Monitoreo e identificación de ataques en redes cubanas

Por Ing. Carlos David Piloto Fonseca, Especialista del Grupo de Redes; y MSc. Nelson William Gamazo Sánchez. Especialista Principal del Grupo de Redes, Segurmática
carlos@segurmatica.cu, ngamazo@segurmatica.cu

Introducción

Las redes conectadas directamente a Internet reciben ataques continuamente [1]. Dichos ataques en su mayoría son ejecutados por herramientas automáticas que buscan identificar máquinas que puedan ser comprometidas y utilizadas posteriormente según los propósitos específicos de los atacantes. Como consecuencia de este flujo continuo de ataques, las redes que no mantienen las medidas de seguridad mínimas quedan comprometidas simplemente por estar conectadas a Internet y pueden quedar a disposición del atacante.

Al conjunto de máquinas comprometidas y controladas remotamente por un atacante se les llama Botnet [2]. Las Botnets son actualmente un negocio lucrativo en Internet y pueden ser vendidas a terceras partes con intenciones diferentes a los del atacante original [1], por ejemplo, para realizar ataques de denegación de servicios, hospedar contenido malicioso como programas malignos, programas falsos, o distribución pirata de contenido informático, entre otros.

Actualmente, en Cuba existen máquinas que forman parte de las Botnets, cuyas consecuencias técnicas y políticas son imprevisibles. Desde el punto de vista técnico, pueden impedir el uso adecuado de los servicios de redes a nivel de país; desde la perspectiva política, esas máquinas pueden ser el origen de ataques informáticos hacia otros países. Aunque por las limitaciones de ancho de banda no somos una red atractiva desde la cual realizar ataques intensos distribuidos, las máquinas comprometidas pueden utilizarse para otros fines por parte de los atacantes, como el envío de correo basura [1].

A pesar de que los problemas antes mencionados pueden mitigarse con la implementación de las medidas de seguridad en las redes conectadas directamente a Internet, como mantener los sistemas actualizados, utilizar cortafuegos y arquitecturas seguras de redes, no son suficientes. Hoy en día, el hallazgo de nuevas vulnerabilidades es más rápido que la capacidad de resolución de estas por parte de los fabricantes de software; y también se ha convertido y extendido como un negocio lucrativo [3]. Muchas de las vulnerabilidades encontradas son intercambiadas y vendidas entre las partes interesadas sin notificar al fabricante del software, y muchas de las notificadas tardan meses en ser resueltas [4].

Ante esta situación es imprescindible introducir en las redes el monitoreo con Sistemas de Detección de Intrusos —*Intrusion Detection System* (IDS)— [5]. El despliegue de estos sistemas requiere recursos de redes y en algunos ambientes no es factible implementarlos, por ejemplo, en los sistemas

arrendados donde solo un usuario queda conectado a Internet y el proveedor no garantiza un monitoreo de los ataques en el tráfico del cliente, o en las redes donde no existen los recursos necesarios tanto económicos como de personal para mantener el IDS. Es por ello que, aunque existen las herramientas para realizar un monitoreo de las redes, a nivel de país siempre quedarán sistemas sin monitorear que pueden ser blanco fácil para los atacantes.

Este artículo da a conocer el uso de un sistema de monitoreo de redes implementado en la Empresa Cubana de Seguridad Informática (Segurmática), que puede ser utilizado a gran escala en las redes cubanas para detectar sistemas comprometidos y alertar tempranamente las máquinas que están comprometidas y desde las cuales se realizan ataques. Además, permite conocer el estado actual de los ataques realizados por redes externas hacia redes cubanas.

El monitoreo constante y el análisis del tráfico que circula en las redes cubanas permite conocer los principales vectores de ataque que están siendo utilizados y, a la vez, tomar las medidas necesarias para mitigar estas amenazas, además permite a Segurmática identificar indicios de propagación de programas malignos entre máquinas cubanas conectadas directamente a Internet. El sistema se nombra Sistema Distribuido TAIPS-net [6] y, actualmente, monitorea cuatro puntos en La Habana, ubicados en la Universidad de Ciencias Informática, en el NAP de Cuba, en la CUJAE y en Segurmática.

El presente trabajo describe el Sistema Distribuido TAIPS-net y sus componentes. Asismismo, se exponen sus ventajas, desventajas y los mecanismos de clasificación y correlación de tráfico. Finalmente, se muestran los resultados obtenidos en forma de estadísticas basadas en los datos recogidos durante el tiempo de funcionamiento del sistema.

Principales características del Sistema Distribuido TAIPS-net

El Sistema Distribuido TAIPS-net está formado por un servidor Prelude [7] y varios sensores TAIPS-net [8]. La figura 1 muestra un esquema genérico del mismo.

