de sistemas, etcétera. Como se muestra en la Figura 3, a partir de estos datos se lleva a cabo una correlación (*correlation*) con el objetivo de filtrar información (*reduction*) para

identificación e interpretación de eventos específicos relacionados, por ejemplo, con incidentes de seguridad.

Los SIEM combinan características de los SIM (Security Information Manager) y de los SEM (Security Event Manager), cuyos enfoques en términos generales son el análisis en tiempo real (SIM) y almacenamiento a largo plazo de registros de eventos (SEM).

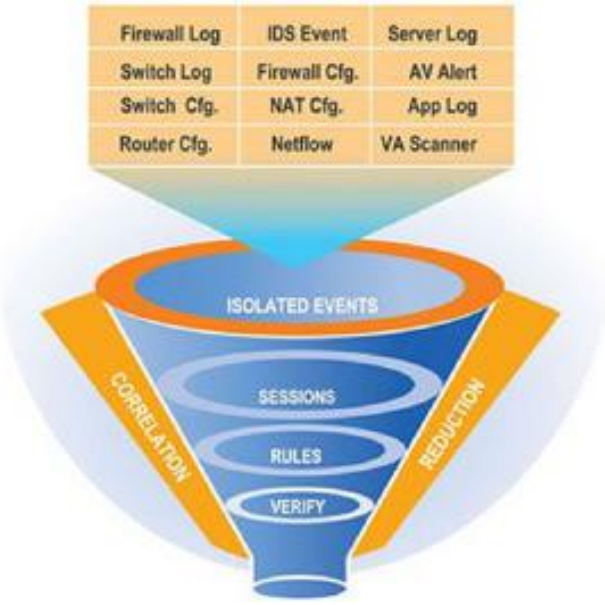


Figura 3. Modelo general de los SIEM [7]

Entre las características principales que los SIEM proporcionan están:

• Acumulación de datos (*data aggregation*): Datos de diferentes fuentes alimentan un motor de análisis centralizado.
• Correlación: Identifican relaciones y se crean interpretaciones significativas.
• Alertas.
• Cumplimiento: Identificar si ciertas políticas se cumplen.
• Retención: Almacenamiento de datos históricos.
• Análisis forense: Creación de líneas de tiempo para reconstrucción de eventos.
• Inteligencia: Descripción del contexto de seguridad para efectos de toma de decisiones.

Actualmente existen herramientas SIEM *open source* tales como OSSIM de Alien Vault[8]. También existen opciones comerciales que integran algunas características adicionales, sin embargo el fundamento base es proveer características de un SIEM. Algunas de ellas son Alien Vault USM[9], Tenable SIEM [10], Splunk[11], entre otros.

Auditoría Pasiva de Tráfico de Red

De manera similar a los SIEM, la Auditoría Pasiva de Tráfico de Red (Passive Network Audit) involucra el análisis de bitácoras y correlación de datos, sin embargo, lo que define a PNA como un modelo de análisis independiente a los SIEM es el uso de tráfico de red como su fuente ***principal y única*** para la obtención de información y generación de reportes. A su vez, PNA implica solamente la utilización de herramientas pasivas para la extracción de información, es decir, ninguna acción llevada a cabo durante el proceso de análisis altera o interviene en la operación de la red que se analiza.

Mientras los SIEM se basan en acumulación de datos (*data aggregation*) de diversas fuentes como *firewalls*, bitácoras de sistemas, IDS, IPS, *routers*, etcétera, PNA se enfoca al tráfico de red como fuente de información. Como se aprecia en la Figura 4, la acumulación de datos ("*Multiple data aggregation*") se hace de manera interna, ya que involucra un proceso adicional que es el procesamiento y decodificación previa de datos ("*Pre-processing & decoding*") para generación de "bitácoras" o datos que normalmente serían la fuente de información inicial para un SIEM, sin embargo, en este caso son obtenidos sólo a partir del tráfico de red y son en realidad una "*aproximación*" a bitácoras reales. Esto quiere decir que en realidad dicha extracción implica una interpretación y en ciertos casos una extrapolación de información a partir de datos que representen una "firma" sobre determinada actividad o sistema (por ejemplo, el tráfico de *headers* HTTP puede contener datos para generar información similar que normalmente se obtendría a partir de una bitácora de un servidor web como Apache, etcétera). Así, a partir de este preprocesamiento es posible entonces identificar y decodificar protocolos, versiones de software, dominios, alertas de

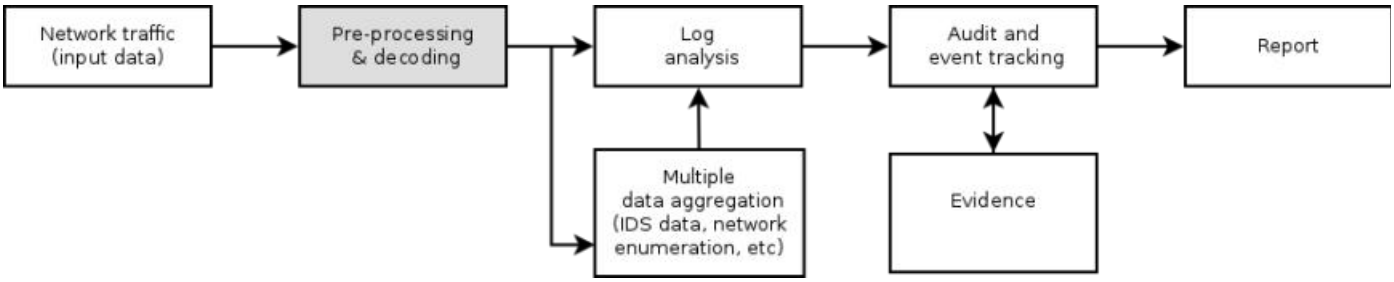


Figura 4. Diagrama de auditoría pasiva de tráfico de red

de IDS, flujos, etcétera que comúnmente serían tomados de bitácoras de sistemas u otros dispositivos, con la ventaja de que todo el proceso se desarrolla de manera pasiva y únicamente a partir de tráfico de red.

PNA también se conoce como Identificación Pasiva de Red (Passive Network Discovery) y algunas fuentes[12] la describen como una tecnología para responder a las preguntas *¿Quién y qué hay en la red de la organización? y ¿Qué se está haciendo en la red de la organización?,* mediante identificación de utilización de la red, análisis forense de eventos, identificación de vulnerabilidades y perfiles de activos (equipos, servidores, entre otros).

Una desventaja de PNA es que el análisis puede ser limitado y no muy preciso debido a que el tráfico de red puede no contener datos suficientes para identificar y generar información confiable sobre la seguridad y el estado de la red.

Prototipo de Auditoría Pasiva: PNAF

A continuación se presenta una introducción al prototipo de un *framework* de PNA llamado **Passive Network Audit Framework (PNAF)** (Santillan, 2014). Este *framework* define un modelo de análisis (Figura 5) para auditoría de tráfico de red a través de la utilización de diversas herramientas las cuales se conjuntan en una implementación de software libre. En este artículo se presenta una breve introducción sobre las características del *framework*, sin embargo en el próximo número se presentará una prueba de concepto con detalles sobre instalación, configuración y análisis de una muestra de tráfico de red.