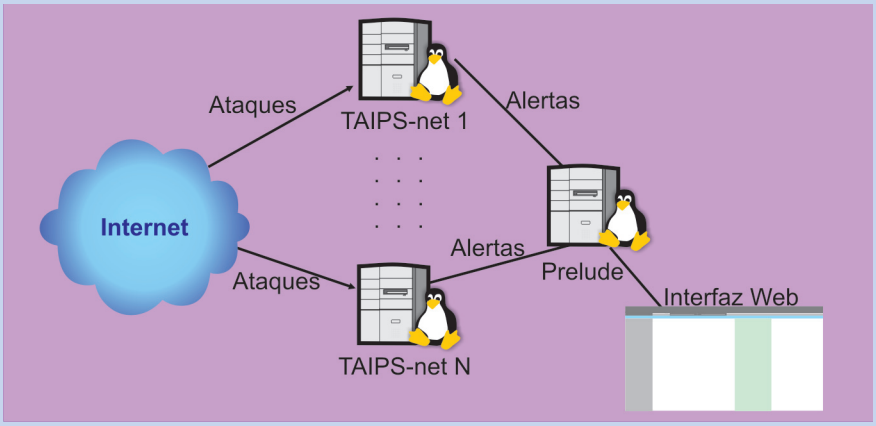

Figura 1 Sistema Distribuido TAIPS-net (Fuente: elaboración propia).

Los sensores TAIPS-net son los encargados de recolectar y clasificar el tráfico de red y tienen la funcionalidad de potes de miel [6] que les permite la captura de programas malignos. A su vez, estos sensores envían todos los eventos recolectados hacia un servidor central —un sistema llamado Prelude—, donde se reciben y almacenan. Esto permite acceder a toda la información recolectada de forma centralizada.

La información enviada al servidor central está formada por las direcciones IP, los puertos fuente y el destino del tráfico monitoreado. También se envían las alertas generadas por el IDS [6] en los sensores TAIPS-net, la cantidad de conexiones iniciadas y la información de descarga de nuevos programas malignos.

Los programas malignos capturados son compartidos con el proyecto MWCollect que tiene sus sensores ubicados en diferentes regiones geográficas del mundo. Esta colaboración permite acceder a toda la información y a los programas malignos capturados por los sensores de MWCollect, siendo una fuente importante de obtención de programas malignos para nuestra Empresa. En la figura 2 se presenta la cantidad de programas malignos descargados por Segurmática desde MWCollect, puede apreciarse que en un período de 7 meses aproximadamente se han obtenido alrededor de 8200 muestras. Aunque la cantidad de muestras es poca, su valor radica en que son programas malignos que están activos y propagándose por las redes de distintos países.

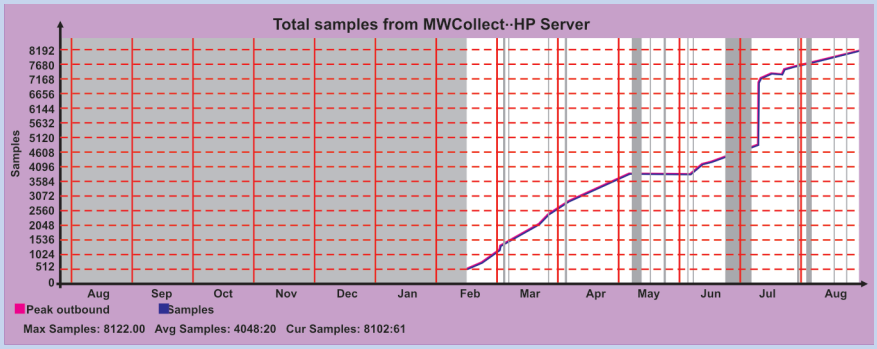

Figura 2 Programas malignos de MWCollect (Fuente: elaboración propia).

A continuación se describe el sensor TAIPS-net, el sistema Prelude, las ventajas y desventajas del sistema distribuido TAIPS-net, así como las características del despliegue de este sistema en Segurmática.

Descripción del sistema TAIPS-net

El TAIPS-net es una herramienta de código abierto desarrollada por Segurmática bajo la licencia GPLv2. Es una combinación de los proyectos Honeywall [9] y Nepenthes [10] con el objetivo fundamental de integrar potes de miel de baja interacción con funcionalidad IDS/IPS, captura y análisis de tráfico en una sola computadora. Una de las características distintivas de TAIPS-net con respecto al proyecto original es la adición al sistema de la funcionalidad de captura de programas malignos.

El despliegue de sensores TAIPS-net permite conocer el estado de las redes a gran escala y detectar a tiempo actividad maliciosa, pero no cuenta con un sistema distribuido de recolección de alertas que facilite el análisis de la información generada por estos de forma centralizada. Con este objetivo se le adiciona al TAIPS-net la funcionalidad de integrarse con Prelude [6].

Descripción del sistema Prelude

Prelude es una herramienta IDS híbrida que permite el análisis centralizado de la información proveniente de múltiples sistemas de seguridad. Posee características que lo hacen idóneo para su uso en este sistema:

- Utiliza el estándar de Formato de Intercambio de Mensajes de Detección de Intrusiones —*Intrusion Detection Message Exchange Format* (IDMEF)—, que le permite a los diferentes tipos de sensores generar sus eventos con el uso de un formato unificado [11].
- Está desarrollado bajo la licencia GPL lo que permite la reutilización, modificación y distribución del código.
- Cuenta con una interfaz Web, Prewikka, que permite acceder a la información recolectada de manera cómoda para el usuario del sistema.
- Permite el envío de correos con las alertas generadas de forma configurable.
- Es tolerante a fallos. Guarda toda la información recolectada en caso de haber problemas de conectividad con el servidor central y la reenvía una vez restablecida la misma.
- El intercambio de mensajes ocurre a través de una conexión TLS —*Transport Layer Security*— compactada y cifrada que garantiza la integridad y confidencialidad de los datos que se envían.

La integración del sistema Prelude con el TAIPS-net le brinda al sistema distribuido muchas ventajas, pero a pesar de esto posee algunas deficiencias.

Ventajas y desventajas del Sistema Distribuido TAIPS-net

El Sistema Distribuido TAIPS-net posee muchas ventajas que lo hacen idóneo para el control de ataques en las redes ya que permite monitorear y analizar el tráfico de forma centralizada a través de una interfaz Web y ahorrar tiempo al analista debido a que no tiene que revisar los sensores individualmente. Al enviar toda la información recolectada hacia un servidor central se evita que esta se pierda en caso de ser comprometido un TAIPS-net o de presentar problemas técnicos como la rotura del hardware de la máquina. La posibilidad de recibir determinadas alertas por correo electrónico, hace posible enfocar el trabajo en las alertas prioritarias. También permite conocer el estado de cada uno de los sensores TAIPS-net en tiempo real.

Al estar distribuido en varias redes ofrece una visión global de los ataques monitoreados pues se recolecta más información y en escenarios diferentes.

Otra de las ventajas del sistema es que las alertas se envían cifradas hacia el servidor central, lo cual impide que esta información sea accesible a terceras personas con fines maliciosos.

Además, el costo de desplegar sensores TAIPS-net es relativamente bajo porque se pueden utilizar máquinas con bajas prestaciones.

A pesar de las ventajas, el sistema posee algunas deficiencias o carencias que son necesarias corregir para lograr mejor aprovechamiento del mismo. Por ejemplo, el tráfico capturado está sin clasificarse y, para conocer los detalles del ataque, el analista debe estudiar el tráfico capturado por los sensores TAIPS-net. Una vez analizado un ataque no queda constancia; entonces, si se repite, hay que realizar nuevamente el proceso, por lo que es imposible el mantenimiento del sistema de forma manual.

Por otra parte, el sistema Prelude no analiza de forma automática los eventos recolectados, por ejemplo, la procedencia de los ataques, los ataques distribuidos, entre otros.

De aquí surge la necesidad de clasificar todo el tráfico capturado e implementar un mecanismo con el cual se pudieran investigar los eventos automáticamente correlacionando diferentes alertas. A continuación se describe el sistema completo, cómo funciona actualmente y las configuraciones necesarias para eliminar las desventajas.

El Sistema Distribuido TAIPS-net de Segurmática

La empresa Segurmática ha desplegado y explotado este sistema. En la actualidad está formado por cuatro sensores TAIPS-net ubicados en diferentes redes del país y un servidor central. En la figura 3 se representa esta distribución.

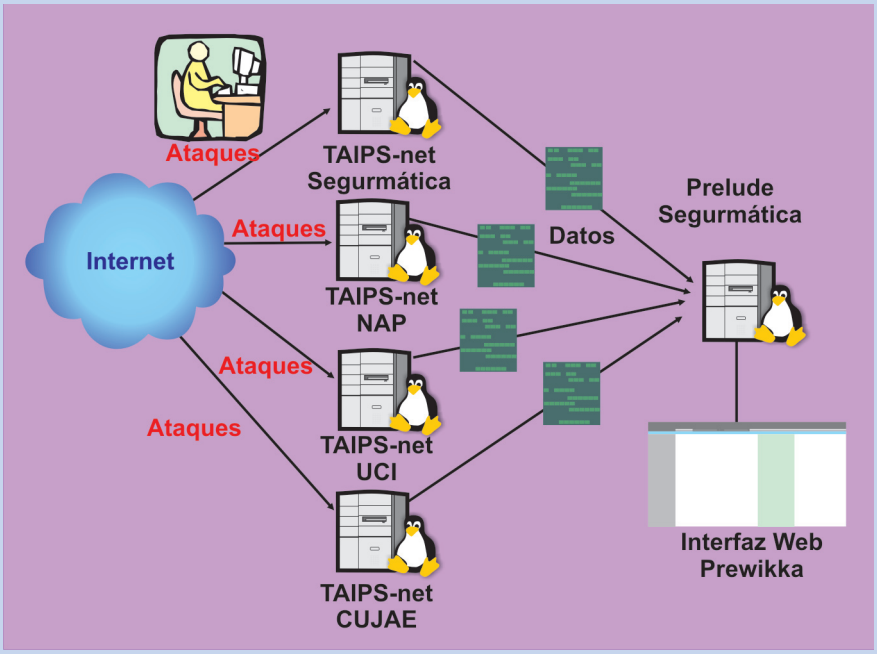

Figura 3 Sistema Distribuido TAIPS-net de Segurmática (Fuente: elaboración propia).