Las principales características de PNAF son:

- Diseño modular con tres principales fases: (1) captura/lectura de tráfico, (2) procesamiento y (3) visualización (Figura 5).Provee un resumen del nivel de seguridad de la red basado en análisis de activos identifica- dos en el tráfico de red.
- Identificación de actividades anómalas.
- Auditoría de políticas de seguridad.
- Análisis de impacto de vulnerabilidades basado en CVE (Common Vulnerabilities and Exposures) de NVD (National Vulnerability Database)[13].
- Recopilación de evidencia.

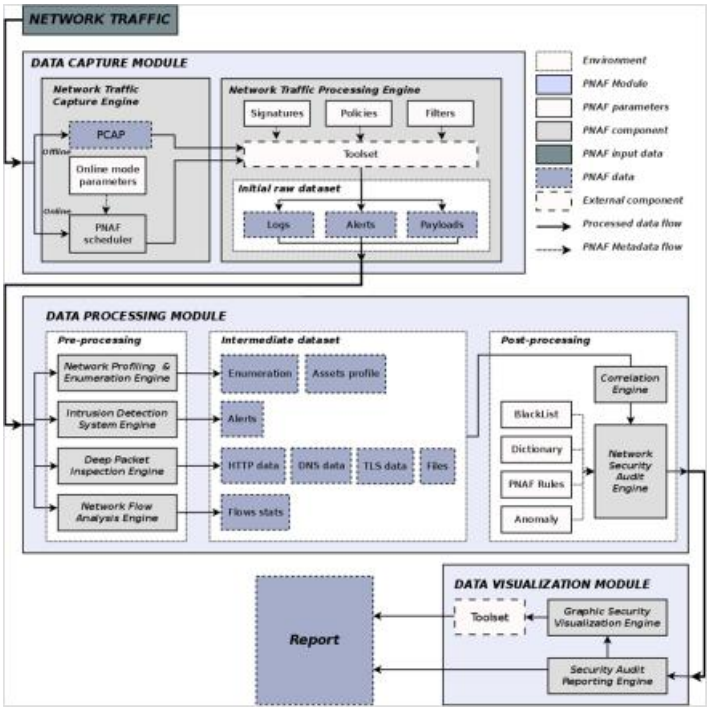


Figura 5. Modelo de análisis de Passive Network Audit Framework (PNAF)

La siguiente tabla presenta un panorama general de algunas de las herramientas que pueden ser utilizadas dentro de PNAF. Cada una de ellas tiene un propósito específico de modo que la información se correlaciona para la identificación de activos y la determinación del contexto de la red.

Herramienta	Propósito	Datos generados	Observaciones
Enumeración e identificación de activos (*Profiling and Enumeration*)			
P0f	Enumeración de red y servicios.	Tipos de conexión (Capa 1), versiones de software y plataformas, roles de equipos.	Detección mediante múltiples métodos: firmas y comportamiento.
Snort Open Appl	Identificación de aplicaciones.	Tipos de aplicaciones usadas en la red.	Identificación mediante análisis de protocolos y no mediante número de puerto.
Prads	Enumeración de red y servicios.	Tipos de conexión (Capa 1), VLAN, versiones de software y plataformas.	Detección mediante múltiples métodos.
Motores de detección de intrusos (*IDS Engines)*			
Suricata	Motor IDS, decodificador de capa de aplicación, captura en tiempo real.	Alertas basadas en firmas, datos de HTTP, TLS, DNS, SSH, extracción de archivos transferidos.	Detección flexible por firmas *(signatures), parsers* de capa de aplicación y captura de alto rendimiento.
Snort IDS	Motor IDS.	Alertas basadas en firmas.	Detección flexible por firmas (*signatures*).
Bro IDS	Motor IDS, decodificador de protocolos y verificador de políticas.	Alertas de IDS, datos decodificados de capa de aplicación como HTTP, TLS, DNS, SSH.	Conjunto de *parsers* de capa de aplicación.
Análisis de flujos de tráfico de red (Network Flow Analysis)			
Cxtracker	Análisis de flujos.	Estadísticas de tráfico de red.	Análisis de gran cantidad de tráfico.
Argus	Análisis de flujos.	Estadísticas de flujos de tráfico de red, protocolos y decodificación de paquetes.	Método eficiente para análisis de grandes cantidades de tráfico.
Silk	Análisis de flujos.	Estadísticas de tráfico de red.	Análisis de gran cantidad de tráfico.
Tcpflow	Reensamblado de sesiones TCP y decodificación HTTP.	Datos HTTP.	Análisis de *payloads*.
Tcpdstat	Identificación de protocolos.	Estadísticas de protocolos.	Clasificación por capas de protocolos.
Inspección profunda de paquetes (Deep Packet Inspection)			
Chaosreader	Decodificación de capa de aplicación.	Datos HTTP, DNS, FTP, SMTP.	Análisis de *payloads*.
PassiveDNS	Análisis pasivo de DNS.	Estadísticas de DNS.	Identificación de *malware* basado en DNS (como Fastflux).
Tcpxtract	Extracción de archivos transferidos.	Lista de archivos transferidos.	Útil para identificación de *malware* y violación de políticas.
TcpExtract	Extracción de archivos transferidos.	Lista de archivos transferidos.	Basado en Python.

Httpry	Decodificación de protocolo HTTP.	Datos de HTTP y *payloads*.	Análisis a fondo de HTTP.
Xplico	Extracción de datos de capa de aplicación.	Datos HTTP, archivos, información de protocolos.	Tiene su propia interfaz web.
Nftracker	Extracción de archivos transferidos.	Lista de archivos transferidos.	Útil para identificación de *malware* y violación de políticas.
Ssldump	Extracción de información de protocolos SSLv3/SSL.	Información de certificados.	Útil en análisis de cadenas de confianza (basadas en PKI) mediante certificados.

Tabla 1. Herramientas de análisis de tráfico de red

PNAF puede ser utilizado sobre entornos GNU/Linux y su utilización es mediante la línea de comandos (CLI, *Command Line Interface*). El *framework* se alimenta de tráfico de red, el cual es analizado usando las herramientas mencionadas en la tabla anterior de modo que el administrador puede visualizar un resumen de una auditoría básica de tráfico de red.

```
=======================================
 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 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

Options:
    -help Print a brief help message and exits.

root@debian:~#
```

Figura 6. Opciones de ejecución en PNAF

Para mayor información y actualizaciones de PNAF se pueden consultar los siguientes sitios web.

- http://www.github.com/jusafing/pnaf
- http://sec.jusanet.org

Referencias

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

The Tao of network security monitoring: beyond intrusion detection. Richard Bejtlich. Pearson Education, 2004.

The Practice of Network Security Monitoring: Understanding Incident Detection and Response. Richard Bejtlich No Starch Press, 2013.

Demystifying the myth of passive network discovery and monitoring systems. Ofir Arkin. InsightiX McAfee, 2012.