Los eventos recolectados por Segurmática carecían de la información necesaria para que el análisis de los ataques se realizara de manera sencilla y rápida. Por ejemplo, aunque se conocían cuáles eran los protocolos que estaban siendo atacados, no se podia identificar mediante la simple inspección visual de las alertas el tipo de ataque que se utilizaba en cada caso.

El desconocimiento del tipo de ataque dificulta y demora el análisis de los mismos, de aquí la necesidad de clasificar el tráfico monitoreado de forma automática.

Clasificación de tráfico

La principal ventaja de contar con un tráfico clasificado es que se evita su análisis reiterado, por lo que los especialistas pueden enfocar sus esfuerzos en el estudio de los nuevos ataques recibidos. Una vez realizada esta operación, queda documentado e implementado el análisis en la misma clasificación . En este sistema hay dos formas de clasificar el tráfico:

- Por el protocolo utilizado
- Por el ataque

Clasificación según el protocolo

El objetivo de la clasificación del tráfico según el protocolo es conocer los protocolos a nivel de aplicación que están siendo atacados y obtener estadísticas de los mismos. A continuación se explica cómo se realiza este proceso en el sistema.

En los sensores TAIPS-net se obtiene la información detallada de los flujos de datos que circulan por el sistema con la herramienta Argus, que es un analizador de tráfico de red en tiempo real. Para enviar los datos de Argus hacia el servidor Prelude es necesario utilizar una herramienta llamada raprelude, encargada de convertir la

información al formato correspondiente y enviarla al servidor central. El raprelude clasifica el tráfico mediante reglas sencillas que solo tienen en cuenta los puertos y el protocolo de transporte. Para crear estas reglas se utiliza la lista de los puertos "bien conocidos" y "registrados" según la Agencia de Asignación de Números de Internet —*Internet Assigned Numbers Authority* (IANA)—.

Si no existe una regla para clasificar un determinado tráfico, se genera una alerta de **tráfico de red desconocido**. En la figura 4 se observan los eventos generados por raprelude.

Si bien es importante conocer el tipo de tráfico involucrado en un ataque, también es imprescindible conocer el objetivo del ataque.

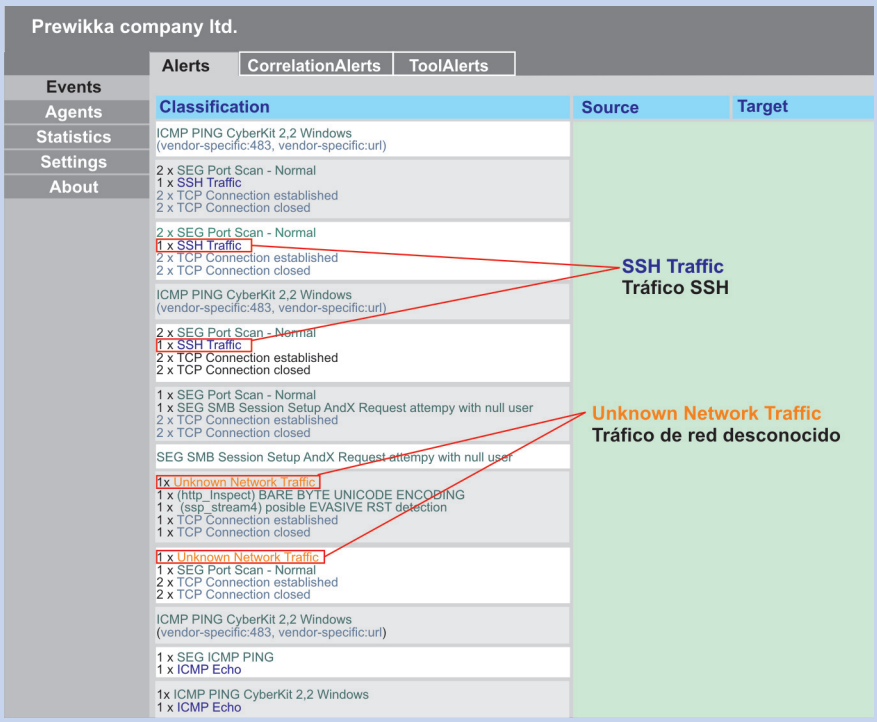

Figura 4 Clasificación del tráfico según el protocolo (Fuente: elaboración propia).