[1] http://bammv.github.io/sguil/index.html

[2] http://www.snort.org

[3] http://qosient.com/argus/

[4] Richard Bejtlich. The Tao of network security monitoring: beyond intrusion detection. Pearson Education, 2004.

[5] Richard Bejtlich. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press, 2013.

[6] Post by Richard Bejtlich's on TaoSecurity blog. http://taosecurity.blogspot.nl/2007/03/ nsm-and-intrusion-detection-differences.html

[7] http://www.cybervally.com/2012/10/siem-technology/

[8] https://www.alienvault.com/open-threat-exchange/projects

[9] http://www.alienvault.com/open-threatexchange

[10] http://www.tenable.com/solutions/log-management-siem

[11] http://www.splunk.com/

[12] Ofir Arkin. Demystifying the myth of passive network discovery and monitoring systems. http://www.mcafee.com/us/resources/white-papers/wp-demystifying-passive-...

[13] https://nvd.nist.gov/

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.

TIC (Internet) y ciberterrorismo - II

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

En el artículo anterior se habló del Derecho y de las Relaciones Internacionales en su intento por regular el uso de las tecnologías para la información y la comunicación; además, de las tres figuras del derecho internacional relacionadas con el conflicto: el uso de la fuerza, el ciberespionaje y el ciberterrorismo.

Sin embargo surge la pregunta: **¿Cuándo una ciberoperación pasa a ser un ataque armado?** Es en este punto donde las opiniones difieren, ya que el término "ataque armado" no es definido por ninguna convención y su significado está abierto a la interpretación de los Estados y los estudiosos, sin embargo, hay que enfocarse en estudiar el alcance, la intensidad y la duración del ataque para entenderlo mejor.

Por una parte, el Gobierno de los Estados Unidos dice que la legítima defensa aplica para cualquier uso ilegal de la fuerza, y por otra, los expertos dicen que no hay un umbral para distinguir un ataque armado y mortal que garantice el uso de la fuerza como respuesta[1]. Carr Feffrey (2012) da los siguientes modelos utilizados para identificar si un ciberataque es un ataque armado:

- *"El **primer** modelo es un instrumento basado en el enfoque, que comprueba si el daño casado por un nuevo método de ataque anteriormente podría haber sido logrado sólo con un ataque cinético.*
- *El **segundo** es un enfoque basado en los efectos, a veces llamado enfoque basado en consecuencia, en la que la similitud del ataque a un ataque cinético es irrelevante y la atención se centra en el efecto general del ataque, estos tienen como víctima al Estado.*
- *El **tercero** es un enfoque de responsabilidad estricta, en la que los ciberataques contra infraestructuras críticas son tratados automáticamente como ataques armados, debido a las graves consecuencias que pueden derivarse de la desactivación de los sistemas"[2].*

Carr Feffrey reconoce que Michael N. Schmitt es el que más ha avanzado en la temática de evaluar los ciberataques, esto, basado en su "Schmitt's six criteria" que es retomado en el Manual Tallinn y el cual dice que cuando la escala de dicha

ciberoperación es comparable a una operación no cibernética, ésta pasará al nivel de uso de la fuerza. Ahora, si el resultado de una actividad en el ciberespacio es próximo a la muerte, lesión o destrucción significativa, es claramente uso de la fuerza; además tenemos otros factores como son:

- **Inmediatez** (velocidad con la que las consecuencias se manifiestan).
- **Relación causal** (entre la ciberoperación y sus consecuencias).
- **Invasividad** (grado en que la ciberoperación llega al sistema-objetivo).
- Lo **mesurable** de los efectos.
- Los personajes **militares involucrados** en la operación.

La determinación se realiza de la siguiente manera:

"1. Se ve en el alcance y la intensidad del ataque. El análisis bajo este criterio examina el número de personas muertas, el tamaño de la zona atacada y la cantidad de daños a la propiedad. Cuanto mayor sea el daño más poderoso el argumento se convierte en el tratamiento de los ataques cibernéticos como un ataque armado.

2. La inmediatez observa la duración de un ataque cibernético así como otros factores de tiempo. El análisis bajo este criterio examina la cantidad de tiempo que el ataque cibernético duró y el tiempo durante el cual los efectos se sintieron. Cuanto más larga sea la duración y los efectos de un ataque, es más fuerte el argumento de que se trataba de un ataque armado.

3. Franqueza, se ve en el daño causado. Si el ataque fue la causa principal del daño, se refuerza el argumento de que el ataque cibernético fue un ataque armado. Si el daño fue causado en su totalidad o en parte por otros ataques paralelos, es más débil el argumento de que el ataque cibernético fue un ataque armado.

4. Invasividad, se ve en el lugar del ataque. Un ataque invasivo es aquel que cruza físicamente las fronteras de los Estados o cruza fronteras electrónicamente y causa daños al Estado víctima. Cuanto más invasivo es el ataque cibernético, más se parece a un ataque armado.

5. Cuantificación, intenta cuantificar el daño causado por el ataque cibernético. Los daños cuantificables se tratan, por lo general, más en serio en la comunidad internacional. Cuanto más un Estado puede cuantificar el daño hecho, más el ataque cibernético se parecerá a un ataque armado. El daño especulativo, en general, hace menos fuerte la teoría de que un ataque cibernético fue un ataque armado.

6. Legitimidad, se centra en la práctica del Estado y las normas aceptadas de comportamiento de la comunidad internacional, es decir, ésta acepta ciertos comportamientos como legítimos. Cuanto menos esta acción se parezca a lo aceptado internacionalmente, más fuerte es el argumento de uso ilegal de la fuerza o de ataque armado"[3].

Es por esto que se debe evaluar necesariamente el contexto en el que se desarrolla, el actor que perpetra la acción, el objetivo y su ubicación, además de otros problemas que se desprendan del caso. Por otra parte, es importante destacar que este criterio también aplica a los daños económicos, ya que el derecho internacional dice que los ataques económicos también son aplicables a la legítima defensa o autodefensa, verbigracia, lo sucedido en Estonia. Relacionado a lo anterior, Harol Hogju Koh da el siguiente ejemplo de ataques a estructuras críticas que estarían en el primer criterio: "Operaciones que desencadenen la fusión nuclear en una planta, operaciones que abran una presa sobre una población causando destrucción, operaciones que desactiven el control aéreo causando la

colisión de aeronaves"[4].
Debe recordarse que, después de los ataques terroristas contra Estados Unidos el 11 de septiembre de 2001, los líderes estadounidenses reformularon la estrategia de seguridad nacional de aquel país para poner mayor énfasis en las amenazas en las que los Estados y los terroristas podrían adquirir armas de destrucción masiva o que simplemente sean considerados una amenaza a su seguridad nacional. Pasaron a una política más activa en el tema, llegando al grado de formular los llamados *ataques preventivos*[5]. Entonces, es el pragmatismo de los Estados Unidos lo que obliga a ser en extremo precisos a la hora de considerar si dicho ataque es un ataque armado, y por ende, causal de legítima defensa.

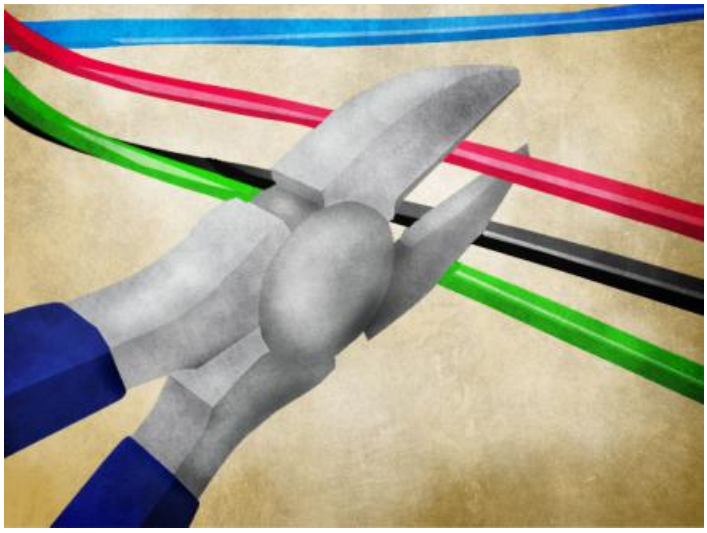
Es normal que el ataque cibernético tenga efectos indirectos y que estos puedan ser reparados relativamente en poco tiempo, sin embargo, como ya se ha dicho, el ciberataque puede recaer en infraestructura física, causando daños materiales. De tal modo, a este tipo de operaciones también aplica el derecho internacional humanitario, cuya finalidad es limitar los sufrimientos causados por los conflictos armados, destacando que esta herramienta también está regulada, tal como otros recursos de guerra.

Finalmente, también es importante diferenciar al combatiente y a la población civil y sus bienes, para que no sean objeto de las hostilidades, por ejemplo, no se debe atacar a hospitales, escuelas, etcétera. Algunos otros ejemplos son:
"*(1) El efecto del arma cibernética tanto en la infraestructura militar y la infraestructura civil, incluida la infraestructura física compartida, por ejemplo una presa o la red eléctrica*
(2) …
(3) los efectos potenciales del ciberataque en objetos civiles que no son objetivos militares, como computadoras personales de civiles que no son relevantes pero están conectadas a computado- res militares que son objetivos militares (hay que mencionar que, dado la infraestructura y las comunicaciones, en estas operaciones se comparte información con privados, sin embargo el jus in bello *nos dice que no se debe usar la infraestructura civil para inmunizar los objetivos militares)*"[6]

Acerca de la responsabilidad, hay que remarcar que los Estados son legalmente responsables por las actividades de sus órganos, personas o instituciones que actúen bajo su control, por tanto hay responsabilidad internacional inmediata en esta materia.

Relativo a la intensidad de la autodefensa, se encuentra relacionada con los principios de distinción y de proporcionalidad, de tal forma que no contribuya a preservar el esfuerzo de guerra. La autodefensa debe ser proporcional al daño recibido y la acción debe darse para evadir un daño mayor sin afán de castigo.

Para concluir esta segunda entrega, es importante destacar las palabras de Harol Hogju Koh para entender la importancia de estos temas a nivel político: **"Porque el cumplimiento del derecho internacional nos da libertad para hacer más y hacerlo legítimo, en el ciberespacio podemos promover nuestro interés nacional de una manera más completa"**[7]**.**



Referencias

[1] N. Schmitt, Michael. International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. Harvard International Law Journal, volume 54 (December 2012). p.10.

[2] Feffrey, Carr (2012), Inside Cyber Warfare, United States of America, O'reilly Media, Inc, second edition. p.59.

[3] Feffrey, Carr (2012), Inside Cyber Warfare, United States of America, O'reilly Media, Inc, second edition. p.61.

[4] Higju Koh, Harold. "International Law in Cyberspace". U.S. Department of State Diplomacy in Action. http://www.state.gov/s/l/releases/remarks/197924.htm (Consultado en 31 de marzo de 2013).
Higju Koh, Harold, International Law un Cyberspace Remarks as Prepared for Delibery by Harold Higju Koh to the USCYBERCOM Inter-Agency Legal Conference ft. Meade, MD, Sept. 18, 2012. Harvard International Law Journal, volume 54 (December 2012). p.4.

[5] Hispanidad, prensa digital española (2013), "EEUU: De los ataques preventivos de Bush a los cierres preventivos de embajadas de Obama", Sección: Confidencial, nota periodística, consultada en agosto 8 del 2013, disponible en: http://www.hispanidad.com/confidencial/eeuu-de-los-ataques-preventivos-de-bush-a-los-cierres-preventivos-de-20130805-157998.html

[6] Higju Koh, Harold. Op.cit. p.5.

[7] Ibídem. p.5.

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.

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.

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.

¿Quién te conoce?

David Treviño

Uno de los temas presentes en los medios es la privacidad y cómo se debe conservar, proteger y garantizar. Sin embargo, la privacidad no es por sí misma un atributo de la seguridad de la información, puesto que descansa sobre el atributo de confidencialidad y este atributo debe ser etiquetado para los activos de información. La privacidad, eso sí, ofrece seguridad y la seguridad ofrece privacidad. En resumen, la privacidad y la seguridad van en paralelo.

El tema es complicado en la era de la información digital, por ejemplo, si hablamos de la propiedad de la información. La principal duda que sale a la vista es quién es el dueño de los datos. Actualmente reproducir un activo de información no requiere de mucho esfuerzo, al final del día un activo como una mesa, un automóvil o un lápiz no se puede reproducir tan fácil (a menos que tengamos una impresora 3D, pero eso será otra historia) pero un archivo digital sí.

Si los sistemas de información digital son propiedad de una empresa y éstos contienen datos, la lógica de propiedad es que los datos deben ser propiedad de la misma (bueno, eso piensan las empresas, sin embargo los datos del cliente no son como las mesas y los escritorios). Por ello, diversas legislaciones europeas y de varios países, incluida la mexicana, aclaran quién es el dueño de la información sin lugar a dudas: El usuario es el dueño de la información en manos de terceros[1]. Quiero aclarar que en los Estados Unidos de América esto no es así, en nuestro país vecino del norte los datos recolectados por sistemas computacionales son propiedad de la empresa que los colecta, a menos que el acuerdo de servicio diga otra cosa[2].

Debe quedar claro que si la empresa que almacena los datos indica lo que hará con aquellos que no son considerados confidenciales por la legislación (ya que existen datos que de acuerdo a la legislación se deben proteger por ley), entonces no existe problema en su uso (si está dentro de lo que se le indicó al usuario que se haría con los datos y se le ofrece, además, las herramientas para ejercer sus derechos ARCO[3]). Eso sí, es posible que el usuario

cambie de opinión respecto al uso de los datos.

Al esquema de nuestra legislación se le conoce como Derechos **ARCO** (**A**cceso, **R**ectificación, **C**ancelación y **O**posición) y no es único, de hecho nuestra legislación fue influida de manera importante por la española.

Si al cliente o consumidor de los servicios se le ofrecen garantías de privacidad, entonces el servicio de la empresa marca una diferencia, pero para esto se deben proteger los datos. En México existe legislación en el tema de protección de datos personales.