Clasificación según el ataque

De forma general, la identificación de ataques contra una red se realiza usando IDS. No obstante, el objetivo primario es mantener un conjunto de reglas que identifiquen los ataques y no generen falsos positivos que alerten a los administradores de forma innecesaria. Esto presupone la existencia de un tráfico que necesariamente no constituye ataque, como es la navegación de los usuarios de la red, el tráfico en los servicios externos publicados, etc. Sin embargo, a los efectos de nuestro sistema donde existen sensores que no ofrecen servicios a los usuarios, es natural considerar que todo el tráfico que llega hacia ellos es maligno o constituye parte de un ataque. Por ejemplo, un simple uso del protocolo ICMP —*Internet Control Message Protocol*— puede estar originado por un sistema comprometido que realiza identificación de sistemas de forma automática. Por lo tanto, es importante saber dentro del protocolo ICMP cuándo se está efectuando este tipo de actividad maligna y desde dónde, sin tener que analizar cada uno de los tráficos provenientes de varios sensores. La clasificación basada en el ataque para el Sistema que se describe en este trabajo consiste en considerar como maligno todo el tráfico que llega a los sensores. A partir de esa consideración, el objetivo es identificar de manera precisa cuál es el ataque realizado y desde qué lugar se hizo, sin tener que acudir al contenido interno de los paquetes una y otra vez.

La clasificación del tráfico en los sensores TAIPS-net se realiza con la combinación de dos funcionalidades existentes en el sistema distribuido: las reglas de

identificación de ataques del Snort [12] y la funcionalidad de correlación de alertas del Prelude. Al coordinar estas dos funcionalidades es posible clasificar diferentes ataques que utilizan un mismo protocolo y, a la vez, identificar todos los puntos monitoreados que reciben este tipo de ataque. La ventaja fundamental de este mecanismo es que mediante la configuración del sistema se obtiene información de los ataques, sin necesidad de hacerle cambios desde el punto de vista de desarrollo.

Motor de correlación

Prelude-Correlator es un motor de correlación basado en reglas escritas en Python [13]. Tiene la capacidad de conectarse y obtener las alertas de un servidor Prelude y correlacionarlas a partir del conjunto de reglas configuradas, creando nuevas alertas IDMEF de correlación. Esta prestación facilita el trabajo de los especialistas, siendo simple, rápido y más incisivo. Además, permite enfocarse con gran eficiencia en los eventos de seguridad más importantes.

Sus funcionalidades son:

- Rápida identificación de los eventos de seguridad importantes, lo que permite al analista asignar prioridades a las tareas.
- Correlación de alertas provenientes de diferentes sensores desplegados en varios escenarios.
- Análisis automático y en tiempo real de los eventos recibidos por Prelude.

La principal utilidad de este componente es que a través de las potentes reglas que se pueden crear para el análisis de los diferentes eventos, se logra gran flexibilidad en cuanto a su uso, en dependencia solamente de las necesidades del analista que utiliza este sistema. En la figura 5 se muestran algunas alertas de correlación.

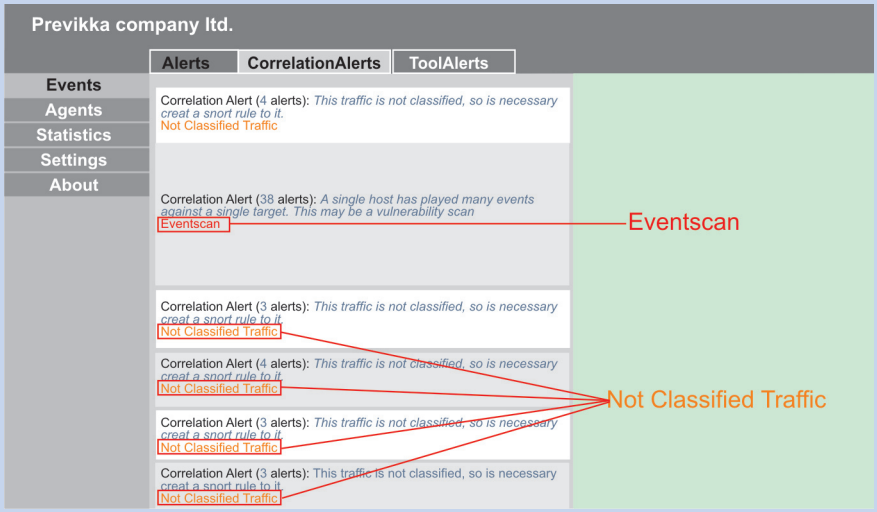

Figura 5 Alertas de correlación (Fuente: elaboración propia).

Resultados

En el Sistema Distribuido TAIPS-net explotado por Segurmática se clasifica la mayor parte del tráfico que se recibe. Esto permite obtener estadísticas de los ataques más frecuentes a las redes cubanas, así como los protocolos más usados. La figura 6 muestra la distribución de ataques clasificados en un mes mientras que la figura 7 expone los protocolos utilizados.