En esta época de servicios gratuitos, si no se leen las condiciones de uso de algún servicio "gratuito" (sobre todo del extranjero) y sólo se aceptan, el usuario termina pagando con sus propios datos, ya que le otorga al oferente del servicio algunos derechos sobre esos datos (como generar analíticos no individualizados).

Como usuarios tenemos acceso a redes sociales gratuitas, a correo electrónico gratuito, a búsquedas gratuitas, a software de juegos gratuito, entre otras cosas. Sin embargo, en este mundo, como me decía un rector de una Universidad, "no existe lonche gratis"; los datos y registro de la actividad son el pago. De hecho, estoy seguro de que muchos servicios gratuitos conocen al usuario mejor de lo que éste se conoce el mismo, y además, tienen el archivo histórico, lo cual es mucho más retador.

En resumen, los usuarios de los servicios que mantienen datos sobre el individuo tienen derechos sobre su información en México, ya que la legislación mexicana reconoce que el individuo (usuario) es el dueño de la misma, no la empresa que los capturó. El usuario del servicio es el único que puede decidir qué hacer con ellos. El reto está en que si los datos están en un servicio ubicado en otros países, sobre todo en los Estados Unidos, habrá un problema de propiedad, pues la legislación norteamericana no es como la mexicana y la europea, es mucho más relajada respecto a los derechos y los deja en manos de la empresa que colecta los datos. Cabe recordar que el gobierno norteamericano, inmediatamente después del 9/11, fue uno de los que compró la base de datos del registro de electores del IFE a ChoicePoint[4].

Ahora bien, creo que aquellas empresas que quieran distinguirse en su servicio al cliente pueden entregar más valor al consumidor, es decir, pueden utilizar de manera responsable la información que proporcionamos, indicar su alcance y uso, y apegarse a los lineamientos de seguridad de la información, ofreciendo transparencia en sus algoritmos. El manejo responsable de la información significa mantener un programa de seguridad de la información en la organización, apegarse a los reglamentos de privacidad vigente y contar con los controles mínimos como *firewalls*, políticas y procedimientos de seguridad. Existen estándares a nivel internacional (como el ISO 27000) y la Norma Mexicana para Gestión de Seguridad (NMX-I-27001-NYCE-2009) que nos proporcionan las herramientas de gestión necesarias para mitigar los riesgos y administrarlos.

El valor que como consumidor se puede conseguir con el rastreo de la información es inmenso. Imagine que al entrar a un negocio se le notifique al cliente sobre las ofertas que le pueden interesar. Imagine que en la factura del restaurante favorito también se entreguen las calorías consumidas en un formato digital listo para ser usado en la *app* favorita de salud del

usuario. Para algunas personas, el aceptar este tipo de valor adicional es un riesgo que no se puede aceptar, sin embargo, otros consumidores desean un valor mayor al de la transacción y están dispuestos, si se les explica, a aceptar el riesgo que conlleva el acceder a estos servicios. Todo esto si se explican los procesos de seguridad que la organización maneja y el cómo hacen las cosas, así, informados aceptamos el riesgo.

Imaginemos que al depositar dinero en un banco nos recompensen con aquellas cosas que en realidad consumimos y no sólo con puntos de "lealtad". Para ello necesitamos que nuestros proveedores se vean como una empresa de software y de seguridad y que les interese entregarnos valor.

Estamos en la era de la explotación de la información (yo prefiero decir "explotación responsable"). Creo que existen las herramientas suficientes para proteger esa información, desde detectores de intrusos (IDS por sus siglas en inglés), sistemas antivirus, detectores de anomalías y comportamiento de tráfico, herramientas de monitoreo de incidentes, Sistemas de Información de Seguridad Empresarial, sistemas de correlación de eventos y otros, pero siempre es necesario entender que el cliente o usuario del servicio al final del día es el que tiene la última palabra.

Asimismo, el concepto de seguridad y conservación de activos no es un concepto fácil de asimilar. Tanto organizaciones como usuarios de servicios necesitamos meditar respecto al riesgo y la oportunidad de que la información sea explotada de manera responsable. Además, nos hace falta un *mindset* para lograrlo: El de entregar valor y el ser una empresa de analíticos de información ligado con los conceptos de "empresa de software" y de "seguridad" como diferenciador.

Conocer al cliente mediante la tecnología permite estar cerca de él. La movilidad de los dispositivos que los consumidores utilizan permite entregar de manera oportuna servicios e información que el cliente valore.
Es necesario reflexionar sobre qué es lo que las organizaciones queremos para nuestros clientes y cómo se les va a atender. Existe la gran oportunidad de que sean las organizaciones las que conozcan a los clientes con la información que ellos proporcionan y que dichas organizaciones puedan ofrecer mayor valor a sus clientes con esa información, tal y como lo hacen algunas redes sociales, que al saber el valor de la comunicación y nuestra naturaleza social, colectan información sobre nuestras actividades y generan valor para los usuarios por pertenecer a dicha red.

Herramientas como "Big Data" nos permiten analizar esta información, y si contamos con los mecanismos de seguridad apropiados, podremos entregar valor de manera responsable. Además, como consumidores, también tenemos que reflexionar al respecto, ya que tenemos una moneda muy poderosa en nuestros datos y una legislación que nos protege. Tal vez los proveedores de servicios gratuitos pudieran ofrecer que, por una compensación, no utilicen tus datos para analizarlos. Al final del día, si el consumidor lo requiere, puede exigir sus derechos ARCO y ejercer acciones con las bases que nuestra legislación permite.

Un caso interesante de rastreo y análisis de datos es el ResearchKit que Apple acaba de anunciar, en el cual el cliente acepta que otras organizaciones utilicen los datos para temas de investigación en salud[5].

Existen los mecanismos para el uso responsable de la información, desde herramientas de tecnología hasta la legislación. Las empresas

necesitan estar conscientes de las implicaciones del manejo de la información de sus clientes y dedicar recursos suficientes para cumplir con la legislación vigente, ofrecer mayor valor a los clientes con base en lo que se especifica en la legislación y no verla como un impedimento sino como una oportunidad.

Las organizaciones deben responsabilizarse de la información de sus consumidores. El usuario debe estar al tanto de sus derechos. El área de oportunidad se encuentra en no ver a la legislación como un obstáculo sino como un habilitador para generar valor adicional con el uso responsable de la información.

Uno de los retos que afecta a la industria y que seguirá estando presente es que los reguladores y autoridades deben buscar que la inseguridad de los datos sea costosa. El primer paso ya se dio al reconocer la propiedad de la información, pero los retos continúan con los defectos en las soluciones de software (*bugs*) y las posibilidades que brindan a los atacantes para acceder a la información de manera no autorizada explotando dichos defectos.

Es necesario seguir trabajando para que sea más rentable ofrecer seguridad y privacidad, aunque esto requiera de controles, procesos, procedimientos, certificaciones, tecnología y personal capacitado. Es posible.

En resumen, el manejo responsable de la información es utilizar la legislación, procesos y tecnología como un diferenciador para generar valor al cliente y en realidad poderlo conocer. Estoy convencido de que en un futuro no muy lejano, la seguridad y privacidad de la información será la manera en que los servicios se evalúen y el cliente decida si los utilizará o no.

Referencias

- *http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf*
- *David & Goliath. Bruce Schneier. https://www.schneier.com/book-dg.html*

[1] Ley Federal de Protección de Datos Personales en Posesión de los Particulares
http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf
http://revista.seguridad.unam.mx/numero-10/ley-federal-de-protecci%C3%B3n-de-datos-personales-en-posesi%C3%B3n-de-particulares
http://inicio.ifai.org.mx/SitePages/Como-ejercer-tu-derecho-a-proteccion-de-datos.aspx?a=m1

[2]Data Protection & Privacy in 26 jurisdictions worldwide
https://www.hunton.com/files/Publication/1f767bed-fe08-42bf-94e0-0bd03bf8b74b/Presentation/PublicationAttachment/b167028d-1065-4899-87a9-125700da0133/United_States_GTDT_Data_Protection_and_Privacy_2014.pdf

Data protection in United States
http://us.practicallaw.com/6-502-0467#a762707

[3] Guía Práctica para ejercer el derecho a la protección de datos personales, pág 7
http://inicio.ifai.org.mx/Publicaciones/01GuiaPracticaEjercerelDerecho.pdf

[4] Atentado contra la Soberanía Nacional
http://www.jornada.unam.mx/2003/04/17/edito.php

ChoicePoint y Soluciones Mercadológicas entregan a la PGR los listados ciudadanos
http://www.jornada.unam.mx/2003/05/17/007n1pol.php?origen=politica.php&fly=2

[5] Apple ResearchKit
https://www.apple.com/researchkit/

David Treviño

Es egresado del ITESM en 1983. Cofundador y directivo en CITI Value in Real Time desde 1994.

Ha participado en diversos foros nacionales e internacionales relacionados con Seguridad y Tecnologías de la Información. Miembro del Comité Consultivo del NIC MX desde el año 2010. Editor desde 1997 del boletín electrónico BitCasting. Ha colaborado en la introducción de servicios de Internet y seguridad en diversas universidades y organizaciones del norte de la república desde 1994.

CPL Malware y su alcance en Brasil

Matías Porolli, Pablo Ramos

Durante la primera semana de mayo, desde el Laboratorio de ESET Latinoamérica, publicamos un artículo relacionado a una de las investigaciones desarrolladas en la región, la implementación de troyanos bancarios propagados como archivos CPL en Brasil. En el artículo completo encontrarán el análisis técnico de estas amenazas y las principales particularidades de sus algoritmos de cifrado. En este texto vamos a analizar la evolución a lo largo del tiempo en cuanto a la actividad de este tipo de archivos en la región latinoamericana, correspondiente a una parte del artículo publicado.

Cuando hablamos acerca de las amenazas que vemos en Brasil, hacemos una mención especial a familias de *malware* conocidas como *Win32/TrojanDownloader.Banload o Win32/Spy.Banker*. El hecho de que diferentes tipos de troyanos bancarios sean las amenazas más detectadas en Brasil puede no ser ninguna novedad, sin embargo, en esta investigación les vamos a contar cómo los cibercriminales de este país utilizaron un tipo especial de archivos ejecutables, los CPL (Control Panel Application), para propagar sus amenazas y cómo evolucionó esta tendencia en los últimos años.

Descripción de los archivos CPL

Para empezar, podemos decir que todo archivo CPL es un tipo de librería de enlace dinámico o DLL. En este sentido, las DLL almacenan código listo para ser utilizado por otros archivos ejecutables; se dice que las DLL exportan funcionalidad que es importada por cualquier programa en el sistema que la solicite. Ahora bien, las DLL no pueden ser ejecutadas por sí mismas. Tal es así que, si se hace doble clic sobre un archivo DLL, no se ejecutará código en forma automática: es necesario que otro programa en ejecución invoque el código de la DLL.

Y es aquí donde debemos mencionar la principal característica que diferencia los archivos CPL y las DLL: la acción del doble clic sobre un CPL sí desencadenará la ejecución automática de

código presente en el archivo. Pero, ¿cómo es esto posible, si un CPL es en realidad una DLL? La respuesta es que, técnicamente, el código en el CPL no es autoejecutable, pero al hacer doble clic sobre él comienza la ejecución de control .exe, la aplicación del Panel de Control de Microsoft Windows invoca el código del CPL.

Alcance en Brasil

Uno de los puntos más importantes acerca de los archivos CPL se relaciona con el impacto y crecimiento que han tenido en los últimos años. Para notar estos cambios podemos observar el Gráfico 1, en el cual se puede apreciar la relevancia que el *malware* en formato CPL ha tenido en la región:

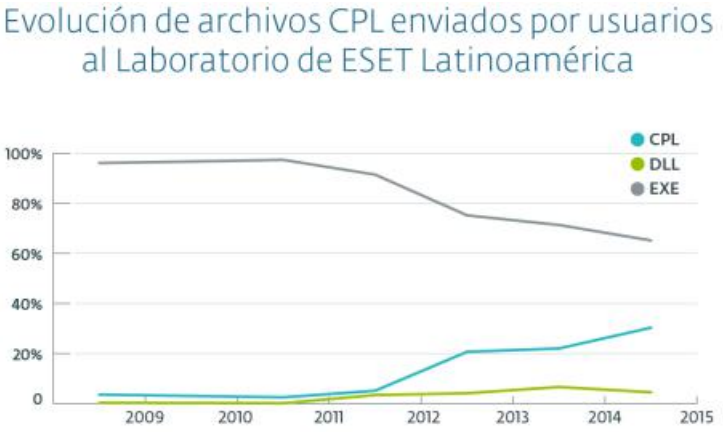


Gráfico 1. Crecimiento de archivos CPL

El gráfico anterior muestra la relación entre los tipos de archivos ejecutables enviados por los usuarios de América Latina al Laboratorio de ESET desde 2009 hasta los primeros meses de 2015. Cuando miramos la relación de los archivos reportados en la región vemos un cambio más que importante. El salto más grande, quizás uno de los indicios de esta tendencia, se da entre 2012 y 2013. A comienzos de 2012, sólo el 5% de los archivos enviados por los usuarios al Laboratorio de ESET correspondieron a *malware* en formato CPL. Sin embargo, para 2013 este valor se elevó al 20%, cuadruplicando su valor respecto al año anterior.

El segundo cambio más importante se sigue observando entre 2014 y los primeros meses de 2015, en donde el porcentaje de muestras recibidas por parte de los usuarios creció en un 50%. Durante los primeros tres meses de 2015, tres de cada diez muestras que los usuarios enviaron al Laboratorio de ESET fueron archivos CPL.