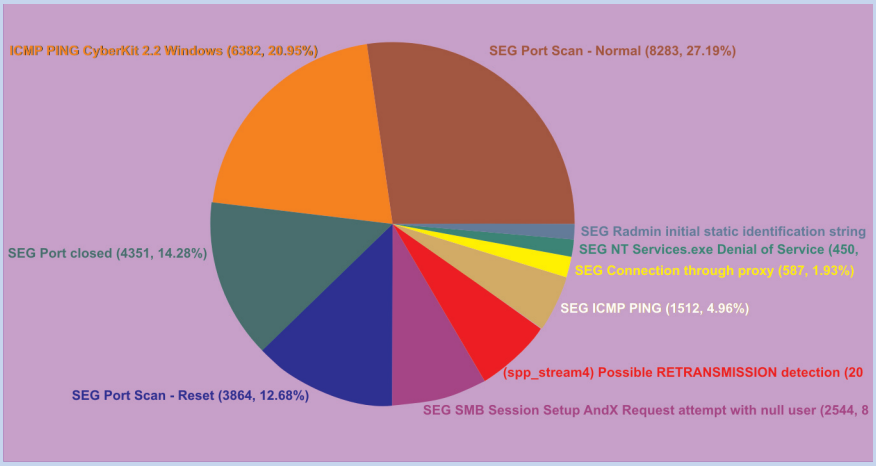

Figura 6 Ataques recibidos en un mes (Fuente: elaboración propia).

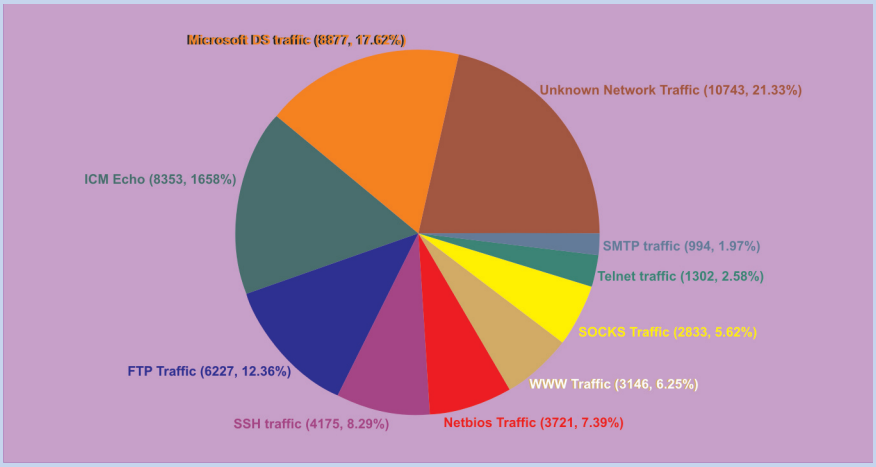

Figura 7 Protocolos atacados en un mes (Fuente: elaboración propia).

La mayoría de los ataques son de puertos “SEG Port Scan” escaneados (Figura 6). Esto se debe a que, generalmente, los atacantes utilizan herramientas automáticas para escanear masivamente los puertos y una vez obtenida esta información tratan de explotar los servicios vulnerables encontrados. En la figura 7 se observa la reducción a un 30% del tráfico desconocido. Además, entre los protocolos más atacados se pueden observar los relacionados con la implementación del protocolo SMB —*Server Message Block*— de Microsoft, debido a la cantidad de vulnerabilidades que ha tenido en las versiones anteriores de Windows [3], siendo un objetivo atractivo para los atacantes.

Los ataques se repiten constantemente, por lo tanto, la mayoría de estos están clasificados, lo que permite a los analistas no perder tiempo en el análisis del mismo ataque.

Con el motor de correlación se crearon dos reglas a fin de detectar el tráfico no clasificado y los ataques provenientes de redes cubanas. En la figura 8 se representan las alertas generadas con estas dos reglas.

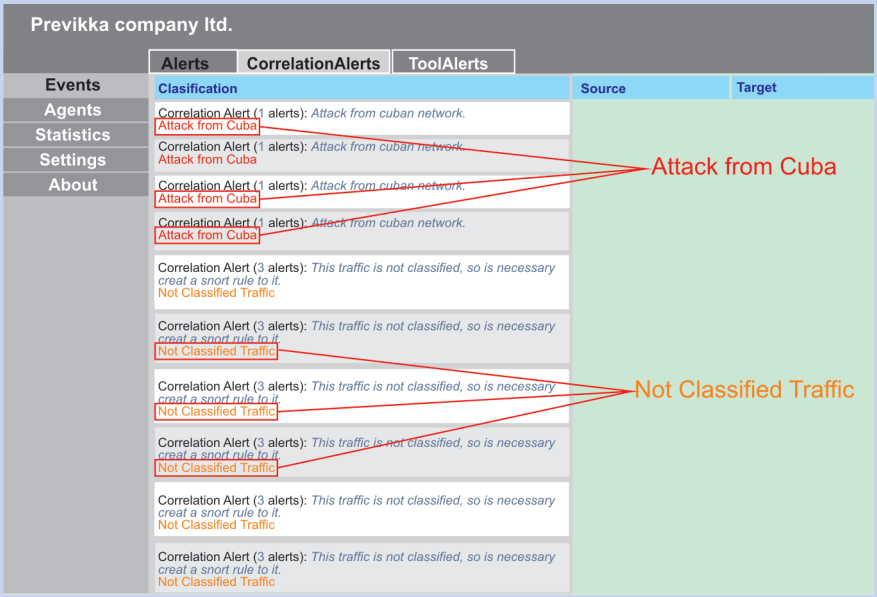

Figura 8 Reglas de correlación (Fuente: elaboración propia).