Sobre las muestras enviadas por parte de los usuarios, es posible analizar la frecuencia con la que estos archivos llegaron al Laboratorio:

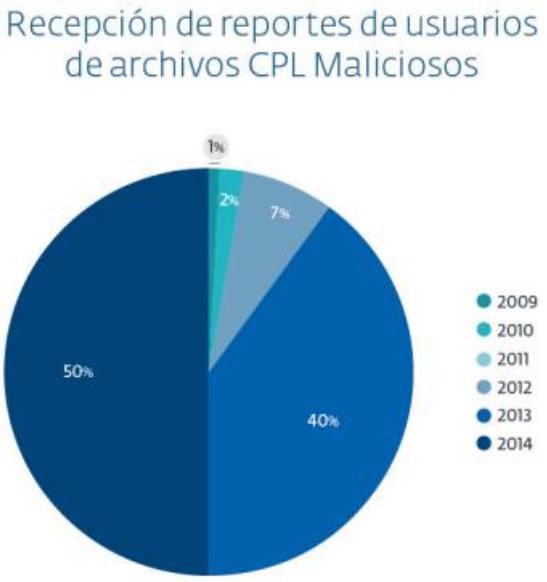


Gráfico 2. Reportes de archivos CPL maliciosos enviados por usuarios

Los dos años con mayor actividad claramente son 2013 y 2014, en donde se reportaron el 90% de las muestras de *malware* en CPL. Si bien sabemos que la actividad es anterior a 2013, analizar lo que los usuarios reportan al Laboratorio nos permite revelar el momento en el que identifican un archivo sospechoso más allá de la extensión que tenga.

Detecciones, amenazas y funciones

Sobre las más de 1,500 muestras que tomamos de ejemplo, el 82% de las detecciones son variantes de *Win32/TrojanDownloader.Banload*, una familia de *malware* que prevalece desde hace años en Brasil como el principal código malicioso. Entre los puntos particulares de esta familia encontramos que, según los datos de telemetría de **ESET LiveGrid**, Brasil es el país más afectado, con una gran diferencia respecto al resto del mundo:

Imagen 1. Detecciones

Cuando cuantificamos el peso de las infecciones de cada país en el listado de los diez países más afectados por esta familia de *TrojanDownloaders*, nos encontramos que el 76% de las detecciones de esta familia en 2014 correspondió a Brasil. Esto es un ejemplo más que claro de que esta familia está dirigida a usuarios de ese país, ya que el siguiente puesto, ocupado por España, tiene casi once veces menos detecciones y la brecha se extiende aún más con países como Argentina, Colombia e incluso Portugal.

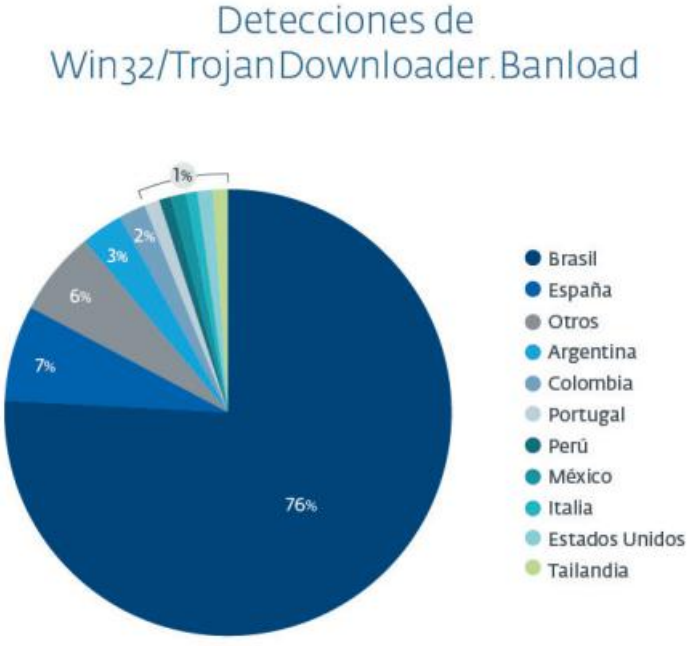


Gráfico 3. Países con más detecciones de Win32/TrojanDownloader.Banload

Prácticamente, una de cada diez amenazas que se detectan en Brasil corresponden a esta familia de troyanos bancarios. El *ranking* de amenazas para el país en el mes de marzo de 2015 es el siguiente:

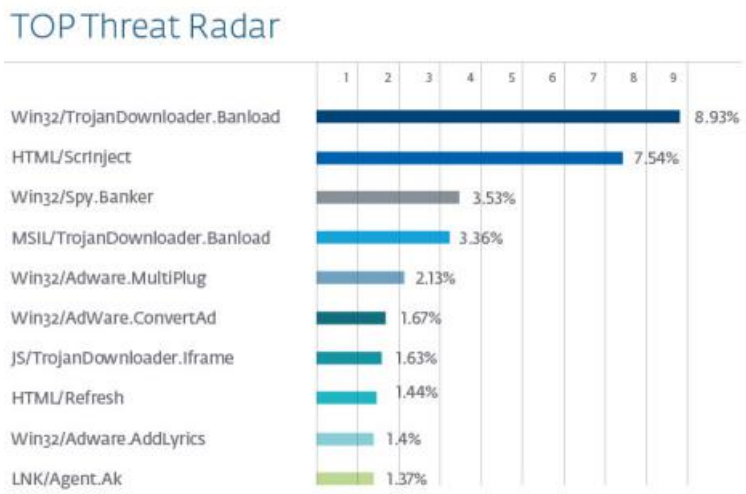


Gráfico 4. Top 10 de propagación de amenazas en Brasil

El objetivo de un *TrojanDownloader* es saltear la protección de un sistema y descargar desde un sitio *web* otra amenaza para instalarla y ejecutarla en el mismo. A través de esta técnica, los atacantes pretenden asegurarse de que el verdadero *payload* del ataque no sea descubierto ante la existencia de un software de seguridad que lo detecte y así no revelar sus verdaderas intenciones.

URL y dominios

A lo largo de las múltiples campañas de estos troyanos bancarios se han identificado un total de 419 URL correspondientes a casi 300 dominios

de 419 URL correspondientes a casi 300 dominios (de diferentes países del mundo) para alojar las amenazas que se intentaban descargar.

Por sobre un total de 298 dominios a los que hemos visto propagando diferentes amenazas desde 2013 hasta principios de 2015, 76 de ellos corresponden a dominios de Brasil que fueron vulnerados para alojar diferentes amenazas. Algunos de los enlaces utilizados dentro de los archivos ejecutables corresponden a URL acortadas con sistemas como Bit.ly. Basados en la información de estos sistemas es posible confirmar la cantidad de clics que los usuarios hicieron sobre estos enlaces y el alcance que contuvo el ataque. En contraparte, los cibercriminales utilizan los servicios de acortadores de URL como parte de sus técnicas de ingeniería social con el fin de ocultar a dónde es que realmente están accediendo. Sin embargo, en los casos que comentaremos a continuación, las URL acortadas fueron extraídas de las variantes de *malware* analizadas.

Como ejemplo, si tomamos uno de los enlaces que los cibercriminales utilizaron a principios de 2014 y que propagaron con un acortador de URL, podríamos ver qué cantidad de clics recibió el enlace y su tiempo de vida:

Gráfico 5. Clics en enlaces propagados con acortadores de URL

En la imagen anterior podemos ver que el enlace (hxxps://bitly.com/KZwqH0) estuvo activo durante los primeros meses de 2014. Además, basados en estos mismos datos, podemos ver que el total de clics fueron más de 9,500:

Imagen 2. Detalle de la cantidad de clics

En total, hubo alrededor de 10 mil clics relacionados con esta amenaza y, según las mismas estadísticas que otorga el sitio, el 88% de ellos provinieron de Brasil. Esto vuelve a remarcar que los cibercriminales en Brasil están atacando principalmente a gente de este país y su efectividad es bastante alta. En la próxima tabla podemos observar otros números para diferentes enlaces acortados que se utilizaron:

Enlace	Actividad	Cant. de clics	% de clics en Brasil	Amenaza
hxxp://bit.ly/15ZkZVq+	Junio 2013	2526	69%	Win32/TrojanDownloader.Banload.RXB
hxxp://bit.ly/19ZHA8D+	Enero 2014	3014	85%	Win32/TrojanDownloader.Banload.SRX
hxxp://bit.ly/KZwqHo+	Febrero 2014	9504	88%	Win32/TrojanDownloader.Banload.SVU
hxxp://bit.ly/1mzhuM7+	Enero 2014	6489	88%	Win32/TrojanDownloader.Banload.SRX

Tabla 1. Detalles de los enlaces utilizados

Packers y protectores

Otro de los aspectos que se pueden destacar de estas campañas es el software que los cibercriminales utilizaron para proteger sus amenazas o incluso evitar ser detectados por las soluciones de seguridad. Como era de esperarse, el *packer* o protector más utilizado fue UPX, que fue visto en el 27% de las ocasiones, seguido por PECompact con el 8%:

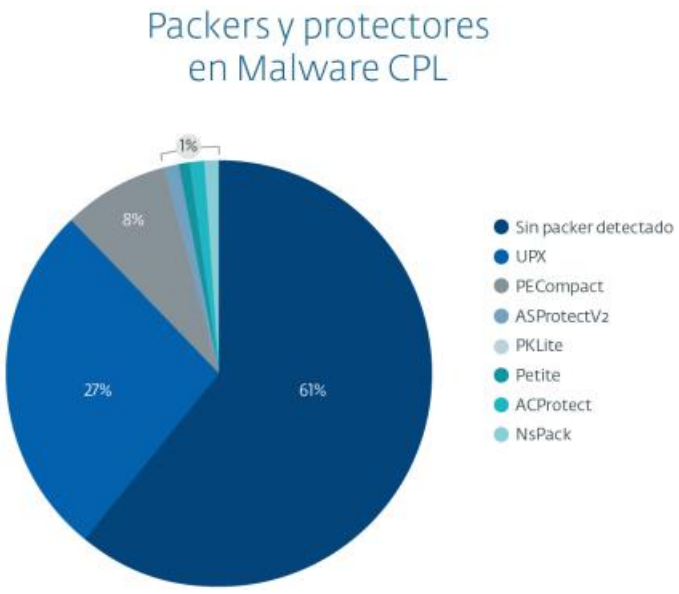


Gráfico6.PackeryprotectoresenarchivosCPL maliciosos

Además, vimos una gran cantidad de amenazas con protectores personalizados o poco comunes, incluyendo el cifrado de las URL mencionadas en secciones anteriores. Habitualmente los atacantes suelen utilizar

estas herramientas para disminuir el tamaño de sus códigos maliciosos así como para evadir la detección.

Detecciones y familias de *malware*

El último punto que vamos a discutir en esta sección son las familias de *malware* que prevalecen en los archivos CPL que hemos recibido por parte de los usuarios en el Laboratorio de ESET.

El 82% de los reportes correspondían a variantes de *Win32/TrojanDownloader. Banload*, cuyo comportamiento y actividades hemos discutido a lo largo de todo el artículo, detallando algunas de las particularidades que vimos en el Laboratorio. Por otro lado, teniendo en cuenta esta tendencia, la segunda familia con mayor cantidad de detecciones corresponde con *Win32/Spy.Banker*[1] y son aquellos códigos maliciosos que se encargan de robar la información desde las computadoras de las víctimas a través de diferentes técnicas para luego enviarlas a los atacantes.

La distribución de todas las familias de *malware* con Archivos CPL que hemos visto en Latinoamérica es:

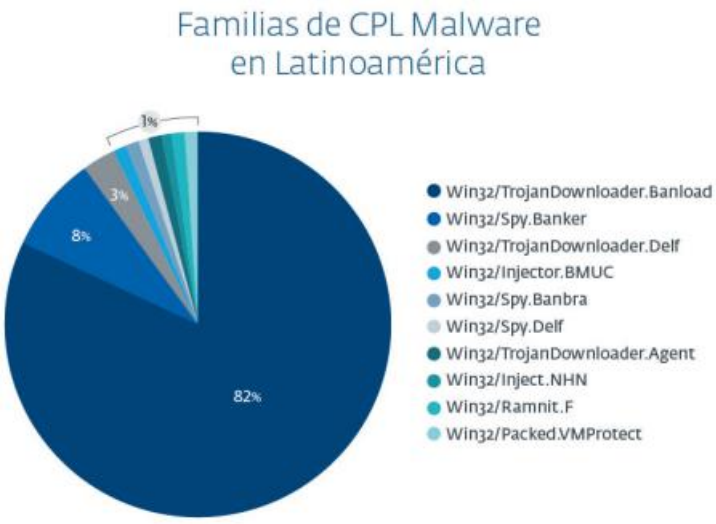


Gráfico 7. CPL malware en Latinoamérica

Otra familia a mencionar es Win32/Spy.Banbra; el *malware* de esta variante ha estado activo en Brasil durante años[2] y en la actualidad continuamos viendo casos en los cuales los cibercriminales utilizan los mismos equipos de los usuarios para enviar miles de correos de spam con enlaces maliciosos para continuar infectando víctimas.

Referencias

[1] ESET Virus Radar, Win32/Spy.Banker, http://virusradar.com/en/Win32_Spy.Banker/detail

[2] 2009-02-20, Sebastián Bortnik, Infección por archivos ¿ejecutables?, http://www.welivesecurity.com/la-es/2009/02/20/infeccion-archivos-no-ejecutables/

Matías Porolli

Porolli es Ingeniero en Sistemas de la Información egresado de la Universidad Tecnológica Nacional, Facultad Regional de Mendoza, Argentina. Previo a su ingreso a ESET Latinoamérica, realizó diversos proyectos de investigación como parte del staff de Fraud Investigation & Dispute Services para la consultora Ernst & Young, dedicándose al análisis de evidencia para identificar y extraer información de valor de discos y equipos, a la adquisición de imágenes forenses y al análisis de la cadena de custodia, entre otras tareas.

Pablo Ramos

Ramos es 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

Aareness & Research, ocupándose de realizar materiales relacionados a las actividades de concientización en seguridad informática de la empresa. En julio de 2012 fue promovido al cargo de Security Researcher, teniendo a su cargo la planificación y realización de investigaciones en la temática.

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Revista .Seguridad Cultura de prevención para TI
No.24 / junio-julio 2015 ISSN: 1251478, 1251477