La creación de estas reglas supone grandes ventajas al sistema y mitiga algunas de las deficiencias del mismo. La regla que detecta el tráfico no clasificado permite conocer de forma automática si el tráfico no está clasificado según el ataque, permitiéndole a los analistas enfocarse en los nuevos ataques recibidos. La regla de detección de los ataques provenientes de Cuba permite tener un monitoreo en tiempo real de las IP cubanas que están siendo utilizadas como plataforma de ataques hacia redes ubicadas en Cuba y hacia redes externas.

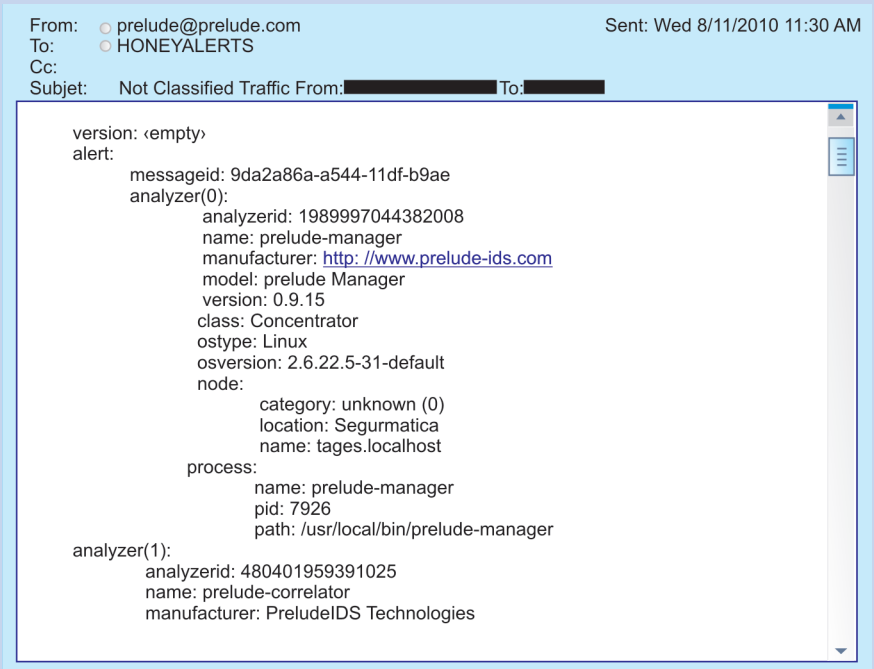

Figura 9 Tráfico no clasificado (Fuente: elaboración propia).

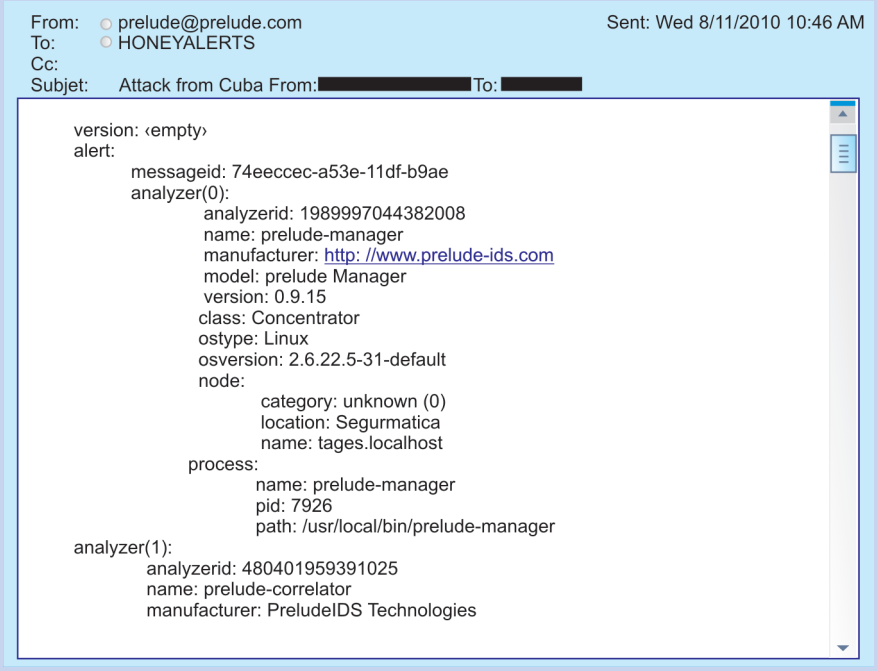

Figura 10 Tráfico desde IP cubanas (Fuente: elaboración propia).

El sistema permite enviar las alertas por correo. Los analistas solo tienen que revisar su correo para conocer el tráfico no clasificado que está llegando a los sensores TAIPS-net y las IP cubanas que están realizando ataques. En estos correos se encuentra la misma información que es accesible por la interfaz Web de las alertas generadas (Figuras 9 y 10).

Conclusiones

Este trabajo demuestra que es posible implementar un sistema de monitoreo e identificación de ataques en redes cubanas, que permite detectar a tiempo los problemas graves de seguridad e implementar medidas para mitigarlos. Debido a las ventajas que posee el sistema es posible mantenerlo con el mínimo de personal, debido a que casi todo se realiza de forma automática, incluso el análisis de los ataques.

La clasificación del tráfico ayudó a conocer los ataques más utilizados hacia redes cubanas y las deficiencias de los sensores TAIPS-net que interactúan con estos ataques. Esto le permite a la empresa Segurmática mejorar las técnicas de captura de programas malignos que se propagan a través de Internet automáticamente, y dirigir los esfuerzos hacia nuevas vías que arrojen mejores resultados. Además, la creación de reglas del Snort crea una base de conocimientos de los ataques recibidos, lo cual evita que tenga que analizarse varias veces un mismo tipo.

Mediante la utilización del motor de correlación de Prelude pudieron implementarse potentes reglas de análisis automático, se detectaron así las redes de computadoras cubanas conectadas directamente a Internet que están atacando a otras redes nacionales. Con esta información se pueden aplicar las medidas pertinentes para mitigar los problemas de forma rápida y minimizar las consecuencias, tanto para las redes comprometidas como para las demás redes del país. También el uso de mecanismos automáticos de análisis evita que los especialistas pierdan tiempo en el análisis de grandes volúmenes de información de forma manual, y disminuye el empleo de los recursos de personal.

Referencias bibliográficas

[1] Sophos Group. "Security Threat Report: 2010". Informe técnico. Burlington, Estados Unidos, enero, 2010. *http://www.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/sophos-security-threat-report-jan-2010-wpna.aspx* (acceso: febrero 10, 2010).

[2] Champ Clark III (Da Beave) et al. *Infosecurity 2008 threat analysis.* EUA: Elsevier, Inc., 2008, pp. 25-63, 2007. *http://www.voiceip.com.ua/lit/Syngress.InfoSecurity.2008.Threat.Analysis.Nov.2007.pdf* (acceso: marzo, 21, 2010).

[3] Sutton, M. and F. Nagle. "Emerging Economic Models for Vulnerability Research". Fifth Workshop on the Economics of Information Security (WEIS), University of Cambridge, England, 2006.

[4] De los Santos, Jorge. "¿Cuánto tardan los grandes fabricantes de software en arreglar una vulnerabilidad?". España, julio 2011. *http://www.hispasec.com/laboratorio/Hispasec_Estudio_Vulnerabilidades_v2.pdf*. (acceso: agosto 22, 2011).

[5] Endorf, Carl; Schultz, Eugene y Mellander, Jim. *Intrusion Detection & Prevention*. 1st ed. EUA: McGraw-Hill/ Osborne, 2004, pp. 3-22.

[6] Sánchez Leyva, P. J. "Sistema centralizado para la recolección de alertas de sensores TAIPS-net". Tesis de Grado, Instituto Superior Politécnico José Antonio Echeverría, Ciudad de La Habana, 2008.

[7] Vandoorselaere, Y. et al. *Prelude 0.9 Handbook*. pp. 2-7, 2007.

[8] Gamazo, N. W. y Lodos, J. "TAIPS-net: Propuesta de Segurmática". *Convención Internacional sobre Tecnologías de la Información y Servicios Telemáticos, CITMATEL, La Habana, Cuba,* 2007.

[9] Honeynet Project. *Know Your Enemy: Learning about Security Threats.* 2nd ed. Boston: Addison-Wesley, 2004, pp. 208-211.

[10] Baecher, P. et al. "The Nepenthes Platform: An Efficient Approach to Collect Malware". Eds. Diego Zamboni and Christopher Kruegel. *Lecture Notes in Computer Science* 4219, Berlín: Springer Berlin Heidelberg , 2006, p 165-184. *http://www.springerlink.com/index/10.1007/11856214* (acceso: septiembre 25, 2010).

[11] Debar, H.; Curry, D. y Feinstein, B. "The Intrusion Detection Message Exchange Format (IDMEF)", RFC 4765exp, marzo, 2007.

[12] Caswell, Brian; Baker, Andrew y Beale, Jay. *Snort IDS and IPS Toolkit: IDS and IPS Toolkit*. Canadá: Syngress, 2007, p. 638.

[13] *Hetland, M. L. Beginning Python: from novice to professional.* 1st ed. California: *Apress, 2005, p. xxix.*